Percepcija privatnosti i sigurnosti web kolačića među korisnicima interneta

Veić, Ivana

SVEUČILIŠTE U SPLITU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET

DIPLOMSKI RAD

PERCEPCIJA PRIVATNOSTI I SIGURNOSTI WEB KOLAČIĆA MEĐU KORISNICIMA INTERNETA

Ivana Veić

Split, rujan 2024.

SVEUČILIŠTE U SPLITU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET

DIPLOMSKI RAD

PERCEPCIJA PRIVATNOSTI I SIGURNOSTI WEB KOLAČIĆA MEĐU KORISNICIMA INTERNETA

Ivana Veić

Mentor: Doc. dr. sc. Jelena Nakić

Split, rujan 2024.

Temeljna dokumentacijska kartica

Diplomski rad

Sveučilište u Splitu
Prirodoslovno-matematički fakultet
Odjel za informatiku
Ul. Ruđera Boškovića 33, 21000, Split, Hrvatska

PERCEPCIJA PRIVATNOSTI I SIGURNOSTI WEB KOLAČIĆA MEĐU KORISNICIMA INTERNETA

Ivana Veić

SAŽETAK

U ovom se diplomskom radu istražuje percepcija privatnosti i sigurnosti web kolačića među korisnicima interneta, s ciljem otkrivanja kako korisnici razumiju funkcionalnost kolačića i kako to utječe na njihove stavove prema privatnosti, sigurnosnim praksama i spremnosti za edukaciju. Istraživanje se temelji na anketi provedenoj među 174 ispitanika, podijeljenoj u šest dijelova, koja ispituje razinu razumijevanja kolačića, zabrinutost za privatnost, sigurnosne mjere koje korisnici poduzimaju, preferencije u vezi s transparentnošću i kontrolom kolačića te njihovu spremnost za edukaciju. Također, istražuje stavove ispitanika prema privolama za kolačiće, analizirajući njihovu reakciju na različite tipove privola prikazanih tijekom korištenja interneta. Prikupljeni podaci omogućuju detaljnu analizu korisničkih percepcija i ponašanja te pružaju važne uvide za razumijevanje njihovog odnosa prema web kolačićima i privatnosti na internetu.

Ključne riječi: web kolačići, vrste kolačića, privola za kolačiće, privatnost, sigurnost

Rad je pohranjen u knjižnici Prirodoslovnog-matematičkog fakulteta, Sveučilišta u Splitu.

Rad sadrži: 62 stranice, 38 grafičkih prikaza, 8 tablica, 46 literaturnih navoda i 6 stranica priloga. Izvornik je na hrvatskom jeziku.

Mentor: **Doc. dr.sc. Jelena Nakić,** docent Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

Ocjenjivači: **Doc. dr.sc. Jelena Nakić**, docent Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

Lucija Bročić, asistent Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

Mirna Marić, asistent Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

Rad prihvaćen: Rujan, 2024.

Basic documentation card

Thesis

University of Split
Faculty of Science
Odjel za informatiku
Ul. Ruđera Boškovića 33, 21000, Split, Hrvatska

PERCEPTION OF PRIVACY AND SECURITY REGARDING WEB COOKIES AMONG INTERNET USERS

Ivana Veić

ABSTRACT

This thesis explores the perception of privacy and security of web cookies among internet users, aiming to discover how users understand the functionality of cookies and how this affects their attitudes towards privacy, security practices, and willingness to educate themselves. The research is based on a survey conducted among 174 respondents, divided into six sections, which examines the level of understanding of cookies, concerns about privacy, security measures users take, preferences regarding transparency and control of cookies, and their willingness to learn more. It also investigates respondents' attitudes toward cookie consent forms, analyzing their reactions to different types of consent forms displayed during internet use. The collected data provide a detailed analysis of user perceptions and behaviors, offering important insights into their relationship with web cookies and online privacy.

Key words: web cookies, types of cookies, cookie consent, privacy, security

Thesis deposited in library of Faculty of Science, University of Split.

Thesis consists of: 62 pages, 38 figures, 8 tables, 46 references and 6 pages of attachments.
Original language: Croatian.

Supervisor: **Jelena Nakić, Ph.D.** Assistant Professor of Faculty of Science, University of Split

Reviewers: **Jelena Nakić, Ph.D.** Assistant Professor of Faculty of Science, University of Split

Lucija Bročić, Assistant of Faculty of Science, University of Split

Mirna Marić, Assistant of Faculty of Science, University of Split

Thesis accepted: September, 2024.

Sadržaj

Uvod

Kolačići su ključni dio današnjeg digitalnog okruženja jer omogućuju web stranicama da pohranjuju informacije o korisnicima kako bi poboljšale korisničko iskustvo i omogućile personalizaciju sadržaja. S obzirom na njihovu povećanu prisutnost u gotovo svim dijelovima interneta, privatnost korisnika je jedna od najvažnijih tema o kojoj se treba voditi računa. Kolačići su male tekstualne datoteke koje se pohranjuju na uređajima korisnika kada posjete određene web stranice, a koriste se za praćenje aktivnosti korisnika, personalizaciju oglasa i pohranu preferencija, što omogućuje prilagođavanje web stranica prema individualnim korisnicima. Iako je njihova upotreba uobičajena, većina korisnika nije potpuno svjesna svih njihovih funkcija, posebice u kontekstu zaštite privatnosti i sigurnosti.

S porastom brige o privatnosti i sigurnosti podataka, implementacija zakonodavnih mjera kao što su Opća uredba o zaštiti podataka (engl. *General Data Privacy Regulation*, GDPR) (Uredba (EU) 2016/679) i Direktiva o privatnosti i elektroničkim komunikacijama (engl. *ePrivacy Directive*) (Direktiva 2002/58/EZ) naglasila je potrebu za transparentnim i pravednim praksama prikupljanja podataka putem kolačića. Unatoč tome, korisnici često izražavaju nesigurnost o tome kako kolačići funkcioniraju i u kojoj mjeri ugrožavaju njihovu privatnost. Osim toga, mnoge web stranice koriste manipulativne dizajne privola za kolačiće kako bi korisnike navele na prihvaćanje svih kolačića bez detaljnijeg informiranja ili razumijevanja.

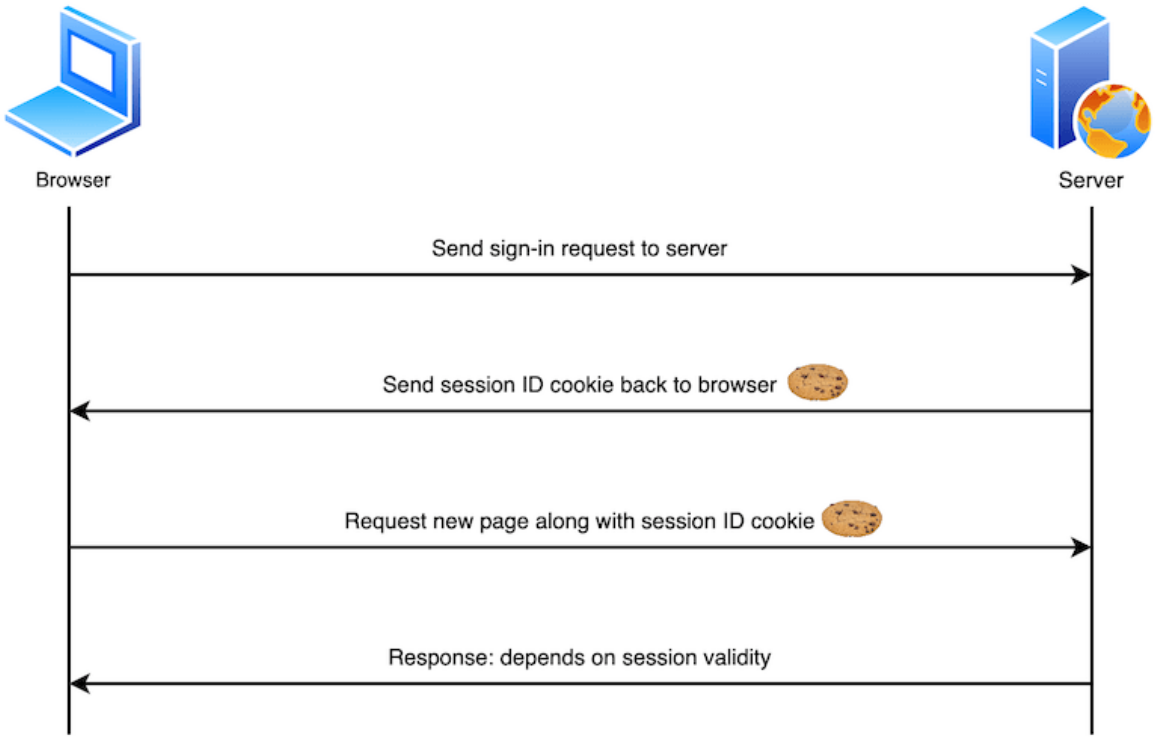
Ovaj rad istražuje percepciju korisnika interneta u vezi s privatnosti i sigurnosti web kolačića, njihovu spremnost na edukaciju te stavove o određenim privolama. Istraživanje je provedeno putem online ankete, s ciljem boljeg razumijevanja načina na koji korisnici doživljavaju kolačiće, svoju privatnost i sigurnost na internetu, te u kojoj su mjeri zainteresirani za edukaciju o kolačićima.

1. Kolačići

Kolačići su male tekstualne datoteke koje web stranice pohranjuju na uređaje svojih korisnika. Napravljeni su kako bi poboljšali korisničko iskustvo na stranici, spremajući korisničke odabire i preferencije i omogučavajući korisnicima da pri povratku na stranicu nastave svoje aktivnosti upravo tamo gdje su u zadnjem posjetu stali (Sipior, Ward, & Mendoza, 2011). Često se nazivaju i HTTP kolačići jer su njegov dodatak – HTTP (engl. *Hypertext Transfer Protocol*) je „protokol bez stanja“ jer poslužitelj ne sprema informacije o korisnicima i svaki primljeni zahtjev s jednog klijenta tretira kao njegov prvi zahtjev, neovisno o broju prethodnih interakcija. Kolačići su nastali upravo kao rješenje ovog problema, tj. za stvaranje „stanja“ HTTP-a (Kristol, 2001). Kada korisnik pristupi nekoj web stranici, njegov preglednik (klijent) šalje zahtjev serveru (poslužitelju), koji u svome odgovoru šalje i kolačić sa informacijama o korisniku (jedinstveni identifikator korisnika, identifikator i trajanje sesije i sl.). Taj se kolačić sprema na korisnikov uređaj i svaki put kad se korisnik vrati na tu web stranicu, njegov preglednik uz zahtjev šalje i sve kolačiće vezane za nju (Sandhu & Park, 2000). Ova razmjena kolačića je ono što omogućuje poslužiteljima da identificiraju klijente, bilo za pružanje najboljeg korisničkog iskustva ili za povezivanje višestrukih zahtjeva sa jednim klijentom (Felten & Schneider, 2000). Uvođenje kolačića predstavlja prekretnicu u povijesti računarstva, jer su prethodno anonimno surfanje internetskim stranicama pretvorili u okruženje u kojem se svaka aktivnost može pohraniti, sortirati, rudariti i prodavati (Schwartz, 2001).

Slika 1.1 prikazuje primjer stvaranja i korištenja kolačića za prijavu na neku web stranicu. Nakon što korisnik web stranici pošalje svoje podatke za prijavu, web stranica u svom odgovoru šalje i kolačić sa jedinstvenim identifikatorom sesije i njenim detaljima koji se sprema na korisnikov uređaj. Svaki idući upit koji korisnik pošalje stranici sadrži taj kolačić, a odgovor stranice ovisi o valjanosti sesije: ako je valjana, dopušta se pristup, a ako nije, treba se ponovno prijaviti (Mozilla, n.d.).

Stvaranje kolačića, jednostavno prikazano na slici 1.2, se događa u HTTP zaglavlju (engl. *header*) *Set-Cookie* odgovora poslužitelja na prvi zahtjev klijenta, a kasnije se kolačići vraćaju u idućim HTTP *GET* zahtjevima klijenta (Fiebrandt, 2018).



Slika 1.1 Razmjena kolačića između korisničkog preglednika i servera (Mozilla, n.d.)

HTTP response from the web server:

```
[...]
Set-Cookie: first.lastname
```

HTTP GET from the client:

```
[...]
Cookie: first.lastname
```

Slika 1.2 Primjer stvaranja kolačića (Fiebrandt, 2018)

1.1. Povijest kolačića

Iako se tek prije nekoliko godina mogao primijetiti ogroman rast u broju stranica sa obavijestima o korištenju kolačića, ta tehnologija postoji i koristi se već trideset godina. 1994. je Lou Montulli, tadašnji programer tvrtke Netscape Communications, izumio kolačiće kao „stalni objekt stanja klijenta“ (engl. *„persistent client state object“*). Sam naziv kolačić (engl. *cookie*) proizlazi iz pojma „čarobni kolačić“ (engl. *magic cookie*) korištenog

u računalnoj znanosti za objašnjavanje razmjene malih dijelova koda radi identifikacije. Originalna svrha kolačića je bila stvaranje i održavanje košarice za kupnju preko interneta (Schwartz, 2001), a prvi put su zapravo upotrijebljeni za provjeru jesu li korisnici već posjetili stranicu Netscape-a ili im je trenutni posjet prvi. 1995. Montulli prijavljuje patent za kolačiće koji je priznat tri godine kasnije (Montulli, 1998), a tu tehnologiju Microsoft iste godine implementira u drugoj verziji svog preglednika Internet Explorer (Hardmeier, Sandi 2005). S obzirom da su obje firme, i Netscape i Microsoft, korištenje kolačića u svojim preglednicima zadržavale za sebe (Kukułka, 2021), korisnike je s njima upoznao Jackson 1996. godine objavivši svoj članak, „*This bug in your PC is a smart cookie*“, u novinama The Financial Times (Jackson, 1996). Krajem iduće godine, 1997., Internet Engineering Task Force (IETF) objavljuje RFC 2109, koji je standardizirao korištenje kolačića. Ovaj je dokument definirao osnovne funkcije i sigurnosne mjere koje kolačići trebaju imati (Chen et al., 2022). 2000. godine je objavljen RFC 2965 koji je proširio i dodatno definirao pravila za kolačiće, uključujući sigurnosne postavke poput *Secure* i *HttpOnly* atributa (Kristol, Montulli, 2000).

Prva zakonska regulacija kolačića je bila Direktiva o privatnosti i elektroničkim komunikacijama (engl. *ePrivacy Directive*), donešena u Europskoj uniji 2002. godine. Poznata kao „*Cookie Law*“, ona zahtjeva da web stranice dobiju pristanak korisnika prije postavljanja kolačića na njihove uređaje ili pristupanja istima, osim kolačića nužnih za funkcioniranje same stranice (Direktiva 2002/58/EZ). 2011. godine je objavljen i trenutni standard za HTTP kolačiće, RFC 6265, koji detaljno opisuje sintaksu i semantiku *Set-Cookie* i *Cookie* HTTP zaglavlja te pruža smjernice za sigurnu implementaciju kolačića (Barth, 2011), a iste godine na snagu stupa i Zakon o kolačićima koji je zabranio dvije važne stvari: postavljanje kolačića treće strane na korisničke uređaje bez korisnikovog dopuštenja, i prikupljanje podataka bez obavještavanja korisnika i dobivanja njihovog pristanka (Direktiva 2009/136/EZ). Draft RFC 6265bis, koji je trenutno u razvoju, donosi dodatna poboljšanja i ažuriranja za standardizaciju kolačića. Uključuje strože sigurnosne mjere i bolje definira postupanje s kolačićima kako bi se uskladilo s modernim sigurnosnim zahtjevima i praksama (Bingler et al., 2024). 2018. godina donosi dvije važne uredbe vezane za kolačiće: GDPR u Europskoj uniji, koja oglašivačima nalaže da za postavljanje kolačića trećih strana prvo moraju dobiti pristanak korisnika (Uredba (EU) 2016/679), i Zakon o zaštiti potrošača u Kaliforniji (engl. *California Consumer Privacy Act*, CCPA), koji ima slične uvjete kao i GDPR ali sa puno više ograničenja (CCPA, 2018).

Promjene vezane za kolačiće u samim web preglednicima predvodi Apple, koji 2017. godine u svom pregledniku Safari uvodi blokiranje kolačića treće strane (Ratcliffe, 2019), a 2020. omogućuje i njihovo automatsko blokiranje (Wilander, 2020). 2019. godine Mozilla prati Apple i najavljuje blokiranje kolačića trećih strana za svoj preglednik Mozilla Firefox (Ratcliffe, 2019), pa 2021. uvodi potpunu zaštitu kolačića kojom ograničava praćenje svojih korisnika na više stranica (Huang, Hofmann & Edelstein, 2021).

Google je odlučio drugačije pristupiti ovom problemu. 2019. godine najavljuje (Schuh, 2019), a 2020. pokreće (Schuh, 2020) svoju inicijativu „Privacy Sandbox“ kojom će u pregledniku Chrome postupno ukidati podršku za kolačiće trećih strana (Sweeney, Zawiślak 2024) i najavljuje potpuno ukidanje njihove podrške do 2022. godine, ali 2021. objavljuje odgodu tog plana za dvije godine (Goel, 2021), a 2022. isti plan opet odgađa za drugu polovicu 2024. godine (Chavez, 2022; Sweeney , Zawadziński 2023). Konačno, Google objavljuje da ipak neće potpuno ukloniti podršku za kolačiće trećih strana već će korisniku omogućiti da donese informiranu odluku o kolačićima koja će se primjenjivati tijekom cijelog njihovog pregledavanja interneta, a taj izbor mogu prilagoditi u bilo kojem trenutku u postavkama preglednika (Chavez, 2024).

1.2. Podjela

Kolačići se mogu podijeliti na više načina: po porijeklu, po trajanju i po namjeni. Unutar svake spomenute grupe se opet može naći nova podjela: po porijeklu razlikujemo kolačiće prve i kolačiće treće strane, po trajanju postoje sesijski i trajni kolačići, a po namjeni imamo neophodne kolačiće, kolačiće za funkcionalnost, za performanse i za praćenje (Koch, n.d.). Osim navedenih, postoje još neke vrste kolačića, kao što su superkolačići i zombi kolačići.

1.2.1. Kolačići prve strane

Kolačići prve strane (engl. *first-party* cookies) su oni koji su postavljeni upravo od one stranice koju korisnik posjećuje. Koriste se u razne svrhe, kao što su pohrana korisničkih odabira i analitičkih podataka.

1.2.2. Kolačići treće strane

Kolačiće treće strane (engl. *third-party cookies*) ne postavlja stranica na kojoj se korisnik nalazi, već neka druga stranica. Uglavnom se koriste u marketinške svrhe, a postavljaju se koristeći oznake (engl. *tags*) ili skripte (engl. *scripts*) koje se pokreću pri učitavanju stranice. Ovi kolačići oglašivačima omogućavaju praćenje korisnika po raznim stranicama: prilikom učitavanja jedne stranice, ona prikazuje reklame s druge stranice, i preko tih reklama korisnik zapravo dobije i kolačiće druge stranice na kojoj sam, svojevoljno, nije bio. Kao što je već navedeno u ovom radu, većina preglednika je zabranila ovu vrstu kolačića i automatski ih blokira.

1.2.3. Sesijski kolačići

Sesijski kolačići (engl. *session cookies*) su kolačići koji se pohranjuju na korisnikov uređaj samo dok korisnik koristi preglednik nakon posjeta stranici koja ih je stvorila, odnosno čim korisnik zatvori preglednik, oni se brišu. Uglavnom se koriste za bitne funkcionalnosti stranice, poput pamćenja proizvoda dodanih u košaricu prilikom kupovine preko interneta ili trenutno unesenih podataka u obrascu (Gourley et al., 2002), što ih čini kolačićima prve strane.

1.2.4. Trajni kolačići

Trajni kolačići (engl. *persistent cookies*) se ne brišu tako jednostavno. U sebi sadrže, osim raznih informacija, korisničkih podataka i postavki korisnika, i svoje trajanje koje može biti postavljeno ili na datum kada ističu, ili na vremenski period koji mora proći prije nego što isteknu. Dok god su važeći, ovi kolačići šalju informacije serveru svaki put kad se korisnik prijavi na stranicu kojoj taj kolačić pristupi, ili kad korisnik učita sadržaj s te stranice (npr. reklame). Olakšavaju korištenje stranica jer pamte korisnikove preferencije o jeziku stranice, temi (svijetla ili tamna tema), veličini teksta i sl. Uz to, koriste se i za pamćenje podataka za prijavu kako ih korisnik ne bi morao upisivati prilikom svake prijave. (Gourley et al., 2002).

1.2.5. Neophodni kolačići

Neophodni kolačići (engl. *strictly necessary cookies* ili *essential cookies*) su kolačići prve strane koji su ključni za osnovno funkcioniranje web stranice. Bez njih, web stranica ne bi

mogla pravilno funkcionirati, jer omogućuju osnovne mogućnosti kao što su navigacija stranicom, pristup sigurnim dijelovima stranice i pamćenje artikala u košarici tijekom online kupovine. Ovi kolačići ne prikupljaju podatke o korisnicima koji bi se mogli iskoristiti za marketing ili praćenje korisnika na drugim web stranicama. Obično su postavljeni kao odgovor na radnje koje korisnik poduzima na web stranici, poput prijave na račun, ispunjavanja obrazaca ili postavljanja postavki privatnosti. Budući da su potrebni za pružanje usluga koje je korisnik zatražio, za ove kolačiće obično nije potreban pristanak korisnik, što znači da web stranice mogu postaviti ove kolačiće bez eksplicitnog odobrenja korisnika, ali je i dalje preporučljivo da korisnici budu obaviješteni o njihovoj prisutnosti i funkciji kroz politiku privatnosti ili obavijest o kolačićima.

Neophodni kolačići su ograničeni na osnovne funkcije i obično ne prate korisnika izvan okvira te web stranice. Primjeri uključuju kolačiće koji čuvaju podatke za prijavu tijekom sesije, kolačiće koji omogućuju punjenje stranica i prikazivanje sadržaja, te one koji omogućuju korisnicima da bez problema koriste usluge na stranici. Ovi kolačići se automatski aktiviraju prilikom pristupa stranici i osiguravaju da korisnik može učinkovito koristiti osnovne funkcije web stranice.

1.2.6. Kolačići za funkcionalnost

Kolačići za funkcionalnost ili funkcionalni kolačići (engl. *functionality cookies*) omogućuju web stranicama da zapamte odabire i preferencije korisnika s ciljem pružanja poboljšanog i personaliziranog korisničkog iskustva. Za razliku od neophodnih kolačića, koji su ključni za osnovno funkcioniranje web stranice, kolačići za funkcionalnost se koriste za pohranu korisničkih postavki koje nisu nužne za osnovnu funkcionalnost ali značajno poboljšavaju interakciju s web stranicom, kao što su: odabrani jezik, veličina fonta, raspored elemenata na stranici ili druge prilagodbe koje je korisnik napravio tijekom posjeta stranici. Također se mogu koristiti za pamćenje korisničkih podataka za prijavu, tako da korisnik ne mora ponovno unositi svoje korisničko ime i lozinku svaki put kad posjeti stranicu.

Funkcionalni kolačići pomažu web stranicama da pružaju usluge prilagođene potrebama korisnika i osiguravaju da korisničko iskustvo bude dosljedno i ugodno. Na primjer, ako korisnik prilagodi postavke pregledavanja na određeni način, funkcionalni kolačići će omogućiti da te postavke ostanu iste prilikom sljedećih posjeta stranici. Iako se ovi kolačići

ne koriste za praćenje korisnika na drugim stranicama ili za ciljanje oglasa, oni ipak mogu prikupljati osobne podatke.

1.2.7. Kolačići za marketing

Kolačići za marketing ili marketinški kolačići (engl. *marketing cookies*) se koriste za praćenje korisnika tijekom njihovog pregledavanja interneta s ciljem pružanja relevantnih i personaliziranih oglasa. Ovi kolačići omogućuju oglašivačima i marketinškim platformama da prikupe podatke o korisnikovim interesima, ponašanju na internetu i interakcijama s oglasima, kako bi prikazali oglase koji su prilagođeni specifičnim preferencijama korisnika. Prikupljaju informacije kao što su web stranice koje je korisnik posjetio, vrijeme provedeno na tim stranicama, klikovi na oglase itd. Ovi podaci omogućuju izradu korisničkih profila i podjelu korisnika prema njihovim interesima, što oglašivačima omogućuje da ciljaju određene grupe korisnika s prilagođenim oglasima. Na primjer, ako korisnik često posjećuje stranice o putovanjima, kolačići za marketing mogu omogućiti prikazivanje oglasa za avionske karte ili smještaj na drugim web stranicama koje korisnik posjećuje.

Kolačići za marketing često su kolačići treće strane, što znači da ih postavljaju vanjski oglašivački servisi ili marketinške platforme koje su integrirane u web stranicu, a ne sama stranica koju korisnik posjećuje. Oni mogu pratiti korisnike preko različitih web stranica i koristiti te podatke za prikazivanje oglasa koji se temelje na prethodnim posjetama ili interesima korisnika.

1.2.8. Analitički kolačići

Analitički kolačići (engl. *analytics cookies*) se koriste za prikupljanje podataka o tome kako korisnici koriste web stranicu. Pomažu vlasnicima web stranica da razumiju ponašanje korisnika, prateći informacije poput broja korisnika, stranica koje su posjećene, vrijeme provedeno na stranici, izvore prometa, i eventualne pogreške na stranici, te im pokazuju gdje opostoje mogućnosti za poboljšanje. Omogućuju prikupljanje tih podataka kako bi se optimiziralo korisničko iskustvo i poboljšala učinkovitost stranice. Za razliku od marketinških kolačića, analitički kolačići nisu usmjereni na praćenje korisnika preko različitih web stranica radi prikazivanja personaliziranih oglasa, već su fokusirani na poboljšanje funkcionalnosti i performansi same web stranice. Primjeri ovih kolačića uključuju Google Analytics, koji se koristi za prikupljanje statističkih podataka o

posjetiteljima i njihovom ponašanju na stranici. Podaci koje prikupljaju analitički kolačići mogu uključivati informacije poput koje stranice korisnici najčešće posjećuju, koliko dugo ostaju na određenim stranicama, te koje su stranice najpopularnije. Sami podaci se obično prikupljaju anonimno, što znači da se podaci prikupljaju grupirani, bez identifikacije pojedinačnih korisnika, i tako se i obrađuju.

1.2.9. Superkolačić

Superkolačić (engl. *supercookie*) se koristi za praćenje korisnikove povijesti i navika po internetu, bez obzira na preglednik koji koristi. Iako tehnički nije HTTP kolačić, on predstavlja informacije koje se ubacuju u pakete podataka poslane s korisnikovog uređaja prema usluzi na koju je povezan. Poznat je i kao zaglavlje za jedinstveno prepoznavanje (engl. *unique identifier header*, UIDH), a s obzirom da nije pohranjen na korisnikovom uređaju, sam korisnik ga ne može niti obrisati, niti blokirati (Wranka, 2019).

Superkolačići prikupljaju veliki raspon podataka o korisničkim navikama na internetu, uključujući posjećene web stranice i vrijeme tih posjeta, a mogu pristupiti i informacijama koje prikupljaju ostali kolačići i zadržati ih čak i nakon brisanja ostalih kolačića. Superkolačići su često skriveni u predmemoriji preglednika, što korisnicima otežava njihovo uklanjanje bez gubitka koristi od predmemoriranja, poput bržeg pregledavanja i manjeg korištenja propusnosti.

1.2.10. Flash kolačić

Flash kolačići su najčešća vrsta superkolačića i djeluju slično kao obični kolačići, ali ih je teže pronaći i izbrisati. Programeri koriste Flash dodatak kako bi sakrili ove kolačiće od alata za upravljanje kolačićima u pregledniku. Flash kolačići su dostupni svim preglednicima, tako da promjena preglednika ne pruža značajne sigurnosne prednosti. Oni mogu pohraniti do 100KB podataka, što je znatno više u usporedbi s 4KB koliko može pohraniti obični HTTP kolačić (Price, 2018).

1.2.11. Zombi kolačić

Zombi kolačić (engl. *zombie cookie*) koji se, kako sam naziv sugerira, ne može jednostavno ukloniti. Čak i ako korisnik obriše sve kolačiće, ova vrsta ostaje netaknuta jer se skriva izvan uobičajenog prostora za pohranu kolačića u pregledniku: lokalnoj memoriji, HTML5

memoriji, RGB kodovima boja i sl. Oglašivač može pronaći postojeći kolačić u bilo kojem od tih prostora i oživjeti ostale. Ako korisnik ne izbriše sve zombi kolačiće iz svih lokacija, oni će se ponovno pojaviti (Phillips, 2019).

1.3. Sigurnosni rizici

Web kolačići se mogu koristiti za razne vrste kibernetičkih napada, i taj sigurnosni rizik je glavni razlog zbog kojeg su razni web preglednici ukinuli podršku za kolačiće trećih strana. U nastavku su navedeni i objašnjeni neki napadi koji mogu iskoristiti kolačiće za nanošenje štete korisnicima.

1.3.1. Krađa kolačića

Krađa kolačića (engl. *cookie theft*) je napad u kojem napadači kradu kolačiće korisnika kako bi dobili neovlašteni pristup web aplikacijama ili sustavima. Do njega dolazi kada napadač uspije doći do kolačića pohranjenih u pregledniku korisnika, koji često sadrže sesijske identifikatore, autentifikacijske tokene ili druge osjetljive i privatne informacije koje omogućuju pristup korisničkim računima. Ako napadač dobije pristup tim kolačićima, može se predstaviti kao korisnik i pristupiti zaštićenim resursima bez odgovarajuće autorizacije.

1.3.2. Otimanje sesije

Otimanje sesije (engl. *session hijacking*) je ozbiljan sigurnosni napad u kojem napadači preuzimaju aktivnu sesiju korisnika kako bi stekli neovlašteni pristup web aplikacijama ili sustavima. Događa se kada napadač uspije ukrasti ili presresti sesijski identifikator korisnika, često pohranjen u kolačićima, koji omogućuje napadaču da se predstavi kao stvarni korisnik i pristupi osjetljivim informacijama ili izvršava radnje kao što su promjene postavki, pristup osobnim podacima ili čak provođenje financijskih transakcija.

1.3.3. XSS

XSS (engl. *cross-site scripting*) predstavlja jedan od najčešćih i najopasnijih sigurnosnih problema u web aplikacijama. Ovaj napad omogućuje napadačima da u kod web stranice ubace zlonamjerni kod, i prilikom korisničkog posjeta, kada se ta stranica učitava, uz sve njene skripte se u pregledniku žrtve izvršava i taj napadačev kod. Ove skripte mogu ukrasti

korisničke podatke, preusmjeriti korisnike na zlonamjerne stranice ili izvesti druge štetne radnje.

Europska akademija za certifikaciju informacijskih tehnologija (2023) navodi kako postoji više vrsta ovog napada:

1. Pohranjeni XSS, poznat i kao trajni XSS, se odnosi na zlonamjerne kodove postavljene direktno na poslužitelju, pa su žrtve svi korisnici stranica tog poslužitelja.
2. Odraženi XSS, poznat i kao nepostojani XSS, ne pohranjuje zlonamjerni kod na poslužitelj već ga ugrađuje unutar poveznica ili obrazaca, pa kad korisnik klikne na njega, on se šalje korisniku u odgovoru poslužitelja te se pokreće u korisnikovom pregledniku.
3. XSS temeljen na DOM-u je ranjivost prilikom koje se zlonamjerni kod ubacuje u skriptu na strani klijenta, pri čemu mijenja ponašanje stranice.
4. Slijepi XSS, poznat i kao pohranjeni DOM XSS ili XSS na strani poslužitelja, je napad kod kojeg se se zlonamjerni kod pohranjuje na poslužitelj i izvršava kad se dogodi određeni događaj. Problematičan je za otkrivanje i otklanjanje jer napadač nije direktno povezan već se oslanja na treću stranu, poput drugih korisnika ili administratora.
5. Self-XSS, poznat i kao self-inflicted XSS, se oslanja tehnike društvenog inženjeringa kako bi prevario korisnike da izvrše zlonamjerni kod u vlastitom pregledniku, što može biti očito iz samog imena. Korisnike se navodi da sami izvrše kod u konzoli svog preglednika.

1.3.4. CSRF

CSRF (engl. *cross-site request forgery*) je napad krivotvorenja zahtjeva na različitim stranicama koji predstavlja ozbiljnu sigurnosnu prijetnju. Omogućuje napadačima da izvrše neovlaštene radnje u ime korisnika bez njihova znanja. CSRF napad nastaje kada napadač prevari korisnika da odradi određene radnje, a da ih nije ni svjestan. Napadač može koristiti napad za izvođenjeradnji bez izravne interakcije s ciljanom web aplikacijom.

1.3.5. Praćenje i profiliranje

Praćenje (engl. *tracking*) putem web kolačića odnosi se na proces prikupljanja informacija o korisnikovom ponašanju na internetu. Kolačići omogućuju web stranicama da zapamte korisnikove aktivnosti i preferencije, kao što su prijave, posjećene stranice i kupljeni proizvodi. Ove informacije mogu se koristiti za pružanje personaliziranog sadržaja i oglašavanja.

Profiliranje (engl. *profiling*) putem web kolačića je stvaranje detaljnog profila korisnika temeljenog na njegovom ponašanju na internetu. Ova metoda omogućava tvrtkama da analiziraju obrasce korištenja, interese i preferencije korisnika. Profiliranje može uključivati prikupljanje podataka kao što su demografski podaci, povijest pretraživanja i interakcije s oglasima.

Sami po sebi, ovi načini korištenja kolačića ne izgledaju kao sigurnosna prijetnja, ali su itekako prijetnja za korisnike, kako za njihovu privatnost, tako i za sigurnost. Osim što se podaci mogu prikupljati bez znanja i dopuštenja korisnika, mogu se prikupljati osjetljivi podaci čija dostupnost neovlaštenim osobama direktno ugrožava korisnika. Opsežni i detaljni korisnički profili mogu dovesti do invazivnog ciljanog oglašavanja ili diskriminacije, i često stvaraju osjećaj nesigurnosti i praćenja kod korisnika.

1.3.6. Man-in-the-Middle (MitM)

Man-in-the-Middle (MitM) je vrsta napada u kojoj napadač presreće, mijenja ili manipulira komunikacijom između dvije strane koje vjeruju da komuniciraju izravno jedna s drugom. MitM napadi uključuju situaciju u kojoj napadač, ili „srednji čovjek“, nesmetano nadgleda i potencijalno mijenja komunikaciju između dvije strane. Ovi se napadi mogu dogoditi u različitim okruženjima, uključujući privatne i javne mreže.

1.3.7. Fiksiranje sesije

Fiksiranje sesije (engl. *session fixation*) omogućuje napadaču da preuzme kontrolu nad sesijom korisnika manipulacijom sesijskog identifikatora. Događa se kada napadač uspije postaviti, tj. fiksirati sesijski identifikator za ciljanu korisničku sesiju prije nego što se korisnik prijavi. Nakon što korisnik prijavi sesiju s tim fiksiranim identifikatorom, napadač

može preuzeti kontrolu nad tom sesijom. Ovaj napad omogućuje napadaču da imitira korisnika.

1.3.8. Iskorištavanje isteka valjanosti kolačića

Iskorištavanje isteka valjanosti kolačića (engl. *expired cookie exploitation*) je sigurnosni rizik koji se događa kada napadači koriste kolačiće koji su istekli ili su u fazi isteka kako bi neovlašteno pristupili korisničkim računima ili podacima. Kada kolačići isteknu, obično se očekuje da postanu nevažeći i da se više ne mogu koristiti za autentifikaciju korisnika. Međutim, u određenim situacijama, napadači mogu pokušati iskoristiti istekle kolačiće za neovlašteni pristup. Ova vrsta napada može omogućiti napadačima da zaobiđu sigurnosne mjere i pristupe osjetljivim informacijama.

1.3.9. Cookie Tossing

Cookie tossing, slobodno prevedeno kao podmetanje kolačića, je napad u kojem napadači manipuliraju kolačićima kako bi postigli neovlašteni pristup. Napad se odvija kada napadač koristi zaražene kolačiće da bi prevario web aplikaciju ili korisnike i stekao neovlašteni pristup ili iskoristio povlastice koje inače ne bi imao. Napadači mogu manipulirati kolačićima koji su pohranjeni u pregledniku korisnika ili ih mogu koristiti za prepisivanje postavki i podataka koji se odnose na sesiju.

1.4. Mjere zaštite

Uz sve do sada navedene opasnosti vezane za kolačiće, postoje i mjere zaštite koje mogu poduzeti ne samo korisnici, već i vlasnici, tj. programeri web stranica koji kodiraju same kolačiće. U nastavku su navedene i ukratko objašnjene neke mjere zaštite protiv napada preko kolačića.

1. **Pridavanje sigurnosnih atributa kolačićima** - postoji nekoliko atributa vezanih za sigurnost koji se mogu pridodati kolačićima:
    - `HttpOnly` - kolačići se mogu čitati samo na strani poslužitelja i nisu dostupni putem JavaScript-a na strani klijenta.

- `Secure` - kolačići se šalju samo preko sigurnih HTTPS veza, čime se sprječava njihovo presretanje. Kolačići s atributom Secure ne mogu se prenijeti putem nešifriranih HTTP veza.
- `SameSite` - ograničava slanje kolačića prema različitim web stranicama. Postavljanjem ovog atributa na `Strict` ili `Lax`, kolačić se neće poslati u zahtjevima koji dolaze s druge stranice, što smanjuje rizik od njihove zlouporabe.

2. **Ograničavanje trajanja kolačića** - ograničavanjem trajanja kolačića na najkraće moguće potrebno vrijeme, smanjuje se vremenski period u kojem napadač može zloupotrijebiti kolačić u slučaju da ga presretne.
3. **Redovito brisanje i obnavljanje sesijskih kolačića** - web aplikacije mogu redovito mijenjati i ponovno generirati sesijske ID-ove i kolačiće, osobito nakon prijave korisnika. Ovo smanjuje rizik od napada poput otmice ili fiksacije sesije, jer napadač nema dovoljno vremena za zloupotrebu sesije.
4. **Šifriranje kolačića** - šifriranje sadržaja kolačića je dodatni sloj sigurnosti jer čak i ako napadač presretne kolačić, neće moći razumjeti njegov sadržaj bez odgovarajućeg ključa za dešifriranje. Ovo je posebno važno za kolačiće koji pohranjuju osjetljive podatke.
5. **Ograničavanje pristupa kolačićima prema putanji i domeni** - web stranice mogu koristiti `Path` i `Domain` atribute kako bi ograničili dostupnost kolačića samo određenim dijelovima web stranice ili određenim domenama, čime se smanjuje rizik od zloupotrebe kolačića na neovlaštenim dijelovima web stranice ili na drugim domenama.
6. **Korištenje sigurnosnih pravila sadržaja** – implementacija sigurnosnih pravila sadržaja (engl. *Content Security Policy*, CSP) pomaže u zaštiti od napada kao što je XSS tako što se ograničavaju izvori s kojih se mogu izvršavati skripte, čime se dodatno smanjuje rizik od krađe kolačića putem zlonamjernog koda.
7. **Redovito ažuriranje preglednika i web aplikacija** - ažuriranja često uključuju sigurnosne zakrpe koje popravljaju ranjivosti vezane za kolačiće i druge sigurnosne aspekte. Korištenje najnovijih verzija softvera pomaže u zaštiti od poznatih prijetnji.

8. **Korištenje alata za detekciju i prevenciju napada** - alati poput vatrozida za web aplikacije (engl. *Web Application Firewall*, WAF) mogu prepoznati i blokirati sumnjive aktivnosti vezane za kolačiće, poput pokušaja krađe kolačića ili napada na sesije, što dodatno osigurava web aplikacije.

1.5. Zakonske regulative

Neke zakonske regulative vezane za zaštitu privatnosti i sigurnost podataka su već spomenute ranije u radu, a u ovom poglavlju će se pojasniti malo opširnije. S razvojem tehnologije i povećanjem količine osobnih podataka koji se prikupljaju i obrađuju, Europska unija i Republika Hrvatska su usvojile niz zakonskih regulativa s ciljem zaštite osobnih podataka i privatnosti građana.

1.5.1. Opća uredba o zaštiti podataka (GDPR)

Kao što je već spomenuto u radu, GDPR je usvojena 27. travnja 2016., a stupila je na snagu 25. svibnja 2018. godine. Predstavlja najznačajniji zakon o zaštiti podataka u Europskoj uniji (EU) i postavlja stroge zahtjeve za prikupljanje, obradu i pohranu osobnih podataka te osigurava pojedincima veća prava u vezi s njihovim podacima. Obvezujuća je za sve organizacije koje obrađuju osobne podatke građana EU, bez obzira na to gdje se nalaze.

Neke od ključnih odredbi GDPR-a, izdvojene iz originalnog dokumenta (Uredba (EU) 2016/679), su slijedeće:

1. Organizacije moraju dobiti jasnu i nedvosmislenu suglasnost pojedinaca prije prikupljanja i obrade njihovih osobnih podataka (članak 7).
2. Pojedinci imaju pravo znati koje se informacije o njima prikupljaju i obrađuju te mogu zatražiti kopiju tih podataka (članak 15).
3. Pojedinci mogu zatražiti brisanje svojih osobnih podataka ako više nisu potrebni za svrhe za koje su prikupljeni ili ako povuku pristanak na njihovu obradu (članak 17).
4. Pojedinci imaju pravo prenijeti svoje podatke iz jednog sustava u drugi, što im omogućuje veću kontrolu nad njihovim informacijama (članak 20).
5. Organizacije moraju prijaviti povrede osobnih podataka nadležnim tijelima unutar 72 sata od otkrivanja povrede (članak 33).

Prekršaji protiv odredbi GDPR-a mogu rezultirati značajnim kaznama. Organizacije mogu biti kažnjene kaznama do 20 milijuna eura ili 4% godišnjeg globalnog prometa, ovisno o tome koja je vrijednost veća (članak 83).

U Republici Hrvatskoj, GDPR se primjenjuje izravno uz dodatne odredbe koje su uvedene Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/2018). Agencija za zaštitu osobnih podataka (AZOP) zadužena je za provedbu GDPR-a u Hrvatskoj, a neke njene ovlasti su nadzor nad obradom podataka, izdavanje smjernica i provođenje inspekcija (AZOP, n.d.). AZOP također može izricati kazne te pokrenuti i sudski postupak radi naknade štete koju su pretrpjeli pojedinci čiji su podaci nezakonito obrađeni.

1.5.2. Direktiva o privatnosti i elektroničkim komunikacijama (ePrivacy)

Pored GDPR-a, ePrivacy direktiva (Direktiva 2002/58/EZ) uređuje privatnost i zaštitu osobnih podataka u kontekstu elektroničkih komunikacija. Ova direktiva, poznata i kao „*cookie law*“, zahtijeva da web stranice dobiju pristanak korisnika prije postavljanja kolačića na njihove uređaje. Planira se zamjena direktive novom uredbom koja će uskladiti pravila o privatnosti u svim državama članicama EU i pružiti veću zaštitu privatnosti korisnika u digitalnom okruženju.

1.6. Legitimni interes

Legitimni interes je jedan od pravnih temelja prema kojem organizacije mogu prikupljati i obrađivati osobne podatke korisnika bez njihovog izravnog pristanka, pod uvjetom da to ne ugrožava prava i slobode pojedinca. Prema GDPR (Uredba (EU) 2016/679), legitimni interes može biti opravdanje za obradu podataka kada organizacija ima valjani poslovni razlog koji ne nadmašuje interese ili temeljna prava korisnika. Drugim riječima, organizacija mora pažljivo procijeniti hoće li obrada podataka biti u skladu s interesima korisnika i pridonosi li onim ciljevima koji se mogu opravdati.

U kontekstu kolačića, legitimni interes se često koristi za određene aktivnosti koje su potrebne za funkcioniranje web stranica ili poboljšanje usluga, ali koje ne zahtijevaju izravnu privolu korisnika. Na primjer, tvrtke mogu tvrditi da imaju legitimni interes za prikupljanje podataka kako bi optimizirale performanse svojih stranica, analizirale promet ili spriječile

sigurnosne prijetnje. Međutim, legitimni interes nije univerzalno opravdanje za sve vrste obrade podataka putem kolačića, posebno kada se radi o praćenju korisnika u marketinške svrhe.

Da bi se opravdalo korištenje legitimnog interesa, organizacija mora proći kroz tri ključna testa (ICO, n.d.). Prvi je test svrhe, koji ocjenjuje je li interes organizacije zakonit i stvaran. Ovaj interes može biti poslovni, društveni ili pravni, no mora imati jasnu osnovu. Nakon toga slijedi test nužnosti, koji procjenjuje je li obrada podataka neophodna za postizanje određenog cilja. Ako postoji neki manje invazivan način za postizanje istog cilja, tada obrada podataka putem legitimnog interesa nije opravdana. Posljednji, i možda najvažniji, je test ravnoteže. Ovdje se interes organizacije mora usporediti s pravima i slobodama pojedinaca čiji se podaci obrađuju. Ako su prava pojedinca, poput prava na privatnost, važnija od interesa organizacije, obrada podataka ne bi trebala biti dozvoljena. Posebna pažnja mora se posvetiti osjetljivim podacima ili ranjivim skupinama, poput djece, čija prava moraju biti posebno zaštićena (Ostendo Group, 2019).

Transparentnost je ključna u korištenju legitimnog interesa. Organizacije moraju jasno informirati korisnike o tome zašto se oslanjaju na ovu osnovu, koje podatke prikupljaju i kako se ti podaci koriste. Također, korisnicima mora biti omogućeno da prigovore obradi svojih podataka ako se s njom ne slažu.

2. Povezani radovi

Od svog nastanka pa do danas, web kolačići su predmet brojnih istraživanja zbog njihove ključne uloge u oblikovanju korisničkog iskustava prilikom korištenja interneta.

Jayakumar (2021) istražuje stavove korisnika prema mehanizmima pristanka na kolačiće u Europskoj uniji nakon implementacije GDPR-a i Direktive o privatnosti u elektroničkoj komunikaciji. Istraživanje, temeljeno na anketi provedenoj među 132 punoljetna korisnika interneta u EU, otkriva da su korisnici općenito svjesni kolačića, ali preferiraju brzi pristup i skloniji su prihvaćanju kolačića zbog praktičnosti, ali se radije odriču kolačića trećih strana koji se koriste za ciljano oglašavanje. Rad predlaže okvir za Direktivu o pristanku za oglašavanje kako bi se poboljšala zaštita podataka korisnika i povećala transparentnost u praksama prikupljanja podataka. Naglašava se i potreba za bolje dizajniranim privolama koje stavljaju prioritet na korisničko iskustvo i stvarni pristanak, a ne samo na ispunjavanje regulatornih zahtjeva. Unatoč uvođenju GDPR-a, usklađenost ostaje niska, a mnoge tvrtke i dalje prioritet daju praktičnosti umjesto privatnosti korisnika.

Kulyk, Hilt, Gerber i Vokamer (2018) istražuju percepcije i reakcije korisnika na obavijesti o kolačićima na web stranicama, s posebnim naglaskom na zabrinutost o privatnosti. Korištena je online anketa, a sudjelovalo je 150 sudionika. Rezultati ukazuju na to da mnogi korisnici obavijesti o kolačićima doživljavaju kao smetnju, iritantnu i neinformativnu, a ne kao korisne informacije, pa tekst obavijesti ima mali utjecaj na odluke korisnika. Umjesto toga, važniji su ugled web stranice i vrsta usluge koju nudi. Sudionici su izrazili zabrinutost zbog privatnosti, posebno za transparentnost korištenja podataka.

Schiefermair i Stabauer (2020) u svom istraživanju analiziraju utjecaj obavijesti o kolačićima na percepciju privatnosti i povjerenje u kontekstu online trgovina. Eksperiment je proveden na način da su ispitanici koristili lažnu online ljekarnu kreiranu za potrebe istraživanja, a koja je prikazivala različite oblike obavijesti o kolačićima: iskačuće prozore (engl. *cookie pop-up*) i trake s kolačićima (engl. *cookie banner*). Iako većina postavljenih hipoteza nije bila potvrđena, rezultati upućuju na to da su *pop-up* privole učinkovitije od traka s kolačićima u povećanju percipirane privatnosti i povjerenja. Istraživanje naglašava da obavijesti o kolačićima ne služe samo za ispunjavanje zakonskih obveza, već također mogu utjecati na ponašanje potrošača u online trgovini. Premda nisu imale značajan utjecaj

na percepciju privatnosti i povjerenja, *pop-up* privole su češće bile primijećene i dovele su do više stope prihvaćanja kolačića.

Božić i Jakšić (2020) istražuju percepcije korisnika o online privatnosti i sigurnosti u Hrvatskoj putem ankete provedene među 311 ispitanika. Iako je korištenje interneta u Hrvatskoj značajno poraslo u vremenskom razdoblju od 2015. do 2020. godine, digitalne kompetencije se nisu razvijale u istom omjeru. To je dovelo do toga da mnogi korisnici nisu svjesni prijetnji vezanih za sigurnost i privatnost, posebno na društvenim mrežama. Ključni rezultati ovog istraživanja uključuju zabrinutost korisnika o sigurnosti podataka, ali i sklonost dijeljenju osjetljivih informacija online. Istraživanje također ukazuje na razlike u percepciji privatnosti prema spolu, dobi i obrazovanju, te naglašava potrebu za poboljšanjem digitalne pismenosti i svijesti o pitanjima online privatnosti među hrvatskim korisnicima interneta.

3. Metodologija istraživanja

3.1. Predmet i cilj istraživanja

Istraživačko pitanje: Kako percepcija korisnika interneta o web kolačićima utječe na njihovu svijest o privatnosti, sigurnosne prakse i spremnosti za edukaciju?

Cilj ovog istraživanja je otkriti na koji način korisnici interneta percipiraju web kolačiće te kako ta percepcija utječe na njihove stavove i ponašanja u vezi s privatnosti, sigurnosnim praksama i edukaciji o kolačićima. Pitanje je važno jer razina razumijevanja i svijesti o kolačićima može značajno utjecati na načine kojima korisnici štite svoje podatke na internetu i koliko su spremni ulagati trud i vrijeme u edukaciju kako bi bolje razumjeli tehnologije koje koriste.

Istraživanje se sastoji od pet dijelova, i svaki dio osim poslijednjeg ima svoju hipotezu. U nastavku su prvo ukratko objašnjeni dijelovi istraživanja, a zatim su nabrojane i objašnjene i hipoteze.

1. Percepcija korisnika o web kolačićima:
   Koliko korisnici razumiju što su web kolačići, koje funkcije obavljaju i kako utječu na njihovu privatnost? Važno je saznati jesu li korisnici svjesni da web kolačići mogu pratiti njihove aktivnosti na internetu i pohranjivati njihove preferencije.
2. Svijest o privatnosti:
   Koliko su korisnici zabrinuti za svoju privatnost kada su u pitanju web kolačići? Jesu li svjesni potencijalnih rizika i sigurnosnih incidenata koji mogu nastati zbog korištenja kolačića? Koliko su oprezni u dijeljenju svojih podataka na internetu?
3. Sigurnosne prakse:
   Koje mjere korisnici poduzimaju kako bi zaštitili svoju privatnost i sigurnost u kontekstu web kolačića? To uključuje korištenje alata za upravljanje kolačićima, promjene postavki privatnosti u preglednicima, te učestalost brisanja kolačića.
4. Spremnost za edukaciju:
   Koliko su korisnici otvoreni za učenje o web kolačićima i sigurnosnim praksama? Koliko su spremni uložiti vrijeme i trud u edukaciju kako bi bolje razumjeli kolačiće, njihove funkcije i načine zaštite privatnosti?

5. Stavovi o privolama

   Znaju li ispitanici prepoznati pravilne privole? Kako količina informacija i ponuđenih odabira na privoli utječe na njihov stav prema samoj stranici?

H1: Nedostatak razumijevanja

Pretpostavljamo da većina korisnika interneta ne razumije u potpunosti svrhu i funkcionalnost web kolačića. Iako su obavijesti o kolačićima prisutne na većini web stranica, mnogi korisnici nemaju dovoljno tehničkog znanja ili interesa da detaljno istraže što su kolačići i kako funkcioniraju. To može rezultirati niskom razinom svijesti i znanja o njihovim prednostima i rizicima.

H2: Visoka razina zabrinutosti za privatnost

Pretpostavljamo da su korisnici koji su svjesni postojanja web kolačića više zabrinuti za sigurnost i privatnost svojih podataka. Kako se povećava svijest o kibernetičkoj sigurnosti i privatnosti, korisnici postaju sve više zabrinuti zbog načina na koji web stranice prate njihove aktivnosti i koriste njihove podatke. Kolačići, kao alat za praćenje, mogu izazvati zabrinutost među informiranim korisnicima.

H3: Preferiranje transparentnosti i kontrole

Pretpostavljamo da korisnici preferiraju web stranice koje pružaju jasne informacije o upotrebi kolačića i omogućuju jednostavne opcije za upravljanje kolačićima. Transparentnost i kontrola nad osobnim podacima su važni faktori za korisnike. Web stranice koje omogućuju jednostavno prilagođavanje postavki kolačića i jasno informiraju korisnike o njihovoj upotrebi vjerojatno će biti bolje prihvaćene.

H4: Spremnost za edukaciju

Pretpostavljamo da su korisnici otvoreni prema edukaciji o kolačićima ako im se pruže jasne i lako razumljive informacije o njihovoj svrsi, upotrebi i načinima upravljanja. Smatra se da je jedan od ključnih problema nedovoljna informiranost korisnika o kolačićima, njihovoj funkcionalnosti, potencijalnim sigurnosnim rizicima i načinima na koje mogu upravljati kolačićima te da edukacija korisnika može poboljšati njihovo razumijevanje i sposobnost donošenja informiranih odluka o svojoj privatnosti na internetu.

3.2. Instrumenti istraživanja

3.2.1. Opis instrumenta istraživanja

Istraživanje je provedeno putem ankete koja se sastoji od 50 pitanja podijeljenih u šest dijelova. Svaki dio ankete prilagođen je za prikupljanje specifičnih podataka koji će omogućiti testiranje postavljenih hipoteza te razumijevanje percepcija i ponašanja korisnika u vezi s web kolačićima i njihovim utjecajem na privatnost i sigurnost.

3.2.2. Struktura ankete

1. Osnovne informacije o korisniku:

Prvi dio ankete sadrži četiri pitanja koja se odnose na demografske karakteristike ispitanika: dob, spol, razina obrazovanja i učestalost korištenja interneta. Ovi podaci omogućuju profiliranje korisnika i uvid u njihove osnovne karakteristike, koje mogu utjecati na odgovore u daljnjim dijelovima ankete.

2. Nedostatak razumijevanja (H1):

Ovaj dio sadrži šest pitanja koja procjenjuju razinu razumijevanja korisnika o svrsi i funkcionalnosti web kolačića. Ispituje se svijest korisnika o tome što su kolačići, zašto se koriste te kako se unutar preglednika može upravljati kolačićima. Cilj je ispitati hipotezu da većina korisnika ne razumije u potpunosti web kolačiće.

3. Visoka razina zabrinutosti za privatnost (H2):

U ovom dijelu korisnici odgovaraju na sedam pitanja koja mjere njihovu zabrinutost za privatnost i sigurnost podataka na internetu te dodatne mjere zaštite koje poduzimaju da bi se bolje zaštitili. Pitanja se fokusiraju na percepciju rizika povezanih s korištenjem kolačića i svijest o mogućnostima praćenja putem kolačića. Ovaj dio istražuje hipotezu da korisnici koji su svjesni postojanja kolačića više brinu o svojoj privatnosti.

4. Preferiranje transparentnosti i kontrole (H3):

Četvrti dio ankete usmjeren je na korisničke preferencije u vezi s transparentnošću i kontrolom nad postavkama kolačića. Kroz sedam postavljenih pitanja istražujemo percepciju korisnika o važnosti transparentnosti web stranica, lakoću upravljanja kolačićima i sklonost prema stranicama koje omogućuju veću kontrolu nad podacima. Ovaj dio testira

hipotezu da korisnici preferiraju web stranice koje nude jasne informacije i jednostavne opcije za upravljanje kolačićima.

5. Spremnost za edukaciju (H4):

Ovaj dio ima šest pitanja i ispituje spremnost korisnika na edukaciju o kolačićima ako im se pruže jasne i razumljive informacije. Pitanja obuhvaćaju interes za edukativne materijale, percepciju važnosti razumijevanja kolačića za sigurnost na internetu, te voljnost da ulože vrijeme u edukaciju. Cilj je testirati hipotezu da su korisnici otvoreni prema edukaciji o kolačićima.

6. Ocjenjivanje privola za kolačiće:

Posljednji dio ankete fokusira se na korisničke percepcije i stavove prema privolama za kolačiće koje se pojavljuju prilikom posjeta web stranicama. Ispitanicima je prikazano pet privola i na svaku se odnose četiri pitanja: smatraju li korisnici da je prikazana privola ispravna, što bi najvjerojatnije kliknuli kada im se prikaže taj tip privola, koliko vjeruju web stranici s obzirom na prikazanu privolu, koliko su zadovoljni količinom informacija sadržanih u privoli. Tih dvadeset pitanja pomaže razumjeti kako korisnici percipiraju privole za kolačiće i kako to utječe na njihovu interakciju s web stranicama, a također mogu pružiti uvid u njihovu razinu zadovoljstva i povjerenja prema web stranicama.

3.2.3. Cilj instrumenta

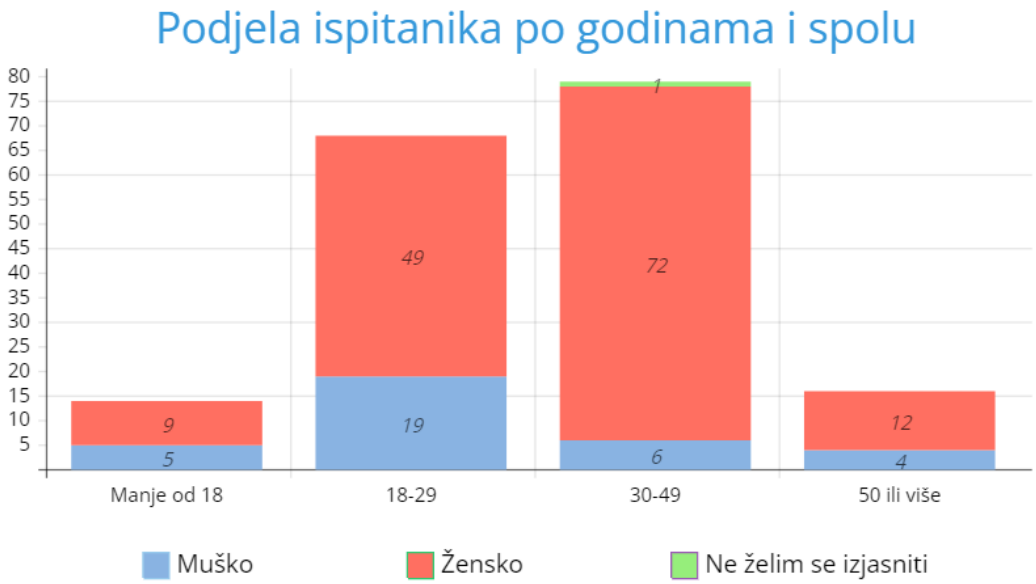
Cilj ove ankete je prikupiti podatke koji će omogućiti sveobuhvatnu analizu korisničkih percepcija, znanja, i ponašanja u vezi s web kolačićima. Svaki dio ankete pažljivo je osmišljen kako bi podržao testiranje specifičnih hipoteza te pružio relevantne uvide koji su ključni za razumijevanje korisničkog iskustva i stavova prema kolačićima na internetu.

3.3. Sudionici

Istraživanje je provedeno od 13. kolovoza 2024. do 21. kolovoza 2024. U istraživanju su sudjelovale 174 osobe. Radi se o namjernom prigodnom uzorku jer se anketa dijelila bliskim osobama i preporukom.

4. Rezultati

Na slici 4.1 je prikazana podjela ispitanika po godinama i po spolu. Većina ispitanika je ženskog spola, i najviše ih spada u dobnu skupinu od 30 do 49 godina. Najmanje ispitanika ima manje od 18 godina, a samo malo više ih ima preko 50 godina.



Slika 4.1 Podjela ispitanika po godinama i spolu

Tablica 4.1 prikazuje podjelu ispitanika prema razini obrazovanja. Treba naglasiti da je svih 14 ispitanika koji su označili da imaju manje od 18 godina, također označilo srednju školu kao stečenu razinu obrazovanja, iako bi to, uzevši u obzir da većina srednjih škola traje četiri godine, ipak trebala biti osnovna škola. Bez obzira na tu moguću grešku, najviše ispitanika i dalje ima samo srednjoškolsko obrazovanje, a zanimljivo je da ih više ima završen diplomski studij (51) nego preddiplomski (37).

Tablica 4.1 Podjela ispitanika po razini obrazovanja

Razina obrazovanja	Broj
Osnovna škola	1
Srednja škola	76
Preddiplomski studij	37
Diplomski studij	51
Poslijediplomski specijalistički studij	5
Doktorski studij	4
Ukupno	**174**

Što se tiče korištenja interneta, rezultati prikazani u tablici 4.2 su očekivani. Preko 80% ispitanika koristi internet više od dva sata dnevno, i to su uglavnom mlađi ispitanici. 25% ispitanika između 30 i 49 godina internet koristi jedan do dva sata dnevno, a jedan ispitanik te dobne skupine ga koristi samo par puta tjedno. Jedan stariji ispitanik, iz dobne skupine 50 ili više, se izjašnjava da internet koristi samo nekoliko puta mjesečno.

Tablica 4.2 Podjela ispitanika po korištenju interneta i godinama

Korištenje interneta	Broj
Više sati dnevno	**141**
18-29	60
30-49	58
50 ili više	9
Manje od 18	14
1-2 sata dnevno	**31**
18-29	8
30-49	20
50 ili više	3
Par puta tjedno	**1**
30-49	1
Nekoliko puta mjesečno	**1**
50 ili više	1
Ukupno	**174**

U tablici 4.3 su prikazani odgovori korisnika na pitanja „Jeste li čuli za pojam "web kolačići" prije ove ankete?“ i „Kako biste ocijenili svoje razumijevanje web kolačića?“ te se odmah može vidjeti da je velika većina ispitanika upoznata sa samim pojmom, ali ne razumiju baš što on znači i što predstavlja. Među ispitanicima koji su upoznati s pojmom, najviše ih je svoje razumijevanje ocijenilo neutralnom ocjenom.

Tablica 4.3 Podjela prema ocjenama vlastitog razumijevanja kolačića

Razumijevanje kolačića	Broj
Da	**168**
1	32
2	30
3	56
4	34
5	16
Ne	**6**
1	3
3	2
4	1
Ukupno	**174**

Slika 4.2 prikazuje korelaciju između odgovora na pitanja „Kako biste ocijenili svoje razumijevanje web kolačića?“ i „Koliko Vam je važno razumjeti što su web kolačići?“.

Pearsonova korelacija između odgovora na ta dva pitanja pokazuje pozitivnu korelaciju srednje jačine, s koeficijentom od 0.461. Korelacija je statistički značajna, s p-vrijednošću manjom od 0.05 (točnije 0.000), što znači da je malo vjerojatno da je ovakva povezanost slučajna.

```
CORRELATION
        /VARIABLES =  Q6 Q7
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		Q6	Q7
Q6	Pearson Correlation	1,000	,461[a]
	Sig. (2-tailed)		,000
	N	174	174
Q7	Pearson Correlation	,461[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

a. Significant at .05 level

Slika 4.2 Korelacija Q6 i Q7

4.1. Prva hipoteza

Na temelju deskriptivne analize odgovora na pitanje "Kako biste ocijenili svoje razumijevanje web kolačića?" rezultati, prikazani u tablici 4.4, pokazuju da je prosječna ocjena razumijevanja 2.810, što ukazuje na relativno nisku razinu samoprocjene znanja o web kolačićima među sudionicima. Medijan, koji iznosi 3, sugerira da je većina odgovora bila koncentrirana oko srednje vrijednosti, što potvrđuje da je najčešća ocjena upravo „zlatna sredina“. Standardna devijacija iznosi 1.232, što znači da postoji umjerena varijabilnost u odgovorima sudionika. Raspon ocjena, koji se proteže od 1 do 5, pokazuje da su sudionici ocijenili svoje razumijevanje u cijelom spektru ponuđenih opcija.

Što se tiče frekvencija (tablica 4.5), 35 sudionika je ocijenilo svoje razumijevanje s 1 (uopće ih ne razumijem), 30 sudionika s 2, 58 sudionika odabralo ocjenu 3, 35 sudionika je odabralo ocjenu 4, a 16 sudionika ocjenu 5 (potpuno ih razumijem).

Ovi rezultati ukazuju na to da većina sudionika ima umjereno razumijevanje web kolačića, dok manji broj sudionika smatra da ih loše razumije, a najmanji dio smatra da ih dobro razumije.

Tablica 4.4 Deskriptivna statistika Q6

Kako biste ocijenili svoje razumijevanje web kolačića?	
Prosjek	2.81
Medijan	3
Standardna devijacija	1.232
Raspon	4

Tablica 4.5 Frekvencije ocjena za Q6

Ocjena	Frekvencija
1	35
2	30
3	58
4	35
5	16
Ukupno	**174**

Rezultati hi-kvadrat testa na pitanju „Znate li zašto web stranice koriste kolačiće?“ prikazani na slici 4.3 pokazuju značajne razlike između opaženih i očekivanih frekvencija odgovora. Konkretno, opažene frekvencije za odgovore variraju: 26 sudionika odabralo je opciju 1 (Da), 17 sudionika opciju 2 (Ne), 90 sudionika opciju 3 (Znam otprilike), i 41 sudionik opciju 4 (Nisam siguran/na). Nasuprot tome, očekivana frekvencija za svaki odgovor bila je 43,5. Nadalje, rezultati $X^2 = 73,03$, $df = 3$, $p < 0,001$ pokazuju vrlo značajnu razliku između opaženih i očekivanih frekvencija. To znači da su odgovori na ovo pitanje daleko od ravnomjerne raspodjele, što sugerira da sudionici nisu nasumično rasporedili svoje odgovore na ovo pitanje. Najveće odstupanje uočeno je za odgovor 3, gdje je zabilježeno mnogo više odgovora (90) nego što bi se očekivalo (43,5), dok su „ekstremni“ odgovori 1 i 2 (Da i Ne) zabilježeni znatno manje nego što je očekivano. Ovi rezultati ukazuju na jasan trend u odgovorima, gdje većina sudionika pokazuje sklonost prema srednjim odgovorima (Znam otprilike i Nisam siguran/na), od kojih su opet skloniji izabrati onaj pozitivniji.

```
NPAR TEST
        /CHISQUARE= Q8.
```

Q8

Value	Observed N	Expected N	Residual
1,00	26	43,50	-17,50
2,00	17	43,50	-26,50
3,00	90	43,50	46,50
4,00	41	43,50	-2,50
Total	174		

Test Statistics

	Chi-square	df	Asymp. Sig.
Q8	73,03	3	,000

Slika 4.3 Rezultati hi-kvadrat testa za Q8

Rezultati t-testa za pitanje „Koliko Vam je važno razumjeti što su web kolačići?“ (slika 4.4) pokazuju da prosječna ocjena iznosi 3,05 (SD = 1,21). Testna vrijednost je postavljena na 3, što odgovara neutralnoj sredini skale. Rezultati pokazuju da nema statistički značajne razlike između prosječne ocjene i testirane vrijednosti (t(173) = 0,50, p = 0,616). Srednja razlika iznosi samo 0,05, s intervalom pouzdanosti od 95% između -0,13 i 0,23. Ovi rezultati sugeriraju da sudionici u prosjeku ocjenjuju svoje odgovore na ovo pitanje kao neutralne, što znači da prosječna ocjena nije značajno ni viša ni niža od 3. Na temelju ovog testa možemo zaključiti da nema značajne sklonosti prema pozitivnim ili negativnim ocjenama među sudionicima za ovo pitanje.

```
T-TEST /TESTVAL=3
        /VARIABLES= Q7  /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation	S.E. Mean
Q7	174	3,05	1,21	,09

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Q7	,50	173	,616	,05	-,13	,23

Slika 4.4 Rezultati t-testa za Q7

Rezultati deskriptivne analize sugeriraju da ispitanici smatraju svoje razumijevanje umjerenim, s prosjekom blizu neutralne ocjene, ali ipak na strani nerazumijevanja što potvrđuje prvu hipotezu. Hi-kvadrat test ukazuje na postojanje značajne distribucije odgovora, što podržava pretpostavku da nisu svi ispitanici jednako raspodijeljeni po razinama razumijevanja. Ipak, one-sample t-test pokazuje da nema značajne sklonosti prema nižoj ili višoj važnosti razumijevanja, već je prosjek blizak neutralnoj ocjeni.

Prva hipoteza koja pretpostavlja da većina ispitanika ne razumije u potpunosti svrhu i funkcionalnost web kolačića i da nemaju dovoljno tehničkog znanja ili interesa da detaljno istraže što su kolačići i kako funkcioniraju **se djelomično potvrđuje** jer postoji obrazac u razumijevanju kolačića među ispitanicima, ali se to razumijevanje uglavnom koncentrira oko srednjih ocjena, što ukazuje na umjereno razumijevanje bez jasnog ekstremnog stava.

4.2. Druga hipoteza

Rezultati deskriptivne analize (tablica 4.6) za drugu hipotezu pokazuju da su ispitanici umjereno zabrinuti zbog privatnosti svojih podataka na internetu, praćenja njihovih online aktivnosti te percepcije o ugroženosti privatnosti zbog kolačića.

Promatrani su odgovori na slijedeća pitanja:

- Q11: Koliko ste zabrinuti zbog privatnosti svojih podataka na internetu?
- Q12: Koliko ste zabrinuti zbog praćenja vaših online aktivnosti?
- Q13: U kolikoj mjeri smatrate da kolačići ugrožavaju vašu privatnost?

Prosječna zabrinutost zbog privatnosti podataka na internetu (Q11) iznosi 3,287, s medijanom 3, što ukazuje da većina ispitanika izražava umjerenu zabrinutost. Standardna devijacija od 1,122 pokazuje relativno konzistentne odgovore, a raspon od 4 sugerira postojanje širokog spektra stavova, od "uopće nisam zabrinut/a" do "vrlo sam zabrinut/a."

Sličan trend primjećen je i u pogledu zabrinutosti zbog praćenja online aktivnosti (Q12), gdje je prosječna ocjena 3,316, također s medijanom 3 i nešto većom standardnom devijacijom od 1,192. To ukazuje na blagu raznolikost u percepciji prijetnje praćenja, ali opet unutar umjerene zabrinutosti.

Kada je riječ o percepciji ugroženosti privatnosti zbog kolačića (Q13), prosjek je nešto niži, 3,155, s medijanom također 3 i standardnom devijacijom od 1,088. Ispitanici u prosjeku

pokazuju umjerenu zabrinutost prema kolačićima, s relativno manjom varijacijom u odgovorima u usporedbi s ostalim pitanjima.

Tablica 4.6 Deskriptivna statistika Q11, Q12, Q13

	Q11	Q12	Q13
Prosjek	3.287	3.316	3.155
Medijan	3	3	3
St. devijacija	1.122	1.192	1.088
Raspon	4	4	4

Sva tri rezultata sugeriraju da ispitanici imaju umjerenu razinu zabrinutosti prema pitanjima koja se odnose na privatnost i praćenje na internetu, pri čemu su ocjene konzistentno smještene oko srednje vrijednosti (3) ali više prema većoj zabrinutosti, bez izraženih ekstremnih stavova.

Rezultati prikazani na slici 4.5 odnose se na hi-kvadrat test za pitanje „Znate li da postoje sigurnosni rizici povezani s kolačićima, poput krađe identiteta ili praćenja?“, gdje su odgovori kodirani kao "1" (Da) i "2" (Ne). Dobiveni rezultati, $X^2 = 0.57$, df = 1, p = 0.448, pokazuju da nema statistički značajne razlike između promatranih i očekivanih frekvencija za odgovore na ovo pitanje. P-vrijednost (0.448) je znatno iznad uobičajene razine značajnosti od 0.05, što znači da se ne odbacuje nulta hipoteza koja tvrdi da su promatrane frekvencije odgovora slične očekivanim frekvencijama.

Drugim riječima, na temelju ovog testa, nema dokaza o statistički značajnoj razlici u distribuciji odgovora na ovo pitanje među ispitanicima.

```
NPAR TEST
        /CHISQUARE= Q16.
```

Q16

Value	Observed N	Expected N	Residual
1,00	92	87,00	5,00
2,00	82	87,00	-5,00
Total	174		

Test Statistics

	Chi-square	df	Asymp. Sig.
Q16	,57	1	,448

Slika 4.5 Rezultati hi-kvadrat testa za Q16

Slika 4.6 prikazuje tablicu korelacija između četiri pitanja:

- Q6: Kako biste ocijenili svoje razumijevanje web kolačića?
- Q11: Koliko ste zabrinuti zbog privatnosti svojih podataka na internetu?
- Q12: Koliko ste zabrinuti zbog praćenja vaših online aktivnosti?
- Q13: U kolikoj mjeri smatrate da kolačići ugrožavaju vašu privatnost?

Vrijednost korelacije za Q6 s ostalim varijablama je relativno niska, što sugerira da nema značajne povezanosti između Q6 i ostalih varijabli. Najveća korelacija između Q6 i neke druge varijable iznosi 0,100 s Q13, ali je ova korelacija također neznatna s p-vrijednošću od 0,191.

S druge strane, primjetna je snažna pozitivna korelacija između Q11 i Q12, s Pearsonovim koeficijentom od 0,771, koja je statistički značajna ($p < 0,001$). Ovo sugerira da su Q11 i Q12 jako povezane i da promjene u jednoj varijabli vjerojatno znače promjene i u drugoj. Također, postoji značajna, ali nešto slabija, pozitivna korelacija između Q11 i Q13, kao i između Q12 i Q13. Korelacija između Q11 i Q13 iznosi 0,536, dok je korelacija između Q12 i Q13 0,582, i obje su statistički značajne.

```
CORRELATION
        /VARIABLES =  Q6 Q11 Q12 Q13
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		Q6	Q11	Q12	Q13
Q6	Pearson Correlation	1,000	,056	,010	,100
	Sig. (2-tailed)		,460	,900	,191
	N	174	174	174	174
Q11	Pearson Correlation	,056	1,000	,771[a]	,536[a]
	Sig. (2-tailed)	,460		,000	,000
	N	174	174	174	174
Q12	Pearson Correlation	,010	,771[a]	1,000	,582[a]
	Sig. (2-tailed)	,900	,000		,000
	N	174	174	174	174
Q13	Pearson Correlation	,100	,536[a]	,582[a]	1,000
	Sig. (2-tailed)	,191	,000	,000	
	N	174	174	174	174

a. Significant at .05 level

Slika 4.6 Tablica korelacija između Q6, Q11, Q12 i Q13

S obzirom da podaci pokazuju da su Q11, Q12, i Q13 međusobno povezane varijable, a da Q6 ne pokazuje značajnu povezanost s ostalim varijablama u analizi, **druga hipoteza** koja tvrdi da su korisnici koji su svjesni postojanja web kolačića više zabrinuti za sigurnost i privatnost svojih podataka, **se odbacuje**.

4.3. Treća hipoteza

Rezultati za pitanje "Koliko Vam je važno da vas web stranice jasno i iskreno informiraju o upotrebi kolačića?" prikazani u tablici 4.7 pokazuju da su ispitanici u prosjeku ocijenili važnost ove informacije kao 3.575 na skali od 1 do 5, gdje je 5 označavalo "vrlo važno". Medijan ocjene je 4, što znači da je većina ispitanika smatrala ovu informaciju prilično važnom. Standardna devijacija iznosi 1.250, što ukazuje na relativno umjerenu varijabilnost odgovora, dok je raspon rezultata 4, što znači da su odgovori obuhvatili cijeli spektar mogućih ocjena (od 1 do 5).

Tablica 4.7 Deskriptivna statistika Q18

Koliko Vam je važno da vas web stranice jasno i iskreno informiraju o upotrebi kolačića?	
Prosjek	3.575
Medijan	4
Standardna devijacija	1.25
Raspon	4

Ovi rezultati sugeriraju da većina ispitanika pridaje visoku važnost transparentnom informiranju o upotrebi kolačića na web stranicama. Iako prosjek ne doseže najvišu moguću ocjenu (5), medijan od 4 ukazuje na to da su stavovi uglavnom usmjereni prema gornjem dijelu skale.

Rezultati hi-kvadrat testa za pitanje „Koliko često čitate uvjete korištenja i politike privatnosti na web stranicama prije prihvaćanja kolačića?“ (slika 4.7) pokazuju značajnu razliku između stvarno dobivenih frekvencija i očekivanih frekvencija u odgovoru na ovo pitanje. Iz tablice je vidljivo da je $X^2 = 84,62$, df = 4, p = 0,000, što je značajno na razini 0,05. Vidljivo je da je većina ispitanika odabrala opcije 1 (Nikad, 59 ispitanika) i 2 (Rijetko, 63 ispitanika), dok je očekivana frekvencija bila 34,80 za svaku od pet ponuđenih opcija. Ova razlika između stvarnih i očekivanih frekvencija ukazuje na to da postoji jaka

preferencija među ispitanicima prema odabiru brzine i jednostavnosti naspram informiranosti i sigurnosti.

```
NPAR TEST
        /CHISQUARE= Q19.
```

Q19

Value	Observed N	Expected N	Residual
1	59	34,80	24,20
2	63	34,80	28,20
3	38	34,80	3,20
4	9	34,80	-25,80
5	5	34,80	-29,80
Total	174		

Test Statistics

	Chi-square	df	Asymp. Sig.
Q19	84,62	4	,000

Slika 4.7 Rezultati hi-kvadrat testa za Q19

Slika 4.8 prikazuje rezultate t-testa za pitanje „Koliko Vam je važno da vas web stranice jasno i iskreno informiraju o upotrebi kolačića?“. Prosječna vrijednost iznosi 3,57 (SD = 1,25),

t-vrijednost iznosi 6,06 sa 173 stupnja slobode, a dobivena p-vrijednost, koja je manja od 0,001 ukazuje na to da postoji statistički značajna razlika između srednje vrijednosti uzorka i testne vrijednosti 3. Interval pouzdanosti od 95% za razliku između srednje vrijednosti uzorka i testne vrijednosti kreće se od 0,39 do 0,76, što također ne uključuje nulu i time dodatno potvrđuje da je razlika značajna i pozitivna, sugerirajući da je prosječna vrijednost varijable Q18 značajno veća od 3. Ukratko, postoji statistički značajna razlika između srednje vrijednosti varijable Q18 i zadane testne vrijednosti 3, pri čemu je srednja vrijednost uzorka veća. To sugerira da ispitanici pridaju veliku važnost jasnom i iskrenom informiranju o upotrebi kolačića, i to značajno više od neutralne vrijednosti koja je korištena kao referentna.

```
T-TEST /TESTVAL=3
        /VARIABLES= Q18 /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Q18	174	3,57	1,25	,09

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Q18	6,06	173	,000	,57	,39	,76

Slika 4.8 Rezultati t-testa za Q18

Rezultati prikazani na slici 4.9 se odnose na t-test za varijablu Q20, tj. pitanje „Smatrate li da su obavijesti o kolačićima na web stranicama jasne i informativne?“. Testna vrijednost je postavljena na 2,5 jer su ispitanici mogli birati jedan od četiri ponuđena odgovora, pa je srednja vrijednost 2.5.

Prosječna vrijednost varijable Q20 iznosi 2,30, sa standardnom devijacijom od 0,99, dok je standardna pogreška srednje vrijednosti 0,08. T-vrijednost iznosi -2,67 s 173 stupnja slobode, a dobivena p-vrijednost je 0,008. S obzirom da je p-vrijednost manja od standardne razine značajnosti od 0,05, rezultati sugeriraju da postoji statistički značajna razlika između srednje vrijednosti uzorka i testne vrijednosti 2,5. Interval pouzdanosti od 95% za razliku između srednje vrijednosti uzorka i testne vrijednosti kreće se od -0,35 do -0,05. Ovaj interval ne uključuje nulu, što potvrđuje da je razlika između srednje vrijednosti uzorka i testne vrijednosti značajna i negativna. To sugerira da je prosječna vrijednost varijable Q20 nešto niža od 2,5. za potrebe provođenja testa, odgovori su prebačeni u brojčane vrijednosti na slijedeći način:

- 1 – Nisu jasne i nisu dovoljno informativne
- 2 – Nisu jasne ali su informativne
- 3 – Jasne su ali nisu dovoljno informativne
- 4 – Jasne su i informativne

Rezultati t-testa pokazuju da ispitanici uglavnom ocjenjuju privole za kolačiće kao nejasne. Postoji statistički značajna razlika između srednje vrijednosti varijable Q20 i zadane testne

vrijednosti 2,5, pri čemu je srednja vrijednost uzorka nešto niža, ali ta razlika je ipak statistički značajna.

```
T-TEST /TESTVAL=2.5
        /VARIABLES= Q20 /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Q20	174	2,30	,99	,08

One-Sample Test

	Test Value = 2,5					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Q20	-2,67	173	,008	-,20	-,35	-,05

Slika 4.9 Rezultati t-testa za Q20

Rezultati na slici 4.10 prikazuju analizu t-testa nad varijablom Q21, tj. pitanjem „Koliko Vam je važno da imate kontrolu nad kolačićima koje prihvaćate?“, s testnom vrijednošću postavljenom na 3. Srednja vrijednost varijable Q21 iznosi 3,41, sa standardnom devijacijom od 1,30 i standardnom pogreškom srednje vrijednosti od 0,10. Dobivena t vrijednost iznosi 4,21 s 173 stupnja slobode, dok je p-vrijednost manja od 0,001. Ovo je značajno ispod praga od 0,05, što sugerira da postoji statistički značajna razlika između srednje vrijednosti uzorka i testne vrijednosti. Interval pouzdanosti od 95% za razliku srednjih vrijednosti kreće se od 0,22 do 0,61. Ovaj interval ne uključuje nulu i pozitivan je, što dodatno potvrđuje da postoji statistički značajna razlika između srednje vrijednosti varijable Q21 i testne vrijednosti 3. Srednja vrijednost varijable Q21 je značajno viša od 3, što implicira da sudionici ocjenjuju stav vezan uz varijablu Q21 iznad neutralne točke od 3.

Slika 4.11 prikazuje Pearsonovu korelaciju između varijabli Q18 i Q21, s ciljem ispitivanja povezanosti među njima. Varijable se odnose na dva pitanja:

- Q18 – Koliko Vam je važno da vas web stranice jasno i iskreno informiraju o upotrebi kolačića?
- Q21 – Koliko Vam je važno da imate kontrolu nad kolačićima koje prihvaćate?

```
T-TEST /TESTVAL=3
        /VARIABLES= Q21 /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Q21	174	3,41	1,30	,10

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Q21	4,21	173	,000	,41	,22	,61

Slika 4.10 Rezultati t-testa za Q21

```
CORRELATION
        /VARIABLES =  Q18 Q21
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		Q18	Q21
Q18	Pearson Correlation	1,000	,662[a]
	Sig. (2-tailed)		,000
	N	174	174
Q21	Pearson Correlation	,662[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

a. Significant at .05 level

Slika 4.11 Tablica korelacije između Q18 i Q21

Korelacijski koeficijent između Q18 i Q21 iznosi 0,662, što ukazuje na relativno jaku pozitivnu korelaciju. To znači da kako se vrijednosti varijable Q18 povećavaju, postoji tendencija da se i vrijednosti varijable Q21 povećavaju. P-vrijednost za ovaj korelacijski koeficijent je 0,000, što je daleko ispod standardnog praga značajnosti od 0,05. To znači da je korelacija statistički značajna, odnosno da postoji vrlo mala vjerojatnost da je ova povezanost nastala slučajno.

Prema ovim rezultatima, **treća hipoteza** koja pretpostavlja da korisnici preferiraju web stranice koje pružaju jasne informacije o upotrebi kolačića i omogućuju jednostavne opcije za upravljanje kolačićima, **se prihvaća**.

4.4. Četvrta hipoteza

Rezultati frekvencijske analize za pitanje u kojem se ispitanici pitaju bi li pročitali više informacija o kolačićima ako bi bile dostupne, prikazani u tablici 4.8, pokazuju jasnu tendenciju prema interesu za dodatne informacije. Većina ispitanika, njih 89, što čini većinu od 51% svih odgovora, izjavila je da bi možda pročitala više informacija o kolačićima, ovisno o dostupnosti tih informacija. 24% ispitanika (42 osobe) izjavilo je da bi svakako pročitali više informacija.

Manji postotak ispitanika pokazuje nezainteresiranost za dodatne informacije: 19% ispitanika (33 osobe) izjavilo je da nemaju vremena za to, dok je 6% ispitanika (10 osoba) izjavilo da ih nije briga za kolačiće.

Ovi rezultati sugeriraju da većina ispitanika pokazuje barem neku razinu interesa za dodatne informacije o kolačićima, osobito ako su te informacije lako dostupne, a samo mali broj uopće ne zanimaju web kolačići i nisu otvoreni prema edukaciji o njima. To može ukazivati na to da je transparentnost u vezi s kolačićima važna tema za mnoge korisnike, no istodobno postoji značajan segment populacije koji nije motiviran ili zainteresiran za dodatno informiranje.

Tablica 4.8 Frekvencijska analiza za Q26

Jeste li spremni posvetiti vrijeme edukaciji o kolačićima ako vam se pruže jasne informacije?		
Da, svakako	42	24%
Možda, ovisi o dostupnosti informacija	89	51%
Ne, nemam vremena	33	19%
Ne, nije me briga za kolačiće	10	6%

S obzorom da su tri četvrtine korisnika pokazale neki stupanj zainteresiranosti za dodatnu edukaciju, **četvrta hipoteza**, koja tvrdi da su korisnici otvoreni prema edukaciji o kolačićima ako im se pruže jasne i lako razumljive informacije o njihovoj svrsi, upotrebi i načinima upravljanja, **se prihvaća**.

4.5. Privole

Na kraju ankete korisnicima je prikazano pet privola za kolačiće s web stranica: Ultragros (ultragros.hr), Index (index.hr), Podravka (podravka.hr), Kraš (kras.hr) i Hrvatska elektroprivreda (hep.hr). Za svaku privolu su trebali pretpostaviti je li ispravna, označiti opciju koju bi odabrali te ocijeniti svoje zadovoljstvo samom privolom i povjerenje prema stranici temeljeno isključivo na prikazanoj privoli.

Ispravnim privolama se smatraju one koje su u skladu sa zahtjevima koje postavlja GDPR, a u Hrvatskoj detalje o privolama postavlja AZOP (AZOP-2, 2024). Odlike ispravne, tj. valjane privole su:

- Pružanje dovoljno informacija korisnicima prije dobivanja njihove privole (politika privatnosti, postavke kolačića i sl.);
- Informacije su napisane na jednostavan i razumljiv način;
- Korisnik ima mogućnost prihvatiti i odbiti sve kolačiće na jednako jednostavan način;
- Opcije za prihvaćanje i odbijanje moraju biti dizajnirane na isti način, odnosno ne smije se koristiti manipulativni (zavaravajući) dizajn kojim se korisnika navodi da prihvati kolačiće;
- Korisnik ima mogućnost odabrati skupine kolačića po njihovoj funkcionalnosti (svrsi) za koje daje privolu;
- Rubrike za odabir kolačića (i za legitimni interes) ne smiju biti unaprijed označene;
- Korisnik ima mogućnost da klikom na oznaku X zatvori traku za kolačiće (engl. *cookie banner*), čime odbija sve kolačiće i neometano nastavlja koristiti stranicu.

Povjerenje stranici temeljeno isključivo na privoli i zadovoljstvo količinom informacija na privoli su kao varijable analizirane korištenjem t-testa i testa korelacije u programu PSPP.

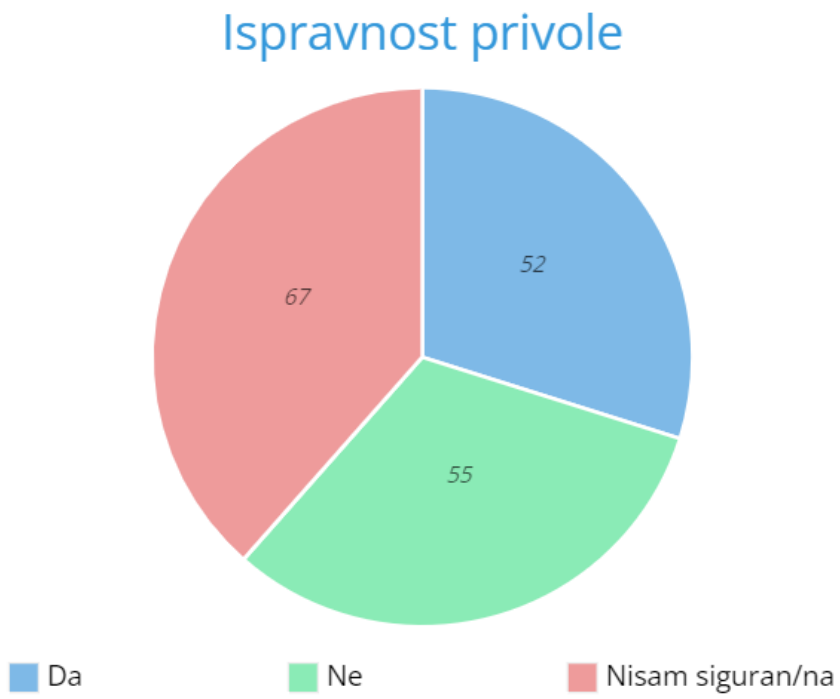
4.5.1. Privola 1: ultragros.hr

Prva privola (slika 4.12) je preuzeta sa stranice Udruženja hrvatskih trgovačkih kuća, Ultragros. Slika 4.13 prikazuje da je skoro jednak broj ispitanika ocijenio ovu privolu ispravnom (52) kao i neispravnom (55), dok ih nešto više nije sigurno (67). Jedini problem

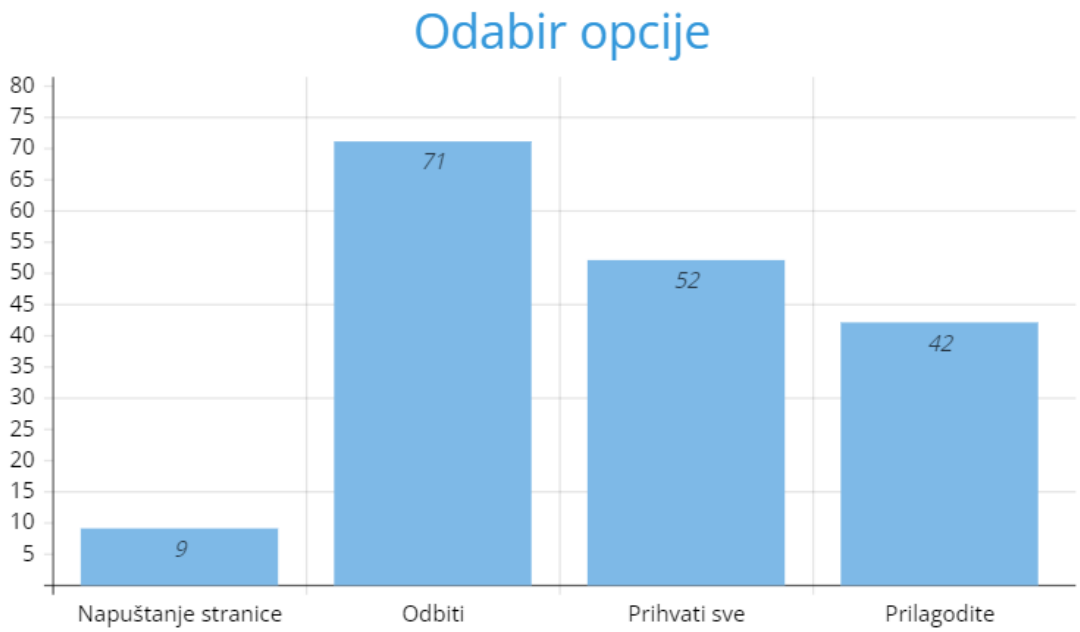
ove privole je zavaravajući dizajn, jer je opcija „Prihvati sve“ obojana žarko crveno, dok su ostale opcije bijele kao i pozadina, čime se korisnika potiče da odabere upravo nju. Svi ostali aspekti privole su u skladu s navedenim AZOP-ovim smjernicama.

Većina ispitanika (71) bi pri susretu s ovom privolom odbila sve kolačiće a manji broj bi ih prihvatio sve (52). 42 ispitanika bi tražila dodatne informacije klikom na opciju Prilagodite, a njih 9 bi napustilo stranicu (slika 4.14).

Slika 4.12 Privola sa stranice ultragros.hr



Slika 4.13 Procjene ispravnosti privole ultragros.hr



Slika 4.14 Odabir opcije na privoli ultragros.hr

Rezultati t-testa za povjerenje stranici temeljem privole i zadovoljstvo količinom informacija na njoj (slika 4.15) pokazuju statistički značajnu razliku od testne vrijednosti (3) za obje varijable. Srednja vrijednost za povjerenje iznosi 2,64 (t = -5,38, p < .001), dok je srednja vrijednost za zadovoljstvo 2,66 (t = -4,83, p < .001). Negativne vrijednosti razlika sugeriraju da su oba rezultata značajno niža od testne vrijednosti, s intervalima pouzdanosti koji ne prelaze vrijednost 3.

```
T-TEST /TESTVAL=3
        /VARIABLES= Povjerenje1 Zadovoljstvo1   /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Povjerenje1	174	2,64	,87	,07
Zadovoljstvo1	174	2,66	,94	,07

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Povjerenje1	-5,38	173	,000	-,36	-,49	-,23
Zadovoljstvo1	-4,83	173	,000	-,34	-,49	-,20

Slika 4.15 Rezultati t-testa za povjerenje prema stranici i zadovoljstvo privolom

Korelacija između navedenih odgovora (slika 4.16) iznosi r = 0,504, što je statistički značajno na razini p < 0,001. Ova korelacija ukazuje na umjerenu pozitivnu povezanost između povjerenja i zadovoljstva u slučaju ove privole.

```
CORRELATION
        /VARIABLES =  Povjerenje1 Zadovoljstvo1
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		ovjerenje1	dovoljstvo
Povjerenje1	Pearson Correlation	1,000	,504[a]
	Sig. (2-tailed)		,000
	N	174	174
Zadovoljstvo1	Pearson Correlation	,504[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

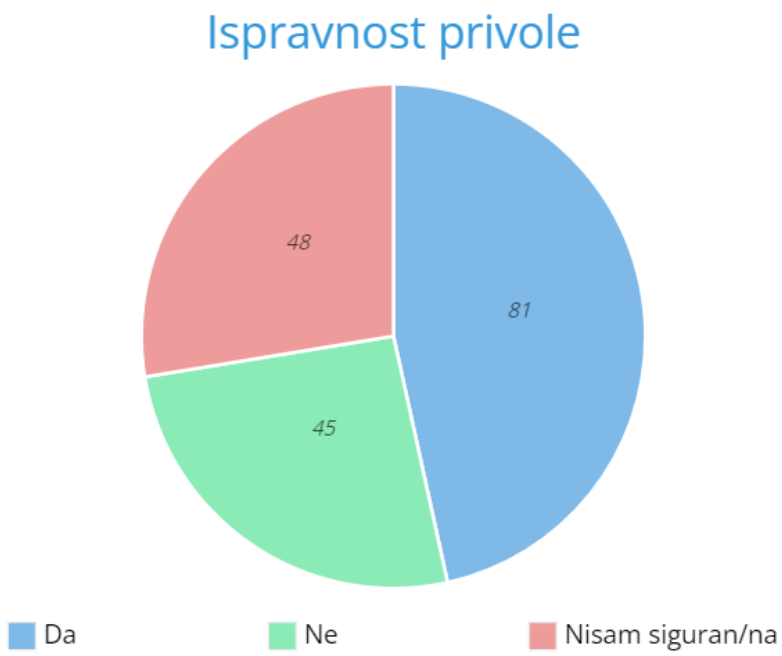
a. Significant at .05 level

Slika 4.16 Tablica korelacije između povjerenja prema stranici i zadovoljstva privolom

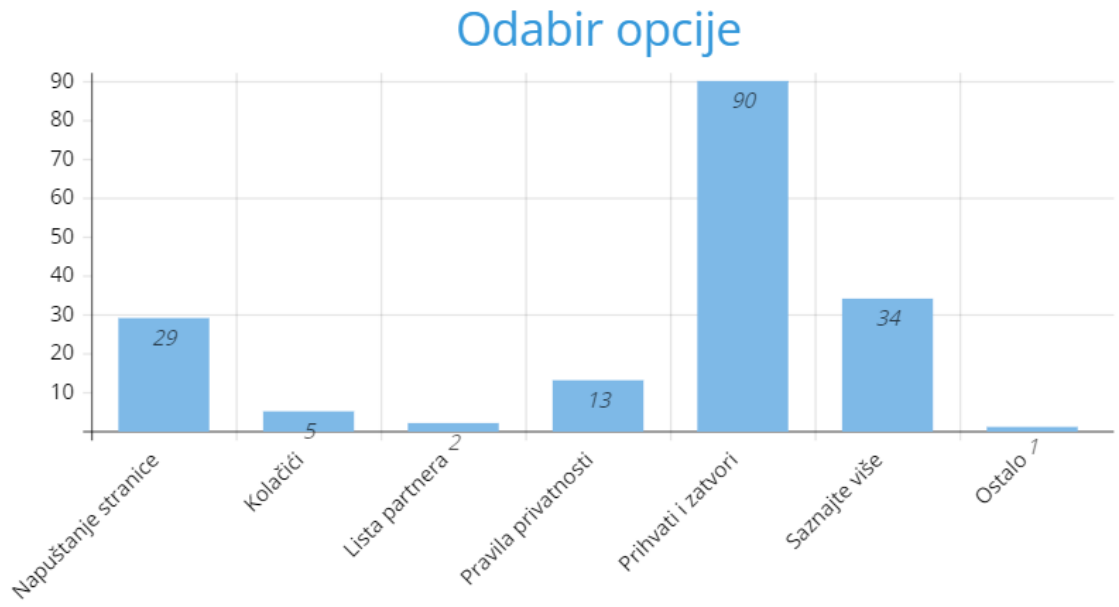
4.5.2. Privola 2: index.hr

Druga privola (slika 4.17) je preuzeta s popularne web stranice za čitanje novosti, Index. Skoro pola ispitanika, njih čak 81, smatra da je ova privola ispravna (slika 4.18). Postoji nekoliko problema kod ove privole zbog kojih ona nije ispravna: korisnik ne može jednako lako odbiti sve kolačiće kao što ih može prihvatiti, koristi se manipulativni dizajn, i unutar teksta na privoli se tvrdi kako neki partneri „ne traže [korisnikov] pristanak za obradu [korisnikovih] podataka i oslanjaju se na svoj legitimni poslovni interes“, što nije valjan razlog za ne traženje dozvole korisnika. Usprkos svemu ovome, skoro pola ispitanika, njih 81, smatra da je ova privola ispravna, njih 45 smatra da nije ispravna, a njih 48 nije sigurno. Više od pola ispitanika bi jednostavno prihvatilo sve kolačiće, a njih 29 bi zatvorilo stranicu (slika 4.19).

Slika 4.17 index.hr



Slika 4.18 Procjene ispravnosti privole index.hr



Slika 4.19 Odabir opcije na privoli index.hr

Rezultati t-testa (slika 4.20) pokazuju da povjerenje nema statistički značajnu razliku od testne vrijednosti 3 (t = -1,67, p = .096), a zadovoljstvo također nije značajno različito od 3 (t = 1,34, p = .182). Intervali pouzdanosti za obje varijable prelaze testnu vrijednost 3, što potvrđuje da nema značajne razlike između srednje vrijednosti uzorka i testne vrijednosti.

```
T-TEST /TESTVAL=3
        /VARIABLES= Povjerenje2 Zadovoljstvo2   /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Povjerenje2	174	2,87	1,04	,08
Zadovoljstvo2	174	3,11	1,13	,09

One-Sample Test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference-	95% Confidence Interval of the Difference	
					Lower	Upper
Povjerenje2	-1,67	173	,096	-,13	-,29	,02
Zadovoljstvo2	1,34	173	,182	,11	-,05	,28

Slika 4.20 Rezultati t-testa za povjerenje prema stranici i zadovoljstvo privolom

Korelacija između povjerenja i zadovoljstva (slika 4.21) iznosi r = 0,762, što je također značajno na razini p < 0,001.

```
CORRELATION
        /VARIABLES =  Povjerenje2 Zadovoljstvo2
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		ovjerenje2	dovoljstvo
Povjerenje2	Pearson Correlation	1,000	,762[a]
	Sig. (2-tailed)		,000
	N	174	174
Zadovoljstvo2	Pearson Correlation	,762[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

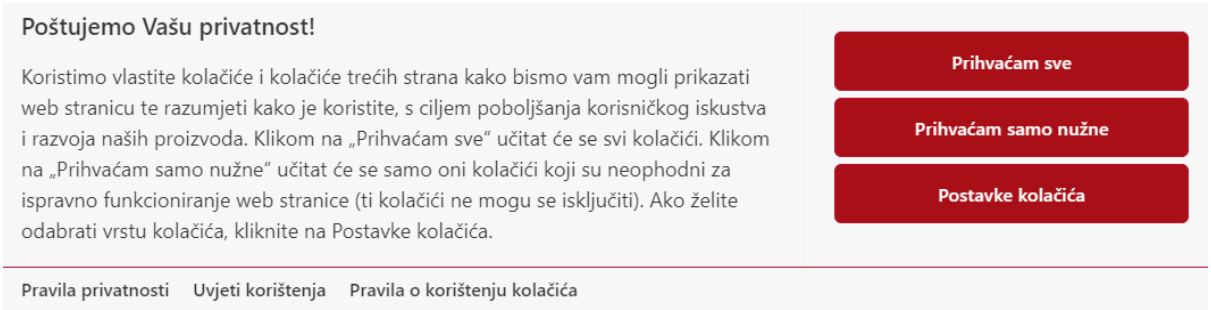
a. Significant at .05 level

Slika 4.21 Tablica korelacije između povjerenja prema stranici i zadovoljstva privolom

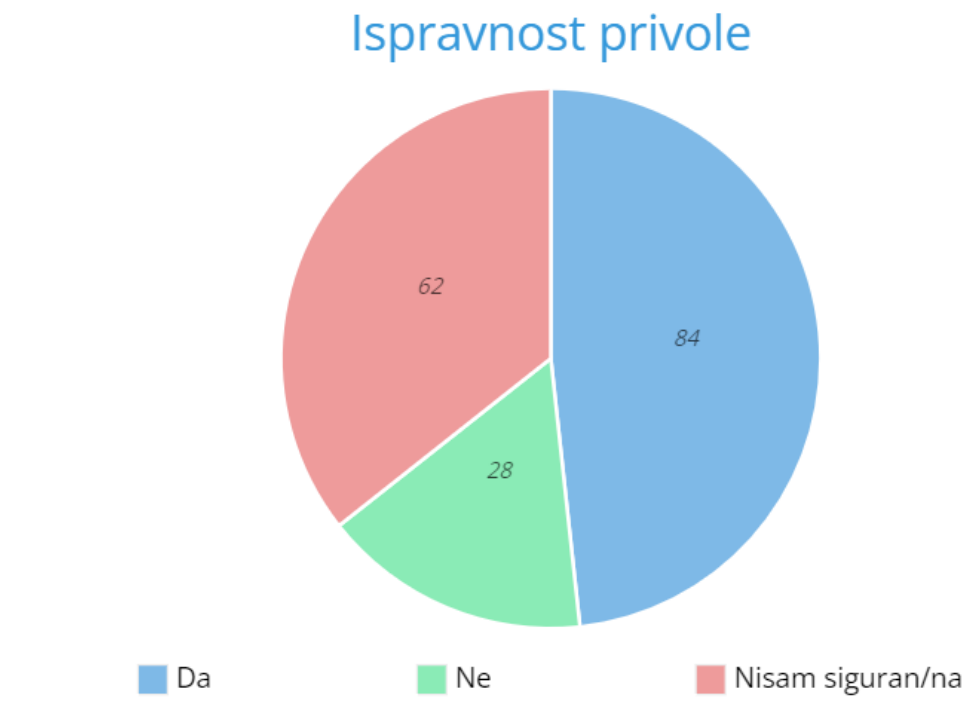
4.5.3. Privola 3: podravka.hr

Treća privola je preuzeta sa stranice Podravke (slika 4.22). U potpunosti je ispravna, što je prepoznalo 84 ispitanika, a samo 28 ih smatra da nije ispravna. Ostala 62 ispitanika nisu sigurna (slika 4.23).

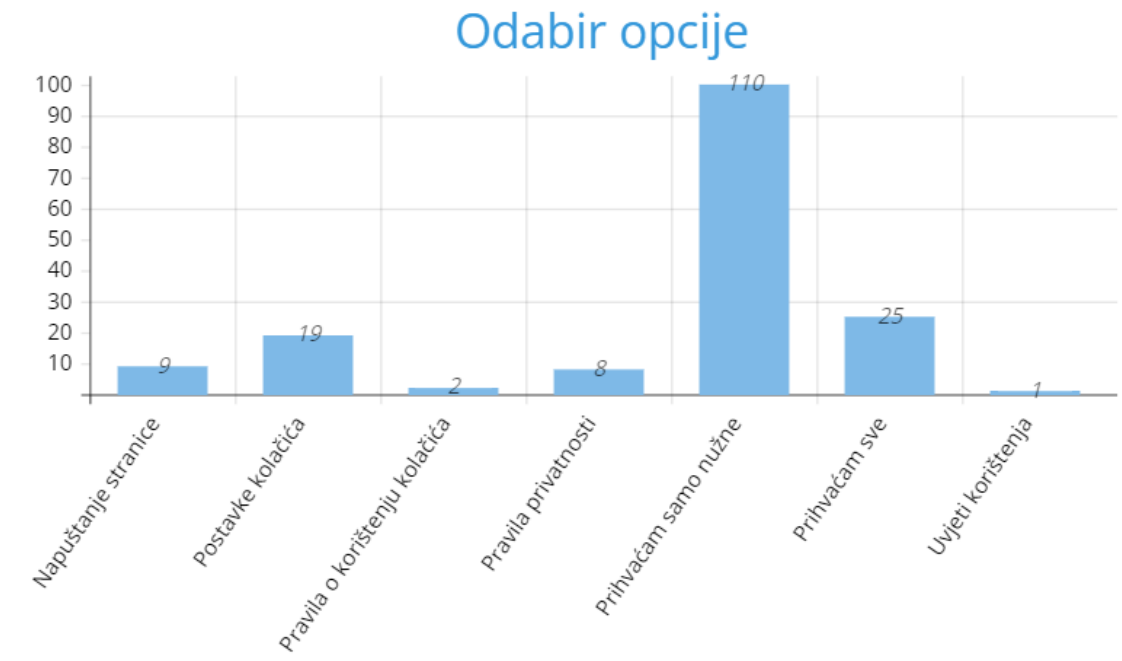
Velika većina ispitanika bi prihvatila samo nužne kolačiće, njih 110, a njih 25 bi prihvatilo sve. Samo iz ovog primjera se može vidjeti kako korisnici koriste opciju odbijanja opcionalnih kolačića ukoliko im je jednako dostupna kao i opcija za njihovo prihvaćanje (slika 4.24).



Slika 4.22 Privola sa stranice podravka.hr



Slika 4.23 Procjene ispravnosti privole podravka.hr



Slika 4.24 Odabir opcije na privoli podravka.hr

Iz rezultata t-testa za treću privolu (slika 4.25) se može vidjeti da niti jedna varijabla ne pokazuje statistički značajnu razliku od testne vrijednosti. Srednja vrijednost za povjerenje je 3,03 (t = 0,49, p = .627), dok je za zadovoljstvo 3,11 (t = 1,52, p = .130). Intervali

pouzdanosti uključuju vrijednost 3, što sugerira da su rezultati uzorka vrlo blizu testnoj vrijednosti i da nema značajnih razlika.

```
T-TEST /TESTVAL=3
        /VARIABLES= Povjerenje3 Zadovoljstvo3   /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Povjerenje3	174	3,03	,93	,07
Zadovoljstvo3	174	3,11	1,00	,08

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Povjerenje3	,49	173	,626	,03	-,10	,17
Zadovoljstvo3	1,52	173	,130	,11	-,03	,26

Slika 4.25 Rezultati t-testa za povjerenje prema stranici i zadovoljstvo privolom

Korelacija između povjerenja i zadovoljstva (slika 4.26) iznosi r = 0,788, također značajno na razini p < 0,001.

```
CORRELATION
        /VARIABLES =  Povjerenje3 Zadovoljstvo3
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		ovjerenje3	dovoljstvo
Povjerenje3	Pearson Correlation	1,000	,788[a]
	Sig. (2-tailed)		,000
	N	174	174
Zadovoljstvo3	Pearson Correlation	,788[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

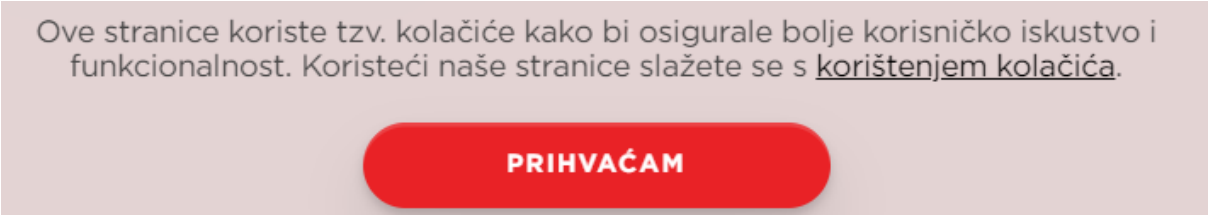
a. Significant at .05 level

Slika 4.26 Tablica korelacije između povjerenja prema stranici i zadovoljstva privolom

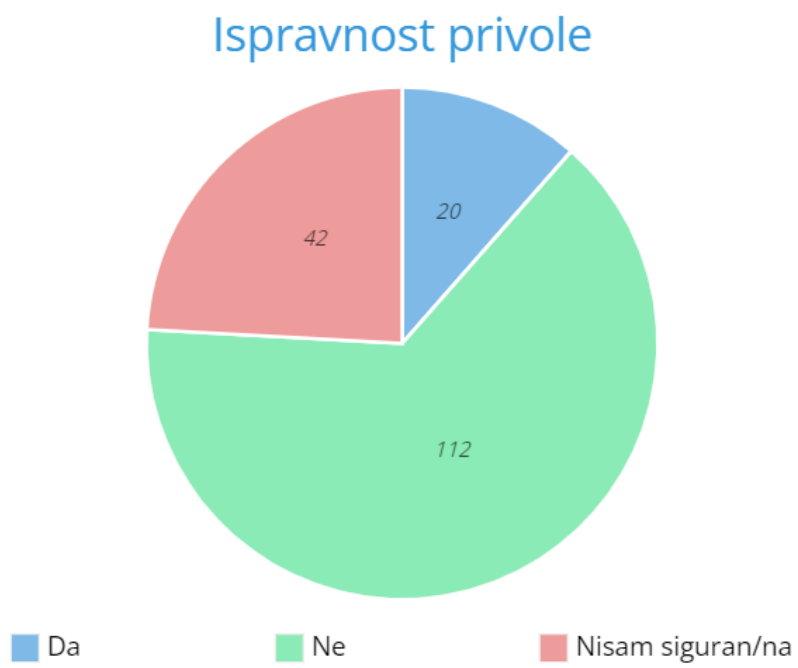
4.5.4. Privola 4: kras.hr

Četvrta privola je preuzeta sa stranice Kraša (slika 4.27). Uopće nije ispravna, što je prepoznao najveći broj ispitanika, njih 112. 42 ispitanika nisu sigurna, a njih 20 smatra da je privola ispravna (slika 4.28).

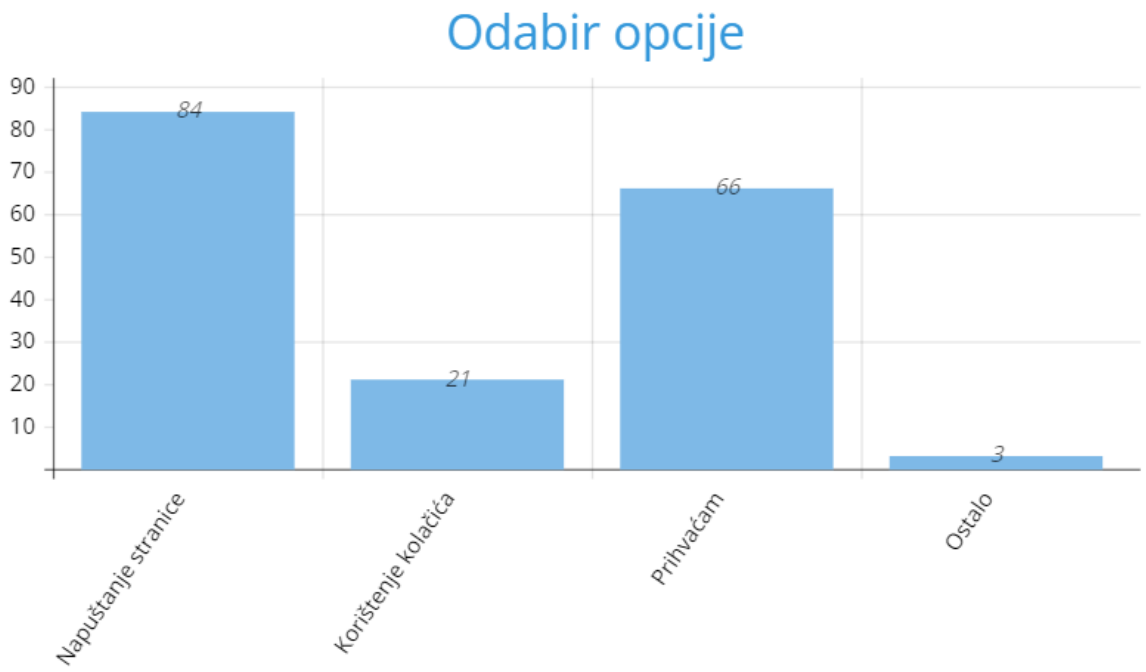
Skoro pola ispitanika (84) je izjavilo da bi pri susretu s ovom privolom napustilo stranicu, a nešto manje (66) da bi prihvatili i nastavili koristiti stranicu. 21 ispitanik bi pokušao saznati više, ili možda pronaći opciju za odbijanje kolačića, putem pružene poveznice na politiku kolačića (slika 4.29).



Slika 4.27 Privola sa stranice kras.hr



Slika 4.28 Procjene ispravnosti privole kras.hr



Slika 4.29 Odabir opcije na privoli kras.hr

Rezultati t-testa za povjerenje i zadovoljstvo ove privole (slika 4.30) pokazuju statistički značajne razlike od testne vrijednosti. Srednja vrijednost za povjerenje iznosi 2,09 ($t = -12,67$, $p < .001$), dok je srednja vrijednost za zadovoljstvo 2,03 ($t = -12,56$, $p < .001$). Obje varijable imaju negativne razlike, što ukazuje na to da su rezultati značajno niži od testne vrijednosti 3, a intervali pouzdanosti također pokazuju da vrijednost 3 nije uključena.

```
T-TEST /TESTVAL=3
        /VARIABLES= Povjerenje4 Zadovoljstvo4   /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Povjerenje4	174	2,09	,95	,07
Zadovoljstvo4	174	2,03	1,01	,08

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference-	Lower	Upper
Povjerenje4	-12,67	173	,000	-,91	-1,05	-,77
Zadovoljstvo4	-12,56	173	,000	-,97	-1,12	-,81

Slika 4.30 Rezultati t-testa za povjerenje prema stranici i zadovoljstvo privolom

Korelacija između povjerenja i zadovoljstva (slika 4.31) iznosi r = 0,769, što je također značajno na razini p < 0,001.

```
CORRELATION
        /VARIABLES =  Povjerenje4 Zadovoljstvo4
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		ovjerenje4	dovoljstvo
Povjerenje4	Pearson Correlation	1,000	,769[a]
	Sig. (2-tailed)		,000
	N	174	174
Zadovoljstvo4	Pearson Correlation	,769[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

a. Significant at .05 level

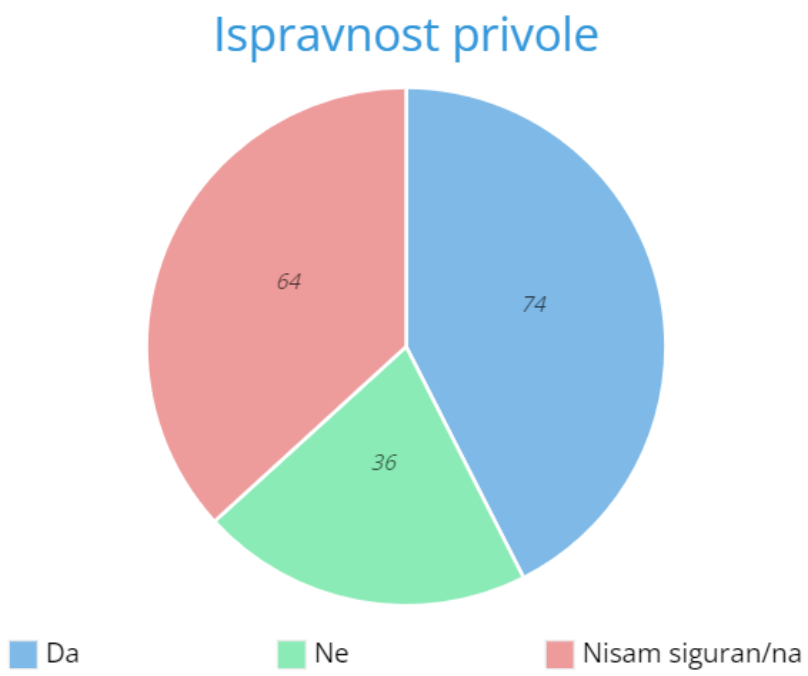
Slika 4.31 Tablica korelacije između povjerenja prema stranici i zadovoljstva privolom

4.5.5. Privola 5: hep.hr (modificirana)

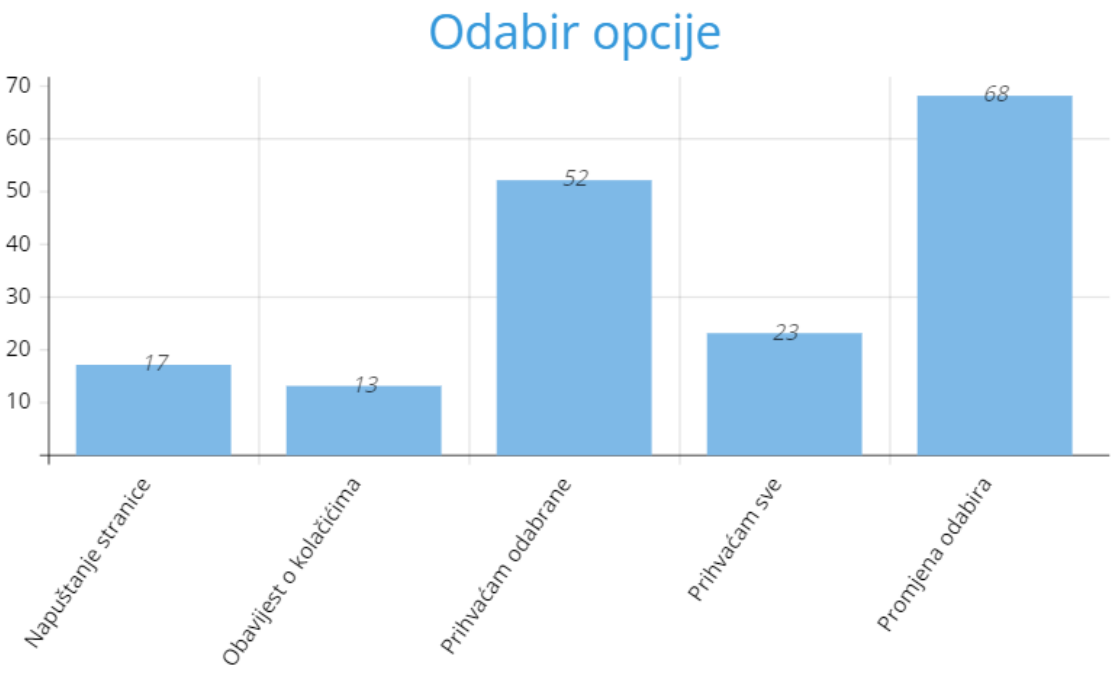
Privola na slici 4.32 je preuzeta sa stranice hep.hr te je modificirana na način da su funkcionalni, statistički i marketinški kolačići odabrani i predočeni ispitanicima kao *default* opcija kako bi se vidjelo prihvaćaju li odabire kolačića onako kako ih web stranice postave ili izdvoje par sekundi za promjenu odabira. Najviše ispitanika, njih 68, bi upravo to i napravilo (slika 4.34). U ovom slučaju, opcije „Prihvaćam sve“ i „Prihvaćam odabrane“ zapravo imaju jednak učinak, ali se dvostruko više ispitanika odlučilo za opciju „Prihvaćam odabrane“ (52) u odnosu na „Prihvaćam sve“ (23).

Što se tiče ispravnosti privole, originalna privola, onakva kakva je na stranici s koje je preuzeta, je u potpunosti ispravna, ali modificirana verzija koja je predočena ispitanicima nije, upravo zbog automatski odabranih kolačića, što znači da njihovo odbijanje nije jednako lagano kao i njihovo prihvaćanje. Slika 4.33 pokazuje da 74 ispitanika smatraju predočenu privolu ispravnom, 64 nisu sigurni a 36 je smatra neispravnom.

Slika 4.32 Modificirana privola sa stranice hep.hr



Slika 4.33 Procjene ispravnosti privole hep.hr



Slika 4.34 Odabir opcije na privoli hep.hr

Rezultati pokazuju da su i povjerenje i zadovoljstvo statistički značajno niži od testne vrijednosti 3. Srednja vrijednost za povjerenje iznosi 2,82 (t = -2,60, p = .010), dok je za zadovoljstvo 2,76 (t = -3,42, p = .002).

```
T-TEST /TESTVAL=3
        /VARIABLES= Povjerenje5 Zadovoljstvo5   /MISSING=ANALYSIS
        /CRITERIA=CI(0.95).
```

One-Sample Statistics

	N	Mean	Std. Deviation-	S.E. Mean
Povjerenje5	174	2,82	,93	,07
Zadovoljstvo5	174	2,76	1,01	,08

One-Sample Test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference-	95% Confidence Interval of the Difference	
					Lower	Upper
Povjerenje5	-2,60	173	,010	-,18	-,32	-,04
Zadovoljstvo5	-3,14	173	,002	-,24	-,39	-,09

Slika 4.35 Rezultati t-testa za povjerenje prema stranici i zadovoljstvo privolom

Korelacija između povjerenja i zadovoljstva (slika 4.36) iznosi r = 0,852, što je također značajno na razini p < 0,001.

```
CORRELATION
        /VARIABLES =  Povjerenje5 Zadovoljstvo5
        /PRINT = TWOTAIL NOSIG.
```

Correlations

		ovjerenje5	dovoljstvo
Povjerenje5	Pearson Correlation	1,000	,852[a]
	Sig. (2-tailed)		,000
	N	174	174
Zadovoljstvo5	Pearson Correlation	,852[a]	1,000
	Sig. (2-tailed)	,000	
	N	174	174

a. Significant at .05 level

Slika 4.36 Tablica korelacije između povjerenja prema stranici i zadovoljstva privolom

4.5.6. Sažetak

U ovom posljednjem dijelu ankete gledani su stavovi ispitanika prema pet različitih vrsta privola, ovisno o informacijama i opcijama koje nude korisnicima. Ocijenjivale su se prema ispravnosti, povjerenju i zadovoljstvu korisnika te se gledalo koje bi opcije korisnici odabrali pri susretu s njima. Treba naglasiti da se ovakvi iskazi često znaju razlikovati od stvarnog ponašanja, ovisno o situaciji i kontekstu pod kojim se korisnici susreću s određenim privolama.

Privola sa stranice Podravka, koja je potpuno ispravna, je imala najbolje ocjene u smislu ispravnosti, povjerenja i zadovoljstva, dok je privola sa stranice Kraš, potpuno neispravna, bila najlošija, s najvećim brojem ispitanika koji bi napustili stranicu. Manipulativni dizajn je kod privola sa stranica Ultragros i Index uzrokovao podijeljene ocjene korisnika, dok je modificirana privola sa stranice HEP pokazala kako automatski odabrane opcije smanjuju povjerenje i zadovoljstvo korisnika.

Privola sa stranice Ultragros je podijelila ispitanike - 52 ispitanika smatralo je privolu ispravnom, 55 ih je smatralo neispravnom, a 67 nije bilo sigurno. Problem je bio zavaravajući dizajn, jer je opcija „Prihvati sve“ bila istaknuta crvenom bojom, dok su ostale opcije bile manje uočljive. Ipak, većina korisnika (71) odlučila bi odbiti sve kolačiće. Statistički testovi pokazali su značajno niže povjerenje (2,64) i zadovoljstvo (2,66) od očekivanih testnih vrijednosti.

Privola sa stranice Podravka je bila jedina potpuno ispravna privola u anketi, i također najispravnija prema ocjenama ispitanika, gdje ju je 84 ispitanika prepoznalo kao ispravnu. Većina korisnika (110) odlučila bi prihvatiti samo nužne kolačiće. Statistička analiza nije pokazala značajne razlike u povjerenju (3,03) i zadovoljstvu (3,11) u odnosu na testnu vrijednost, što ukazuje na neutralne ocjene povjerenja i zadovoljstva.

Glavna razlika ove dvije privole je u dizajnu (Ultragros koristi manipulativni dizajn, za razliku od Podravke), ali upravo ta razlika je rezultirala u dvostruko više prihvaćanja svih kolačića na stranici Ultragros (52) u odnosu na stranicu Podravka (25).

Privola sa stranice Index nije ispravna, ali je ispravnom smatra gotovo pola ispitanika (81). S obzirom na količinu informacija na privoli, korisnici su svoje zadovoljstvo ocijenili jednako kao i za privolu sa stranice Podravka (3,11). To su ujedno i najveće ocjene zadovoljstva od svih pet prikazanih privola.

Privola sa stranice Kraš je zapravo samo traka obavijesti o kolačićima. Većina ispitanika je ocijenila kao neispravnu (112), što i je slučaj. Veći dio bi odlučio napustiti stranicu (84), što ukazuje na vrlo negativnu percepciju, koju potvrđuju i statistički značajno niže vrijednosti povjerenja (2,09) i zadovoljstva (2,03). Ovako negativni stavovi su bili očekivani, s obzirom da privola ne nudi mnogo informacija niti daje mogućnost odabira, tj. upravljanja kolačićima korisnicima, već ih samo upozorava da stranica koristi te tehnologije.

Modificirana privola sa stranice HEP je imala unaprijed odabrane opcije kolačića, što je navelo većinu korisnika (68) da promijeni ove zadane postavke. Unatoč tome, korisnici su ocijenili ovu, inače ispravnu privolu nižim povjerenjem (2,82) i zadovoljstvom (2,76), a oba rezultata su bila statistički značajno niža od očekivanih vrijednosti.

5. Rasprava

Istraživanje korisničkih percepcija i razumijevanja web kolačića pružilo je uvid u ključne aspekte povezane s privatnosti, sigurnosti i transparentnosti. Dobiveni rezultati jasno pokazuju kako korisnici imaju umjereno razumijevanje web kolačića, što je u skladu s nalazima iz literature.

Istraživanje Jayakumara (2021) ukazuje na to da su korisnici interneta općenito svjesni postojanja kolačića, ali su skloniji prihvaćanju kolačića zbog praktičnosti, unatoč niskoj razini razumijevanja njihovih funkcija i utjecaja na privatnost. Ova sklonost korisnika prema praktičnosti vidljiva je i u rezultatima ovog istraživanja, gdje je većina ispitanika ocijenila svoje razumijevanje kolačića kao srednje, a mnogi su u dijelu o provolama preferirali opcije koje ne zahtijevaju dublje razmišljanje ili istraživanje o funkcionalnosti kolačića, to jest jednostavno prihvaćanje ili odbijanje kolačića jednim klikom.

Rezultati koji ukazuju na to da korisnici nisu previše zabrinuti zbog privatnosti, unatoč svijesti o kolačićima, također su u skladu s nalazima istraživanja Kulyka i suradnika (2018). Njihovo istraživanje pokazalo je da su obavijesti o kolačićima često iritantne i da nisu informativne, zbog čega korisnici ne obraćaju pažnju na njihov stvarni sadržaj. Ovo je istraživanje također pokazalo da korisnici imaju umjereno razumijevanje i zabrinutost, ali i da mnogi sudionici, iako izražavaju brigu oko privatnosti, nisu spremni posvetiti više pažnje detaljnim informacijama o kolačićima.

Schiefermair i Stabauer (2020) su u svom istraživanju utvrdili da obavijesti o kolačićima mogu utjecati na povjerenje korisnika, ali da su korisnici skloniji prihvatiti kolačiće kada im se obavijesti prikazuju u obliku *pop-up* prozora. Ova je tvrdnja potvrđena dobivenim rezultatima, gdje su ispitanici pokazali veću sklonost prema jednostavnim, jasno prikazanim informacijama o kolačićima. Preferencije ispitanika prema transparentnim i jednostavnim obavijestima, kao i njihova želja za većom kontrolom nad kolačićima, pokazale su značajnu povezanost, što dodatno potvrđuje nalaze Schiefermaira i Stabauera. Iako je transparentnost važna, manipulativni dizajni poput onih s privolom na stranici Ultragros, gdje se opcija "Prihvati sve" posebno ističe, smanjuju povjerenje korisnika, što je također potvrđeno u literaturi.

Božić i Jakšić (2020) su naglasile važnost digitalne pismenosti i svijesti o privatnosti među korisnicima interneta u Hrvatskoj. U ovom se istraživanju pokazao sličan trend, pri čemu su ispitanici pokazali interes za dodatno informiranje o kolačićima, ali samo ako su informacije lako dostupne. Većina ispitanika pokazala je određenu razinu spremnosti za edukaciju, što dodatno podupire tvrdnju da postoji potreba za poboljšanjem digitalne pismenosti i edukacije korisnika kako bi mogli donositi informiranije odluke o privatnosti i sigurnosnim mjerama prilikom korištenja web stranica.

Istraživanje ovog diplomskog rada o preferencijama korisnika prema privolama za kolačiće također je u skladu s literaturom. Studija Kulyka i suradnika (2018) pokazuje da korisnici obavijesti o kolačićima doživljavaju kao smetnju, a rezultati ovog istraživanja potvrđuju tu tvrdnju, osobito kada su privole bile složene ili koristile manipulativni dizajn. Istovremeno, kada su ispitanicima bile ponuđene ispravne privole poput one sa stranice Podravke, oni su bili skloniji birati opcije koje im omogućuju veću kontrolu, što sugerira da su jednostavniji dizajni privola učinkovitiji u povećanju povjerenja i transparentnosti.

Dobiveni rezultati potvrđuju nalaze iz literature i otkrivaju jasne obrasce ponašanja korisnika u vezi s razumijevanjem i percepcijom web kolačića. Iako korisnici preferiraju praktičnost jednostavnog prihvaćanja kolačića, nisu zadovoljni trenutnom transparentnosti vezanoj za njihovu upotrebu niti imaju puno povjerenja u web stranice koje ih koriste. Prepoznaju važnost razumijevanja i kontrole nad kolačićima, ali im nedostaju jasne i pristupačne informacije kako bi mogli donijeti informirane odluke.

Ovo istraživanje ima nekoliko važnih ograničenja koja uključuju prvenstveno činjenicu da je korišten prigodni uzorak, što znači da rezultati nisu nužno reprezentativni za širu populaciju. Ispitanici su odabrani prema dostupnosti, što može utjecati na generalizaciju rezultata. Nadalje, istraživanje se oslanja na samoprocjenu ispitanika, što može dovesti do problema pristranosti ili nepreciznosti u odgovorima, tj. do precijenjivanja ili podcijenjivanja vlastitih znanja, sposobnosti i stavova, posebice kada je riječ o tehničkim temama kao što su kolačići i njihove funkcionalnosti. Također, istraživanje se fokusiralo na opću percepciju kolačića bez detaljne analize svih oblika kolačića, uključujući one koji se koriste u specifičnim kontekstima kao što su aplikacije ili društvene mreže. Nedostatak takve detaljne analize mogao je ograničiti razumijevanje preciznijih stavova korisnika o različitim funkcijama kolačića. Buduća istraživanja trebala bi uključivati reprezentativniji uzorak, kvalitativne metode te detaljniju analizu specifičnih vrsta kolačića i sigurnosne rizike koje

donose, kao i na izradu edukacijskih alata koji će korisnicima omogućiti bolje razumijevanje i upravljanje svojim digitalnim tragom.

Zaključak

Ovaj rad o percepciji privatnosti i sigurnosti web kolačića među korisnicima interneta naglasio je nekoliko ključnih problema koji zahtijevaju daljnju pažnju i poboljšanja. Kroz analizu rezultata, pokazalo se da većina ispitanika ima umjereno razumijevanje funkcionalnosti web kolačića, ali im nedostaje detaljno znanje o njihovim sigurnosnim aspektima i potencijalnim rizicima. Većina ispitanika prepoznala je važnost transparentnosti prilikom korištenja kolačića, ali su također istaknuli da trenutne obavijesti o kolačićima često nisu jasne ili informativne, što dovodi do niskog povjerenja u web stranice i njihove prakse prikupljanja podataka.

Jedan od ključnih zaključaka istraživanja je da, unatoč relativno visokoj svijesti o kolačićima i njihovoj svrsi, ispitanici nisu izrazito zabrinuti zbog potencijalnih sigurnosnih prijetnji. Ovo može biti posljedica nedovoljnog razumijevanja složenih sigurnosnih implikacija koje web kolačići mogu imati, ili pak zbog prekomjerne izloženosti kolačićima koja umanjuje osjećaj ugroženosti. Ipak, rezultati sugeriraju da postoji značajan interes za dodatnu edukaciju o kolačićima, posebno ako bi informacije bile lako dostupne i prezentirane na razumljiv način.

Unatoč općem trendu prihvaćanja kolačića iz praktičnih razloga, postoji jasna potreba za poboljšanjem transparentnosti vezane uz njihovu upotrebu i boljom edukacijom korisnika, što bi moglo poboljšati njihovo razumijevanje i povjerenje u web stranice. Korisnici prepoznaju važnost razumijevanja i kontrole nad kolačićima, no trenutno im nedostaju jasne i pristupačne informacije. Nadalje, iako su privole za kolačiće danas uobičajena praksa, njihova učinkovitost u pružanju stvarnog informiranog pristanka ostaje upitna. Uz širenje digitalne pismenosti i bolju regulaciju, web stranice bi trebale usmjeriti pažnju na dizajn koji potiče informirano donošenje odluka, a ne samo ispunjavanje formalnih zakonskih obveza.

Iako je ovo istraživanje imalo nekoliko važnih ograničenja, dobiveni rezultati pružaju korisne uvide u korisničke percepcije i ponašanja vezane uz kolačiće te ukazuju na potrebu za većom transparentnošću i edukacijom. Buduća istraživanja trebala bi obuhvatiti šire i reprezentativnije uzorke, kao i detaljnije ispitati specifične sigurnosne prijetnje koje kolačići predstavljaju, kako bi se mogli razviti bolji alati i strategije za zaštitu privatnosti korisnika na internetu.

Literatura

[1] Sipior, J., Ward, B., & Mendoza, R. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. Journal of Internet Commerce 10, pp. 1-16. doi:10.1080/15332861.2011.558454

[2] Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics. ACM Transactions on Internet Technology, 1(2), 151–198

[3] Sandhu, R., Park, J. (2000) Secure Cookies on the Web. IEEE Internet Computing, 36-44. doi:10.1109/4236.865085. Preuzeto s: https://www.researchgate.net/publication/3419358_Secure_cookies_on_the_Web

[4] Felten, E. W., Schneider, M. A. (2000). Timing Attacks on Web Privacy. Secure Internet Programming Laboratory, Department of Computer Science, Princeton University. Preuzeto s: https://dl.acm.org/doi/pdf/10.1145/352600.352606

[5] Schwartz, J. (2001). Giving Web a Memory Cost Its Users Privacy, The New York Times. Preuzeto s: https://www.nytimes.com/2001/09/04/business/giving-web-amemory-cost-its-users-privacy.html

[6] Fiebrandt, S. (2018). What are cookies? What are the differences between them (session vs. persistent)?. Cisco. Preuzeto s: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html

[7] Mozilla (n.d.). HTTP cookies. Mozilla Developer Network. Preuzeto s: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

[8] Montulli, L. (1998). Persistent client state in a hypertext transfer protocol based client-server system. US5774670. Preuzeto s: https://worldwide.espacenet.com/publicationDetails/originalDocument?CC=US&NR=5774670A&KC=A&FT=D&ND=&date=19980630&DB=&locale=en_EP

[9] Hardmeier, S. (2005). The history of Internet Explorer. Dostupno na: https://test94133.tripod.com/IEHistory.htm

[10] Kukułka M. (2021). What's Happening with Browser Cookies? Advertising Industry in the Face of Third-Party Cookie Phase-Outs. NewProgrammatic Blog.

Preuzeto s: https://newprogrammatic.com/blog/third-party-cookies-in-programmaticadvertising-news

[11] Jackson, T., (1996), This Bug in Your PC Is a Smart Cookie, The Financial Times. Preuzeto s: https://archive.org/details/FinancialTimes1996UKEnglish/Feb%2012%201996%2C%2Financial%20Times%2C%20%2312%2C%20UK%20%28en%29/page/n29/mode/2up

[12] Chen, L., S. Englehardt, S., West, M., Wilander, J. (2022). Cookies: HTTP State Management Mechanism. Internet Engineering Task Force. Preuzeto s: https://www.ietf.org/archive/id/draft-ietf-httpbis-rfc6265bis-10.html (L. Chen,

[13] Kristol, D., Montulli, L. (2000). HTTP State Management Mechanism (RFC 2965). Internet Engineering Task Force. Preuzeto s: https://www.rfc-editor.org/rfc/rfc2965

[14] Barth, A. (2011). HTTP State Management Mechanism (RFC 6265). Internet Engineering Task Force. Preuzeto s: https://www.rfc-editor.org/rfc/rfc6265.txt

[15] Bingler, S., West, M., Wilander, J. (2024). Cookies: HTTP State Management Mechanism (RFC 6265bis). Internet Engineering Task Force. Preuzeto s: https://www.ietf.org/archive/id/draft-ietf-httpbis-rfc6265bis-15.txt

[16] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama). Preuzeto s: https://eurlex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[17] Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama, Direktiva 2002/58/EZ o privatnosti i elektroničkim komunikacijama i Uredbe (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača. Preuzeto s: https://eur-lex.europa.eu/legal-content/hr/TXT/?uri=CELEX%3A32009L0136

[18] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Preuzeto s: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1724494732416

[19] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (2018). Preuzeto s: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[20] Ratcliffe, C. (2019). Firefox follows Apple in blocking third-party cookies online. Adage. Preuzeto s: https://adage.com/article/news/firefox-follows-apple-blocking-third-party-cookies-online/2175306

[21] Wilander, J. (2020) Full Third-Party Cookie Blocking and More. WebKit. Preuzeto s: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more

[22] Huang, T., Hofmann J., Edelstein, A. (2021.), Firefox 86 Introduces Total Cookie Protection, Mozilla Security Blog. Preuzeto s: https://blog.mozilla.org/security/2021/02/23/total-cookie-protection

[23] Goel, V. (2022). Get to know the new Topics API for Privacy Sandbox. Google. Preuzeto s: https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/

[24] Schuh, J. (2019). Building a more private web. Google. Preuzeto s: https://blog.google/products/chrome/building-a-more-private-web/

[25] Schuh, J. (2020). https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[26] Sweeney, M., Zawiślak, P. (2024). The Demise of Third-Party Cookies in AdTech: Why Are They Being Phased Out?. Clearcode. Preuzeto s: https://clearcode.cc/blog/third-party-cookies-demise/#toc-label-4

[27] Goel, V. (2021). An updated timeline for Privacy Sandbox milestones. Google. Preuzeto s: https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/

[28] Chavez, A. (2022). Expanding testing for the Privacy Sandbox for the Web. Google. Preuzeto s: https://blog.google/products/chrome/update-testing-privacy-sandbox-web/

[29] Sweeney, M., Zawadziński, M. (2023). Google Chrome To Kill Off Third-Party Cookies: What It Means for AdTech. Clearcode. Preuzeto s: https://clearcode.cc/blog/chrome-impact-adtech/#toc-label-4

[30] Chavez, A. (2024). A new path for Privacy Sandbox on the web. Google. Preuzeto s: https://privacysandbox.com/news/privacy-sandbox-update/

[31] Opća uredba o zaštiti podataka. (2016). Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. *Službeni list Europske unije, L119*, 1-88. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679

[32] Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/2018. (2018). *Narodne novine*. https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

[33] AZOP-1. Agencija za zaštitu osobnih podataka, n.d. AZOP. Preuzeto s: https://azop.hr/djelokrug/

[34] Koch, R. (n.d.). Cookies, the GDPR, and the ePrivacy Directive. GDPR.eu. Preuzeto s: https://gdpr.eu/cookies/

[35] Gourley, D., Totty, B., Sayer, M., Reddy, S., Aggarwal, A. (2002). HTTP: The Definitive Guide. O'Reilly Media, Inc., 246-251.

[36] EITCA akademija (2023). Koje su različite vrste XSS napada i po čemu se međusobno razlikuju?. EITCA akademija. Preuzeto s: https://hr.eitca.org/Cybersecurity/eitc-je-osnove-sigurnosti-web-aplikacija-wasf/skriptiranje-s-vi%C5%A1e-mjesta/skriptiranje-vi%C5%A1e-stranica-xss/ispit-pregled-cross-site-scripting-xss/koje-su-razli%C4%8Dite-vrste-xss-napada-i-kako-se-me%C4%91usobno-razlikuju/

[37] AZOP-2. Agencija za zaštitu osobnih podataka, 6. Kolovoz 2024. AZOP. Preuzeto s: https://azop.hr/obrada-osobnih-podataka-kolacici/

[38] Wranka, M., 2019. Znate li što su 'supercookies' i kako ih ukloniti?. Preuzeto s: https://www.tportal.hr/tehno/clanak/znate-li-sto-su-supercookies-i-kako-ih-ukloniti-20190829

[39] Price, D., 2018. 7 Types of Browser Cookies You Need to Know About. MakeUseOf. Preuzeto s: https://www.makeuseof.com/tag/types-browser-cookies-to-know-about/

[40] Phillips, G., 2019. What Are Supercookies? Here's How to Remove Them Properly. MakeUseOf. Preuzeto s: https://www.makeuseof.com/tag/what-are-supercookies-and-why-are-they-dangerous/

[41] Information Commissioner's Office, (n.d.). What is the 'legitimate interests' basis? ICO. Preuzeto s: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/

[42] Ostendo Group, (2019). *Legitimni interes*. Preuzeto s: https://ostendogroup.com/hr/wp-content/uploads/2019/10/Legitimni-interes.pdf

[43] Jayakumar, L.N. (2021). Cookies "n" Consent: an Empirical Study on the Factors Influencing Website Users' Attitudes towards Cookie Consent in the EU. Preuzeto s: https://www.researchgate.net/publication/360866641_Cookies_'n'_Consent_An_empirical_study_on_the_factors_influencing_of_website_users'_attitude_towards_cookie_consent_in_the_EU

[44] Kulyk, O., Hilt, A., Gerber, N., Volkamer, M. (2018). "ThisWebsiteUses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. European Workshop on Usable Security (EuroUSEC). Preuzeto s: https://www.researchgate.net/publication/326108192_This_Website_Uses_Cookies_Users'_Perceptions_and_Reactions_to_the_Cookie_Disclaimer

[45] Schiefermair, J., Stabauer, M. (2020). The Effects of Cookie Notices on Percieved Privacy and Trust in E-Commerce. HCI in Business, Government and Organisations. Preuzeto s: https://www.researchgate.net/publication/342828515_The_Effects_of_Cookie_Notices_on_Perceived_Privacy_and_Trust_in_E-Commerce

[46] Božić, S. i Jakšić, D. (2020). Users' Perception of Online Privacy and Security in Croatia – A Survey. Communication Management Review, 05 (02), 6-29. https://doi.org/10.22522/cmr20200258

1. Prilog: Anketa o kolačićima

Osnovne informacije o korisnicima

1. Koliko imate godina? (<18, 18-29, 30-49, 50<)
2. Koji je Vaš spol? (M, Ž)
3. Koja je Vaša razina obrazovanja? (Osnovna škola, Srednja škola, Preddiplomski studij, Diplomski studij, Poslijediplomski specijalistički studij, Doktorski studij)
4. Koliko često koristite internet? (Više sati dnevno, 1-2 sata dnevno, Par puta tjedno, Nekoliko puta mjesečno, Nikad ili skoro nikad)

H1: Nedostatak razumijevanja

5. Jeste li čuli za pojam "web kolačići" prije ove ankete? (Da/Ne)
6. Kako biste ocijenili svoje razumijevanje web kolačića? (1 - Uopće ih ne razumijem, 5 - Potpuno ih razumijem)
7. Koliko Vam je važno razumjeti što su web kolačići? (1 – Nimalo, 5 – Jako važno)
8. Znate li zašto web stranice koriste kolačiće? (Da, Ne, Znam otprilike, Nisam siguran/na)
9. Znate li da preglednici (npr. Microsoft Edge, Google Chrome) pružaju korisnicima opcije upravljanja kolačićima? (Da/Ne)
10. Kako biste ocijenili svoju sposobnost korištenja tih opcija upravljanja kolačićima u pregledniku? (1 - Vrlo loša, 5 - Vrlo dobra)

H2: Visok nivo zabrinutosti za privatnost

11. Koliko ste zabrinuti zbog privatnosti svojih podataka na internetu? (1 - Uopće nisam zabrinut/a, 5 – Vrlo sam zabrinut/a)
12. Koliko ste zabrinuti zbog praćenja vaših online aktivnosti? (1 - Uopće nisam zabrinut/a, 5 - Vrlo sam zabrinut/a)
13. U kolikoj mjeri smatrate da kolačići ugrožavaju vašu privatnost? (1 – Nimalo, 5 - Potpuno)

14. Koliko često brišete kolačiće iz svog preglednika? (Dnevno, Tjedno, Mjesečno, Nikad)
15. Koliko često koristite anonimni način pregledavanja kako biste izbjegli praćenje kolačićima? (Uvijek, Često, Ponekad, Rijetko, Nikad)
16. Znate li da postoje sigurnosni rizici povezani s kolačićima, poput krađe identiteta ili praćenja? (Da/Ne)
17. Koristite li dodatne sigurnosne mjere za zaštitu svojih podataka na internetu (npr. VPN ili 2FA)? (Da/Ne)

H3: Preferiranje transparentnosti i kontrole

18. Koliko Vam je važno da vas web stranice jasno i iskreno informiraju o upotrebi kolačića? (1 - Uopće nije važno, 5 - Vrlo važno)
19. Koliko često čitate uvjete korištenja i politike privatnosti na web stranicama prije prihvaćanja kolačića? (Uvijek, Često, Ponekad, Rijetko, Nikad)
20. Smatrate li da su obavijesti o kolačićima na web stranicama jasne i informativne? (1 - Uopće nisu jasne, 5 - Vrlo jasne)
21. Koliko Vam je važno da imate kontrolu nad kolačićima koje prihvaćate? (1 - Uopće nije važno, 5 - Vrlo važno)
22. Jeste li ikada prilagođavali postavke kolačića u svom pregledniku? (Da/Ne)
23. Jeste li ikada koristili opciju "Do Not Track" u svom pregledniku? (Da/Ne)
24. Koristite li proširenja (ekstenzije), dodatke (add-ons) za preglednike ili aplikacije koje upravljaju kolačićima? (Da/Ne)

H4: Otvorenost prema edukaciji

25. Jeste li ikada tražili informacije o kolačićima na internetu? (Da/Ne)
26. Jeste li spremni posvetiti vrijeme edukaciji o kolačićima ako vam se pruže jasne informacije? (Da, svakako, Možda, ovisi o dostupnosti informacija, Ne, nemam vremena, Ne, nije me briga za kolačiće)
27. Koje vrste edukativnih materijala biste preferirali (video, tekst, infografike)? (Video, Tekstualni članci, Infografike, Kombinacija svih navedenih, Drugo)

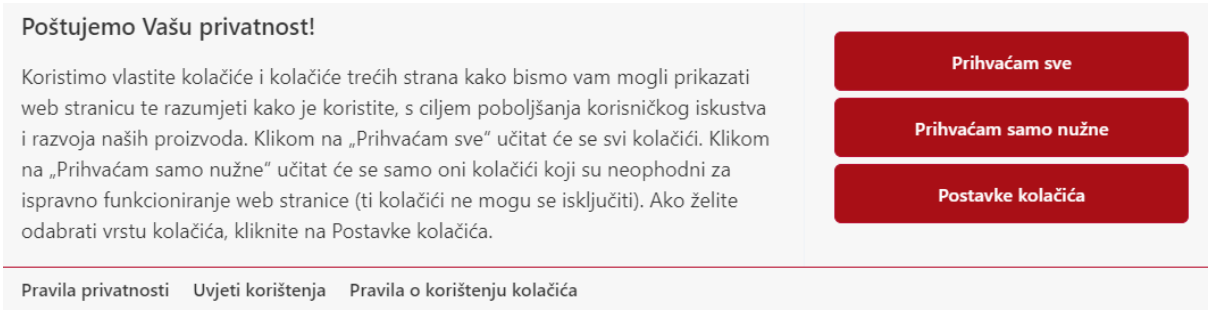
28. Smatrate li da bolje razumijevanje kolačića može poboljšati Vašu sigurnost na internetu? (Da, značajno, Da, donekle, Ne, ne vidim kako, Nisam siguran/na)
29. Smatrate li da bi škole i obrazovne institucije trebale uključiti osnovne informacije o web kolačićima u svoje kurikulume? (Da/Ne)
30. Jeste li znali da postoje zakonske regulative o kolačićima kao što su GDPR i ePrivacy uredba? (Da, potpuno sam upoznat/a s njima, Da, čuo/la sam za njih, Ne, nisam znao/la da postoje, Nisam siguran/na što to znači)

Ocijenjivanje privola za kolačiće

31. Smatrate li ovu obavijest o kolačićima ispravnom? (Da, Ne, Nisam siguran/na)

32. Koju biste opciju prvu odabrali da Vam se ovakva obavijest prikaže na web stranici koju posjećujete prvi put? (Prilagodite, Odbiti, Prihvati sve, Napuštanje stranice, Ostalo)
33. Razina povjerenja prema stranici isključivo na temelju prikazane obavijesti? (1 - iznimno niska, 5 - izrazito visoka)
34. Razina zadovoljstva količinom pruženih informacija na obavijesti? (1 - iznimno niska, 5 - izrazito visoka)
35. Smatrate li ovu obavijest o kolačićima ispravnom? (Da, Ne, Nisam siguran/na)

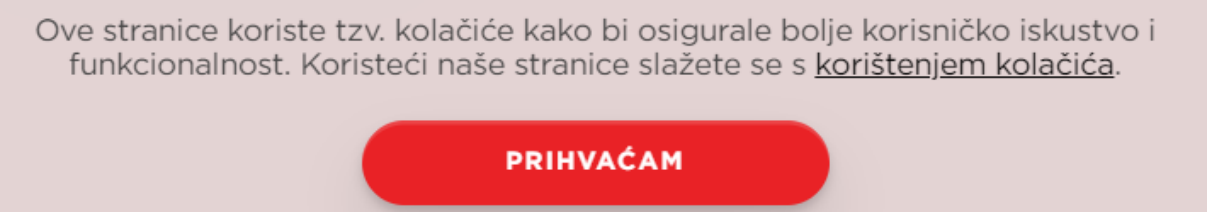
36. Koju biste opciju prvu odabrali da Vam se ovakva obavijest prikaže na web stranici koju posjećujete prvi put? (Pravila privatnosti, Kolačići, Saznajte više, Prihvati i zatvori, Lista partnera, Napuštanje stranice, Ostalo)
37. Razina povjerenja prema stranici isključivo na temelju prikazane obavijesti? (1 - iznimno niska, 5 - izrazito visoka)
38. Razina zadovoljstva količinom pruženih informacija na obavijesti? (1 - iznimno niska, 5 - izrazito visoka)
39. Smatrate li ovu obavijest o kolačićima ispravnom? (Da, Ne, Nisam siguran/na)



40. Koju biste opciju prvu odabrali da Vam se ovakva obavijest prikaže na web stranici koju posjećujete prvi put? (Prihvaćam sve, Prihvaćam samo nužne, Postavke kolačića, Pravila privatnosti, Uvjeti korištenja, Pravila o korištenju kolačića, Napuštanje stranice, Ostalo)
41. Razina povjerenja prema stranici isključivo na temelju prikazane obavijesti? (1 - iznimno niska, 5 - izrazito visoka)

42. Razina zadovoljstva količinom pruženih informacija na obavijesti? (1 - iznimno niska, 5 - izrazito visoka)

43. Smatrate li ovu obavijest o kolačićima ispravnom? (Da, Ne, Nisam siguran/na)



44. Koju biste opciju prvu odabrali da Vam se ovakva obavijest prikaže na web stranici koju posjećujete prvi put? (Korištenjem kolačića, Prihvaćam, Napuštanje stranice, Ostalo)

45. Razina povjerenja prema stranici isključivo na temelju prikazane obavijesti? (1 - iznimno niska, 5 - izrazito visoka)

46. Razina zadovoljstva količinom pruženih informacija na obavijesti? (1 - iznimno niska, 5 - izrazito visoka)

47. Smatrate li ovu obavijest o kolačićima ispravnom? (Da, Ne, Nisam siguran/na)

48. Koju biste opciju prvu odabrali da Vam se ovakva obavijest prikaže na web stranici koju posjećujete prvi put? (Prihvaćam odabrane, Prihvaćam sve, Obavijest o kolačićima, Ručna promjena privole za kolačiće, Napuštanje stranice, Ostalo)

49. Razina povjerenja prema stranici isključivo na temelju prikazane obavijesti? (1 - iznimno niska, 5 - izrazito visoka)

50. Razina zadovoljstva količinom pruženih informacija na obavijesti? (1 - iznimno niska, 5 - izrazito visoka)