WEB KOLAČIĆI I PRIVATNOST KORISNIKA: ULOGA, SVJESNOST I ZAŠTITA SIGURNOSTI

Gagula, Monika

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

DIPLOMSKI RAD

WEB KOLAČIĆI I PRIVATNOST KORISNIKA: ULOGA, SVJESNOST I ZAŠTITA SIGURNOSTI

Mentor:

Izv.prof.dr.sc. Marko Hell

Studentica:

univ. bacc. oec. Monika Gagula

Split, srpanj 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, Monika Gagula,

izjavljujem i svojim potpisom potvrđujem da je navedeni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja na objavljenu literaturu, što pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio navedenog rada nije napisan na nedozvoljeni način te da nijedan dio rada ne krši autorska prava. Izjavljujem, također, da nijedan dio rada nije korišten za bilo koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Split, 2024. godine

Vlastoručni potpis : 

SADRŽAJ

1. UVOD

1.1. Problem istraživanja

U kontekstu 21.stoljeća često se tvrdi da se trenutno nalazimo u karakterističnom razdoblju koje se često naziva „digitalno doba“ ili se preciznije opisuje kao „era tehnološke evolucije“. Ovu tvrdnju potkrepljuje pojava transformacijskih inovacija poput Interneta stvari, društvenih mreža kao što su Facebook, Instagram, LinkedIn i drugi, e-trgovine, usluge mobilnog bankarstva, elektroničkih vozila i mnogi drugi, koji su u prethodnim desetljećima bili ne postojeći. World Wide Web (WWW) je pratio digitalnu eru i razvio se od World Wide Web-a 1.0 do World Wide Web-a 3.0 izrazito ubrzanim i dinamičnim tokom. World Wide Web je postao iznimno popularan i moćan medij u posljednjem desetljeću koji igra ključnu ulogu u svim aspektima naših života. Ova tehnologija ne poznaje geografske, političke, društvene ili rasne granice, što omogućava svim pojedincima da je koriste (Patel & Jurić, 2001). Danas korisnici pristupaju internetu putem različitih web preglednika kao što su Chrome, Safari ili Firefox. Ovi preglednici koriste HTTP (eng. Hyper Text Transfer Protocol) ili HTTPS (eng. Hyper Text Transfer Protocol Secure) za komunikaciju s web poslužiteljima i tako pružaju željeni sadržaj. HTTP je protokol bez stanja i sesije, što znači da ne pamti zahtjeve preglednika. Način na koji je ovaj izazov riješen jest implementacijom tehnologije poznate kao web kolačići ili http kolačići (eng. Web cookies) (Wagner, 2020). Web kolačići su postali nužan i ključan alat za suvremeni Internet. Smatralo ga se kao elegantnim rješenjem u kojem web poslužitelj može zapamtiti kada netko posjeti njegovu web stranicu. Online kupovina, personalizirani sadržaj i ciljano oglašavanje postali su bolji upotrebom web kolačića (LaCroix et al., 2017). Web kolačić suštinski je komadić informacije koji se prenosi između web poslužitelja i web preglednika, također poznatog kao klijent. Količina informacija obično je mala, a jednostavno ispitivanje vrijednosti kolačića neće otkriti svrhu kolačića ili što vrijednost predstavlja (Kristol, 2001). Web kolačići su po prirodi bezopasni i sastoje se od jednostavnih ne kompiliranih tekstualnih datoteka koje pomažu u koordinaciji korisničkog preglednika i web poslužitelja kako bi omogućili prikaz punog spektra značajki koje web stranice nude. Neke od tih značajki uključuje automatske prijave i autentifikacija, funkcionalnosti košarice za e-kupovinu, postavke odabira jezika i mnogi drugi (Privacy Issues For Computer Cookies, 2023). Ipak, isto tako predstavljaju rizik po privatnosti korisnika jer mogu poslužiti kao vrijedan izvor osobnih informacija kojima zlonamjerni akteri mogu lako pristupiti.

Pretpostavimo situaciju u kojoj pojedinac posjećuje svoj omiljeni fizički maloprodajni objekt. Prije potpunog ulaska u navedeni objekt, zahtjeva se od pojedinca da priloži određeni oblik identifikacije koji se zatim kopira i pohranjuje. Nakon toga, „asistent“ prati aktivnosti pojedinca unutar maloprodajnog objekta, pomno dokumentirajući svaki korak, svaki proizvod koji se uzima s polica i vraća te proizvode koje pojedinac odluči staviti u svoju košaricu za kupnju. Prilikom procesa plaćanja, osobni podaci pojedinca se prikupljaju, evidentiraju i pohranjuju. Tijekom navedenog procesa kupovine različiti statistički podaci se bilježe na temelju prikupljenih informacija. Ovaj scenarij se može nastaviti tako da taj isti „asistent“ prati pojedinca dok posjećuje druge maloprodajne objekte, bombardirajući ga s različitim ponudama i oglasima, ili pak zlouporabi pohranjene informacije pojedinca kako bi se predstavljao kao ta osoba pri posjeti drugim trgovinama i time obavljao kupovinu pod ukradenim identitetom. Većina ljudi bi se složila da je navedeno ponašanje „asistenta“ u opisanom scenariju neprihvatljivo, a ipak, to se događa kada korisnici pretražuju internet i posjećuju različite web stranice (Wagner, 2020). I dok mnogi korisnici interneta nisu svjesni kako web kolačići funkcioniraju i potencijalnu štetu koju mogu prouzročiti, za druge, web kolačići predstavljaju izvor brojnih zabrinutosti vezanih za privatnost. Iako kolačići suštinski nisu opasni jer se radi o jednostavnim tekstualnim datotekama bez virusa ili drugih zlonamjernih programa, s njima su povezani opći rizici vezani za sigurnost i privatnost korisnika interneta. Upotreba kolačića i izloženost istih tipičan su scenarij u kojem se ovi rizici često manifestiraju. Kolačići imaju sposobnost zadržavanja informacija o korisniku, te u slučaju njihovog neovlaštenog pristupa, potencijalno otvaraju mogućnost prikrivanja korisničkog identiteta ili neovlaštenog pristupa web stranicama, kako je prethodno istaknuto (Wagner, 2020). Hvatanje kolačića putem nesigurnih kanala, poput fiksiranje sesija (eng. session fixation), cross-site skriptiranje, poznati kao XSS napadi (eng. Cross-site scripting), cross-site krivotvorenje zahtjeva, poznati kao CSRF napadi (eng. Cross-site request forgery) i bacanje kolačića (eng. Cookie tossing) samo su neki od različitih načina na koje se kolačići mogu zloupotrijebiti (Dodt, 2020). Unatoč očitim rizicima za sigurnost i privatnost korisnika, korisnici i dalje prihvaćaju korištenje kolačića kako bi dobili osnovan i kvalitetan sadržaj koji zahtijevaju od web stranica (Wagner, 2020).

Za razliku od kolačića prvih strana, koji se postavljaju od strane domene prikazane na web traci preglednika i koje se često koriste na e-trgovinama omogućujući, na primjer, očuvanju proizvoda stavljenih u košaricu za kupovinu, kolačići trećih strana su kolačići koje postavlja domena koja se razlikuje od one koja je prikazana na web traci preglednika. Kolačići trećih strana koriste se od strane kompanija, internetskih oglašivača i platformi za praćenje kao što je Google Analytics, kako bi prikupili što više informacija o korisnicima, te im time pružili ciljane oglase. Tijekom godina su se izražavale zabrinutosti putem medija i raznih istraživačkih radova, što je rezultiralo razvojem različitih

alata koji olakšavaju s upravljanjem kolačićima i njihovim uklanjanjem, kao i zakonima koji reguliraju privatnost korisnika, kao što je Opća uredba o zaštiti podataka (eng. General Data Protection Regulation) (Cahn et al., 2016). Unatoč tome što se web kolačići koriste već više od dvadeset godina, zakonodavstvo poput GDPR-a i Agencija za zaštitu privatnosti u Kaliforniji (eng. California Privacy Protection Agency, skraćeno CPPA)nisu uspostavljene sve do 2018. godine. Međutim, trenutni propisi čini se da manjkaju dovoljnu regulatornu zaštitu (Wagner, 2020). Danas se posjetitelji susreću s različitim oblicima „skočnih prozora", bannera i „pop-up-ova" na web stranicama koji ih pitaju daju li svoj pristanak za prikupljanje osobnih podataka i praćenje prije nego što započnu s korištenjem web stranice. Iako navedene obavijesti o pristanku pružaju korisnicima dojam da imaju kontrolu nad vlastitim privatnim podacima i pravima, mnoge web stranice smognu načine kako bi zavarale korisnike, ignorirajući njihove izričite postavke privatnosti (Bollinger, 2021). Osiguravanje zaštite privatnosti korisnika i dan danas predstavlja znatan, izazovan i osjetljiv problem u digitalnom svijetu. Iako su mnogi zaista zabrinuti za svoju privatnost i sigurnost na web mrežama, većina korisnika i dalje ne posvećuje dovoljno vremena pažljivom čitanju politika privatnosti niti utvrđivanju koje strane uistinu koriste koje podatke i u koje svrhe. Prikupljene informacije predstavljaju vrijednu imovinu industriji oglašavanja, gdje se navedene informacije u nekim slučajevima prodaju radi profita drugim zainteresiranim trećim stranama. Prodaja podataka korisnikazaista predstavlja izričito kršenje zakona o privatnosti jer može sadržavati osjetljive informacije poputidentiteta, geografske lokacije, političke orijentacije i slično. Kako je povijest pokazala, navedene informacije se mogu koristiti u zlonamjerne svrhe, van navedene personalizacije oglasa, već kao manipulacija nad demografskim skupinama na ciljani način (Bollinger, 2021). U svijetu koji je sve više digitaliziran, web kolačići su postali sastavni dio online interakcije, služeći korisnicima i kompanijama u različitim svrhama, kao što su poboljšanje korisničkog iskustva na web stranicama, omogućavanja ciljanog oglašavanja, praćenje ponašanja korisnika i sl. Međutim, sveprisutna upotreba web-kolačića izazvala je značajnu zabrinutost u svezi privatnosti korisnika i zaštite osobnih podataka. U tom kontekstu, sveobuhvatni problem Istraživačkog rada II, a pritom i Diplomskog rada, bavit će se oko razumijevanja i rješavanja višestrukih izazova povezanih s web- kolačićima i njihovim implikacijama za pojedince koji se kreću digitalnim svijetom. Ovaj rad obuhvatit će dva istraživanja, a to je procjena svijesti i percepcije korisnika o web kolačićima, te analizirati „skočne prozore" pristanka na kolačiće na selektiranim web stranicama različitih sektora, kao i analizi njihovoj usklađenosti s GDPR-om. Cilj je istražiti i ispitati razumijevanje korisnika o tome da li imaju shvaćanje u načine kako kolačići funkcioniraju i potencijalne rizike za privatnost koje predstavljaju. Također, istražit će se i učinkovitost, jednostavnost i razumnost skočnihprozora/bannera za pristanak na web kolačiće koji se prikazuju na različitim web stranicama. Analiza će se protezati od same „estetike" skočnih prozora, a pri tome se

razumijeva dizajn, sadržaj, „lakoća“odbitka kolačića, te usklađenost s propisima o privatnosti kao što je Opća uredba o zaštiti podataka (GDPR). Navedeno istraživanje ima za cilj pridonijeti dubljem razumijevanju izazova vezanih za web kolačiće i privatnost korisnika. Ocjenjujući svijest korisnika, mehanizme pristanka i usklađenost web stranica sa zakonskim regulativama, ovaj rad nastoji pružiti vrijedne uvide u poboljšanje prakse privatnosti na internetu i time osnažiti i osvijestiti pojedince da donose informirane odluke o svojim osobnim podacima. U radu će se koristiti pristup mješovitih metoda, kombinirajući kvalitativne i kvantitativnemetode. Navedeni zaključci će pružiti preporuke za poboljšanje praksi, ali i ograničenja u provedbi navedenog istraživanja.

1.2. Predmet istraživanja

Diplomski rad će se temeljiti na različitim ključnim elementima koji će činiti temeljnu strukturu i osnovu analize koja će se provoditi. Bitan aspekt ovog istraživanja leži u sveobuhvatnoj analizi sljedećih ključnih komponenata:

- Ključna uloga i svrha web kolačića – glavna svrha jest dublje razumijevanje ključne uloge koju web kolačići igraju u kontekstu digitalnog svijeta, odnosno, njihove funkcionalnosti i svrhe te načina na koje ovi tehnološki entiteti omogućuju složene interakcije između korisnika i digitalne platforme tj. web stranice. Svaka rasprava o kolačićima mora započeti s odgovorima na dva pitanja: Što su ustvari kolačići? Zašto su potrebni? Odgovori na ova pitanja zahtijevaju skromno razumijevanje kako World Wide Web (WWW) funkcionira. Protokol za prijenos hipertekstualnih dokumenata, skraćeno HTTP (eng. Hypertext Transfer Protocol), pruža temelj za World Wide Web, a kolačići su dodatak HTTP-u. Kada korisnik klikne na hipertekstualnu vezu u svom web pregledniku, navedeni web preglednik, često nazvan „klijent“, se povezuje s web poslužiteljem i šalje mu zahtjev, na što poslužitelj šalje odgovarajući odgovor na poslan zahtjev. Nakon što je web preglednik zaprimio odgovor, web preglednik prekida vezu s web poslužiteljem. Budući da web preglednik, klijent u ovom slučaju, svaki put uspostavlja novu vezu za novi zahtjev, web poslužitelj svaki zahtjev tretira kao da je prvi koji je primio od navedenog klijenta, odnosno svaki se zahtjev tretira kao potpuno neovisnim o bilo kojem prethodnom. Navedeno stanje koje „ne pamti“ otežavalo bi stvaranje današnjih sveprisutnih web stranica za internetsku kupovinu ukoliko se ne bi moglo pratiti što se nalazi u košarici za kupovinu (Kristol, 2001). Time, web kolačići igraju ključnu ulogu kako bi se zadržale informacije o stanju u protokolu HTTP koji je inače „bez stanja“. Time su postali ključnim dijelom za suvremeni internet. Omogućuju web stranicama da pohrane informacije na korisničkom uređaju, kao što su preferencije i jezik, pridonose

oblikovanju korisničkog iskustva na internetu kroz personalizaciju sadržaja i ciljano oglašavanje, čime unaprjeđuju interakciju korisnika s digitalnim svijetom. Nadalje, omogućuju web stranicama da saznaju na koji način su korisnici došli do njihove stranice, bilo putem društvenih mreža, raznih linkova ili pak putem pretraživača, što predstavlja važan aspekt za definiranje marketinške strategije.

- Svijest i percepcija korisnika – web kolačići zaista imaju raznoliku ulogu i svrhu, međutim neki od njih mogu biti kontroverzni. Kroz kolačiće, web poslužitelj može identificirati računalo korisnika i zapamtiti što je korisnik kupovao, kako se „kretao“ po internetu i sl. Jasno razumijevanje razine svijesti korisnika o tome što su zapravo web kolačići, za što se koriste i kako se njima može upravljati je temeljno za svako razmatranje razine detalja koje je potrebno pružiti o kolačićima. PricewaterhouseCoopers LLP (PwC) je od strane britanskog Ministarstva kulture, medija i sporta (eng. Department for Culture, Media and Sport) bio zadužen za provođenje istraživanja o razini razumijevanja potrošača o internetu i kolačićima. Istraživanje je pokazalo da je trenutačna svijest o načinu korištenja kolačića i dostupnim opcijama za njihovo upravljanje veoma ograničena (Lancefield et al., 2011). PwC je 2011. godine proveo online anketu s više od 1000 pojedinaca obuhvaćajući cijelu Veliku Britaniju, sve dobne skupine kao i socio-ekonomske skupine. Iako izvješće priznaje da su najintenzivniji korisnici interneta pretežito zastupljeni u uzorku, rezultati pokazuju da značajni postotak navedenih „Internet stručnjaka“ imaju ograničeno razumijevanje kolačića i načina njihova upravljanja:
- Samo 13% ispitanika je navelo da potpuno razumije kako web kolačići funkcioniraju, dok je 45% ispitanika navelo da ih donekle razumiju. Nasuprot tome, 37% ispitanika je čulo za web kolačiće, međutim ne razumiju kako funkcioniraju, dok 2% ispitanika nije nikad čulo za web kolačiće prije nego što su sudjelovali u istraživanju;
- Anketa je testirala znanje ispitanika o web kolačićima, tražeći od njih da potvrde jesu li određene izjave o kolačićima ispravne ili ne. Samo za jednu od šesnaest izjava većina ispitanika znala je točan odgovor;
- 37% ispitanika je izjavilo da ne znaju kako upravljati kolačićima na svom računalu (Lancefield et al., 2011).

Oni koji ne redovito koriste Internet ili imaju općenito nižu razinu tehničke osviještenosti, dovodi do manje vjerojatnosti da će razumjeti način rada kolačića i kako njima upravljati. U izvješću je zaključeno da bi šira edukacija korisnika o osnovnim postavkama privatnosti na internetu mogla

znatno doprinijeti da korisnici preuzmu veću kontrolu nad svojom privatnošću dok su na mrežama (Information Commissioner's Office, 2012.)

- Pravna regulativa i usklađenost – ovo područje istraživanja usmjerava se na detaljnu analizu relevantnih zakonodavnih okvira, s posebnim naglaskom na Opću uredbu o zaštiti podataka (GDPR), uključujući njegove ključne odredbe, propise o privatnosti, zahtjeve za prikupljanje i obradu osobnih podataka te druge relevantne aspekte. Analizom zakonodavnih okvira GDPR-a i drugih pravnih okvira, identificirat će se ključni aspekti koji se odnose na kolačiće i njihovu usklađenost s ovim propisima. Opća uredba o zaštiti osobnih podataka, poznata i kao GDPR (General Data Protection Regulation), pruža građanima Europske unije veću kontrolu nad njihovim osobnih podacima. GDPR se direktno primjenjuje u državama članicama Europske unije, što znači da nema potrebe za dodatnim prenošenjem u nacionalno zakonodavstvo. Cilj GDPR-a je usklađivanje regulative o upravljanju osobnim informacijama i svim ostalim podacima povezanim s pojedincima na razini cijele Europske unije i njenih država članica (Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća, 2016). Navedenom se Uredbom utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila koja su povezana sa slobodnim kretanjem osobnih podataka. Također, ovom se Uredbom štite i temeljna prava i slobode pojedinaca, a osobito njihovo pravo na zaštitu osobnih podataka.

U svibnju 2019. godine GDPR.EU proveo je istraživanje među 716 lidera malih poduzeća na području Španjolske, Ujedinjenog Kraljevstva, Francuske i Irske s ciljem boljeg razumijevanja kako se njihova poduzeća nose s novim zahtjevima Opće uredbe o zaštiti podataka (GDPR). GDPR.EU predstavlja online resurs posvećen olakšavanju usklađivanja s GDPR-om za mala i srednja poduzeća. Njihova web stranica obiluje s objašnjenjima na razumljivom jeziku, tekstom same uredbe, kao i popisima za provjeru. Navedeni izvještaj pruža uvid u usklađivanje s GDPR-om iz perspektive malih poduzeća. Mali poduzetnici u ovom su izvještaju definirani kao oni s manje od 500 zaposlenika. Iako čine većinu poduzeća, oni se suočavaju s jedinstvenim izazovima u pogledu usklađivanja s GDPR-om. Raspolažu s najmanjim resursima za pridržavanje novih propisa zbog ograničenih proračuna u usporedbi s velikim korporacijama, što ih dovodi u poziciju da podliježu i mogućim kaznama, što mala poduzeća ne mogu financijski priuštiti. Rezultati istraživanja otkrili su opću spremnost za usklađivanje s GDPR-om. Međutim, dvije trećine ispitanika tvrdi da njihova tvrtka koristi „end-to-end“ enkripciju kako bi zaštitila svoju komunikaciju od povrede podataka (GDPR.EU, 2019). „End-to-end“ enkripcija je sustav komunikacije u kojem jedino sudionici komunikacije mogu čitati poruke. Pošto ne postoji treća strana koja ima saznanja o podacima koji se komuniciraju i pohranjuju, time nadzor te

manipulacija su onemogućeni ("Važnost „End-to-end" Enkripcije," 2020). Međutim, kad su pozvani da specificiraju koji pružatelj usluge koriste, samo 9% je navelo uslugu s ovakvom vrstom ugrađenog šifriranja, kao što je Boxcryptor, MEGA i sl. Što je iznenađujuće, punih 44% ispitanika nije bilo sigurno da uvijek utvrđuju zakonsku osnovu pri korištenju osnovnih podataka (GDPR.EU, 2019).

- Sigurnosni aspekti web kolačića – razmatranje sigurnosnih aspekata web kolačića iznimno je bitna da bi se shvatilo kako web kolačići, koji se često koriste za praćenje i pružanje personaliziranih iskustava na internetu, mogu zloupotrijebiti. Ranjivosti i napadi na web kolačiće nisu novost. Napadači koriste različite metode kako bi iskoristili potencijalne slabosti i ostvarili neovlašteni pristup kolačićima ili osjetljivim podacima koje oni pohranjuju. Primjeri ovih ranjivosti uključuju Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) i Session Hijacking. Web kolačići igraju ključnu ulogu u procesima identifikacije i autentifikacije korisnika na web stranicama i uslugama. Oni se koriste kako bi se održavale korisničke sesije i omogućavali pristup računima korisnika, čime se osigurava jednostavnost korištenja. Međutim, da bi se osigurala sigurnost kolačića, web stranice su dužne primijeniti različite tehničke i organizacijske mjere kako bi se osigurala sigurna komunikacija te spriječilo dovođenje bilo kakvih potencijalnih napada. Korisnici se time sve više oslanjaju na različite tehnike i alate kako bi sačuvali svoju privatnost i osigurali sigurno pregledavanje na internetu. Kao primjer se mogu navesti razni Ad-blockeri, softverski alati i proširenja, koja blokiraju prikazivanje oglasa na web stranicama koje korisnik posjećuje. Osim što znatno poboljšavaju iskustvo pregledavanja, mnogi ad-blockeri također blokiraju kolačiće treće strane. Za razliku od kolačića prve strane koje postavlja web stranica koju korisnik posjećuje, a koji se koriste za pravilno funkcioniranje web stranice ili za prikupljanje osobnih podataka korisnika, kolačići treće strane su kolačići koje postavljaju druge domene osim one koju korisnik posjećuje. Uglavnom se koriste za praćenje korisnika između raznih web stranica i prikazivanje relevantnih oglasa. Dok kolačići prve strane dopuštaju praćenje korisnika samo na web stranici koja ih postavlja, kolačići treće strane omogućuju praćenje ponašanja i kretanje korisnika od web stranice do web stranice i prikuplja informacije kao što su dob, obrasci potrošnje i sl. Navedene se informacije mogu daljnje razvijati što najčešće može biti vrlo detaljno i nametljivo (Alternative kolačićima trećih strana, 2022).

Većina modernih preglednika omogućuje korisnicima veću kontrolu nad kolačićima. Korisnici mogu konfigurirati postavke preglednika kako bi blokirali kolačiće treće strane ili ih odbili s web stranica koje ih pokušavaju postaviti. Time se pridaje veća kontrola korisnicima nad njihovim podacima.

Privatni načini pregledavanja, što uključuje Tor (eng. The Onion Router) ili pak opcije poput „Incognito“ u Google Chrome koja omogućuje automatsko brisanje povijesti pregledavanja i kolačića nakon završetka sesije, pomaže u očuvanju korisničke privatnosti. Istraživanje upotrebe ovih tehnika i alata zaštite, kao i motivacija korisnika da ih koriste, može pružiti vrijedan uvid u percepciju sigurnosti i privatnosti u kontekstu web kolačića. Razumijevanje ovih pristupa također pomaže oblikovati smjernice za korisnike o tome kako bolje zaštiti svoju privatnost na internetu.

1.3. Ciljevi istraživanja

Navedeni opis problema istraživanja i predmeta istraživanja pruža jasno razumijevanje područja istraživanja diplomskog rada, te se na osnovu toga definiraju sljedeći glavni istraživački ciljevi:

- Ispitati svijest korisnika o web kolačićima - cilj ovog dijela istraživanja je procijeniti razinu razumijevanja korisnika o tome što su zapravo web kolačići, kako funkcioniraju i koja je svrha. Navedeno istraživanje će se postići provedbom anketnog upitnika izabranog uzorka populacije i time će omogućiti bolje razumijevanje percepcije ljudi o prikupljanju i obradi podataka putem web kolačića.
- Analizirati usklađenost izabranih popularnih web stranica s propisima EU o transparentnoj obradi podataka i korištenju web kolačića - cilj ovog dijela istraživanja jest utvrditi koliko su izabrane web stranice uistinu usklađene s Općom uredbom o zaštiti podataka (GDPR) u vezi s web kolačićima. Usmjerit će se na procjenu učestalosti i kvalitete informacija o obradi podataka koje su dostupne posjetiteljima izabranih web stranica te razumijevanje načina kako se ti podaci prikupljaju i koriste. Također će se istražiti dostupnost i praktičnost opcija za odbijanje ili pak upravljanjem web kolačićima na izabranim stranicama kako bi se utvrdila razina zaštite privatnosti i korisničkog iskustva. Definiranje relevantnih kriterija, metoda i pokazatelja za procjenu usklađenosti web stranica s zahtjevima EU u vezi transparentne obrade podataka ključno je kako bi se provela analiza.
- Ispitati sigurnosne aspekte web kolačića – cilj ovog dijela istraživanja temelji se na identificiranju i analizi potencijalnih sigurnosnih prijetnji i rizika povezani s web kolačićima, kao što su Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Session Hijacking i drugi. Razmotrit će se i identificirati potencijalni rizici i prijetnje s korištenjem web kolačića na web stranicama, odnosno analizirat će se scenariji u kojima napadači mogu dobiti neovlašteni pristup podacima pohranjenim u kolačićima,

analizirati scenarije u kojima bi kolačići mogli biti narušeni ili manipulirani i sl. Na temelju prikupljenih podataka i analiza, prepoznat će se područja gdje bi se praksa privatnosti na internetu mogla poboljšati. To uključuje i pružanje preporuka korisnicima za bolju informiranost i zaštitu podataka.

1.4. Istraživačka pitanja

Uz prethodno navedeni problem, predmet i ciljeve istraživanja potrebno je postaviti određena istraživačka pitanja na koja će se odgovoriti u narednom diplomskom radu:

- Kakvu ulogu web kolačići igraju u praćenju i personalizaciji korisničkog iskustva na internetu?
- Koliko su korisnici svjesni prikupljanja osobnih podataka putem web kolačića i kako to utječena njihovo povjerenje web stranicama?
- Imaju li zakonodavstvo i regulative značajan utjecaj na praksu upotrebe web kolačića i zaštituprivatnosti korisnika?
- Nedostaju li izabranim web stranicama transparentnost i jasnoća svrhe obrade osobnih podataka?
- Kako se različite tehnike zaštite sigurnosti mogu primijeniti kako bi se zaštitila privatnost korisnika u kontekstu web kolačića?

1.5. Metode istraživanja

U radu će se primijeniti opće znanstvene metode za istraživačke svrhe kao što su:

- Metoda indukcije – podrazumijeva sustavnu primjenu induktivnog načina zaključivanja kako bi se na temelju analize pojedinačnih činjenica došlo do zaključaka o općim zakonitostima. Navedena metoda omogućava da se, polazeći od konkretnih pojedinačnih slučajeva, izvedu opći zaključci. Metoda indukcije će se koristiti kako bi se iz konkretnih pojedinačnih slučajeva iskustava korisnika s web kolačićima izveo opći zaključak o tome kako korisnici percipiraju na web kolačiće.
- Deskriptivna metoda – navedena metoda se uglavnom primjenjuje u početnoj fazi znanstvenog istraživanja detaljnim opisivanjem temeljnih pojmova web kolačića i pojave vezane uz web kolačiće i privatnost korisnika kako bi se postigla veća objektivnost i točnost usvim ostalim fazama istraživanja.
- Metoda dedukcije – podrazumijeva sustavnu primjenu deduktivnog načina zaključivanja gdje se iz općih principa izvode specifični i individualni zaključci. U suštini, deduktivni

proces zahtijeva poznavanje općih spoznaja na temelju kojih se dolazi do razumijevanja onog što je specifično.

- Metoda analize – postupak u kojem se izvode zaključci postupkom raščlanjivanja složenih pojava vezanih uz web kolačiće i privatnost kako bi se shvatila njihova struktura i međuodnos.
- Komparativna metoda – koristi se za usporedbu među pojavama, događajima ili predmetima s ciljem prepoznavanja sličnosti, isticanja zajedničkih karakteristika ili razlika. Navedena metoda će se koristiti kako bi se uspoređivali različiti aspekti web kolačića između različitih web stranica, što će istaknuti zajedničke karakteristike ali i razlike.
- Statističke metode – koristit će se za analizu anketa i podataka prikupljeni na temelju odabrane skupine, odnosno uzorka, i time izvesti zaključci o stavovima korisnika. Svaka od navedenih metoda će pomoći kako bi se dublje istražila tema diplomskog rada i odgovorila na istraživačka pitanja koja su postavljen ranije.

1.6. Doprinos istraživanja

Kroz navedeno istraživanje nastojat će se identificirati praznine u postojećem razumijevanju ili praksi te ukazati na područja gdje su potrebna dodatna istraživanja. Istraživanje provedeno u navedenom radu će doprinijeti povećanju svijesti o važnosti privatnosti korisnika na internetu. Identificiranjem razina svijesti i razumijevanja korisnika o web kolačićima pridonijet će boljem razumijevanju istih. Pronalaženjem stavova i očekivanja korisnika u vezi zaštite privatnosti, pružit će smjernice za unaprjeđenje prakse zaštite podataka koji će korisnicima omogućit veću kontrolu nad njihovim osobnim podacima. Na temelju rezultata u ovom radu, budući istraživači mogu razmotriti smjernice u ocjeni različitih regulativnih okvira, odnosno analizirati učinkovitost postojećih zakonskih okvira i propisa što može rezultirati preporukama za poboljšanje. S obzirom na ubrzani razvoj Internet svijeta i digitalne tehnologije, buduća istraživanja mogu pratiti promjene u korisnikovom ponašanju vezano za web kolačiće.

Navedeni diplomski rad može postati polazišna točka za daljnja istraživanja i razvoj u području web kolačića, percepcije korisnika, privatnosti korisnika kao i njihove zaštite na internetu. Navedeni rezultati u radu mogu doprinijeti budućim naporima usmjerenim ka poboljšanju prakse i politika na ovim važnim područjima.

1.7. Struktura rada

Diplomski rad će se sastojati od 8 poglavlja. U prvom poglavlju definirat će se problem i predmet istraživanja. Nadalje, navest će se ciljevi istraživanja kao i istraživačka pitanja na koje će se odgovoriti kroz navedeni rad. Također će se u uvodnom dijelu navesti metode koje su korištene tijekom izrade diplomskog rada kao i doprinos istraživanja samog rada.

U drugom poglavlju predstavit će se pojmovno određenje web kolačića kao i njihovo povijesno podrijetlo. Razmotrit će se uloga i svrha kolačića kao i različiti tipovi web kolačića koji postoje na internetu, kao što su trajni i sesijski kolačići. Nadalje, istražit će se kako se web kolačići koriste u različitim sektorima.

U trećem poglavlju istražit će se kako su zakoni u Europskoj Uniji usmjereni na zaštitu privatnosti korisnika u kontekstu web kolačića. Nadalje, fokusirat će se i na Opću uredbu o zaštiti podataka (GDPR) i kako je navedena uredba promijenila pravila za upotrebu kolačića. Također, analizirat će se zakoni i regulative o privatnosti koji se primjenjuju izvan EU, kao i moguće kazne i sankcije za organizacije koje krše zakone o privatnosti.

Četvrto poglavlje će razmotriti različite rizike koji proizlaze iz upotrebe web kolačića, kao što su praćenje korisničke aktivnosti, profiliranju korisnika i personalizacija, te identifikacija uređaja. Također će se opisati sigurnosne prijetnje kao što su XSS napadi i CSRF napadi.

Peto poglavlje će istražiti i analizirati kako budući razvoj tehnologije može utjecati na privatnost korisnika, te trenutačne i buduće trendove u praćenju i oglašavanju putem interneta. U zadnjem pod poglavlju petog poglavlja razmotrit će se potencijalne promjene u regulativama.

U šestom poglavlju će se provesti analiza svjesnosti korisnika o web kolačićima. Definirat će se problem, cilj, metodologija istraživanja, kao i rezultati istraživanja provedeni putem anketnog upitnika na izabranom uzorku.

Sedmo poglavlje donosi analizu upotrebe web kolačića na izabranim web stranicama. Definirat će se problem, cilj i metodologija istraživanja kao i rezultati dobiveni analizom kolačića na navedenim web stranicama.

Nakon provedbe istraživanja u navedenim poglavljima, moći će se donijeti zaključak u osmom poglavlju.

2. WEB KOLAČIĆI

2.1. Pojmovno određenje web kolačića

Tijekom 80-ih godina, Internet je postao najznačajnija računalna mreža, predstavljajući globalnu međupovezanost računalnih mreža koji komuniciraju korištenjem zajedničkog protokola. Tijekom tog razdoblja, milijuni računala bili su integrirani na Internet, a koristili su ga većinom istraživači na sveučilištima i nacionalnim laboratorijima za razmjenu znanstvenih informacija. S porastom prepoznatljivosti, Internet je privukao i korisnike izvan akademske zajednice, prvenstveno zbog prijenosa elektroničke pošte. Godine 1989. uveden je novi informacijski sustav poznat kao Svjetska mreža (eng. World Wide Web, u nastavku Web), opisan kao hipermedijski sustav za pretraživanje informacija s ciljem široke dostupnosti dokumenata. Web je tada bio poznat i korišten isključivo u akademskim i istraživačkim zajednicama, budući da nije postojao pristupačan alat za tehnički neobučene korisnike. Međutim, 1993. godine istraživači Nacionalnog centra za super-računalne aplikacije (eng. National Center for Supercomputing Applications) predstavili su web preglednik "Mosaic" s grafičkim korisničkim sučeljem. Grafičko korisničko sučelje Mosiaca bilo je jednostavno za učenje, omogućavajući korisniku dohvaćanje dokumenata putem jednostavnih naredbi, ne zahtijevajući tehničku obuku, čime se otvorio potencijal širokom dijelu populacije. Arhitektura Weba pratila je konvencionalni model klijent-poslužitelj, a komunikacija se odvijala putem protokola "HyperText Transfer Protocol" (HTTP) (Persistent client state in a hypertext transfer protocol based client-server system, 1998). HTTP predstavlja ključni element svake razmjene podataka na webu te funkcionira kao klijent-poslužitelj protokol omogućujući korisnicima pristup web stranicama i drugim online resursima (Mustapha,2023). Kada korisnik klikne na hipertekstualnu poveznicu u web pregledniku, preglednik, često nazivan klijent, uspostavlja vezu s web poslužiteljem. Nakon uspostavljanja veze, klijent šalje zahtjev, na što poslužitelj odgovara traženim odgovorom. Budući da klijent za svaki zahtjev stvara novu vezu, poslužitelj tretira svaki zahtjev kao da je prvi koji je primio od tog klijenta. Ovaj ciklus, poznat kao zahtjev-odgovor, predstavlja proces komunikacije između klijenta i poslužitelja, koji ima cilj dobiti traženi odgovor ili izvršiti određene radnje. Stoga se svaki zahtjev smatra zahtjevom „bez stanja“, neovisnim o prethodnim zahtjevima (Kristol, 2001). Iako je sama srž HTTP „bez stanja“, upotreba HTTP kolačića omogućuje održavanje stanja sesije i pruža dodatnu funkcionalnost, čime se uspješno rješavaju izazovi komunikacije s određenim web stranicama. (An Overview of HTTP - HTTP | MDN, 2024). HTTP kolačić ili web kolačić predstavlja mali podatak koji web poslužitelj šalje web pregledniku korisnika. Djeluju putem jednostavnog, ali učinkovitog mehanizma koji poboljšava korisničko iskustvo na internetu. Kada korisnik posjeti određenu web stranicu, poslužitelj web stranice šalje maleni podatak – kolačić – pregledniku

korisnika. Taj kolačić obično sadrži informacije relevantne za interakciju korisnika s web stranicom. Kada se kolačić pohrani na korisnički uređaj, svaki put kad korisnik navigira na navedenoj web stranici, preglednik šalje kolačić natrag poslužitelju čime omogućuje web stranici da „zapamti“ prethodne radnje korisnika (Simon, 2023). HTTP kolačić se može opisati kao informacija koju poslužitelj i klijent međusobno razmjenjuju. Količina navedene informacije je mala, te općenito pregledavanje same vrijednosti kolačića neće otkriti čemu kolačić služi niti što njegova vrijednost predstavlja (Kristol, 2001).

2.2. Povijest web kolačića

Tijekom devedesetih godina, dok su se web stranice suočavale s izazovima u očuvanju informacija o identitetu korisnika i njihovim prethodnim aktivnostima tijekom posjeta, programer Lou Montulli razvio je HTTP kolačić, poznat kao i web kolačić ili jednostavno kolačić. Ovaj inovativni mehanizam omogućio je učinkovito pohranjivanje podataka o korisnicima te je postao ključan u pružanju personaliziranog iskustva na webu. Kolačići su se prvi put pojavili u web pregledniku Netscape 1994. godine, a pomagali su pregledniku u utvrđivanju je li korisnik prethodno posjetio web stranicu. Ovim izumom, kolačići su postali najinovativnija značajka koja je zauvijek transformirala svjetsku mrežu (Shah & Kesan, 2004). Koncept je bio usmjeriti web preglednik da pohrani osnovne informacije – poput korisničkog ID-a. Na taj način, tijekom korisnikove navigacije web lokacijom, stranica bi mogla dohvatiti te informacije i pružiti koherentno i personalizirano iskustvo. Uvođenje kolačića nije bilo široko poznato javnosti u to vrijeme. Posebno je važno napomenuti da su kolačići bili automatski prihvaćeni, te korisnici nisu bili obaviješteni o njihovom prisustvu. Neki su pojedinci bili svjesni postojanja kolačića početkom 1995. godine, no šira javnost saznala je o njima nakon što je *Financial Times,* jedna od vodećih svjetskih novinskih organizacija, objavila članak o njima 1996. godine. Istu godinu, kolačići su privukli znatnu medijsku pažnju, posebice zbog potencijalnih implikacija na privatnost (Shwartz, 2001). Naime, Netscapeova specifikacija kolačića dopuštala je trećim stranama da postave vlastite kolačiće, što je stvorilo ogroman problem. Ova „rupa“ u sustavu dovela je do pojave novog oblika poslovanja – tvrtki za upravljanje online oglašavanjem. Ovaj proces se zbiva kad preglednik učita stranicu s jedne web stranice, a ta stranica sadrži oglase koji se učitavaju s druge web stranice. U tom scenariju, potonja web stranica šalje kolačiće zajedno s oglasima. Zabrinutost proizlazi iz činjenice da korisnik, iako može očekivati kolačić s prve web stranice, nema razloga pretpostaviti, ili čak znati, da će preglednik posjetiti i „komunicirati“ s drugom web stranicom, te da će primiti kolačić od druge stranice, što dovodi do stvaranja sveobuhvatnog profiliranja korisnika (Kristol, 2001). S ciljem rješavanja ovog problema, Netscape elaborira 3 strategije s kojima su se suočavali u vezi s izazovom kolačića treće strane. Prvi pristup implicirao je pasivnost, odnosno ne

poduzimanje konkretnih koraka, čime bi se oglašivačima omogućilo neograničeno korištenje kolačića treće strane. Druga opcija predviđala je potpunu blokadu kolačića treće strane. Treća opcija, koju su odabrali, uključivala je razvoj rješenja koje bi korisnicima pružilo kontrolu nad kolačićima, posebno nad načinom na koji ih oglašivači koriste za praćenje. Ova strategija uključivala je implementaciju različitih funkcionalnosti unutar preglednika, omogućujući korisnicima pregled kolačića na njihovim uređajima te pružajući mogućnost kontrole nad načinom njihove uporabe. Na ovaj način, korisnici su imali mogućnost isključivanja kolačića treće strane u potpunosti ili njihovo isključivanje za određenu web stranicu. (Rivero, 2021). Na pitanje zašto nisu implementirali potpunu eliminaciju kolačića treće strane još 1996. godine, odgovor leži u činjenici da je oglašavanje tada predstavljalo jedini izvor prihoda za web stranice, s obzirom na manju prisutnost e-trgovine. Većina weba oslanjala se na prihode generirane putem oglašavanja, a isključivanje kolačića namijenjenih oglašavanju značajno bi umanjilo sposobnost generiranja prihoda (Rivero, 2021). Javna diskusija o kolačićima manifestirala se putem medijskog uzburkanja zbog problema s privatnošću, što je rezultiralo da kolačići budu predmet rasprave na dva saslušanja pred američkom Saveznom komisijom za trgovinu 1996. i 1997. godine. Međutim, navedena saslušanja samo su dotakla površinu pitanja privatnosti i pripadajuća tehnička razmatranja (Shah & Kesan, 2004).

2.3. Uloga i svrha kolačića

Primarna namjena kolačića obuhvaća tri ključna područja. Prvo, kolačići se koriste za upravljanje sesijom, omogućujući očuvanje korisničke prijave, stanja košarice za kupnju ili bilo kojeg drugog podatka koji server treba zapamtiti. Navedeno je ključno kako bi se osiguralo neprekidno korisničko iskustvo na webu. Drugo, kolačići se koriste za personalizaciju, čuvajući korisničke preferencije poput jezičnih postavki i druge. To omogućuje prilagodbu internetskog iskustva prema individualnim željama korisnika kako bi korisnici mogli lako navigirati stranicom. Treće, kolačići se koriste u svrhu praćenja, bilježeći i analizirajući ponašanje korisnika (Using HTTP Cookies - HTTP | MDN, 2024). Time, razlikuju se dvije vrste praćenja. Prva se može sumirati pod općim pojmom web analitike. Kolačići ove vrste koriste se za praćenje korisnika samo unutar domene koju trenutno pregledavaju. Primjeri uključuju vrijeme provedeno na stranici, preglednik koji je korišten za pristup stranici, broj posjetitelja i njihova lokacija (Bollinger, 2021). Navedeno se prati s ciljem poboljšanja web stranice, ali i za mjerenje performansi web stranice u marketinške svrhe. Praćenje za navedenu svrhu ne zahtijeva osjetljive informacije korisnika. Međutim, GDPR ipak smatra da ovi kolačići sadrže osobne informacije te stoga zahtijevaju pristanak od korisnika. Druga forma praćenja odvija se na više web mjesta, obično u svrhu oglašavanja i prodaje korisničkih podataka. Takvi kolačići prikupljaju

informacije o ponašanju prilikom pregledavanja i osobnim interesima korisnika kako bi izgradili detaljan profil (Bollinger, 2021).

2.4. Vrste web kolačića

2.4.1. Klasifikacija prema porijeklu

U slučaju klasifikacije web kolačića prema porijeklu, razlikuju se kolačići prve strane i kolačići treće strane. Kolačići prve strane postavljaju se od strane same web stranice koju korisnik posjećuje. Ovi kolačići predstavljaju ključnu komponentu u prikupljanju analitičkih podataka, pamćenju postavki jezika, pružanju opcije pregleda nedavno posjećenih stranica unutar same web stranice te obavljanju drugih korisnih funkcija koje doprinose ukupnom korisničkom iskustvu na web stranici. Konkretno, primjer kolačića prve strane odnosi se na situaciju kada se korisnik prijavljuje na web stranicu e-trgovine. Ukoliko korisnik onemogući kolačiće prve strane, bit će mu potrebno ponovno prijavljivanje pri svakom posjetu stranici, te će mu biti onemogućeno višestruko online kupovanje, jer bi se košarica resetirala nakon dodavanja svakog proizvoda (What's the Difference Between First and Third-Party Cookies?, 2022). Kolačići treće strane su kolačići koji se postavljaju na korisnički uređaj, ne od strane posjećene web stranice, već od treće strane, poput oglašivača kako bi isporučili ciljane oglase korisnicima weba. Milijuni potrošača svakodnevno posjećuju web stranice, a kolačići treće strane ključna su komponenta tih web stranica. Pohranjuju se na računalu korisnika, čime se trećim stranama omogućuje kompilacija detaljnih profila svakog pojedinog korisnika. Ako određena oglašivačka tvrtka ima saznanja o lokaciji određene osobe, njezinim preferencijama, interesima i nedavnih kupnji, može ciljati oglase na više web stranica kako bi toj osobi pružila reklame za proizvode u koje zaista ima interes. Način na koji kolačići treće strane funkcioniraju i nađu mjesto na web stranicama jest da mnoge web stranice iznajmljuju prostor za oglase na njihovim stranicama radi monetizacije. Kao rezultat toga, dopuštaju trećim stranama da postave kolačiće na njihovoj web stranici u obliku oglasa (What's the Difference Between First and Third-Party Cookies?, 2022).

2.4.2. Klasifikacija prema trajanju

Ukoliko bi se kolačići klasificirali prema vijeku trajanja, oni se dijele na trajne kolačiće i sesijske kolačiće. Trajni kolačići zadržavaju se na korisničkom uređaju tijekom određenog razdoblja ili dok ih korisnik ne izbriše. Oni igraju ključnu ulogu u prepoznavanju povratnih posjetitelja, pamćenju korisničkih preferencija te praćenju ponašanja korisnika kroz više sesija. Na taj način olakšavaju interakcije na web mjestu te se prilagođavaju individualnim preferencijama i potrebama (Monique, 2023). Sesijski kolačići su privremeni i traju samo tijekom jedne sesije. Prate korisničke radnje tijekom

sesije i brišu se kada se preglednik zatvori. Sesijski kolačići pridonose funkcionalnost web mjesta osiguravajući da podaci, poput proizvoda u košarici, ostanu sačuvani tijekom te jedne sesije, poboljšavajući tako korisničko iskustvo (What Are Session Cookies?, 2024).

2.4.3. Klasifikacija prema svrsi

Kada se govori o svrsi, kolačići se dijele na striktno nužne kolačiće, kolačiće postavki, statističke kolačiće i marketinške kolačiće. Striktno nužni kolačići su neophodni za korisnika kako bi mogao pregledavati web stranicu i koristiti njene funkcionalnosti. Ovi kolačići su obično kolačići prve strane i sesijski kolačići. Iako za ove kolačiće nije potreban pristanak od strane korisnika, korisniku bi trebalo svakako biti objašnjeno koju funkciju obavljaju i zašto su nužni (Koch, n.d.). Kolačići postavki, poznati i kao funkcionalni kolačići, spadaju u kategoriju kolačića koji su ključni za pravilan rad web stranice. Njihova svrha, kako sam naziv sugerira, leži u unapređenju performansi i funkcionalnosti web stranice. Ovi kolačići pružaju podršku web stranicama da zapamte korisničke podatke, uključujući korisničko ime i lozinku za automatsku prijavu, te korisničke postavke poput jezičnih preferencija i regije (All about Internet Cookies, 2024). Statistički kolačići anonimno prikupljaju podatke i koriste ih u svrhu poboljšanja performansi web stranice. Primjerice, ovi kolačići mogu brojati posjete stranici, analizirati koliko vremena korisnici provode na web mjestu te ispitati brzinu učitavanja kako bi poboljšali ukupnu efikasnost (What Are Different Types of Web Cookies?, 2022). Marketinški kolačići prate aktivnost korisnika s ciljem poboljšanja relevantnosti oglasa ili ograničavanja broja prikazivanja određenog oglasa. Informacije prikupljene putem ovih kolačića mogu biti dijeljene s drugim organizacijama oglašivačima. Marketinški kolačići su dugotrajni i gotovo uvijek potječu od trećih strana (Koch, n.d.).

2.5. Korištenje kolačića u različitim sektorima

Osim svoje široke primjene u sektoru e-trgovine, web kolačići se strateški implementiraju u specifičnim sektorima, posebice u domenama zdravstva, financija, obrazovanja i javnih službi. Mnoge zdravstvene organizacije, uključujući bolnice, sve više prenose dio svojih usluga digitalnim putem kao što je zakazivanje termina, pregled medicinskih rezultata i slično. Time je Sveučilište Concordia u Kanadi provelo istraživanje u kojem su uspješno analizirane 19.483 internetske stranice bolnica iz 152 zemlje i provincijskih jurisdikcija smještenih u Aziji, Europi, Sjevernoj Americi, Latinskoj Americi, Africi i Oceaniji. Tijekom istraživanja primijećena je opsežna upotreba praćenja na internetskim stranicama bolnica – 53,5% stranica bolnica sadržavale su kolačiće za praćenje. Osim pitanja privatnosti, također su identificirane stranice s potencijalnim sigurnosnim problemima – 33

stranice označene su kao zlonamjerne prema VirusTotal, a 699 stranica uključivale su usluge ponavljanja sesije poput FullyStory, Yandex i Hotjar koje su potom slale osjetljive informacije vanjskim poslužiteljima. Na bolničkim se stranicama razmjenjuje raznolik skup osjetljivih informacija, kao što su identifikacijski podaci, zdravstveni status, mentalno zdravlje, reproduktivna skrb i slično. Ove osjetljive informacije mogu procuriti trećim stranama, a rizici otkrivanja takvih osjetljivih informacija mogu uključivati diskriminaciju, društvenu stigmu i fizičku štetu (Yu, et.al., 2022).

Korištenje internetskih stranica za predstavljanje sveučilišta na mreži sveprisutno je unutar sektora visokog obrazovanja. Kao digitalna reprezentacija sveučilišta, internetske stranice pružaju sve potrebne informacije o instituciji, od elemenata prospekta do istraživačkih radova, što privlači potencijalno široku publiku. Međutim, upotreba kolačića potencijalno mijenja odnos s publikom, jer omogućuje praćenje korisnika, posebice putem društvenih medijskih platformi. Iako je korištenje takvog prikupljanja podataka i marketinga standardno za komercijalne internetske stranice, pitanje primjerenosti i posljedice za sektor visokog obrazovanja ostaju otvorena (Jordan, 2018). Istraživanje ovog pitanja provedeno je kroz analizu obujma i prirode kolačića koji se trenutno koriste na internetskim stranicama institucija visokog obrazovanja u Velikoj Britaniji. Korištenjem alata Tracker Tracker ukupno je pronađeno 138 jedinstvenih kolačića u uzorku od 150 internetskih stranica. Najčešće korišteni kolačići uključuju Google Analytics, DoubleClick, Google Tag Manager, Facebook Connect, Facebook Custom Audience, Hotjar, Twitter Advertising i slično. Korištenjem kolačića, sveučilišta ne samo da plaćaju za uslugu online oglašavanja, što postavlja pitanje o primjerenosti korištenja javnih sredstava, već i dijele podatke o ponašanju svojih korisnika s platformama (često društvenih medija) koje te podatke koriste za ostvarivanje profita (Helmond et.al., 2017).

U posljednjih nekoliko godina, vlade diljem svijeta premještaju svoje usluge na Internet kako bi bolje služile svojim građanima. Unatoč koristima, ova odluka povećava opasnost od praćenja putem takvih web stranica. (Gotze et.al., 2022.). Mogući rizik e-uprave leži u činjenici da predstavlja jedinstvenu točku interakcije za obvezne i neophodne usluge za sve građane, što može rezultirati, bez obzira na namjeru, postojanjem centralnom točkom nadzora i praćenja za čitavo stanovništvo jedne zemlje. Jednostavan način postizanja toga je korištenjem internetskih kolačića. (Gotze et.al., 2022.) Očekivalo bi se da to ne čine, s obzirom na to da iste te vlade provode inicijative protiv praćenja putem zakona poput GDPR. Međutim, situacija je složenija. Često se kolačići treće strane „neprimjetno“ uvlače putem uključenih veza na društvene mreže i video portale ili putem „besplatnih“ softverskih modula i okvira korištenih za razvoj web stranice ili usluge. (Gotze et.al., 2022.) Istraživanje koje je provedeno na više od 5.500 vladinih web stranica zemalja članica G20, fokusiralo se na vlasništvo i vijek trajanja kolačića korištenih na tim web stranicama. Istraživanje je otkrilo široko rasprostranjeno praćenje između 9% i 90% vladinih web stranica. Više od polovice kolačića na web stranicama pripada trećim

stranama, pri čemu mnogi od tih kolačića imaju vijek trajanja duži od jednog dana, a neki traju godinu ili duže. Jedan od argumenata je da se kolačići prve strane koriste za optimizaciju korisničkog iskustva, no nijedan stručnjak za privatnost ne bi podržavao dodavanje kolačića trećih strana na službene vladine web stranice (Gotze, et.al., 2022.)

Područje internetskog bankarstva zahtijeva visoku razinu sigurnosti kako bi se osigurala zaštita novčanih sredstava i zaštita podataka korisnika. Naime, bankovne informacije iznimno su osjetljive za većinu potrošača, koji ne žele da se te informacije dijele s drugim tvrtkama bez njihovog izričitog dopuštenja. Kako bi se analizirao način korištenja usluga trećih strana na portalima internetskog bankarstva, provedeno je istraživanje među njemačkim bankama, s fokusom na identifikaciju mjesta na kojima se treće strane uključuju na stranicama internetskog bankarstva, što se učitava te identifikaciju tih trećih strana (Macbeth, 2016). Rezultati istraživanja pokazuju da od 12 testiranih portala internetskog bankarstva, samo njih 5 nije proslijedilo podatke trećim stranama tijekom tipične internetske bankarske sesije. Nakon odjave, primijećen je najveći broj slučajeva praćenja, pri čemu polovica web mjesta šalje podatke velikim tvrtkama za praćenje i analitiku. Iz uobičajenih primjera korištenja usluga trećih strana mogu se zaključiti razlozi njihova korištenja i uključivanja na bankarskim stranicama kao što su:

- Analitika web mjesta; pružatelji usluga softvera kao usluge pružaju analitiku o korištenju web mjesta i njegovoj učinkovitosti.
- Marketing; tvrtke za oglašavanje pomažu klijentima, u ovom slučaju bankarskim stranicama, praćenje korisnike banke kako bi spriječile oglašavanje bankarskih proizvoda/usluga postojećim korisnicima ili kako bi uvidjele koliko novih korisnika određena marketinška kampanja privlači.
- Pouzdanost; tvrtke poput Verisign omogućuju svojim klijentima sigurnost, stabilnost i otpornost internetske infrastrukture;
- Alati za podršku; omogućuju bankama vanjsku pomoć putem sustava za online chat. (Macbeth, 2016).

Primjena ovih usluga izravno donosi prednosti bankama omogućujući im optimizaciju poslovnih procesa, smanjenju troškova te pružanju sofisticiranijih softverskih alata nego što bi bilo moguće razviti interno. Ipak, prisutni su i određeni rizici, posebice u pogledu sigurnosti i privatnosti korisnika. Banke su podložne visokim sigurnosnim zahtjevima, budući da su primarne mete prijevara i hakiranja. (Macbeth, 2016).

3. ZAKONSKE ODREDBE U SVRHU ZAŠTITE PRIVATNOSTI KORISNIKA

3.1. Zaštita privatnosti u Europskoj Uniji

Osobni podaci obuhvaćaju sve informacije koje se odnose na pojedinca, neovisno o tome jesu li vezane uz privatni, profesionalni ili javni život. Takve informacije uključuju, primjerice, osobno ime, fotografije, e-mail adrese, bankovne podatke, sadržaj objava na društvenim mrežama, medicinske informacije ili IP adresu računala. Prema Europskoj povelji o temeljnim pravima, svakom pojedincu zajamčeno je pravo na zaštitu osobnih podataka u svim aspektima života, bez obzira radi li se o privatnom prostoru, radnom okruženju, procesu kupovine, medicinskoj obradi ili internetskim aktivnostima (Commission proposes a comprehensive reform, 2012). Direktiva Europske unije o zaštiti podataka (Direktiva 95/46/EC), koju je Europska komisija usvojila 1995. godine, postavila je smjernice za zakonodavstvo o zaštiti podataka unutar EU-a. Temelji se na sedam načela „Preporuke Vijeća o smjernicama za zaštitu privatnosti i prijenos osobnih podataka“ od strane Organizacije za ekonomsku suradnju i razvoj (OECD). Stvorena 1980. godine, sedam načela uključuju:

- Obavijest – pojedinci bi trebali biti obaviješteni kada se njihovi osobni podaci prikupljaju;
- Svrha – korištenje osobnih podataka trebala bi biti ograničena na izričitu svrhu za koju su prikupljeni;
- Suglasnost – prije dijeljenja osobnih podataka s drugim stranama, potrebna je individualna suglasnost;
- Sigurnost – prikupljeni podaci trebaju biti zaštićeni od zloupotrebe;
- Informiranje – pojedinci bi trebali biti informirani tko prikuplja njihove podatke;
- Pristup – pojedinci bi trebali imati mogućnost pristupa svojim osobnim podacima i ispravljanja eventualnih netočnosti;
- Odgovornost – pojedinci bi trebali imati mehanizme osiguranja da se subjekti koji vrše prikupljanje podataka pridržavaju prethodno navedenih šest načela (Lord, 2017.)

Budući da je svaka od 27 država članica EU-a, kao i zemlje koje čine Europski ekonomski prostor neovisno je implementirala direktivu u nacionalno zakonodavstvo, postojale su manje razlike u zakonima i propisima o zaštiti podataka u svakoj od zemalja. Time, Opća uredba o zaštiti podataka (GDPR) (2016/679) usvojena je od strane Europskog parlamenta i Vijeća 25. svibnja 2018. godine, zamjenjujući prethodnu direktivu. Ova nova uredba imala je neposredan učinak u svim državama članica Europske Unije, time eliminirajući potrebu za daljnjom provedbom zakonodavstva (EU Data Protection Directive, n.d.).

Direktiva o e-privatnosti (2002/58/EC) uspostavljena je s ciljem rješavanja svih pitanja vezanih uz elektroničke komunikacije, podržavajući Direktivu o zaštiti podataka, te poboljšavajući sigurnost i transparentnost korisnika. Značajno je da je Direktivom o e-privatnosti uspostavljen zakon koji regulira kolačiće i tehnologije praćenja, koje su u to vrijeme bile praktički nekontrolirane (Ferraresi, 2023.) Međutim, kao i druge direktive Europske unije, ona nije obvezujući zakon sam po sebi, već uputa državama članicama EU-a da donesu vlastite zakone koji se usklađuju s direktivom, gdje je Republika Hrvatska postupila usvajanjem Zakona o elektroničkim komunikacijama. Direktiva o e-privatnosti usvojena je 2002. godine, zatim modificirana 2009. godine, a u skoroj budućnosti će biti zamijenjena Uredbom o e-privatnosti. Prvi prijedlog ove Uredbe objavljen je 10. siječnja 2017. godine, no konačni tekst još uvijek nije usvojen. Sveukupno gledano, Direktivu o e-privatnosti se može promatrati kao skup normi koje se usklađuju s prethodnom Direktivom o zaštiti podataka i aktualnom Općom uredbom o zaštiti podataka (GDPR), regulirajući nekoliko važnih pitanja, poput suglasnosti, povjerljivosti, neželjene pošte, kolačića i postupanja s podacima. Direktiva o e-privatnosti stekla je nadimak „zakon o kolačićima“ zbog toga što je njezin najzapaženiji učinak bio naglo povećanje pojavljivanja pop-up prozora za pristanak na kolačiće nakon njezinog stupanja na snagu. Ona nadopunjuje (i u određenim slučajevima premašuje) GDPR, obrađujući ključne aspekte o povjerljivosti elektroničkih komunikacija i praćenju korisnika putem interneta (Koch, n.d.).

Primarna kontaktna točka za pitanja vezanim uz zaštitu podataka jest Tijelo za zaštitu podataka (TZP) u svakoj državi članici Europske unije. TZP-ovi su neovisna tijela koja, putem svojih istražnih i korektivnih ovlasti, nadziru provedbu zakonodavstva o zaštiti podataka. Pružaju stručno savjetovanje u području zaštite podataka i rješavaju pritužbe koje proizlaze iz povreda Opće uredbe o zaštiti podataka i relevantnih nacionalnih zakona. Svaka država članica Europske unije ima jedno TZP (Što Su Tijela Za Zaštitu Podataka?, n.d.). Sukladno tome, na području Republike Hrvatske djeluje Agencija za zaštitu osobnih podataka (AZOP) koja je odgovorna za nadzor i provedbu zakona o zaštiti osobnih podataka.

3.2. GDPR i njegov utjecaj na upotrebu kolačića

Opća uredba o zaštiti podataka (GDPR) predstavlja najstrožu regulativu o privatnosti i sigurnosti na globalnoj razini. Iako je koncipirana i ratificirana od strane Europske unije, nameće obveze poduzećima diljem svijeta, ukoliko ciljaju ili prikupljaju podatke o građanima EU-a. S GDPR-om, Europa jasno pokazuje svoj čvrsti stav o privatnosti i sigurnosti podataka u trenutku kada sve veći broj ljudi povjerava svoje osobne podatke uslugama u „oblaku“, a povrede sigurnosti postaju svakodnevna pojava (Wolford, 2023). Obrada podataka obuhvaća širok spektar radnji koji se provode

nad osobnim podacima, bilo ručno ili automatizirano. Ukoliko pojedinac ili poduzeće provodi obradu podataka, obvezan je to činiti sukladno sedam načela zaštite i odgovornosti navedenih u članku 5.1-2:

- Zakonitost, poštenost i transparentnost obrade – obrada podataka mora biti zakonita, pravedna i transparentna prema subjektu podataka. Subjekt podataka predstavlja osoba čiji se podaci obrađuju.
- Ograničavanje svrhe – podaci se smiju obrađivati isključivo u legitimne svrhe koje su jasno navedene subjektu podataka prilikom prikupljanja.
- Smanjenje količine podataka (načelo minimizacije) – smije se prikupljati i obrađivati samo onoliko podataka koliko je apsolutno potrebno za navedene svrhe.
- Točnost – potrebno je održavati osobne podatke točnima i ažurnima.
- Ograničenje pohrane – osobne podatke se smije čuvati samo onoliko dugo koliko je neophodno za navedenu svrhu.
- Cjelovitost i povjerljivost – obrada mora biti obavljena na način koji osigurava odgovarajuću sigurnost, integritet i povjerljivost.
- Odgovornost – organizacije su odgovorne za mogućnost dokazivanja usklađenosti s GDPR-om u skladu sa svim navedenim načelima (Wolford, 2023).

Neosporno je da osobni podaci predstavljaju značajnu vrijednost. Podaci omogućuju razvoj poslovnih modela, stjecanje uvida u korisnike, provedbu učinkovitih marketinških kampanja te razvoj proizvoda i usluga. Međutim, nužno je odgovorno korištenje podataka temeljeno na općeprihvaćenim pravilima. U proteklih nekoliko godina svjedočilo se o povredama osobnih podataka i skandalima vezanim uz Facebook, eBay, Uber i dr. Opća uredba o zaštiti podataka (GDPR) ne samo da jasno ističe da osobni podaci pojedinca pripadaju tom pojedincu, već i prijeti ozbiljnim novčanim kaznama za poduzeća koji ne poštuju navedena pravila (GDPR Summary, n.d.). Kolačići se izravno spominju u stavci (30) GDPR-a u kojem se ističe da „*pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli, kao što su adrese internetskog protokola, identifikatori kolačića ili drugim identifikatorima poput oznaka za radiofrekvencijsku identifikaciju. Tako mogu ostati tragovi, koji se posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju*“ (Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća). Ono što se implicira ovim tekstom jest da kolačići, ukoliko se koriste za identifikaciju korisnika, spadaju u kategoriju osobnih podataka te su sukladno tome podložni odredbama Opće uredbe o zaštiti podataka.

Sukladno Direktivi o e-privatnosti i GDPR-u web stranice su dužne:

- Prije korištenja bilo kojih kolačića, osim onih koji su strogo nužni, zatražiti suglasnost korisnika;
- Prije nego što zatraže suglasnost, pružiti precizne i jasne informacije o podacima koje svaki kolačić prikuplja, kao i njegovu svrhu, na jasan i razumljiv način;
- Dokumentirati i pohraniti suglasnost korisnika;
- Omogućiti korisnicima korištenje usluge čak i ako odbiju korištenje određenih kolačića;
- Omogućiti korisnicima jednako jednostavno povlačenje svoje suglasnosti kao što je bio i postupak davanja suglasnosti (Koch, n.d.).

Ukoliko web stranica provodi obradu osobnih podataka putem web kolačića, dužna je transparentno obavijestiti posjetitelje putem jasno vidljive obavijesti, primjerice putem skočnog prozora ili bannera. Osim toga, na web stranici bi trebala biti objavljena obavijest o kolačićima, uz politiku privatnosti, koja pruža detaljne informacije o vrstama kolačića i njihovoj funkcionalnosti. Važno je istaknuti da traka ili banner koji se automatski prikaže s označenom opcijom „prihvaćam kolačiće“, bez mogućnosti odbijanja kolačića, nije u skladu s GDPR-om (Vodič o obradi osobnih podataka putem kolačića, n.d.).

3.3. Relevantni zakoni i regulative u drugim dijelovima svijeta

Nekoliko zemalja i regija izvan Europske unije donijelo je zakone i propise koji se odnose na privatnost, e-privatnost i web kolačiće. Među značajnijima su:

- PECR (The Privacy and Electronic Communications Regulations), poznat kao Zakon o privatnosti i elektroničkim komunikacijama, predstavlja britansku verziju europske Direktive o e-privatnosti. Slično Direktivi, PECR regulira elektroničke komunikacije na teritoriju Ujedinjenog Kraljevstva, obuhvaćajući aspekte poput marketinga putem raznih kanala, uključujući telefonske pozive, SMS poruke, e-poštu, te korištenje kolačića i alata za praćenje na web stranicama. Britanska verzija Opće uredbe o zaštiti podataka (GDPR), implementirana je nakon izlaska Ujedinjenog Kraljevstva iz Europske unije. U kontekstu poslovanja, britanski GDPR se primjenjuje na poslovne subjekte sa sjedištem u Ujedinjenom Kraljevstvu koji obrađuju osobne podatke na tom području, ali i na poslovne subjekte izvan Ujedinjenog Kraljevstva koji nude proizvode ili usluge stanovnicima Ujedinjenog Kraljevstva ili nadziru njihovo ponašanje na web stranicama (What is UK GDPR, n.d.).

- CCPA (California Consumer Privacy Act), poznat kao Kalifornijski zakon o privatnosti potrošača predstavlja sveobuhvatan zakon o privatnosti donesen od strane Kalifornije. Kalifornija je bila prva država koja je preuzela inicijativu u donošenju sveobuhvatnog zakonodavstva o zaštiti podataka u SAD-u i pruža stanovnicima Kalifornije kontrolu nad načinom na koji tvrtke koriste njihove osobne podatke (What is CCPA: A Quick Guide to Compliance, 2024). Nasuprot europskom GDPR-u koji zahtijeva od poduzeća dopuštenje za dijeljenje podataka i pruža pojedincima prava na pristup, brisanje ili kontrolu korištenja tih podataka, Sjedinjene Američke Države nemaju jedinstveni zakon koji regulira privatnost svih vrsta podataka. Umjesto toga, imaju mješavinu zakona koji su osmišljeni kako bi ciljali samo određene vrste podataka u posebnim (često zastarjelim) okolnostima (Klosowski, 2021).

3.4. Kazne i sankcije za kršenje zakona o privatnosti

S porastom učestalosti povreda podataka i briga o privatnosti, pridržavanje propisa pomaže organizacijama uspostaviti temelje zaštite i sigurnosti podataka. Nepoštivanje propisa može dovesti do ozbiljnih financijskih kazni i narušavanja reputacije. Time, usklađivanjem s GDPR-om, organizacije pokazuju predanost poštivanju prava pojedinaca i zaštiti njihovih osobnih podataka, time izgrađujući povjerenje kod klijenata i dionika (Understanding the Consequences, 2023). Posljedice kršenja GDPR-a mogu biti značajne. U prvoj godini primjene GDPR-a prijavljeno je više od 89.000 povreda podataka, što je rezultiralo kaznama u ukupnom iznosu od 56 milijuna eura. Organizacije koje ne poštuju propise GDPR-a suočavaju se s različitim sankcijama i kaznama. Najteža kazna je novčana kazna od 20 milijuna eura ili 4% godišnjeg prihoda organizacije. Osim novčanih kazni, organizacije mogu biti podvrgnute sankcijama poput privremenih ili trajnih zabrana obrade. Prema GDPR-u, kazne se određuju od strane nadzornih tijela za zaštitu podataka u svakoj državi članici Europske unije. Ta tijela određuju postoji li povreda i ozbiljnost povrede. Među najčešćim kršenjima su nedostatak dobivanja pristanka, povrede podataka, nedostaci u politikama zaštite podataka, neusklađenost s pravima subjekata, te kršenja koja se odnose na prijenos podataka izvan područje EU/EAA (Understanding the Consequences, 2023).

4. ZLOUPOTREBA KOLAČIĆA I SIGURNOSNI RIZICI

4.1. Rizici povezani s web kolačićima

4.1.1. Praćenje korisničke aktivnosti

Web praćenje se odvija preko različitih platformi, a uključuje kontinuiranu ekstrakciju i manipulaciju nad podacima u svrhu marketinških ili analitičkih aktivnosti. Naime, jedan od osnovnih ciljeva tvrtkama za oglašavanje jest akumulirati što veću količinu informacija o korisnicima kako bi im dostavili ciljane oglase (Cahn et.al., 2016). Problemu se može pristupiti kroz primjer uobičajenog korisničkog iskustva na webu, gdje se korisnik susreće sa oglasom tvrtke X na web stranici Y, što je obično povezano sa aktivnostima tvrtki za oglašavanje koje ih ciljano postavljaju. Ugrađen u kod navedenog oglasa nalazi se oznaka, usmjeravajući korisnički preglednik da uspostavi kontakt sa poslužiteljem tvrtke za oglašavanje i „povuče“ povezanu oznaku. Prilikom prvog dohvaćanja oznake, preglednik dohvaća i kolačić s nasumičnim ID-om. Taj kolačić služi kao mehanizam praćenja, omogućujući tvrtki za oglašavanje praćenje aktivnosti korisnika na različitim web stranicama. Nasumični ID u kolačiću djeluje kao jedinstveni identifikator pohranjen na korisničkom uređaju koji igra ključnu ulogu u prepoznavanju i praćenju aktivnosti korisnika dok se kreće webom. Svakim naknadnim posjetom drugim web stranicama koje prikazuju oglase od iste tvrtke za oglašavanje, preglednik šalje kolačić i ID skupa sa URL-om posjećene web stranice, što dovodi do sveobuhvatnog stvaranja profila korisnika (Mitchell & Khu-smith, 2001). Ti profili, koji odražavaju navike pregledavanja i interese, dovode do stvaranja ciljanih oglasa. Kako su se korisnici interneta navikli na online oglase, oglašivači su postali sve kreativniji u svojim marketinškim taktikama, razvijajući strategiju poznatu kao remarketing oglasa. Ova strategija im omogućuje prikazivanje oglasa na drugim web mjestima ako osoba pregleda određeni proizvod, ali ne izvrši kupnju. Cilj je podsjetiti ih da dovrše transakciju, a osnovna ideja jest da oglas cilja pojedince koji već pokazuju interes za proizvod. Umjesto da se određeni oglas prikazuje nasumičnim ljudima, retargetiranje oglasa prilagođava se onima koji pokažu interes, u nadi da će se vratiti (Fisher, 2023).

4.1.2. Profiliranje korisnika i personalizacija

Primarna svrha online profiliranja, od samih početaka, bila je bilježenje online ponašanja korisnika s ciljem generiranja ciljanog oglašavanja. Ciljano oglašavanje takve vrste u obzir uzima prethodno online ponašanje kako bi korisnicima predstavilo proizvode i usluge za koje se pretpostavlja da bi najvjerojatnije bili zainteresirani za kupnju (Bennett, 2011). Jedan od rasprostranjenih oblika profiliranja jest bihevioralno profiliranje koje funkcionira tako što prikuplja osobne podatke o korisničkom ponašanju na internetu, uključujući navike pregledavanja, pretraživanja i povijest

posjećenih web stranica. Takva vrsta profiliranja nastoji povećati relevantnost oglasa koji se prikazuju korisniku, temeljem prikupljenih podataka, s ciljem jačanja veze između marketinških napora i kupovnih navika (Bennett, 2011). Koncepcija online profiliranja prve strane omogućuje web stranici praćenje interakcija korisnika s istom. Uz pomoć web kolačića, web stranice su u mogućnosti nadzirati sadržaj koje korisnik pregledava, uz dodatne detalje kao što su vrijeme provedeno na pojedinoj stranici i stupnju izvršenja kupnje. Navedeni detalji korisnika se pohranjuju u bazu podataka, a služi kako bi web stranica prepoznala korisnika nakon svakog ponovnog posjeta stranici, omogućujući stranici da pruži relevantne preporuke i oglase prilagođene njihovim interesima (Simple Behavioral Advertising, 2009). S druge strane, online profiliranje trećih strana uključuje prikupljanje veće količine podataka od raznih operatera web stranica. Kada više operatera surađuje s oglašivačkim tvrtkama, odnosno trećim stranama, kako bi prodali prostor za oglašavanje, dopuštaju tim tvrtkama da postave vlastite web kolačiće na uređaje korisnika. To omogućuje trećoj strani praćenje ponašanja korisnika na više web stranica što dovodi do stvaranja jedinstvenog profila korisnika (Behavioral Advertising Across Multiple Sites, 2009). Prisutnost i identitet oglašivačke tvrtke na određenoj web stranici, postavljanje kolačića na računalo korisnika, praćenje kretanja korisnika i ciljanje oglasa jednostavno su nevidljivi u većini slučajeva. Neki su mišljenja da je ciljano oglašavanje inherentno nepravedno i obmanjujuće. Tvrde da je manipulativno te da se koristi slabosti potrošača kako bi stvorilo potražnju koja inače ne bi postojala te da kao rezultat toga, ciljano oglašavanje narušava autonomiju korisnika na internetu (Pitofsky et.al, 2000). Mnogi potrošači ističu da bi se njihove zabrinutosti zbog prikupljanja osobnih podataka za online profiliranje smanjile ukoliko bi ih se jasno obavijestilo o tome koje će podatke o njima biti prikupljene, kako će biti korištene, te da im se omogući jasni izbor za prihvaćanje ili odbijanje prikupljanja određenih osobnih podataka (Pitofsky et.al, 2000).

4.1.3. Podaci o lokaciji i identifikacija uređaja

Uz sveprisutnu uporabu internetskih usluga na mobilnim uređajima poput mobilnih telefona, postaje sve izvedivije pratiti i odrediti fizičku lokaciju potrošača putem GPS-a. Ta tehnološka mogućnost potiče porast profiliranja temeljenog na lokaciji, čime se ciljaju potrošači na temelju njihove trenutačne fizičke lokacije. Oglašivači mogu prilagoditi svoje ponude ovisno o lokaciji pojedinca u određenom trenutku, s ciljem povećanja relevantnosti i učinkovitosti oglasa (Privacy Impact, 2009). Primjerice, mogu se prikazati lokalne vijesti, oglasi ili ponude temeljene na regiji u kojoj se korisnik nalazi, s ciljem pružanja relevantnijih informacija koje su povezane s njihovim geografskim kontekstom. Iako se takvo oglašavanje čini praktičnim, može se također doživjeti kao nametljivim.

Briga oko privatnosti s oglašavanjem temeljenim na lokaciji proizlaze iz prikupljanja i korištenja podataka o lokaciji pojedinaca bez izričitog pristanka ili svijesti.

4.2. Sigurnosni rizici

4.2.1. Cross-site scripting (XSS) napadi

XSS (eng. *Cross-site scripting*) podrazumijeva mogućnost umetanja zlonamjernih podataka od strane napadača unutar ranjive web stranice. Spomenuti zlonamjerni podaci obično su sastavni dio pažljivo konstruiranog hiperlinka koji potencijalni napadač može umetnuti na svoju web stranicu ili unutar sadržaja elektroničke pošte, s ciljem da navede korisnika da ga aktivira. Kada legitimni web poslužitelj primi zahtjev za ranjivom stranicom putem takvog hiperlinka, popraćen s malicioznim podacima, rezultirajući HTML sadržaj bit će oblikovan kao valjana web stranica s legitimnog poslužitelja, ali koja će, unutar korisničkog preglednika, izvršiti zlonamjerni skriptni kod (Analiza XSS sigurnosnih propusta, 2006). Dakle, predstavlja napadačku tehniku koja web aplikaciju prisiljava da korisnikovom pregledniku proslijedi preoblikovani odgovor koji se zatim učitava i prikazuje. XSS napadi proizlaze uslijed nedovoljne provjere ispravnosti ulaznih podataka web aplikacije. Bilo koja web stranica koja dopušta korisnicima unos podataka može potencijalno biti pogođena XSS napadima. Ova vrsta ranjivosti često se javlja prilikom pretraživanja web stranica, ispunjavanja obrazaca na web stranicama, sudjelovanja na forumima i blogovima. Kada napadač uspije navesti web preglednik korisnika da izvrši manipulirani programski kod, taj kod će se izvoditi unutar tzv. sigurnosne zone web aplikacije. Korištenjem ovog pristupa, napadač može pristupiti i promijeniti osjetljive podatke dostupne u web pregledniku, poput krađe kolačića, usmjeravanja web preglednika na neke druge lokacije ili prosljeđivanje štetnog sadržaja iz druge web aplikacije (Provjera XSS i SQL Injection ranjivosti Exploit Me skupom alata, 2008). Posljedice zloupotreba XSS napada obuhvaćaju sljedeće scenarije:

- Korisnici mogu nesvjesno izvršavati zlonamjerni skriptni kod dok pregledavaju web stranice na temelju ulaznih podataka napadača;
- Napadač može preusmjeriti korisnika na proizvoljni zlonamjerni poslužitelj;
- Krađom korisničkih kolačića, napadač može preuzeti korisničku sesiju i zloupotrijebiti korisnikov identitet, mijenjati postavke računa ili iskorištavati druge potencijalne sigurnosne propuste na poslužitelju za koje inače nema ovlasti;
- Korisnici mogu nesvjesno izvršavati napadačev zlonamjerni skriptni kod unutar potencijalno nesigurnog web preglednika (Analiza XSS sigurnosnih propusta, 2006).

4.2.2. Cross-site request forgery (CSRF) napadi

Postoji širok spektar metoda koje se koriste za ugrožavanje sigurnosti web sjedišta, pri čemu se često radi o nedovoljnoj provjeri sadržaja koji se razmjenjuje između stranica i povezanost između sadržaja koji se prikazuje kao i koda koji upravlja prikazivanjem tog sadržaja. Jedna od takvih metoda, koja se oslanja na ovu specifičnu povezanost između sadržaja i koda u web programima, naziva se CSRF (eng. *Cross-Site Request Forgery*) napadi. Ova ranjivost proizlazi iz nedovoljne provjere zahtjeva za web sadržajem i samog sadržaja koji se učitava. Učitani web sadržaj može sadržavati zahtjeve za drugim web sadržajem i tako pokrenuti njihovo slanje iz korisničkog web preglednika. Ako su veze već uspostavljene između korisnika i drugog web odredišta, zloćudna stranica može iskoristiti podmukli zahtjev kako bi izvršila radnje u ime korisnika. Ako je veza s ranjivim odredištem već memorirana u web pregledniku, prilikom slanja zahtjeva s druge stranice, automatski će se koristiti odgovarajući autentikacijski kolačići za tu ranjivu domenu (CSRF napadi, 2010). CSRF ranjivost često je povezana s nesigurno oblikovanim web poslužiteljima i nedovoljno sigurnim radom web preglednika korisnika. CSRF napad cilja na web stranice koje se u interakciji s korisnicima i njihovom aktivnošću oslanja na poznavanje korisničkom identiteta. U CSRF napadu, identitet pošiljatelja zahtjeva se lažira tako što se potiče web preglednik korisnika da šalje HTTP zahtjeve u ime tog korisnika (CSRF napadi, 2010). Za izvođenje CSRF napada potrebni su određeni preduvjeti:

- Stranica koja je meta napada ne provjerava izvor poruke;
- Web preglednik korisnika omogućuje lažiranje HTTP Referer zaglavlja;
- Koristi se HTTP zahtjev koji može izmijeniti sadržaj na ciljanoj stranici ili korisničkom računu, kao što je promjena lozinke;
- Napadač ima pristup autentikacijskim kolačićima i sigurnosnim značkama koje omogućuju pristup ranjivoj stranici;
- Napadač je sposoban navesti žrtvu da otvori zloćudnu web poveznicu (CSRF napadi, 2010).

Izazovna karakteristika CSRF napada proizlazi iz činjenice da je u web pregledniku zadržana aktivna sesija prijave korisnika na ranjivu web stranicu. U takvim situacijama, zajedno s zahtjevom, web preglednik šalje autentikacijski kolačić koji omogućuje izvođenje zlonamjernog zahtjeva na ranjivoj web stranici u ime prijavljenog korisnika. Primjer ove vrste zlouporabe jest primjerice napad na internetsko bankarstvo i korisnički račun klijenta, gdje uspješna zlouporaba može rezultirati preusmjeravanjem novčanih transakcija s računa klijenta na račun napadača (CSRF napadi, 2010).

4.2.3. Cookie tossing napadi

Napad „cookie tossing“ je oblik napada na sigurnost web stranica koji se oslanja na manipulaciju web kolačićima kako bi izvršile zlonamjerne radnje. Temelji se na pružanju korisniku ranjive web stranice zlonamjernog web kolačića koji je dizajniran tako da izgleda kao da je došao s poddomene ciljane stranice. Ovo postaje posebno problematično kada ranjiva web stranica dopušta napadačima da smjeste poddomene pod svojim domenama. Kada korisnik posjeti ciljanu web stranicu, svi kolačići se šalju kako valjani tako i oni koji izgledaju kao da potječu s poddomena (Dodt, 2020). Ukoliko je napad uspješan, napadač može preuzeti sesiju korisnika i dobiti pristup korisničkom računu.

4.2.4. Napadi krađom korisničkih sjednica

Napadi krađom korisničkih sjednica (eng. session hijacking) događaju se kad napadač preuzima kontrolu nad ukradenom korisničkom sjednicom s ciljem ilegalnog pristupa podacima ili uslugama ili manipulacije podacima. U kontekstu računalnih mreža, pod pojmom sjednica podrazumijeva se postojana veza između klijenta i poslužitelja. Autorizacija korisnika obično se odvija prilikom stvaranja sjednice, što napadači sjednica iskorištavaju izvodeći napade tijekom same aktivne sjednice (Napadi krađom korisničkih sjednica, 2007). Napadi se mogu klasificirati prema razini na kojoj se izvode, bilo na mrežnoj ili aplikacijskoj razini. Napadi na mrežnoj razini uključuju presretanje i manipulaciju podatkovnim paketima, posebice na protokolima kao što su TCP (eng. *Transmission Control Protocol*) i UDP (eng. *User Datagram Protocol*) jer oni implementiraju korisničke sjednice. S druge strane, krađa sjednice na aplikacijskoj razini sastoji se od pribavljanja ID oznake HTTP sjednice koja je definirana unutar same aplikacije (Napadi krađom korisničkih sjednica, 2007). ID oznaka sjednice može se nalaziti ugrađena u URL oznaku koju aplikacija zaprima putem „HTTP GET“ zahtjeva, unutar polja formulara proslijeđenog aplikaciji ili u posebnim podatkovnim strukturama odnosno u web kolačićima. Napadač može pristupiti korisničkoj sjednici putem podataka spremljenih unutar web kolačića, a to može učiniti napadom na sam uređaj na kojem su pohranjeni ti podaci ili presretanjem poruka koje se šalju i primaju tijekom aktivne sjednice (Napadi krađom korisničkih sjednica, 2007).

4.2.5. Krađa identiteta

U prethodnim poglavljima spomenuti su sigurnosni rizici poput XSS napada, XSRF napada, cookie tossinga i napada krađom korisničkih sjednica, koji predstavljaju ozbiljnu prijetnju sigurnosti korisnika. Krađa identiteta, kao rezultat tih napada, istaknuta je kao jedan od najbrže rastućih zločina na internetu. Mnogi korisnici nisu svjesni obujma podataka koje dijele putem različitih internetskih usluga, niti činjenice da se ti podaci mogu lako povezati, što može dovesti do potencijalne krađe

identiteta. Kada bi se sve aktivnosti jednog korisnika na internetu agregirale – od online pretraživanja, komuniciranja, kupovine, pregledavanja, čitanja do dijeljenja informacija, postalo bi očito da korisnik otkriva potpunu sliku o sebi (A¨ımeur & Schonfeld, 2011).

5. BUDUĆI IZAZOVI U ZAŠTITI PRIVATNOSTI

5.1. Razvoj tehnologije i njegov utjecaj na privatnost

Razvoj tehnologije u digitalnom dobu donosi brojne prednosti, ali i izazove, posebno kada je riječ o zaštiti privatnosti korisnika. Neki od ključnih aspekata tehnološkog razvoja koji utječu na privatnost korisnika uključuju ulogu umjetne inteligencije, sigurnosni izazovi povezani sa Internetom stvari (eng. *Internet of Things*), potencijal blockchain tehnologije za zaštitu podataka te nadolazeće 5G mreže. Umjetna inteligencija (AI) više nije samo apstraktni pojam ili tehnološka inovacija usredotočena na robote. AI mijenja paradigmu digitalnog marketinga pružajući nove mogućnosti pretraživanja i pronalaženja informacija na internetu, interakcije s brendovima (primjer chatbotova) te pristupa informacija putem glasovnih pretraga (O'Brien, 2024). Međutim neki od nedostataka primjene umjetne inteligencije jesu osjetljivost i sigurnost podataka u slučajevima kada AI sustavi koriste ogromne količine podataka koji mogu sadržavati osjetljive informacije koje je važno sigurnosno obrađivati. Također se počinju javljati etičke dileme koje obuhvaćaju pitanja poput pristanka, manipulacije korisničkim podacima i ponašanjem te invazivne prirode hiper-ciljanih oglasa (O'Brien, 2024). Rast mrežno povezanih uređaja, poznatih kao „Internet stvari“ (IoT), otvara dosad neviđene mogućnosti kako za korisnike tako i za poslovne subjekte. Mnoge tvrtke ističu poboljšanja i efikasnost ostvarene uvođenjem IoT-a te predviđaju značajne koristi u godinama koje dolaze. IoT zaista ima potencijal poboljšati kvalitetu života, međutim, uređaji poput fitness tracker-a, osobnih kućnih asistenata i digitalnih aparata mijenjaju koncept privatnosti prenoseći podatke o širokom spektru ljudskih aktivnosti i ponašanja. Kako „pametno“ danas postaje uobičajeno svojstvo uređaja, korisnici sve više gube mogućnost nadzora i kontrole nad prikupljenim podacima te često imaju vrlo malo znanja o tome kako se njihovi podaci dalje koriste (Rosner & Kenneally, 2018.). Kao decentralizirani registar koja bilježi transakcije preko mreže računala, blockchain tehnologija onemogućuje izmjenu ili manipulaciju zabilježenim podacima (Lopez, 2024). Blockchain tehnologija je sustav za pohranu i prijenos podataka koji funkcionira na peer-to-peer (P2P) osnovi. Jedan od najznačajnijih prednosti blockchain tehnologije jest njezina sposobnost pružanja sigurne platforme za online transakcije. Transakcije se bilježe u decentraliziranoj mreži, što otežava hakerima neovlaštenu promjenu ili manipulaciju podacima. Razlog tome je što, jednom kada se blok podataka pridoda u blockchain, nije moguće modificirati ili brisati podatke bez koncensusa unutar mreže blockchain tehnologije. Također se može primijeniti i u osiguranju drugih vrsta online transakcija, poput razmjene osobnih podataka kao što su medicinski zapisi i osobni identifikacijski dokumenti i upravljanja digitalnim imovinama, što omogućava pojedincima kontrolu nad njihovim podacima i osigurava da se podaci pravilno koriste i

adekvatno rukuje (Lopez, 2024). „Peta generacija“ telekomunikacijskih sustava, poznata kao 5G, novi je globalni bežični standard koji omogućuje znatno veći podatkovni kapacitet i brzinu prijenosa. 5G usluge ključne su za širok raspon inovativnih aplikacija koje imaju potencijal transformirati brojne sektore gospodarstva i unaprijediti svakodnevni život građana, ali također donose određene rizike. U svojoj preporuci iz 2019. godine o kibernetičkoj sigurnosti 5G mreža, Komisija je upozorila da bi oslanjanje velikog broja ključnih usluga na 5G mreže moglo imati ozbiljne posljedice u slučaju većih kvarova (Tematsko Izvješće: Sigurnost 5G Mreža, n.d.). Povjerljivost i privatnost također mogu biti ugrožene jer telekomunikacijski operateri često eksternaliziraju pohranu svojih podataka vanjskim podatkovnim centrima. Postoji rizik da se navedeni podaci pohranjuju na opremi dobavljača 5G tehnologije u zemljama izvan EU-a, gdje razine pravne zaštite i zaštite podataka mogu biti različite u usporedbi s onima unutar EU-a (Tematsko Izvješće: Sigurnost 5G Mreža, n.d.).

5.2. Trendovi u praćenju i oglašavanju na internetu

Daljnji razvoj web kolačića bit će potaknut sve većom brigom za privatnost na internetu. Nakon rastuće zabrinutosti potrošača u vezi s privatnošću i u nastojanju da se udalji od kolačića treće strane, Google je odlučio u 2024. godini potpuno ukloniti kolačiće treće strane iz svog preglednika Chrome. Chrome je ograničio kolačiće trećih strana za 1% korisnika od 4. siječnja 2024. godine, a planira povećati ograničenja kolačića trećih strana za 100% u trećem kvartalu 2024. godine (Preparing for the End of Third-Party Cookies, n.d.). Čini se kako Google predvodi napore za okončanje upotrebe kolačića treće strane, što bi se na kraju moglo zamijeniti manje invazivnim rješenjima koja se mogu koristiti za ciljana oglašavanja. Google je predstavio planove i trenutno gradi „Privacy Sandbox“ koji ima za cilj biti manje invazivna alternativa kolačićima treće strane (The Privacy Sandbox, n.d.). Uklanjanje web kolačića moglo bi rezultirati smanjenjem učinkovitosti ciljanog oglašavanja i posljedično smanjenjem prihoda od oglasa, a može se očekivati porast korištenja alternativnih metoda poput kolačića prve strane ili fingerprintiga (The Evolution of Web Cookies, 2022). Također je vjerojatno da će doći do usvajanja modela oglašavanja koji više poštuju privatnost korisnika, poput kontekstualnog oglašavanja. Ovaj pristup podrazumijeva prikazivanje oglasa koji su relevantni za sadržaj koji korisnik trenutno pregledava na web stranici. Pruža prednosti poput poboljšane privatnosti i smanjenju ovisnosti o podacima koji su specifični za korisnika u usporedbi s bihevioralnim oglašavanjem (Cookieless Future, 2022). Nadalje, umjetna inteligencija (AI) i strojno učenje (ML) će odigrati ključnu ulogu u budućnosti web kolačića. S ograničenjima koja su nametnuta trećim stranama, AI algoritmi mogu se koristiti za personalizaciju korisničkih iskustava bez snažne ovisnosti o kolačićima (Cookieless Future, 2022).

5.3. Potencijalne promjene u regulativama i njihov utjecaj na upotrebu kolačića

U 2024. godini, poduzeća će se suočavati s novim prilikama i izazovima u području zaštite privatnosti, suočavajući se s još složenijim regulatornim okvirom koji nadilazi Opću uredbu o zaštiti podataka (GDPR). Nekoliko zakona donesenih u SAD-u tijekom 2023. stupit će na snagu 2024. godine, čime će se znatno povećati broj saveznih država s propisima o zaštiti privatnosti podataka. U Europskoj uniji, Direktiva o privatnosti i elektroničkim komunikacijama (ePD) je na snazi od 2018. godine, zajedno s Općom uredbom o zaštiti podataka (GDPR). Međutim, Uredba o privatnosti (ePR), koja bi zamijenila ePD, još nije stupila na snagu. Uredba o privatnosti bi, između ostalog, ustanovila jasnija pravila o korištenju kolačića i regulirala bi novije elektroničke komunikacijske usluge koje nisu obuhvaćene ePD-om, poput Whatsappa i Facebook Messengera. Međutim, s prijelaznim razdobljem od 24 mjeseca, ako i bude finalizirana 2024. godine, neće biti potpuno na snazi prije 2026. godine (Usercentrics, 2024). U međuvremenu, EU je donijela i druge zakone koji sadrže elemente zaštite privatnosti podataka u proteklim godinama, uključujući Zakon o digitalnim tržištima, a očekuje se da će se Zakon o umjetnoj inteligenciji finalizirati početkom 2024. godine (Usercentrics, 2024).

6. SVJESNOST KORISNIKA O WEB KOLAČIĆIMA

6.1. Definiranje problema istraživanja

S obzirom na sveprisutnost interneta u svakodnevnom životu, web kolačići su postali osnovni alat koji omogućava praćenje korisničkih aktivnosti, personalizaciju sadržaja i poboljšanju korisničkog iskustva na web stranicama. Međutim, dok web kolačići pružaju korisne funkcionalnosti, poput opcije „Zapamti me“ prilikom prijave na web stranicama, pamćenje stavki u košarici u e-trgovinama i mnogi drugi, postoji sve veća zabrinutost među korisnicima interneta u vezi s njihovom privatnošću i sigurnošću. Web kolačići također mogu i omogućiti pristup osjetljivim informacijama korisnika i stvaranju sveobuhvatnog profila u svrhu personaliziranog oglašavanja, remarketinga i sl. što rezultira povećanim osjećajem ranjivosti među korisnicima u pogledu privatnosti. Stoga se postavlja ključno pitanje: Jesu li korisnici informirani o svrsi i funkcionalnosti web kolačića? Koliko su korisnici svjesni utjecaja web kolačića na njihovu privatnost? Kako reagiraju na obavijesti o korištenju web kolačića na web stranicama? Smatraju li da postoji nedostatak transparentnosti i regulacije u vezi s web kolačićima?

6.2. Definiranje cilja istraživanja

Cilj ovog istraživanja je istražiti razinu svijesti korisnika interneta o web kolačićima, razumijevanju uloge i funkcionalnosti istih te njihovoj percepciji privatnosti na internetu. Osim toga, cilj je analizirati reakcije korisnika na različite primjere obavijesti o web kolačićima, one loše i dobre prakse privola o web kolačićima, njihove stavove o transparentnosti i regulaciji web kolačića te navike u upravljanju istima. Kroz ovo istraživanje želi se identificirati mogući nedostaci u razumijevanju web kolačića i sigurnosnim rizicima povezanim s njima. Ovo istraživanje je potaknuto prethodnim istraživačkim radovima koje su se bavile sličnim temama, uključujući diplomski rad autorice Ane Sertić iz 2022. godine na temu „Uloga HTTP kolačića u CRM-u i percepcija korisnika o prikupljanju i obradi osobnih podataka“, istraživanje provedeno od strane PricewaterhouseCoopers LLP (PwC) u suradnji sa Department for Culture, Media & Sport iz 2011. godine pod nazivom „Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework“ te rad autora Lakshmi Narayanan Jayakumara iz 2021. godine pod nazivom „Cookies 'n' Consent: An empirical study on the factors influencing of website users' attitude towards cookie consent in the EU“. Cilj ovog istraživanja je procijeniti moguće promjene u percepciji korisnika te identificirati nove trendove u vezi s upotrebom i sviješću o web kolačićima. Osim toga, anketa je imala i edukativnu svrhu, pružajući ispitanicima korisne informacije o svrsi web kolačića, njihovoj funkcionalnosti, dobrim i lošim praksama obavijesti o web kolačićima, brisanju web kolačića i

slično. Cilj je bio približiti tematiku svim ispitanicima te ih educirati o web kolačićima kako bi nakon odgovaranja ankete otišli sa širom i dubljom razinom znanja o toj temi. Napori su bili usmjereni na to da se koncept web kolačića što jednostavnije, slikovitije i interesantnije prenese ispitanicima. Primjerice, putem ilustracija objašnjena je svrha web kolačića, njihova uloga u personalizaciji korisničkog iskustva te načini na koje se koriste na različitim web stranicama. Osim toga, ispitanicima su ponuđene informacije o tome kako mogu upravljati web kolačićima, uključujući postupak brisanja istih. Pristupilo se temi na način koji je bio prilagođen različitim razinama poznavanja teme, s ciljem da se čak i onima koji su manje upućeni u tehničke aspekte internetskog sučelja omogući razumijevanje važnosti i utjecaja web kolačića na njihovo online iskustvo.

6.3. Metodologija istraživanja

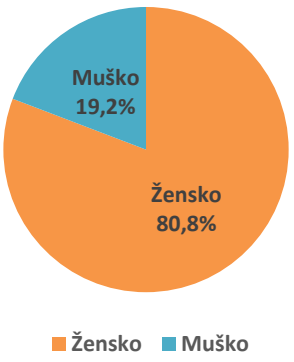
Anketno istraživanje provedeno je putem online obrasca među 224 ispitanika u razdoblju od 03.06. do 07.06.2024. godine. Anketni upitnik sastojao se od pitanja koja su obuhvatila demografske podatke ispitanika, učestalost korištenja interneta, zabrinutost zbog online privatnosti te njihovu percepciju i razumijevanje web kolačića. Također, ispitanici su bili upitani o svojim reakcijama na različite obavijesti o web kolačićima, stavovima o transparentnosti i regulaciji te navikama u upravljanju web kolačićima putem preglednika. Istraživanje je bilo potpuno anonimno i dobrovoljno, čime je osigurana privatnost ispitanika.

6.4. Rezultati istraživanja

6.4.1. Demografski podaci

Grafički prikaz 1.

Spol ispitanika

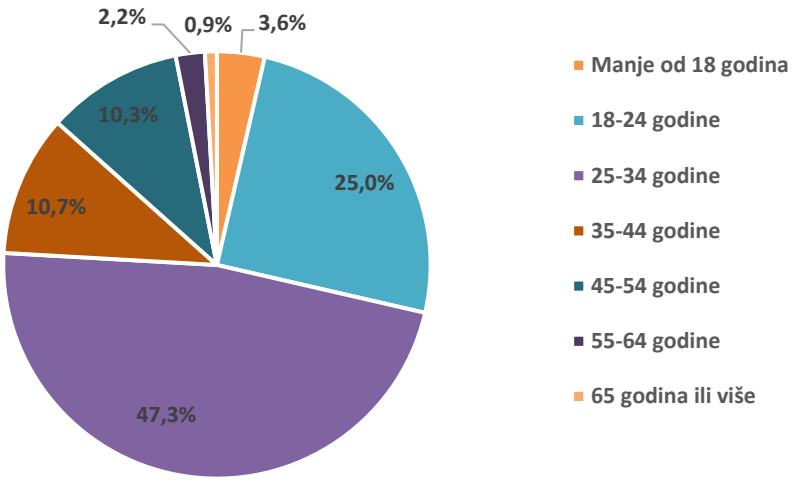


Prikaz autorice

Grafički prikaz 1. distribucije spola ispitanika prikazan je pomoću pie charta. Rezultati pokazuju da je 80,8% ispitanika ženskog spola (181 ispitanik), dok je 19,2% ispitanika muškog spola (43 ispitanika). Nadalje, na grafičkom prikazu 2. prikazana je dobna struktura ispitanika, u kojem najveći udio čine osobe u dobi od 25 do 34 godine, što čini 47,3% ispitanika (106 ispitanika). Slijede ih ispitanici u dobi od 18 do 24 godine, koji čine 25% ukupnog uzorka (56 ispitanika). Dobna skupina od 35 do 44 godine čini 10,7% ispitanika (24 ispitanika), dok ispitanici u dobi od 45 do 54 godine čine 10,3% (23 ispitanika). Manje su zastupljene dobne skupine: mlađi od 18 godina s udjelom od 3,6% (8 ispitanika), te ispitanici od 55 do 64 godine koji čine 2,2% (5 ispitanika). Najmanje su zastupljeni ispitanici stariji od 65 godina, koji čine 0,9% uzorka (2 ispitanika).

Grafički prikaz 2.

Dob ispitanika

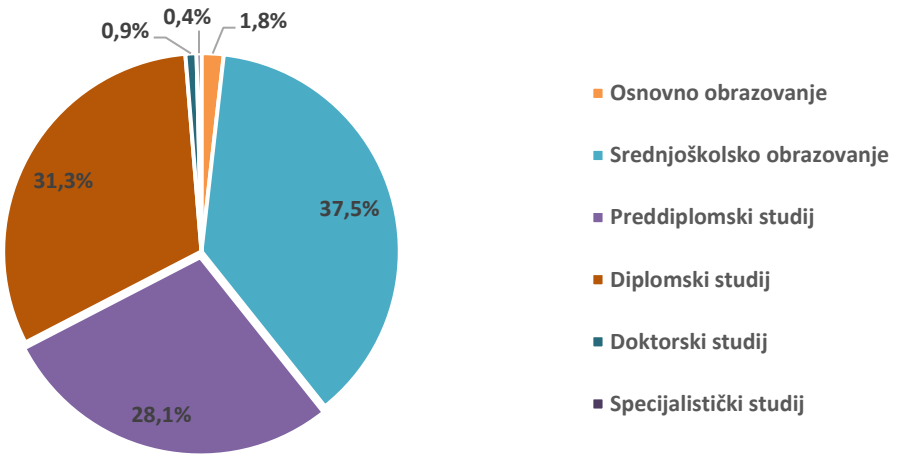


Prikaz autorice

Što se tiče najvećeg stupnja obrazovanja, Grafički prikaz 3. pokazuje da je najzastupljenija obrazovna skupina među ispitanicima ona sa srednjoškolskim obrazovanjem, koja čini 37,5% uzorka (84 ispitanika). Slijede ispitanici s diplomskim studijem, koji čine 31,3% (70 ispitanika), te oni s preddiplomskim studijem, koji čine 28,1% (63 ispitanika). Manji udio ispitanika ima osnovno obrazovanje, čineći 1.8% uzorka (4 ispitanika), dok 0,9% ispitanika (2 ispitanika) ima završeni doktorski studij. Najmanje su zastupljeni ispitanici sa specijalističkim studijem, koji čine 0,4% uzorka (1 ispitanik).

Grafički prikaz 3.

Najveći stupanj obrazovanja



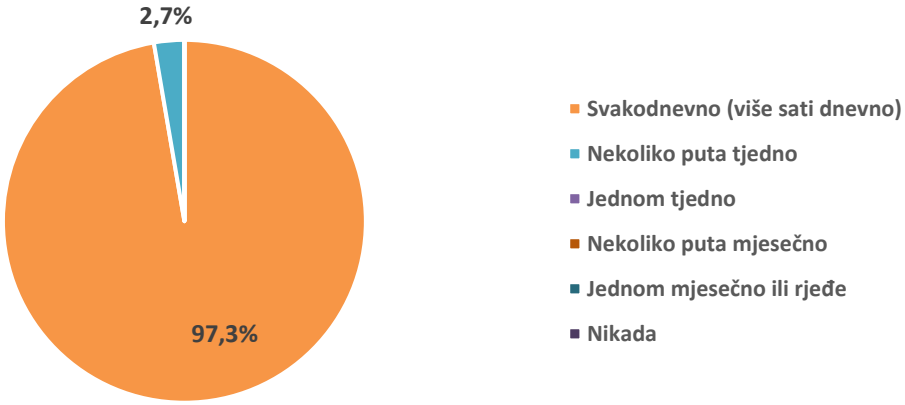
Prikaz autorice

6.4.2. Učestalost korištenja interneta

Rezultati iz Grafičkog prikaza 4. pokazuje da velika većina ispitanika koristi Internet svakodnevno (više sati dnevno), što čini 97,3% ispitanika (218 ispitanika). Preostalih 2,7% ispitanika, njih 6, koristi Internet nekoliko puta tjedno. Niti jedan ispitanik nije odabrao opcije „jednom tjedno“, „nekoliko puta mjesečno“, jednom mjesečno ili rjeđe“ ili „nikada“. Ovi rezultati jasno ukazuju na visoku razinu uporabe interneta među ispitanicima, što je u skladu s očekivanjima u suvremenom digitalnom dobu.

Grafički prikaz 4.

Učestalost korištenja interneta među ispitanicima



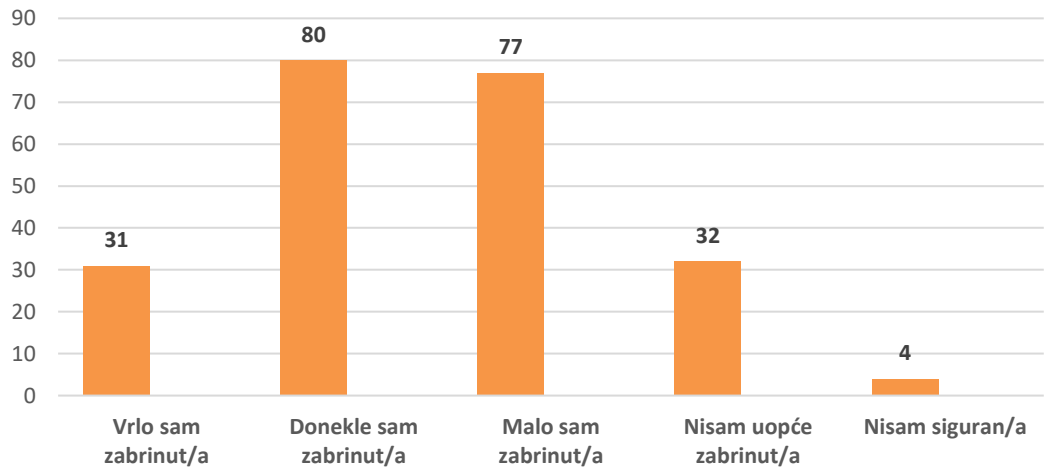
Prikaz autorice

6.4.3. Zabrinutost zbog online privatnosti

Rezultati anketnog pitanja vezano za zabrinutost zbog online privatnosti tijekom korištenja interneta pokazuju različite razine među ispitanicima. Od ukupno 224 ispitanika, 13,8% (31 ispitanik) je izrazilo da su vrlo zabrinuti zbog svoje online privatnosti. Donekle zabrinutih ispitanika ima 35,7% (80 ispitanika), dok je 34,4% (77 ispitanika) ispitanika izjavilo da su malo zabrinuti. Ispitanici koji nisu uopće zabrinuti čine 14,3% (32 ispitanika), a najmanji broj ispitanika, njih 1,8% (4 ispitanika) nije sigurno u svoj odgovor. Ovi rezultati upućuju na to da većina ispitanika iskazuje barem neki stupanj zabrinutosti zbog svoje online privatnosti, s time da gotovo polovica (49,5%) ispitanika pokazuje značajnu zabrinutost („vrlo zabrinuti“ ili „donekle zabrinuti“). Ova razina zabrinutosti može biti rezultat rastuće svijesti o sigurnosnim prijetnjama na internetu i značaju zaštite osobnih podataka (Grafički prikaz 5).

Grafički prikaz 5.

Stupanj zabrinutosti zbog online privatnosti na internetu među ispitanicima



Prikaz autorice

Ispitanici su u slijedećem anketnom pitanju trebali ocijeniti svoj stupanj suglasnosti (Potpuno se ne slažem/Ne slažem se/Neutralan/a/Slažem se/Potpuno se slažem) s dvije tvrdnje:

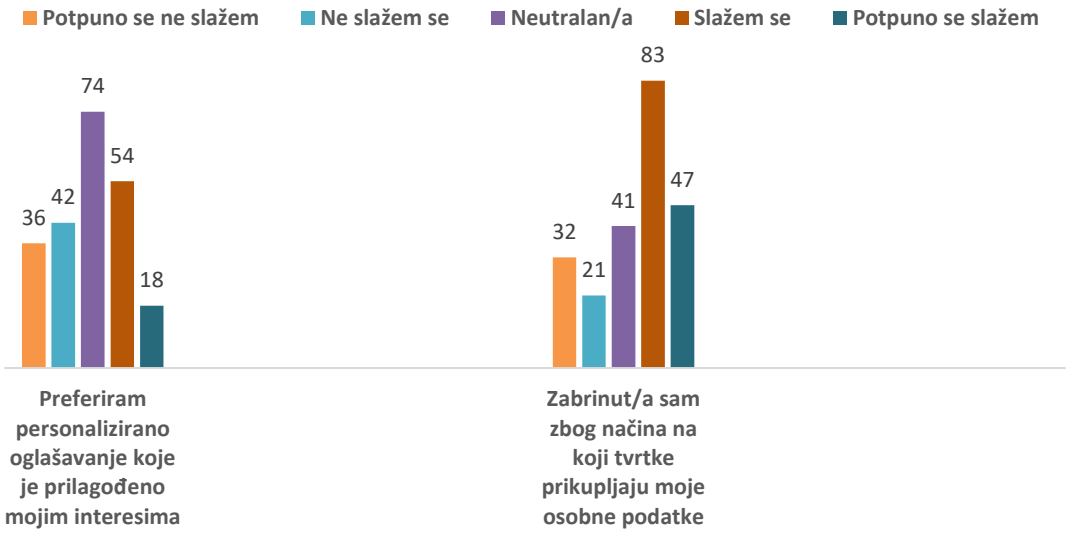
1. Preferiram personalizirano oglašavanje koje je prilagođeno mojim interesima
2. Zabrinut/a sam zbog načina na koji tvrtke prikupljaju moje osobne podatke

Namjera ovog dijela anketnog pitanja bila je ispitati balans između preferencija ispitanika za personaliziranim oglašavanjem i njihove razine zabrinutosti zbog načina na koji tvrtke prikupljaju osobne podatke. Budući da personalizirano oglašavanje zahtijeva određenu količinu osobnih podataka kako bi se učinkovito ciljalo korisnike, željelo se uvidjeti kako ispitanici percipiraju ovu

dinamiku između privatnosti i personalizacije. Rezultati za prvu tvrdnju pokazuju da se 16,1% ispitanika (36 ispitanika) potpuno ne slaže, 18,8% ispitanika (42 ispitanika) ne slaže, 33% ispitanika (74 ispitanika) je neutralno, 24,1% ispitanika (54 ispitanika) slaže se, dok se 8% ispitanika (18 ispitanika) potpuno slaže. Ovi rezultati ukazuju na raznolike stavove prema personaliziranom oglašavanju, s najvećim brojem neutralnih odgovora. Za drugu tvrdnju, rezultati pokazuju da se 14,3% ispitanika (32 ispitanika) potpuno ne slaže, 9,4% ispitanika (21 ispitanika) ne slaže se, 18,3% ispitanika (41 ispitanika) je neutralno, 37,1% ispitanika (83 ispitanika) slaže se, dok se 21% ispitanika (47 ispitanika) potpuno slaže. Ovdje rezultati jasno pokazuju značajnu razinu zabrinutosti među ispitanicima o načinu na koji tvrtke prikupljaju njihove osobne podatke, s ukupno 58,1% ispitanika koji su izrazili zabrinutost (slažu se ili potpuno slažu), što ukazuje na rastuću svijest i brigu o privatnosti na internetu. Navedeni rezultati prikazani su Grafičkim prikazom 6.

Grafički prikaz 6.

Stupanj suglasnosti s navedenim tvrdnjama



Prikaz autorice

6.4.4. Percepcija i razumijevanje web kolačića

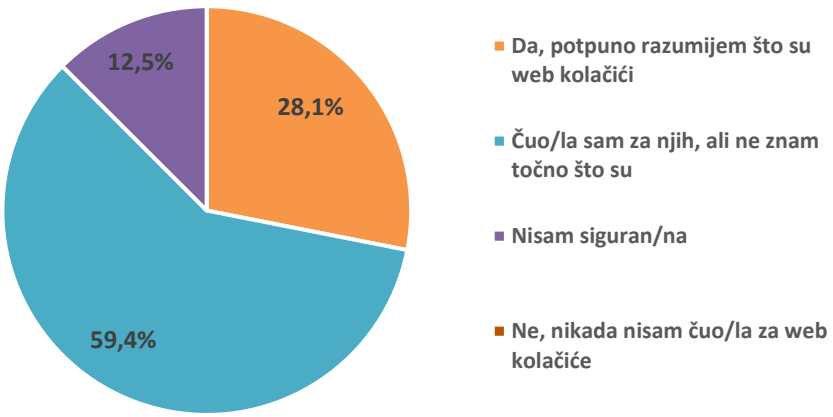
U ovom dijelu ankete fokus je bio na analizi razine upoznatosti ispitanika s pojmom web kolačića. Analiza dobivenih rezultata omogućuje dublji uvid u percepciju ispitanika i identificiranje eventualnih nedoumica ili nedostataka u njihovom razumijevanju. Nakon odgovaranja na pitanja o upoznatosti s pojmom web kolačića, ispravnosti izjava o web kolačićima te dodatnim svrhama web kolačića, u ovom dijelu ankete grafičkim prikazima se pokušalo dočarati pojam web kolačića, te njihove

funkcionalnosti. Time se ispitanicima omogućilo da nakon odgovaranja na set pitanja bolje razumiju koncept i nauče nešto novo.

Ispitanicima je predstavljeno anketno pitanje „Jeste li upoznati s konceptom web kolačića?“ a analiza odgovora je pružena putem grafičkog prikaza 7. Ispitanici su imali mogućnost odabrati jednu od četiri ponuđene opcije u skladu s njihovim poznavanjem web kolačića. Rezultati pokazuju da 28,1% ispitanika (63 ispitanika) potpuno razumije što su web kolačići, dok je većina, odnosno 59,4% ispitanika (133 ispitanika), čulo za njih, ali ne zna točno što su. Manji postotak ispitanika, 12,5% (28 ispitanika), nesigurno je u svoj odgovor. Značajno je primijetiti da nijedan od ispitanika nije izjavilo da nikada nisu čuli za web kolačiće. Rezultat ukazuje na to da postoji različita razina upoznatosti ispitanika s konceptom web kolačića, pri čemu većina ispitanika ima barem osnovno znanje o njima, međutim, znatan broj ispitanika još uvijek nije potpuno upoznat njihovom svrhom i funkcijom. Ovo je ključna točka za daljnje istraživanje, jer omogućuje identificiranje područja koja zahtijevaju dodatno obrazovanje i informiranje kako bi se osigurala veća svijest i razumijevanje među korisnicima interneta o važnosti i utjecaju web kolačića.

Grafički prikaz 7.

Upoznatost s konceptom web kolačića



Izrada autorice

U anketnom pitanju „Molimo označite odgovarajuću opciju za svaku izjavu o web kolačićima“, ispitanicima je prikazano nekoliko izjava o funkciji i svrsi web kolačića te smatraju li da je svaka od tih izjava točna ili netočna. Odgovori su sažeti u grafičkom prikazu 8., pri čemu su točni odgovori prikazani podebljano. Prva izjava „Web kolačići su male datoteke koje se pohranjuju na mom

računalu“ je točna. Od 224 ispitanika, 80 je ovu izjavu označilo ispravno, dok je 58 ispitanika označilo netočno, a 86 nije znalo odgovor. Druga izjava, „Web kolačići omogućuju brže prikazivanje web stranica“, netočna je, no 80 ispitanika je vjerovalo da je točna, dok je 79 ispitanika odgovorilo ispravno kao netočna, a 65 nije znalo odgovor. Treća izjava, „Web kolačići mi omogućuju automatsku prijavu bez potrebe za ponovnim unošenjem lozinke“, je točna. Ovdje je 69 ispitanika točno označilo ovu izjavu, dok je 78 ispitanika smatralo da je netočna, a 77 nije znalo odgovor. Četvrta izjava, „Web kolačići omogućuju personalizirano oglašavanje na temelju mojih prethodnih aktivnosti“, također je točna. Većina ispitanika (149) je prepoznala točnost ove izjave, dok je 17 ispitanika označilo netočno, a 58 nije znalo odgovor. Posljednja izjava, „Web kolačići se ne razlikuju od povijesti mog internetskog preglednika“, netočna je. Ovdje je 85 ispitanika ispravno označilo netočno, dok je 30 ispitanika smatralo da je točna, a 109 nije znalo odgovor.

Grafički prikaz 8.

Razina znanja ispitanika o web kolačićima

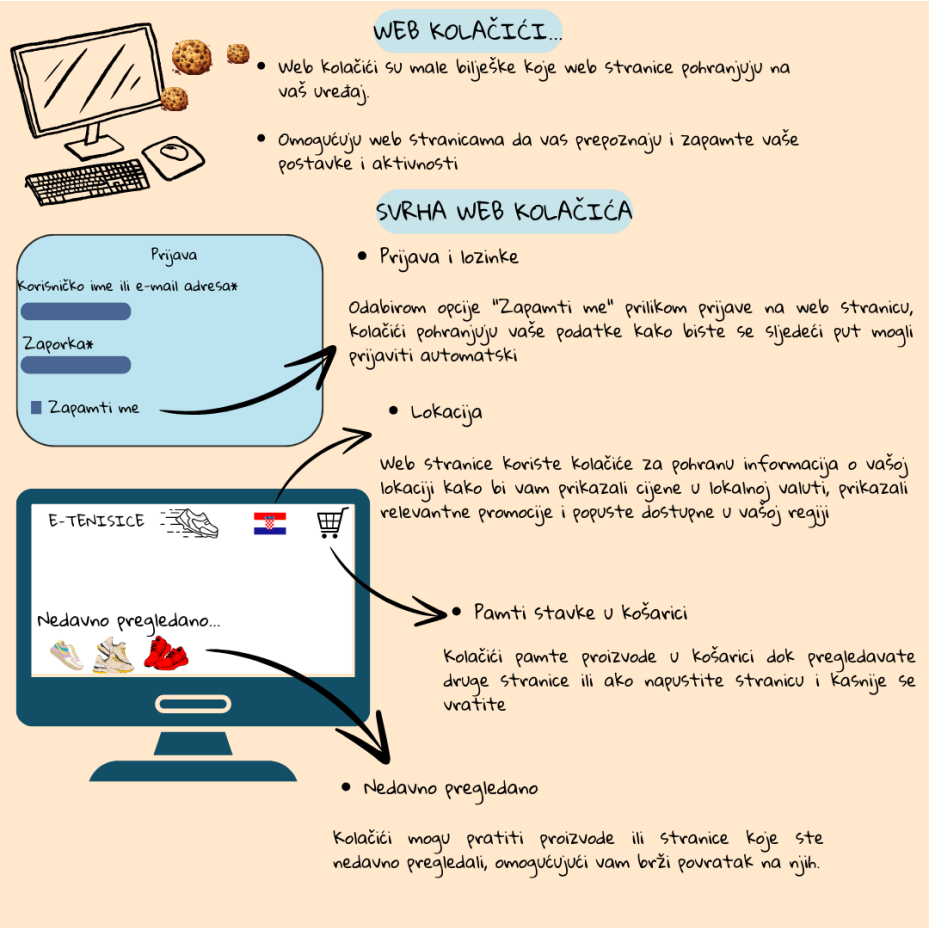
	TOČNO	NETOČNO	NE ZNAM
Web kolačići su male datoteke koje se pohranjuju na mom računalu	**80**	58	86
Web kolačići omogućuju brže prikazivanje web stranica	80	**79**	65
Web kolačići mi omogućuju automatsku prijavu bez potrebe za ponovnim unošenjem lozinke	**69**	78	77
Web kolačići omogućuju personalizirano oglašavanje na temelju mojih prethodnih aktivnosti	**149**	17	58
Web kolačići se ne razlikuju od povijesti mog internetskog preglednika	30	**85**	109

Izrada autorice

Ova analiza pokazuje da, iako neki ispitanici pokazuju dobro razumijevanje funkcija web kolačića, postoji značajan broj onih koji su nedovoljno informirani. Nakon odgovaranja različitih seta izjava o web kolačićima, ispitanicima je u slijedećem dijelu ankete prikazana ilustracija koja jednostavnim jezikom nastoji ilustrirati koncept web kolačića i neke osnovne funkcionalnosti koje donosi na Internet. Ilustracija koja je priložena u anketi je također priložena u nastavku (Grafički prikaz 9).

Grafički prikaz 9.

Pojam i funkcionalnost web kolačića



Autorski rad

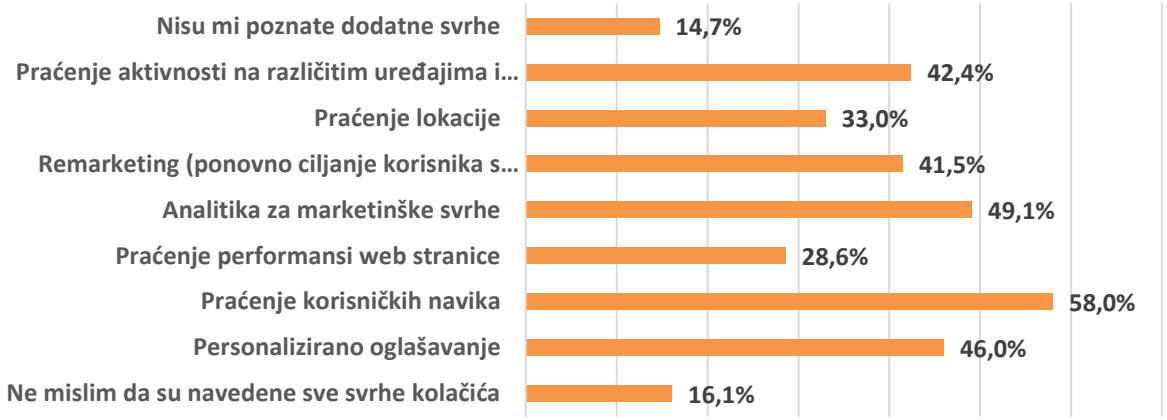
Nakon priložene ilustracije ispitanicima, postavljeno je drugo anketno pitanje koje je ispitivalo njihovo mišljenje o dodatnim svrhama web kolačića. Ispitanici su mogli odabrati sve relevantne opcije iz ponuđenih odgovora. Grafički prikaz 10. prikazuje navedene opcije i odgovore ispitanika.

Prema rezultatima, 58% ispitanika (130) smatra da web kolačići služe za „praćenje korisničkih navika“. Slijedi „analitika za marketinške svrhe“, koju je odabralo 49,1% ispitanika (110), dok je 46% ispitanika (103) odabralo „personalizirano oglašavanje“. „Praćenje aktivnosti na različitim uređajima i

platformama“ prepoznalo je 42,4% ispitanika (95), dok je „remarketing (ponovno ciljanje korisnika s oglasima)“ odabralo 41,5% ispitanika (93). Manji broj ispitanika, 33% (74 ispitanika), smatra da web kolačići imaju funkciju „praćenja lokacije“, dok 28,6% (64 ispitanika) vjeruje da kolačići služe za „praćenje performansi web stranice“. Samo 16,1% ispitanika (36 ispitanika) smatra da su sve svrhe web kolačića već navedene u prijašnjem grafičkom prikazu, a 14,7% (33 ispitanika) nije upoznato s dodatnim svrhama web kolačića. Ovi rezultati ukazuju na to da većina ispitanika prepoznaje višestruke funkcije web kolačića, osobito u kontekstu praćenja i analitike. Važno je naglasiti da su sve opcije koje su bile ponuđene ispitanicima točne.

Grafički prikaz 10.

Dodatne svrhe web kolačića

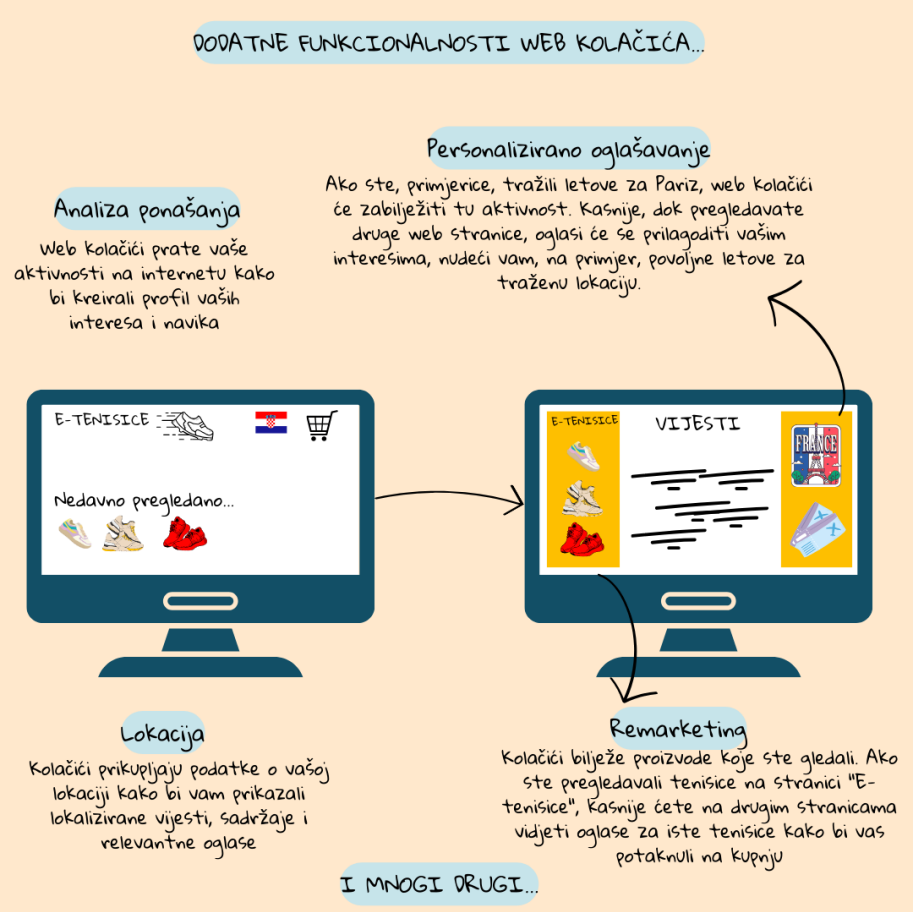


Izrada autorice

Nakon prethodnog anketnog pitanja, ispitanicima je prikazana ilustracija s ciljem da im se približe dodatne funkcionalnosti web kolačića, i time povećali svijesti o važnosti i načinu rada web kolačića. Ilustracija prikazana ispitanicima nalazi se u nastavku (Grafički prikaz 11).

Grafički prikaz 11.

Dodatne funkcionalnosti web kolačića



Autorski rad

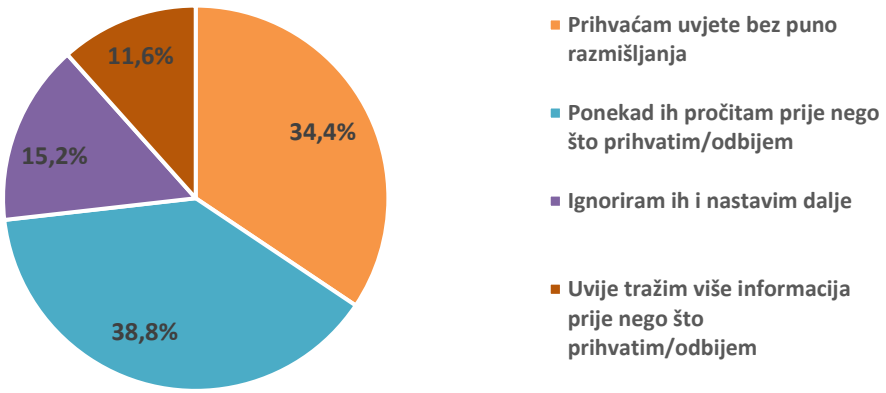
6.4.5. Reakcije na obavijesti o web kolačićima

U ovom odjeljku analizira se percepcija ispitanika o različitim obavijestima o web kolačićima na web stranicama. Cilj je bio istražiti prepoznaju li ispitanici dobru i lošu praksu obavijesti o web kolačićima, uključujući dizajn, vidljivost opcija kao što su „prihvaćam“ i „odbijam“, te navedene svrhe prikupljanja web kolačića (marketinške, nužne, analitičke, statističke). Kroz ovaj dio ankete ispitanici su ocjenjivali različite obavijesti o kolačićima, procjenjujući njihovu ispravnost. Ovaj odjeljak imao je i edukativni karakter, slično kao i prethodni. Nakon odgovaranja na set pitanja, ispitanicima su prikazani edukativni sadržaji koji pojašnjavaju zašto je određena obavijest o web kolačićima dobra ili loša praksa, s ciljem da se poveća njihovo razumijevanje i svijest o istima.

Prije prvog anketnog pitanja u ovom odjeljku ispitanicima je prikazan primjer obavijesti o web kolačićima na web stranici. Nakon toga uslijedilo je anketno pitanje o tome kako ispitanici generalno reagiraju na obavijesti o web kolačićima na web stranicama. Ovi rezultati pokazuju da je većina ispitanika svjesna obavijesti o web kolačićima, ali im pristupaju na različite načine. Značajan broj ispitanika, njih 38,8% (87 ispitanika) ponekad pročita obavijesti prije nego što donese odluku o prihvaćanju ili odbijanju, dok trećina njih, 34,4% ispitanika (77 ispitanika) prihvaća uvjete bez puno razmišljanja. Manji postotak ispitanika, 15,2% (34 ispitanika), obavijest ignorira i nastavi dalje, a 11,6% ispitanika (26 ispitanika) pokazuje visok stupanj svjesnosti i opreza, tražeći više informacija prije donošenja odluke (Grafički prikaz 12).

Grafički prikaz 12.

Reakcije ispitanika na obavijest o web kolačićima na web stranicama

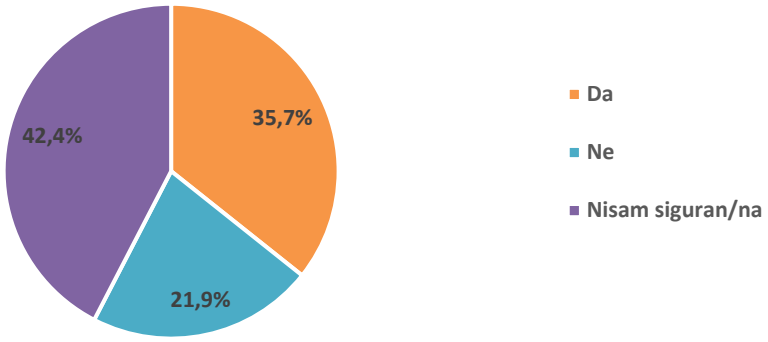


Izrada autorice

Sljedeće anketno pitanje uključivalo je grafički prikaz primjera obavijesti o web kolačićima, koji je zapravo primjer loše prakse. Ispitanici su upitani smatraju li navedenu suglasnost ispravnom. U ovom pitanju, od ispitanika se tražilo da detaljno istraže i pregledaju obavijest o web kolačićima te da uoče potencijalne greške. Rezultati su pokazali da 35,7% ispitanika (80 ispitanika) smatra suglasnost ispravnom, 21,9% ispitanika (49) smatra je neispravnom, dok se 42,4% ispitanika (95) izjasnilo kao nesigurno. Ovi rezultati ukazuju na značajnu razinu nesigurnosti i nepoznavanja među ispitanicima u pogledu ispravnih i neispravnih praksi u obavijestima o web kolačićima (Grafički prikaz 13).

Grafički prikaz 13.

„Smatrate li navedenu suglasnost ispravnom“

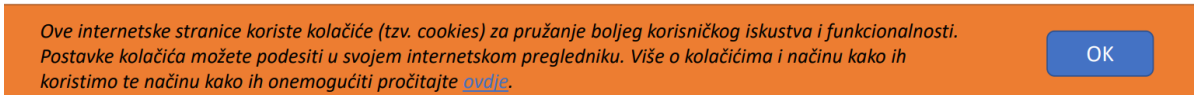


Izrada autorice

Nakon odgovora na navedeno pitanje, ispitanicima je ponovno prikazana ista obavijest o web kolačićima, ali sada s dodatnim informacijama u edukativnom obliku (Grafički prikaz 14). Objašnjeno je da je navedena obavijest primjer loše prakse, a razlog za to je što, kada korisnik klikne na poveznicu više informacija, otvara se stranica koja opisuje kolačiće i njihove svrhe, ali ne nudi mogućnost odabira skupina kolačića prema funkcionalnosti. Umjesto toga, korisnika se upućuje da postavke kolačića regulira putem svog preglednika, s uputama gdje pronaći daljnje informacije o podešavanju kolačića (Vodič o obradi osobnih podataka putem kolačića, n.d.).

Grafički prikaz 14.

Primjer loše prakse obavijesti o web kolačićima



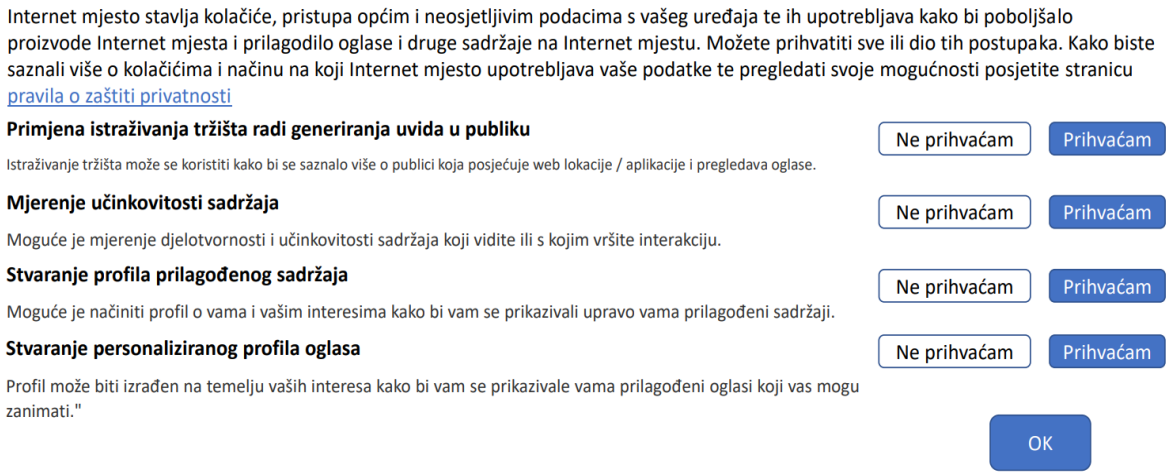
Izvor: AZOP, Vodič o obradi osobnih podataka putem kolačića - Agencija za zaštitu osobnih podataka

Ispitanicima je prikazan drugi primjer obavijesti o kolačićima, u kojem su jasno navedene svrhe prikupljanja kolačića, ali je gumb „Prihvaćam“ unaprijed odabran. Ovo predstavlja očiti primjer loše prakse obavijesti o prihvaćanju ili ne prihvaćanju kolačića. Iako obavijest sadrži kratko objašnjenje o tome koji se podaci prikupljaju i u koju svrhu te nudi mogućnost izbora za svaku skupinu kolačića, ovakva privola nije u skladu s europskim zakonodavstvom jer unaprijed odabrana opcija „Prihvaćam“ nije dopuštena. Prema zahtjevima za privolama, opcije ne smiju biti unaprijed odabrane (Vodič o

obradi osobnih podataka putem kolačića, n.d.). Privola koja je prikazana ispitanicima nalazi se u nastavku (Grafički prikaz 15).

Grafički prikaz 15.

Praksa unaprijed označene opcije „Prihvaćam“ u obavijesti o kolačićima

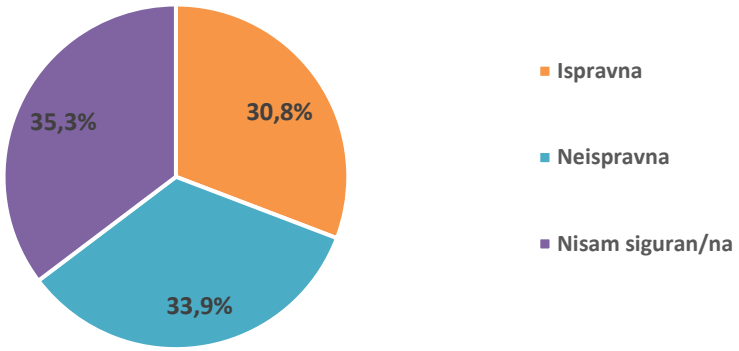


Izvor: AZOP, Vodič o obradi osobnih podataka putem kolačića - Agencija za zaštitu osobnih podataka

Rezultati na pitanje o tome kako ispitanici ocjenjuju praksu unaprijed označene opcije „Prihvaćam“ u obavijesti o web kolačićima pokazali su da je 30,8% ispitanika (69 ispitanika) ocijenilo ovu praksu kao ispravnu, dok je 33,9% ispitanika (76 ispitanika) ocijenilo kao neispravnu. Njih 35,3% (79 ispitanika) izjavilo je da nisu sigurni. Iako je trećina ispitanika prepoznala da unaprijed označena opcija „Prihvaćam“ predstavlja lošu praksu, gotovo jednako toliko ispitanika smatralo je tu praksu ispravnom. Navedeni rezultat ukazuje na potrebu za dodatnom edukacijom korisnika o pravilima i regulacijama vezanim uz privole za kolačiće, kako bi se povećala svijest o važnosti transparentnog postupanja s njihovim podacima (Grafički prikaz 16).

Grafički prikaz 16.

Percepcija ispitanika o praksi unaprijed označene opcije „Prihvaćam“

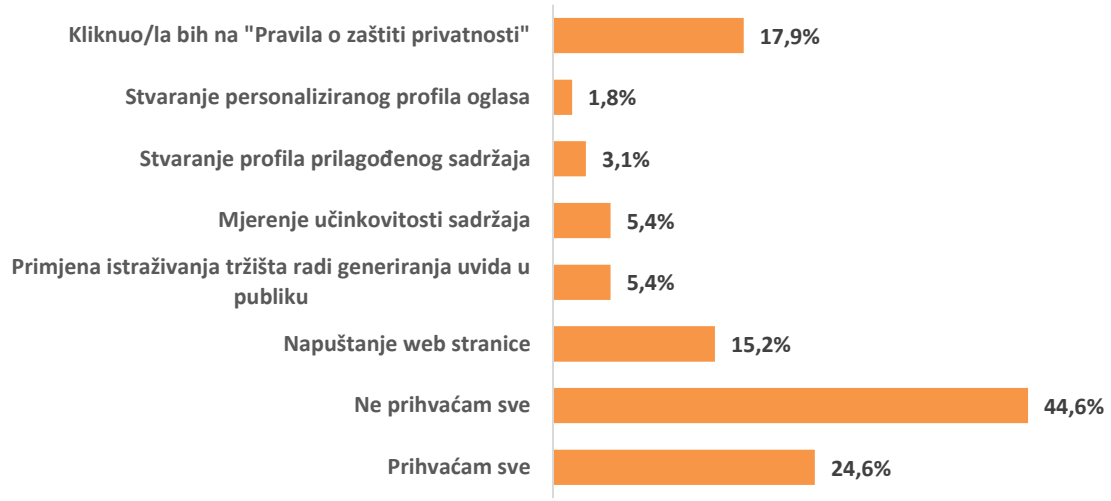


Izrada autorice

Nakon odgovora na prethodno anketno pitanje, ispitanicima je postavljeno pitanje koju bi opciju odabrali da im se navedena suglasnost prikaže na web stranici. Ispitanici su mogli birati jednu ili više opcija među osam ponuđenih. Najveći postotak glasova, 44,6%, odnosno 100 ispitanika, izjasnilo se da bi odabralo opciju „Ne prihvaćam sve“. Slijedi opcija „Prihvaćam sve“ s 24,6%, odnosno 55 ispitanika. Opciju „Pravila o zaštiti privatnosti“ odabralo bi 17,9% ispitanika (40 ispitanika), dok bi 15,2%, odnosno 34 ispitanika, napustilo web stranicu. Opcije „Primjena istraživanja tržišta radi generiranja uvida u publiku“ i „Mjerenje učinkovitosti sadržaja“ odabralo je po 5,4% ispitanika, odnosno 12 ispitanika za svaku. Opciju „Stvaranje profila prilagođenog sadržaja“ odabralo je 3,1% ispitanika (7 ispitanika), a najmanje glasova dobila je opcija „Stvaranje personaliziranog profila oglasa“ s 1,8%, odnosno 4 ispitanika (Grafički prikaz 17). Većina ispitanika preferira odbijanje svih kolačića, dok manji broj ispitanika bez razmišljanja prihvaća sve opcije. Također, značajan broj ispitanika traži dodatne informacije ili bi napustilo web stranicu, što pokazuje opreznost među ispitanicima.

Grafički prikaz 17.

Odabir opcija navedene u suglasnosti o web kolačićima



Izrada autorice

Nakon odgovora na prethodna dva anketna pitanja vezana uz istu obavijest o web kolačićima, ispitanicima je ponovno prikazana navedena obavijest, ali ovaj put s detaljnim objašnjenjem zašto je ta obavijest primjer loše prakse. Na taj način, pružene su im dodatne informacije kako bi bolje razumjeli zašto unaprijed označena opcija „Prihvaćam“ nije u skladu s europskim zakonodavstvom i kako takva praksa može utjecati na njihovu privatnost. U sljedećem anketnom pitanju također je korišten primjer obavijesti o kolačićima, u kojem opcija „Odbijam“ nije prikazana na transparentan niti jasan način kao opcija „Prihvaćam i zatvori“. Potrebno je kliknuti na „Saznajte više“ kako bi se web kolačići odbili ili kako bi odabrali koje kolačiće prihvatiti, a koje ne. Ova privola jasan je primjer loše prakse. Bitno je naglasiti da svaka web stranica mora omogućiti jednostavnu i lako dostupnu opciju za odbijanje web kolačića, jednako kao i za prihvaćanje. Opcije za prihvaćanje i odbijanje moraju biti jednako vidljive, međutim mnoge web stranice se koriste varljivim taktikama, kao što su boje i fontovi, kako bi se korisnike navelo na prihvaćanje web kolačića. Obavijest koja je prikazana ispitanicima nalazi se u nastavku (Grafički prikaz 18).

Grafički prikaz 18.

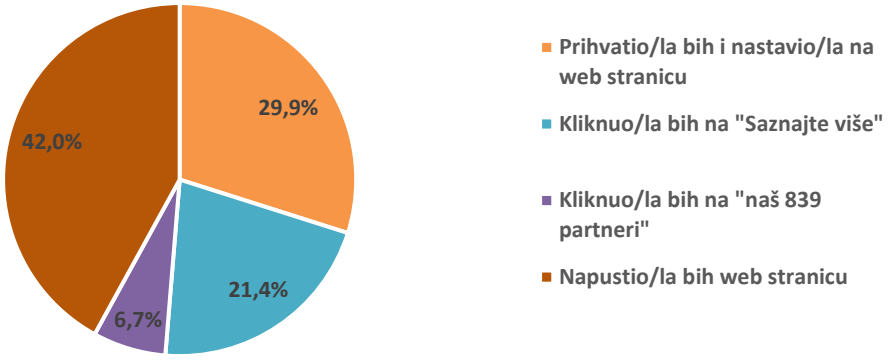
Primjer obavijesti o web kolačićima

Izvor: Jutarnji.hr, https://www.jutarnji.hr/

Ispitanicima je postavljeno anketno pitanje uz priloženu obavijest o kolačićima (Grafički prikaz 18.), tražeći da odgovore kako bi postupili u situaciji da se suoče s navedenom obaviješću na web stranici. Među ponuđenim opcijama 42% ispitanika (94 ispitanika) odgovorilo je da bi napustilo web stranicu, dok bi 29,9% ispitanika (67 ispitanika) prihvatilo web kolačiće i nastavilo na web stranicu. Nadalje, 21,4% ispitanika (48 ispitanika) kliknulo bi na „Saznajte više“, dok bi 6,7% ispitanika (15 ispitanika) kliknulo na „naš 839 partneri“. Navedeni odgovori prikazani su u grafičkom prikazu 19. Nakon toga, ispitanici su ocijenili povjerenje prema web stranici koja prikazuje ovu obavijest o web kolačićima. Rezultati pokazuju da je 48,7% ispitanika (109 ispitanika) odgovorilo sa „srednje“, 26,3% ispitanika (59 ispitanika) sa „nisko“, a 19,2% ispitanika (43 ispitanika) sa „vrlo nisko“. Manji broj ispitanika odgovorilo je s „visoko (4,9% ili 11 ispitanika) i „vrlo visoko“, njih 0,9% ili 2 ispitanika (Grafički prikaz 20). Većina ispitanika sklona je napustiti takve stranice ili tražiti dodatne informacije prije prihvaćanja kolačića, što naglašava važnost transparentnih obavijesti o web kolačićima.

Grafički prikaz 19.

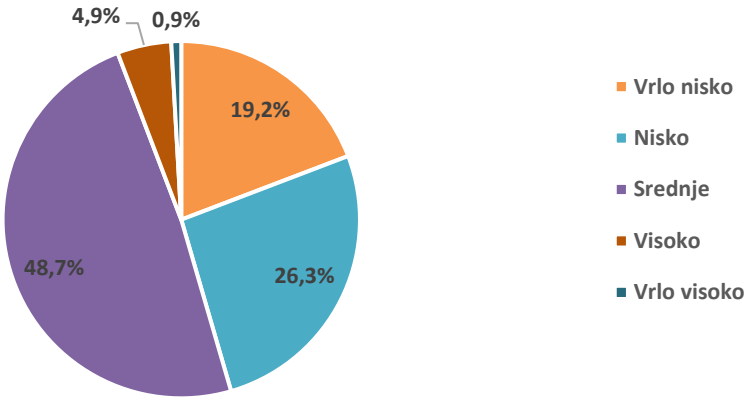
Postupak suočavanja s obavijesti o web kolačićima na web stranici



Izrada autorice

Grafički prikaz 20.

Povjerenje u web stranicu koja prikazuje navedenu obavijest

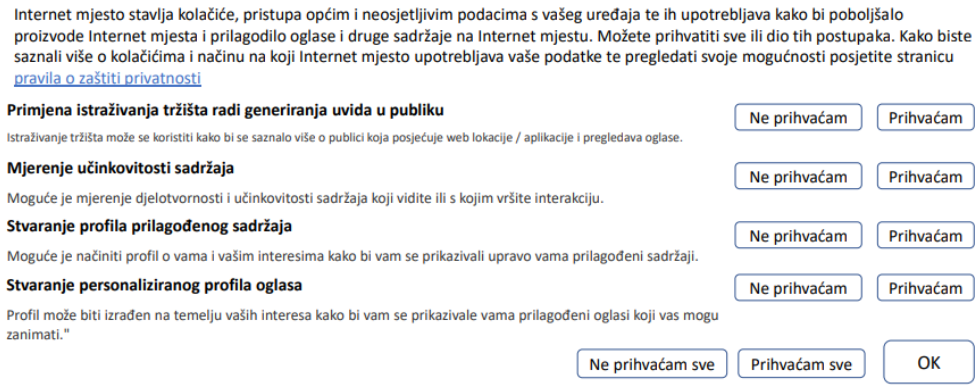


Izrada autorice

Slijedi posljednje anketno pitanje vezano uz primjere obavijesti o web kolačićima, u kojem je ispitanicima prikazan primjer dobre prakse obavijesti o web kolačićima (Grafički prikaz 21).

Grafički prikaz 21.

Primjer dobre prakse obavijesti o web kolačićima



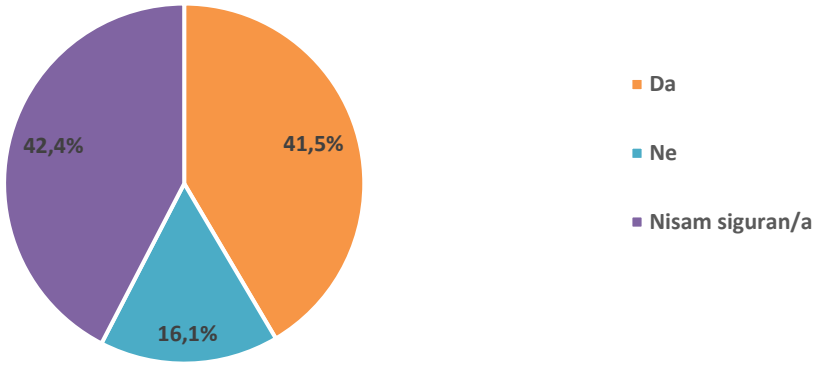
Izvor: AZOP, Vodič o obradi osobnih podataka putem kolačića - Agencija za zaštitu osobnih podataka

Ispitanicima je postavljeno pitanje smatraju li navedenu suglasnost ispravnom. Rezultati pokazuju da 41,5% ispitanika (93 ispitanika) suglasnost smatra ispravnom, a 16,1% ispitanika (36 ispitanika) suglasnost smatra ne ispravnom, dok je 42,4% ispitanika (95 ispitanika) nesigurno u svoj odgovor (Grafički prikaz 22). Iako značajan broj ispitanika prepoznaje primjer dobre prakse u obavijestima o web kolačićima, postoji značajan udio ispitanika koji su nesigurni ili ne prepoznaju u potpunosti elemente dobre prakse. Ispravne obavijesti ne samo da povećavaju povjerenje korisnika, već su i u skladu s europskim zakonodavstvom. Nakon navedenog anketnog pitanja, ispitanicima je prezentiran primjer dobre prakse obavijesti o prihvaćanju ili ne prihvaćanju web kolačića, uz popratno objašnjenje zbog čega privola predstavlja primjer dobre prakse:

- Jasno su objašnjeni podaci koji se prikupljaju i u koje svrhe;
- Detaljne informacije o obradi podataka dostupne u Pravilima o zaštiti privatnosti;
- Korisnik samostalno odlučuje o pristanku za svaki opseg podataka;
- Nema unaprijed definiranih opcija pristanka (Vodič o obradi osobnih podataka putem kolačića, n.d.).

Grafički prikaz 22.

Mišljenje ispitanika o ispravnosti obavijesti o kolačićima



Prikaz autorice

6.4.6. Stavovi korisnika o transparentnosti i regulaciji web kolačića

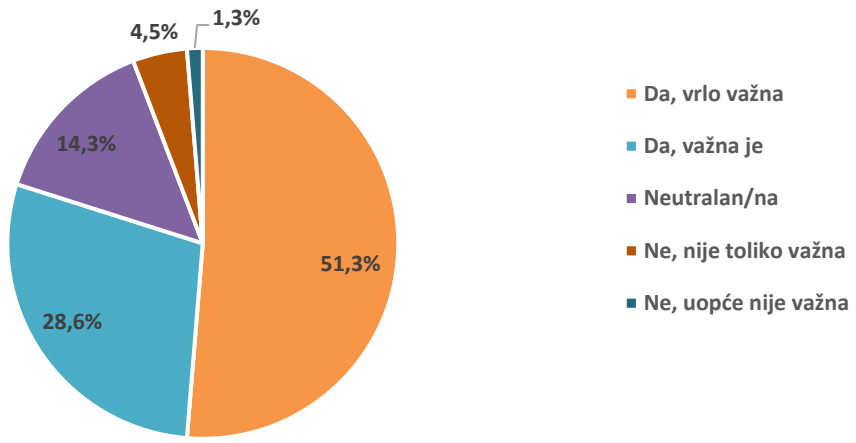
Ovaj segment ankete usmjeren je na ispitivanje stavova korisnika o transparentnosti i regulaciji web kolačića. Nakon prezentacije različitih primjera obavijesti o web kolačićima, uključujući primjere dobre i loše prakse, cilj je bio dobiti uvid u stavove ispitanika o transparentnosti i važnosti jasne komunikacije u vezi s web kolačićima. Također, istraživalo se smatraju li ispitanici da je potrebno strože zakonodavstvo za regulaciju korištenja web kolačića radi zaštite privatnosti korisnika te koje su njihove glavne brige u vezi s web kolačićima na internetu.

Jedno od ključnih anketnih pitanja ispitivalo je stav ispitanika o važnosti transparentnosti u vezi s web kolačićima za korisnike interneta. Rezultati su pokazali da većina ispitanika pridaje veliku važnost transparentnosti web kolačića: 51,3% (115 ispitanika) smatra da je transparentnost vrlo važna, dok 28,6% (64 ispitanika) smatra da je važna. Neutralan stav imalo je 14,3% ispitanika (32 ispitanika), dok se manji postotak od 4,5% (10 ispitanika) izjasnio da transparentnost nije toliko važna. Samo 1,3% ispitanika (3 ispitanika) smatra da transparentnost u vezi s web kolačićima nije uopće važna (Grafički prikaz 23). Ovi rezultati ukazuju na visoku svijest među ispitanicima o značaju transparentnih i zakonski usklađenih obavijesti o web kolačićima. Anketno pitanje je strateški postavljeno odmah nakon prikaza primjera dobre i loše prakse obavijesti o web kolačićima. Na taj način, ispitanici su mogli bolje razumjeti razliku između kvalitetne i neadekvatne obavijesti te donositi informirane

zaključke o važnosti transparentnosti u svakodnevnim susretima s web kolačićima na različitim web stranicama.

Grafički prikaz 23.

Stav ispitanika o važnosti transparentnosti i regulaciji web kolačića

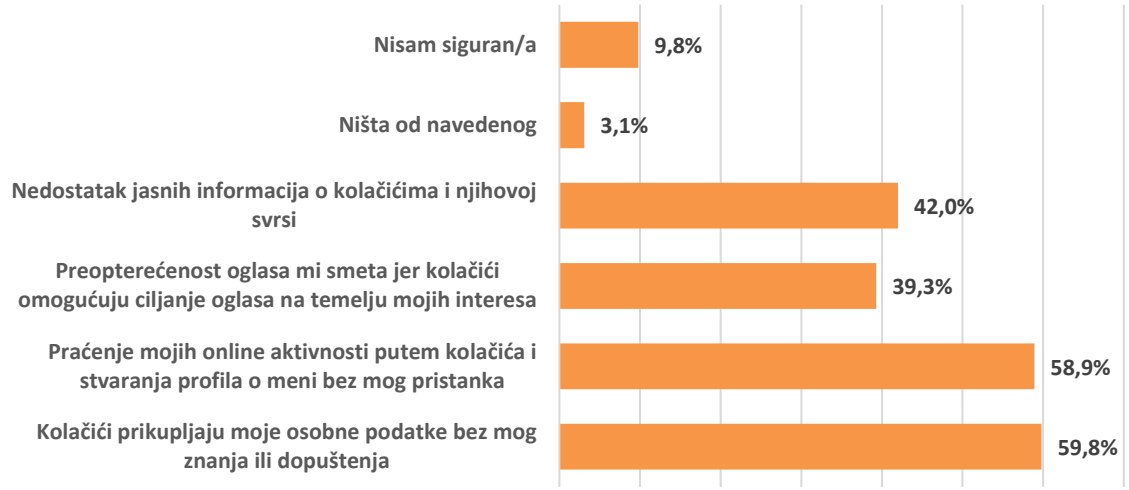


Izrada autorice

Ispitanicima je postavljeno pitanje o njihovim glavnim brigama u vezi s web kolačićima na internetu. Od ponuđenih šest opcija, ispitanici su mogli odabrati jednu ili više njih. Najviše odgovora dobile su dvije opcije: 59,8% ispitanika (134 ispitanika) zabrinuto je zbog prikupljanja njihovih osobnih podataka bez njihovog znanja ili dopuštenja, dok je 58,9% ispitanika (132 ispitanika) zabrinuto zbog praćenja njihove online aktivnosti i stvaranja profila o njima bez pristanka. Ovi odgovori jasno pokazuju stav ispitanika i njihovu svjesnost o tome kako web kolačići prate njihove aktivnosti i stvaraju profile za personalizirano oglašavanje i praćenje. Nadalje, 42% ispitanika (94 ispitanika) kao glavnu brigu navodi nedostatak jasnih informacija o web kolačićima i njihovoj svrsi, dok 39,3% ispitanika (88 ispitanika) brine preopterećenost oglasima, jer kolačići omogućuju ciljanje oglasa na temelju njihovih interesa. Manji postotak ispitanika, njih 9,8% (22 ispitanika), nije sigurno u svoj odgovor, dok samo 3,1% (7 ispitanika) smatra da nema nikakvih briga u vezi s web kolačićima (Grafički prikaz 24). Zabrinutost zbog neovlaštenog prikupljanja podataka i praćenja online aktivnosti naglašava potrebu za transparentnim i jasnim informacijama o web kolačićima. Također, prekomjerno oglašavanje dodatno povećava brigu ispitanika, što ukazuje na potrebu za strožim regulacijama i boljim praksama u vezi s upotrebom web kolačića.

Grafički prikaz 24.

Glavna briga ispitanika u vezi s web kolačićima na internetu

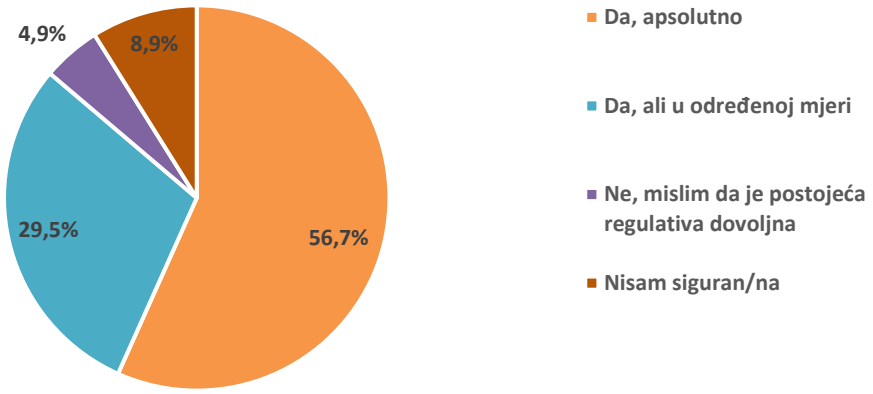


Izrada autorice

Ispitanici su upitani smatraju li da zakonodavstvo treba strože regulirati korištenje web kolačića na internetu radi zaštite privatnosti korisnika. Više od polovice ispitanika, njih 56,7% (127 ispitanika), smatra da je apsolutno potrebno strože regulirati korištenje web kolačića. Dodatnih 29,5% ispitanika (66 ispitanika) smatra da zakonodavstvo treba strože regulirati, ali u određenoj mjeri. Manji broj ispitanika, njih 8,9% (20 ispitanika) nije sigurno u svoj odgovor, dok 4,9% ispitanika (11 ispitanika) smatra da je postojeća regulativa dovoljna (Grafički prikaz 25). Postoji jasna percepcija među korisnicima da trenutne prakse često ne poštuju regulative i zakone o transparentnoj privoli i korištenju osobnih podataka. Navedeno naglašava potrebu za strožim zakonodavstvom, odnosno, uvođenjem Uredbe o e-privatnosti koja bi detaljno regulirala i postrožila pravila u vezi s obradom osobnih podataka putem web kolačića.

Grafički prikaz 25.

Potreba za strožom regulacijom radi zaštite privatnosti korisnika



Izrada autorice

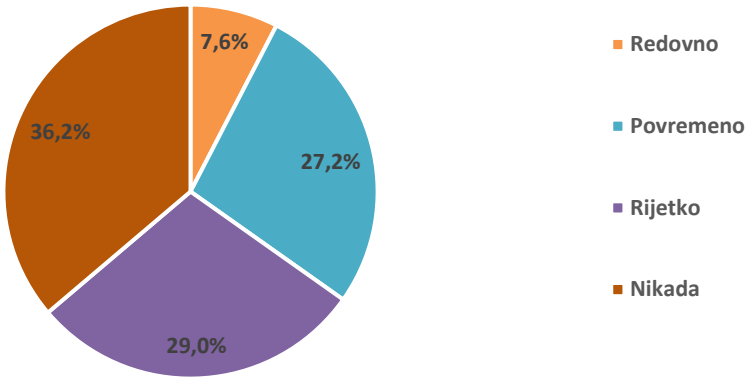
6.4.7. Navike i prakse korisnika u vezi s upravljanjem web kolačićima

Upravljanje web kolačićima važno je za očuvanje privatnosti korisnika i sigurnost pregledavanja interneta. Redovito brisanje kolačića može spriječiti praćenje online aktivnosti, smanjiti rizik od krađe identiteta i zaštiti osjetljive podatke. Brisanjem kolačića korisnici mogu imati veću kontrolu nad svojom privatnošću. Ovaj odjeljak ankete istražuje koliko često ispitanici upravljaju web kolačićima na svojim računalima, odnosno, koliko često ih brišu iz povijesti pregledavanja. Rezultati su pokazali da 36,2% ispitanika (81 ispitanik) nikada ne briše web kolačiće sa svog uređaja, 29% ispitanika (65 ispitanika) rijetko briše web kolačiće sa svog uređaja, 27,2% ispitanika (61 ispitanik) povremeno briše web kolačiće, dok samo 7,6% ispitanika (17 ispitanika) redovito briše web kolačiće sa svojih uređaja (Grafički prikaz 26). Ovi rezultati upućuju na to da mnogi korisnici nisu svjesni mogućnosti brisanja web kolačića ili ne vide potrebu za time, možda i zbog neinformiranosti o važnosti ovog postupka. Nakon odgovora na navedeno pitanje, ispitanicima je pružen kratak informativni dio o tome kako mogu obrisati web kolačiće sa svog preglednika, a koraci su slijedeći:

1. Otvoriti postavke preglednika;
2. Otvoriti odjeljak „Privatnost i sigurnost“;
3. Odabrati „Brisanje podataka o pregledavanju“ i unutar te opcije odabrati „Kolačići i ostali podaci o web lokacijama“, zatim odabrati opciju „Izbriši“.

Grafički prikaz 26.

Navika brisanja web kolačića sa uređaja



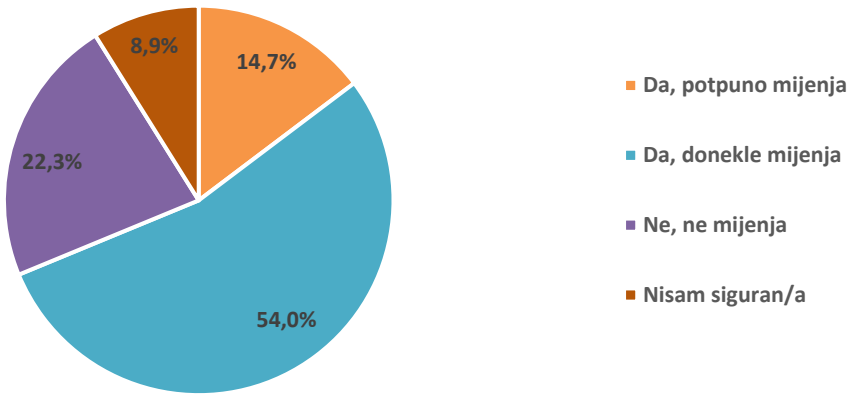
Izrada autorice

6.4.8. Utjecaj informacija o web kolačićima na korisničko ponašanje

Zadnji odjeljak ankete bio je posvećen evaluaciji trenutnog stava ispitanika prema web kolačićima. Nakon što su dobili detaljne informacije o funkcioniranju web kolačića, ispitanici su upitani mijenja li to njihov uobičajen način reagiranja na obavijesti o kolačićima u budućnosti, gdje više od polovice ispitanika, njih 54% (121 ispitanik), je izjavilo da donekle mijenja njihov način reagiranja na obavijesti o web kolačićima, dok je 14,7% ispitanika (33 ispitanika) izjavilo da potpuno mijenja njihov način reagiranja. Ovi rezultati ukazuju na to da je edukacija i informiranje ispitanika o web kolačićima imalo pozitivan utjecaj, potičući da budu pažljiviji i svjesniji prilikom prihvaćanja ili odbijanja web kolačića na web stranicama. Samo 22,3% ispitanika (50 ispitanika) izjavilo je da njihovo uobičajeno ponašanje neće biti promijenjeno, dok je 8,9% ispitanika (20 ispitanika) bilo nesigurno u vezi svog odgovora (Grafički prikaz 27).

Grafički prikaz 27.

Promjena načina reagiranja na obavijesti o kolačićima

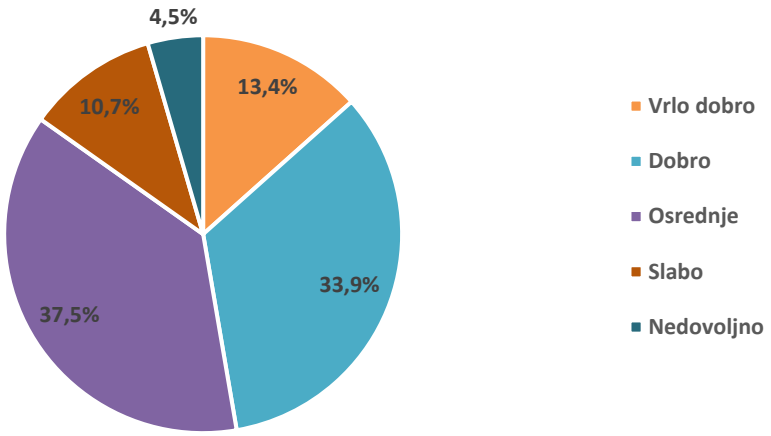


Izrada autorice

U posljednjem anketnom pitanju, ispitanici su trebali ocijeniti svoje vlastito znanje o web kolačićima nakon sudjelovanja u anketi, gdje je 37,5% ispitanika (84 ispitanika) ocijenilo svoje znanje kao „osrednje“, 33,9% ispitanika (76 ispitanika) smatra da je njihovo znanje „dobro“, dok 13,4% ispitanika (30 ispitanika) ocijenilo je svoje znanje sa „vrlo dobro“. Samo 10,7% ispitanika (24 ispitanika) smatra da je njihovo znanje „slabo“, dok 4,5% ispitanika (10 ispitanika) ocjenjuje svoje znanje kao „nedovoljno“ (Grafički prikaz 28). Navedeno anketno pitanje pokazuje značajan porast u samoprocjeni znanja ispitanika o web kolačićima nakon sudjelovanja u anketi. Mnogi ispitanici u početku ankete nisu bili potpuno svjesni što su web kolačići i kako funkcioniraju. Međutim, nakon što su prošli kroz različite odjeljke ankete koji su uključivali objašnjenja, slikovne prikaze te primjere, većina ispitanika osjeća da je njihovo razumijevanje poboljšano.

Grafički prikaz 28.

Ocjena vlastitog znanja o web kolačićima nakon sudjelovanja u anketi



Izrada autorice

6.5. Osvrt na rezultate istraživanja

Cilj ovog istraživanja bio je ispitati svijest korisnika o web kolačićima, procijeniti razinu razumijevanja korisnika o tome što su web kolačići, kako funkcioniraju i koja im je svrha, kao i istražiti koliko su korisnici svjesni prikupljanja osobnih podataka putem web kolačića te kako to utječe na njihovo povjerenje prema web stranicama. Rezultati ankete jasno pokazuju da je početna svijest korisnika o web kolačićima bila prilično ograničena. Na početku ankete, 59,4% ispitanika izjavilo je da su čuli za web kolačiće, ali nisu točno znali što su. Ovaj rezultat ukazuje na znatan deficit u osnovnom znanju o web kolačićima među korisnicima interneta. Kroz anketu, ispitanici su bili izloženi različitim vrstama obavijesti o web kolačićima, uključujući primjere dobre i loše prakse. Ovi primjeri su imali značajan edukativni učinak, što se odrazilo na njihove odgovore u kasnijim pitanjima. Nakon detaljne ankete, 54% ispitanika izjavilo je da će njihovo novo stečeno znanje donekle promijeniti njihov način reagiranja na obavijesti o kolačićima, dok je 14,7% ispitanika izjavilo da će potpuno promijeniti svoj pristup. Ovo jasno ukazuje na povećanu svijest i razumijevanje važnosti transparentnosti i regulacije web kolačića.

U vezi s prikupljanjem osobnih podataka putem web kolačića, 59,8% ispitanika izrazilo je zabrinutost da se njihovi osobni podaci prikupljaju bez njihovog znanja ili dopuštenja, dok je 58,9% ispitanika zabrinuto zbog praćenja njihovih online aktivnosti i stvaranja profila bez njihovog pristanka. Ovi rezultati pokazuju visoku razinu svijesti o potencijalnim rizicima povezanim s web kolačićima i

njihovim utjecajem na privatnost korisnika. Povjerenje korisnika prema obavijestima o web kolačićima na web stranicama, posebno onima s lošom praksom, također je bio važan aspekt istraživanja. Više od polovice ispitanika (56,7%) smatra da zakonodavstvo treba strože regulirati korištenje web kolačića kako bi se zaštitila privatnost korisnika. Ovaj stav dodatno je potkrijepljen time što je 41,5% ispitanika prepoznalo primjere dobre prakse obavijesti o web kolačićima kao ispravne, dok je 42,4% ispitanika ostalo nesigurno u svom odgovoru. Ovi rezultati ukazuju na jasnu potrebu za većom transparentnošću u načinu na koji web stranice koriste web kolačiće i za strožom regulacijom kako bi se povećalo povjerenje korisnika. U posljednjem dijelu ankete, ispitanici su procijenili svoje znanje o web kolačićima nakon sudjelovanja u istraživanju. Većina ispitanika, njih 37,5%, ocijenila je svoje znanje kao „osrednje“, dok je značajan dio ispitanika, njih 33,9% ocijenilo svoje znanje kao „dobro“. Manji postotak ispitanika, njih 13,4% ocijenilo je svoje znanje kao „vrlo dobro“. Ovi rezultati jasno pokazuju da je edukacija kroz anketu bila uspješna, povećavajući razumijevanje i svijest o web kolačićima među ispitanicima.

Sveukupno, rezultati istraživanja pokazuju da postoji značajan nedostatak početnog razumijevanja o web kolačićima među ispitanicima, ali također ukazuju na to da se kroz edukaciju može postići značajan napredak. Ovi rezultati mogu poslužiti kao smjernice za daljnje unaprjeđenje politika i praksi u vezi s web kolačićima, s ciljem bolje zaštite korisničkih podataka i prava na privatnost.

6.6. Ograničenja istraživanja

Kao i svako istraživanje, ovo istraživanje o svijesti korisnika o web kolačićima suočilo se s određenim ograničenjima koje treba uzeti u obzir prilikom interpretacije rezultata. Iako je uzorak ispitanika bio dovoljno velik za dobivanje preliminarnih uvida, nije nužno reprezentativan za cjelokupnu populaciju internetskih korisnika. Uzorak bi se mogao smatrati pristranim u smislu demografskih karakteristika kao što su dob, spol i obrazovanje, što može uvelike utjecati na rezultate. Nadalje, Internet i regulative vezane uz privatnost na internetu dinamično se mijenjaju. Rezultati ovog istraživanja predstavljaju stanje u trenutku provođenja ankete i možda neće biti jednako relevantno u budućnosti s obzirom na stalne promjene u tehnologiji. Međutim, unatoč ograničenjima, rezultati istraživanja pružaju vrijedne uvide u percepciju korisnika o web kolačićima i njihovom utjecaju na privatnost. Ova ograničenja nude smjernice za buduća istraživanja koji bi mogla koristiti veće i reprezentativnije uzorke, kombinirati kvantitativne i kvalitativne metode, te pratiti promjene u percepcijama korisnika u skladu s razvojem tehnologije i zakonodavstva.

7. ANALIZA UPOTREBE WEB KOLAČIĆA NA POPULARNIM WEB STRANICAMA

7.1. Definiranje problema istraživanja

Obrada osobnih podataka putem web kolačića u zakonodavnom okviru EU regulirana je Direktivom o privatnosti i elektroničkim komunikacijama te Direktivom o univerzalnim uslugama, koje su implementirane u Zakon o elektroničkim komunikacijama u Republici Hrvatskoj (Obrada Osobnih Podataka Putem Kolačića, n.d.). Navedeni Zakon zahtijeva da korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili pristup već pohranjenim podacima na uređajima korisnika bude dopušteno samo uz njihovu privolu. Privola mora biti dana nakon što su korisnici dobili jasne i potpune informacije o svrsi obrade podataka u skladu s propisima o zaštiti osobnih podataka (Obrada Osobnih Podataka Putem Kolačića, n.d.). GDPR definira privolu kao svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka. Za valjanost privole, ispitanici moraju biti dovoljno informirani u skladu s člankom 5. GDPR-a, koji zahtijeva transparentnost kao jedno od temeljnih načela (Obrada Osobnih Podataka Putem Kolačića, n.d.).

Unatoč tome, mnoge web stranice ne ispunjavaju ove zahtjeve u potpunosti. Obavijesti o kolačićima često su dizajnirane na način koji potiče korisnike da prihvate kolačiće bez dovoljno informacija ili jednostavne mogućnosti odbijanja. Neki od problema uključuju nedostatak jasnoće i transparentnosti, dizajn koji favorizira prihvaćanje kolačića, unaprijed označene opcije za prihvaćanje svih kolačića, skrivenim ili teško dostupnim opcijama za odbijanje kolačića i slično. Ovi problemi nisu specifični samo za međunarodne web stranice, hrvatske web stranice također pokazuju slične nedostatke. Mnoge hrvatske web stranice koriste slične taktike koje ne poštuju u potpunosti pravila o transparentnosti i informiranju korisnika, često favorizirajući prihvaćanje kolačića kroz obavijesti koje su zbunjujuće ili neprovidne.

7.2. Ciljevi istraživanja

Ovo istraživanje usmjereno je na prepoznavanje nedostataka u zaštiti privatnosti i osobnih podataka posjetitelja hrvatskih web stranica te se nastoji utvrditi koliko su hrvatske web stranice usklađene s relevantnim zakonodavstvom. Fokusira se na analizu „skočnih prozora“ za pristanak na web kolačiće kod 100 najpopularnijih web stranica sa hrvatskom domenom, klasificiranih u deset različitih kategorija (lifestyle, mediji i novinarstvo, financije, e-trgovina, zdravlje, obrazovanje, sport/klađenje, turizam, tehnologija, javne usluge). Specifični ciljevi istraživanja su:

1. Analizirati prisutnost jasnih obavijesti o korištenju web kolačića na web stranicama;
2. Ispitati da li obavijesti o web kolačićima uključuju opcije za prihvaćanje i odbijanje kolačića;

3. Procijeniti jednostavnost procesa odbijanja kolačića, uspoređujući ga s prihvaćanjem;
4. Utvrditi da li su opcije za prihvaćanje i odbijanje kolačića jednako vidljive i lako dostupne;
5. Provjeriti kategorizaciju i transparentnost kolačića prema svrsi obrade;
6. Utvrditi prisutnost unaprijed označenih opcija za prihvaćanje kolačića;
7. Provjeriti dostupnost i jasnoću politike privatnosti i kolačića na obavijestima o kolačićima.

Ova analiza će pružiti uvid u trenutnu praksu i razinu usklađenosti najpopularnijih hrvatskih web stranica s propisima o zaštiti osobnih podataka, te ponuditi preporuke za poboljšanje zaštite privatnosti korisnika.

7.3. Metodologija istraživanja

Detaljna dokumentacija vođena je putem Excel tablice. Web stranice su kategorizirane prema prethodno spomenutim kategorijama te je tablica sadržavala stupce s pitanjima koja su navedena u ciljevima istraživanja. Svaka tvrdnja odgovorena je sa jasnim „da“ ili „ne“ čime se osigurala jasnost i preciznost podataka. Prije svake posjete web stranici, web kolačići su brisani iz preglednika kako bi se osiguralo da nema preostalih podataka iz prethodnih sesija. Kriteriji analize temelje se na zahtjevima iz GDPR-a i Zakona o elektroničkim komunikacijama u RH koji naglašavaju transparentnost, razumljivost, jasnost, nedvosmislenost i dostupnost informacija o obradi podataka. Tijekom istraživanja koristilo se kvalitativnom i kvantitativnom metodom kako bi se osigurala detaljna i pouzdana analiza. Pomoću funkcija u Excelu izračunati su postotci odgovora za svako pitanje, a rezultati su prikazani grafički uz detaljan pregled dodatnih zapažanja i informacija zabilježenih tijekom istraživanja kako bi se olakšala interpretacija. Ručna analiza odabrana je kao primarna metoda, s obzirom na njezinu temeljitost i preciznost jer omogućuje osobno bilježenje specifičnih informacija i kontekstualno razumijevanje načina na koji se kolačići koriste i kako su obavijesti o kolačićima prezentirane posjetiteljima web stranica.

Kriterij za odabir najpopularnijih web stranica temelji se na mjerilu „popularnosti“ web stranica unazad dva mjeseca, od 1. travnja do 31. svibnja 2024. godine, što uključuje metrike poput broja posjeta i vremena provedenog na stranici. Ove metrike su dobivene pomoću alata SimilarWeb, Semrush i Ahrefs. Ovi alati pružaju detaljne informacije o prometu na web stranicama, što uključuje broj posjeta, vrijeme provedeno na stranici, te druge metrike relevantne za procjenu popularnosti web stranica.

7.4. Rezultati istraživanja

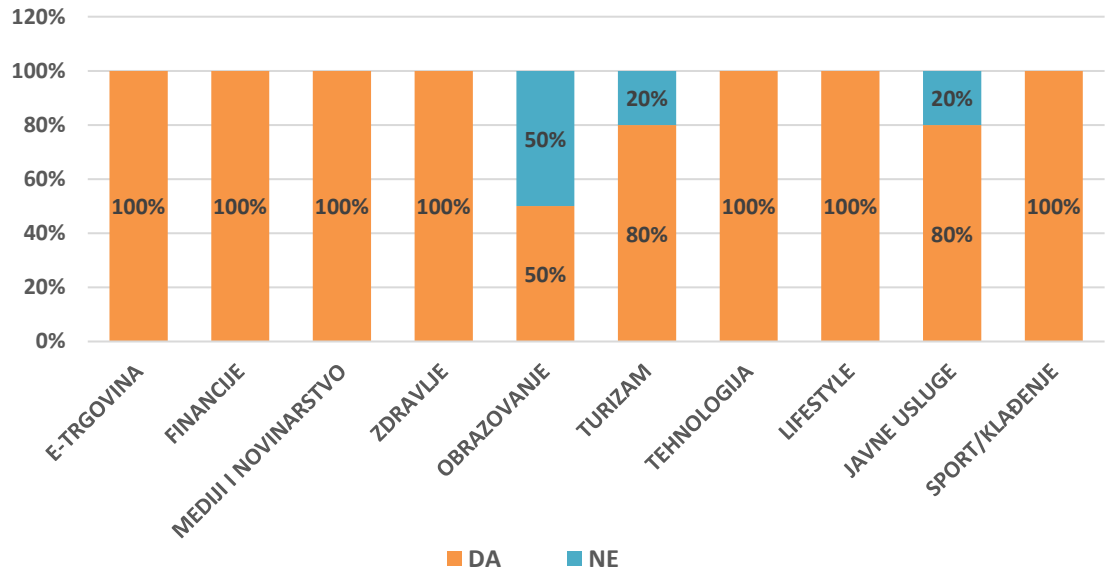
7.4.1. Prisutnost obavijesti o web kolačićima

U ovom odjeljku istražuje se prisutnost jasnih obavijesti o korištenju web kolačića na 100 najpopularnijih hrvatskih web stranica. Analiza je provedena kako bi se ustanovilo koliko su navedene web stranice usklađene sa lokalnim zakonodavstvom i GDPR-om, koje zahtijevaju jasnu i transparentnu komunikaciju prema posjetiteljima o prikupljanju i korištenju web kolačića.

Analiza je pokazala da od ukupnog broja web stranica (100), velika većina web stranica, odnosno 91 web stranica pruža jasne obavijesti o korištenju web kolačića, dok 9 web stranica još uvijek nema jasnu obavijest o kolačićima, što podrazumijeva da ne ispunjavaju zakonske zahtjeve. Grafičkim prikazom 29. prikazan je postotak po kategorijama web stranica.

Grafički prikaz 29.

Prisutnost obavijesti o web kolačićima na web stranicama



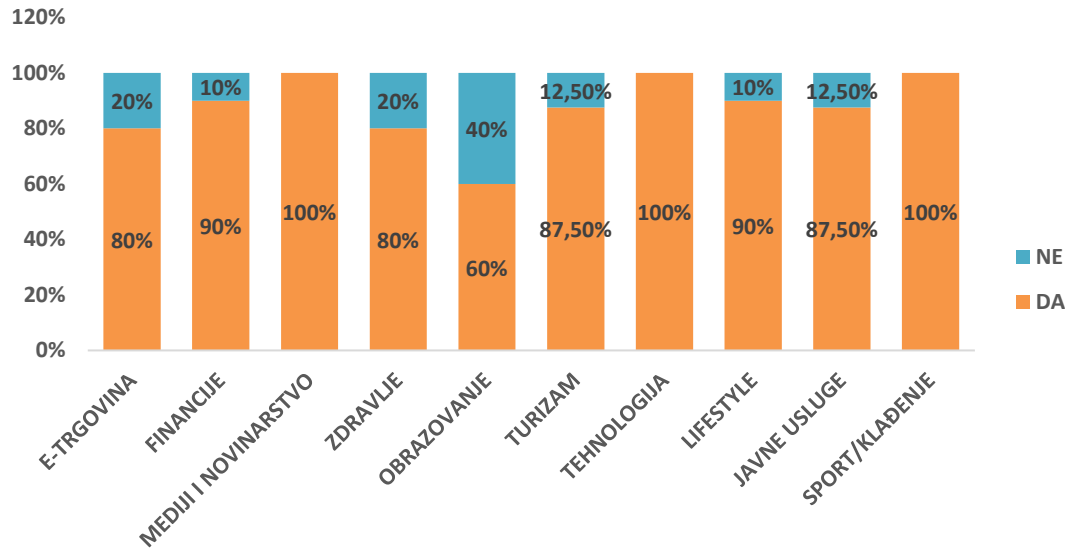
Prikaz autorice

7.4.2. Opcije za prihvaćanje i odbijanje web kolačića

U ovom poglavlju analizira se prisutnost opcije na obavijesti o web kolačićima koje omogućuju posjetiteljima web stranice da prihvate ili odbiju kolačiće. Fokus je na osnovnoj prisutnosti opcija za odbijanje kolačića, bez detaljne analize njihove praktične primjenjivosti ili vidljivosti, što će se dalje istraživati u kasnijim dijelovima istraživanja. Kriterij je postavljen tako da se svaka opcija koja omogućuje posjetiteljima da odbiju kolačiće smatra pozitivnim odgovorom (DA), bez obzira na broj koraka odnosno klikova potrebnih da bi se došlo do te opcije. Primjeri uključuju opcije poput „Upravljanje opcijama“, „Saznajte više“ gdje se pod tim opcijama može pronaći mogućnost odbijanja web kolačića. Specifične formulacije poput „Prihvaćam samo nužno“, „Prihvaćam samo neophodno“ također su bile prihvaćene kao pozitivan odgovor. Prethodno poglavlje je utvrdilo da od 100 analiziranih hrvatskih web stranica, 9 njih uopće nema obavijest o kolačićima, pa se u ovoj analizi fokusira na preostalih 91 web stranicu. Grafički prikaz 30. prikazuje rezultate ovog dijela analize gdje 81 hrvatska web stranica, odnosno 89%, od 91 pruža opciju odbijanja web kolačića, dok njih 10 (11%) od 91 nema opciju odbijanja web kolačića, odnosno da obavijest pruža korisniku samo opciju poput „OK“, „Slažem se“ i „Prihvaćam“ (Grafički prikaz 31). Opća uredba o zaštiti podataka (GDPR) propisuje člankom 4. stavkom 1. točkom 11 da privola mora biti dobrovoljna, što znači da korisnik web mjesta mora imati stvaran izbor. Ukoliko korisnik nema pravi izbor i osjeća se prisiljenim pristati na obradu osobnih podataka privola se ne smatra valjanom (Obrada osobnih podataka putem kolačića, n.d.).

Grafički prikaz 30.

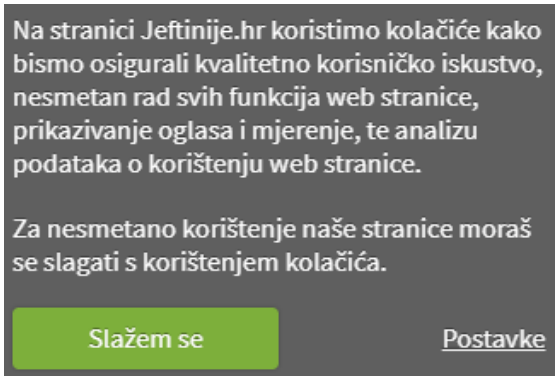
Prisutnost opcije za prihvaćanje i odbijanje web kolačića



Izrada autorice

Grafički prikaz 31.

Prisutnost samo opcije „Slažem se“



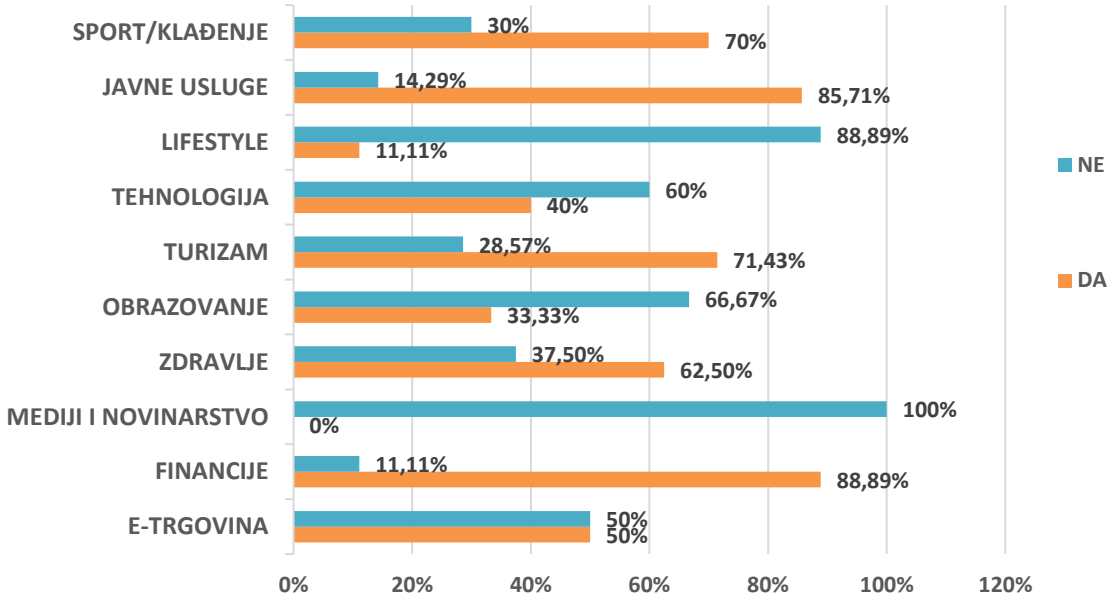
Izvor: Jeftinije.hr, https://www.jeftinije.hr/

7.4.3. Jednostavnost odbijanja web kolačića

U ovom poglavlju analizirana je jednostavnost procesa odbijanja web kolačića na 81 hrvatskoj web stranici koje su prethodno identificirane kao stranice koje su ispunile kriterije a) imaju obavijest o web kolačićima i b) imaju opciju za prihvaćanje i odbijanje web kolačića. Pojam „jednostavnost“ ovdje se odnosi na to koliko je lako odbiti web kolačiće u odnosu na prihvaćanje, bez dodatnih koraka ili potrebe za traženjem skrivenih opcija, odnosno, ako je opcija odbijanja pod „Saznajte više“, „Upravljanje opcijama“ ili slično, navedena tvrdnja se označavala sa „ne“, odnosno, opcija odbijanja nije jednako dostupna kao opcija prihvaćanja. Od ukupno 81 web stranice, 41 web stranice (50,62%) imaju jednostavnu opciju odbijanja kolačića, dok 40 (49,38%) web stranica nemaju (Grafički prikaz 32). Primjeri jednostavnog odbijanja kolačića i „kompliciranog“ prikazano je Grafičkim prikazom 33. i grafičkim prikazom 34. Jedno od ključnih zapažanja iz ove analize je da su web stranice iz kategorije „Mediji i novinarstvo“ imale 100% stopu kompliciranog odbijanja kolačića. Na svim tim web stranicama opcija odbijanja kolačića skrivena je pod „Upravljanje opcijama“ ili „Saznajte više“, što zahtijeva dodatne korake. To može biti povezano s činjenicom da mediji često prate ponašanje posjetitelja putem kolačića za potrebe personaliziranog oglašavanja i praćenja. Slijedeće poglavlje istražuje varljive dizajne i vidljivost gumba „Odbaci“ kako bi se dodatno razumjele taktike koje web stranice koriste u vezi s kolačićima.

Grafički prikaz 32.

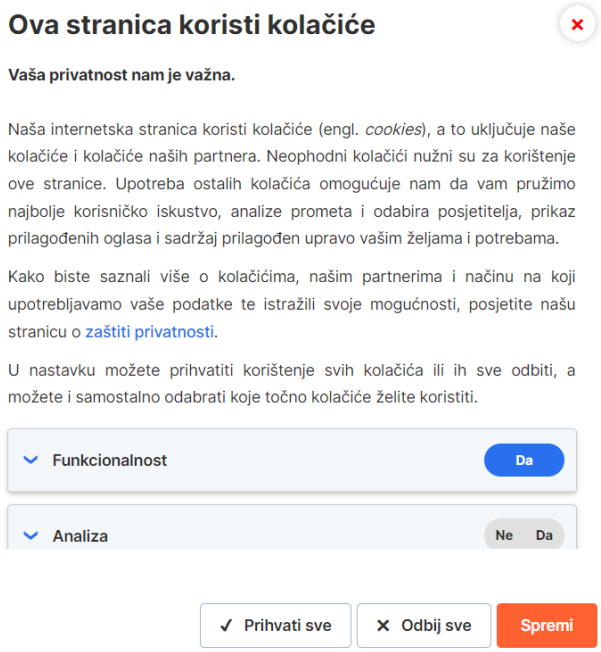
Jednostavnost odbitka web kolačića



Izrada autorice

Grafički prikaz 33.

Primjer jednostavnosti odbitka kolačića



Izvor: Erste banka, https://www.erstebank.hr/hr/gradjanstvo

Grafički prikaz 34.

„Kompliciranost“ odbitka kolačića

Izvor: Index, https://www.index.hr/

7.4.4. Vidljivost i dizajn opcija za prihvaćanje i odbijanje web kolačića

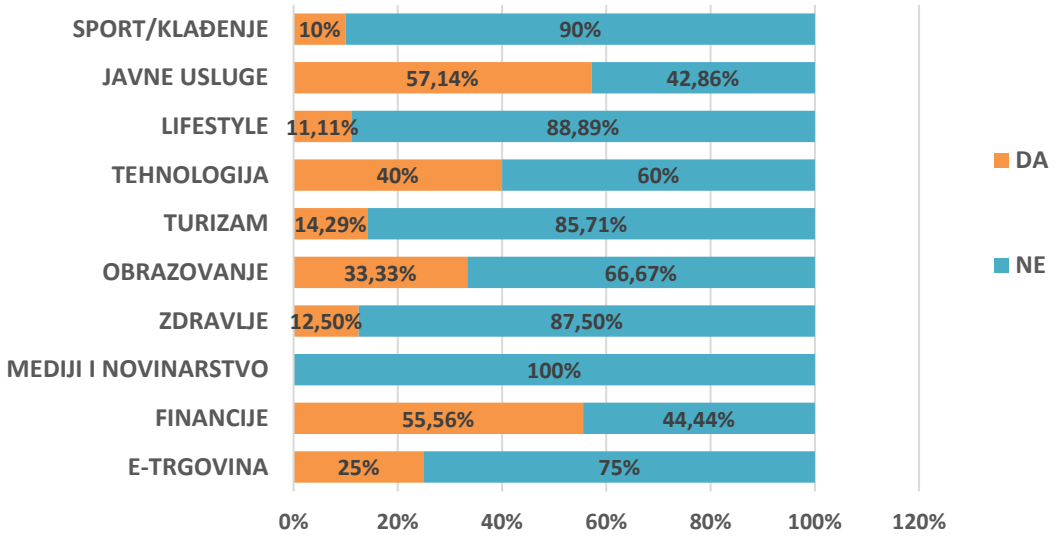
U ovom poglavlju analizira se jesu li opcije za prihvaćanje i odbijanje web kolačića jednako vidljive. Ako opcije nisu jednako vidljive, to znači da web stranica koristi varljive dizajne bojom, fontom ili kontrastom kako bi potaknula posjetitelja na prihvaćanje web kolačića, primjerice ako je gumb za „Prihvati“ istaknutiji i pristupačniji u usporedbi sa „Odbaci“. U analizu je uključeno 81 web stranica koje ispunjavaju kriterije a) Imaju obavijest o web kolačićima i b) Nude opcije za prihvaćanje i odbijanje web kolačića. Web stranice koje nemaju obavijest o web kolačićima ili nude samo opcije „OK“ ili „Slažem se“ nisu uključene.

Rezultati ukazuju da web stranice koje imaju jasno vidljivu opciju odbijanja kolačića kao i prihvaćanja je 20 od 81 web stranica, a 61 web stranica od njih 81 se koriste varljivim dizajnom kako bi potaknuli na prihvaćanje web kolačića. Navedena analiza pokazuje da većina web stranica koristi varljive dizajne s naglaskom na isticanje gumba za prihvaćanje u odnosu na odbijanje. Primjetno je da kategorija „Mediji i novinarstvo“ ima 100% stopu korištenja varljivih dizajna, dok „Sport/klađenje“ ima 90% stopu, odnosno, nemaju jasno vidljive opcije za odbijanje kolačića. S druge strane, kategorije „Financije“ i „Javne usluge“ pokazale su najbolju praksu, s najvećim postotkom web stranica koje imaju jednako vidljive opcije za prihvaćanje i odbijanje kolačića (Grafički prikaz 35). U grafičkom

prikazu 36. prikazan je primjer jednake vidljivosti prihvaćanja i odbijanja dok grafički prikaz 37. prikazuje loš primjer vidljivosti odbijanja.

Grafički prikaz 35.

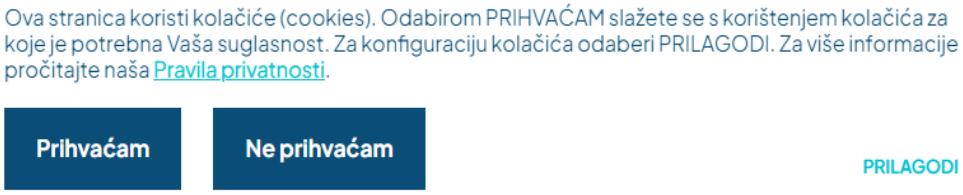
Jednaka vidljivost i dizajn opcija za prihvaćanje i odbijanje web kolačića



Izrada autorice

Grafički prikaz 36.

Primjer jednake vidljivosti i dizajna opcije prihvaćanja i odbijanja kolačića



Izvor: Jadrolinija, https://www.jadrolinija.hr/

Grafički prikaz 37.

Nejednaka vidljivost i dizajn opcije prihvaćanja i odbijanja web kolačića

Izvor: Bauhaus, https://www.bauhaus.hr/

7.4.5. Kategorizacija i transparentnost web kolačića

U ovom poglavlju analizira se kategorizacija i transparentnost web kolačića, tj. jesu li svi web kolačići na obavijesti jasno i transparentno kategorizirani prema svrsi za koju posjetitelj web stranice daje privolu. Prema GDPR-u i smjernicama koje iz njega proizlaze, privola za web kolačiće mora biti informirana, specifična, slobodno dana i nedvosmislena, što znači da korisnik mora biti jasno informiran o svrsi svakog kolačića i imati mogućnost odabira za koje svrhe daje privolu.

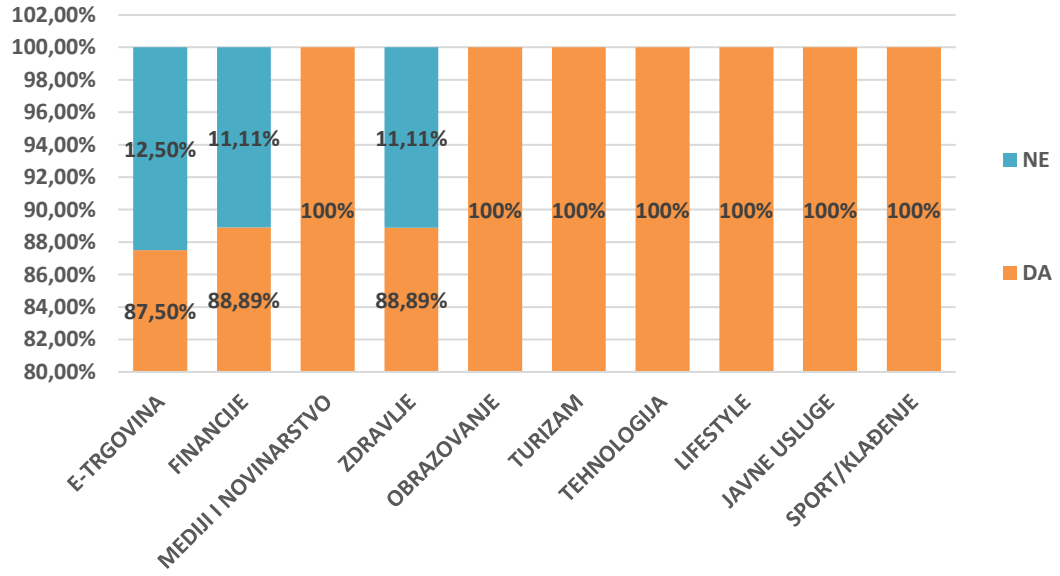
U ovoj analizi uključeno je 82 web stranice. Ovo je za jednu više nego u prethodnim poglavljima jer je u kategoriji „Zdravlje“ dodana web stranica koja nije imala izričitu opciju odbijanja kolačića u poglavlju 7.4.3. te time nije računata za poglavlje 7.4.4., ali ima opciju kategorizacije, pa je uključena u ovu analizu. Članak 6. stavka 1. točka a) Opće uredbe o zaštiti podataka (GDPR) naglašava da korisnik mora dati privolu u jednu ili više posebnih svrha, pri čemu mora imati mogućnost izbora za svaku od tih svrha. Time će se privola odnosno obrada osobnih podataka smatrati zakonita (Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća, 2016). Prema načelu „ograničenja obrade“ iz članka 5. Opće uredbe o zaštiti podataka, da bi obrada bila zakonita i poštena, moraju se ispuniti tri zahtjeva: podaci se moraju prikupljati za posebne, izričite i zakonite svrhe. Voditelj obrade mora pažljivo definirati svrhe obrade i ne smije prikupljati podatke koji nisu nužni za te svrhe. Kako bi se utvrdila zakonitost obrade, konkretne svrhe obrade moraju biti jasno definirane prije samog prikupljanja

podataka, odnosno svrha obrade mora biti dovoljno detaljna kako bi se moglo procijeniti poštivanje zakona (Obrada osobnih podataka putem kolačića, n.d.).

Iz analize, mnoge web stranice koriste model gdje osnovne informacije o kolačićima budu dostupne odmah, dok detaljnije informacije zahtijevaju dodatni klik. Važno je naglasiti da takav pristup ne smije biti varljiv niti smije otežavati korisnicima razumijevanje svrhe kolačića. Ukupno 79 od 82 stranice jasno kategoriziraju kolačiće prema svrsi, dok 3 stranice to ne čine. Ovi rezultati pokazuju visok stupanj transparentnosti i jasne kategorizacije kolačiće kod većine analiziranih hrvatskih web stranica (Grafički prikaz 38).

Grafički prikaz 38.

Kategorizacija i transparentnost web kolačića



Izrada autorice

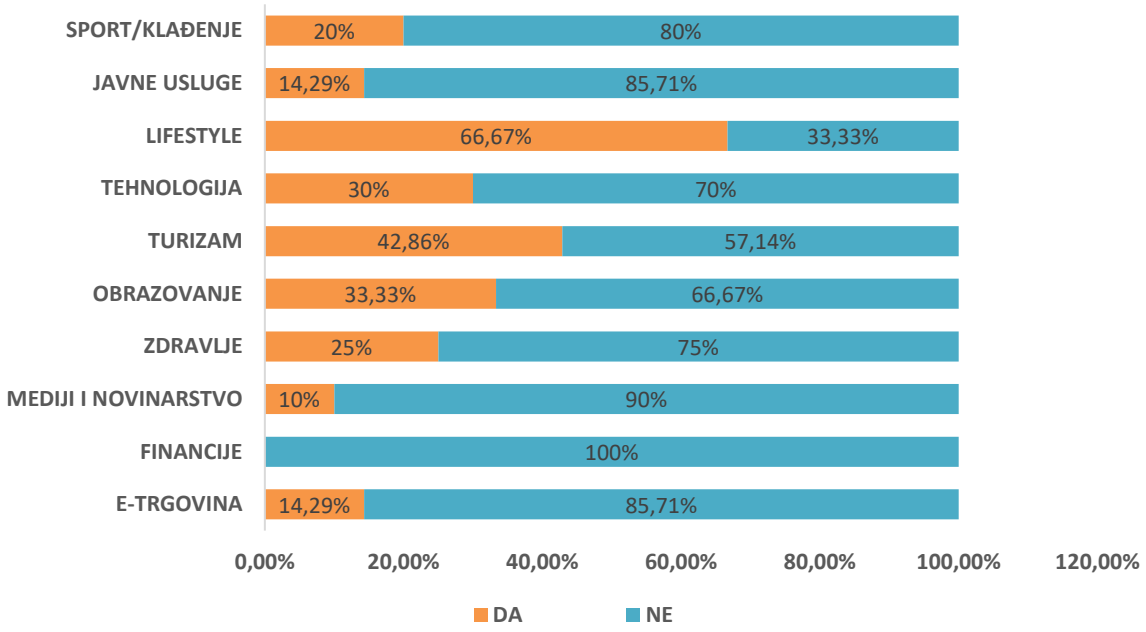
7.4.6. Unaprijed označen gumb „Prihvaćam“

Ovo poglavlje analizira je li unaprijed označen gumb „Prihvaćam“ prisutan u obavijestima o kolačićima na web stranicama koje omogućuju odabir svrhe kolačića. U ovoj analizi obuhvaćeno je 79 web stranica, s obzirom da su tri stranice odbačene iz prethodnog poglavlja jer nisu imale kategorizaciju kolačića. Web stranice koje imaju unaprijed označen gumb „Prihvaćam“ implicitno traže korisnički pristanak bez aktivnog izbora korisnika za svaku svrhu kolačića, što je jasan dokaz ne valjanosti privole prema smjernicama GDPR-a i Direktive o e-privatnosti.

Sveukupno, rezultati pokazuju da većina analiziranih web stranica, 59 od 79 hrvatskih web stranica, ne koristi unaprijed označene gumbe „Prihvaćam“, dok ih 20 od 79 web stranica ipak koristi (Grafički prikaz 39). Najveći postotak primijećen je u kategoriji „Lifestyle“ u kojem 66,67% analiziranih web stranica koristi unaprijed označen gumb prihvaćam dok svega 33,33% ne koristi (Grafički prikaz 40).

Grafički prikaz 39.

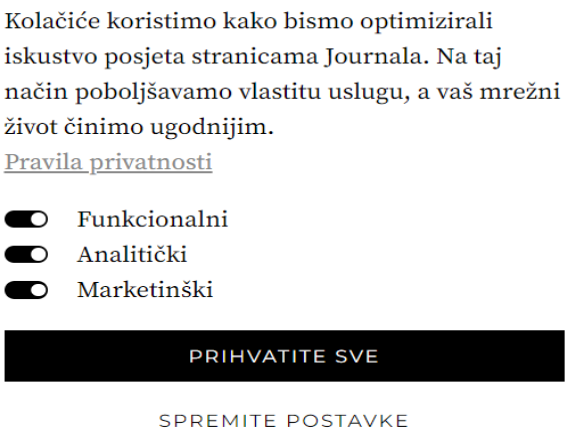
Analiza stranica koja imaju unaprijed označen gumb „Prihvaćam“



Izrada autorice

Grafički prikaz 40.

Unaprijed označen gumb „Prihvaćam“



Izvor: Journal.hr, https://www.journal.hr/

7.4.7. Dostupnost politike kolačića

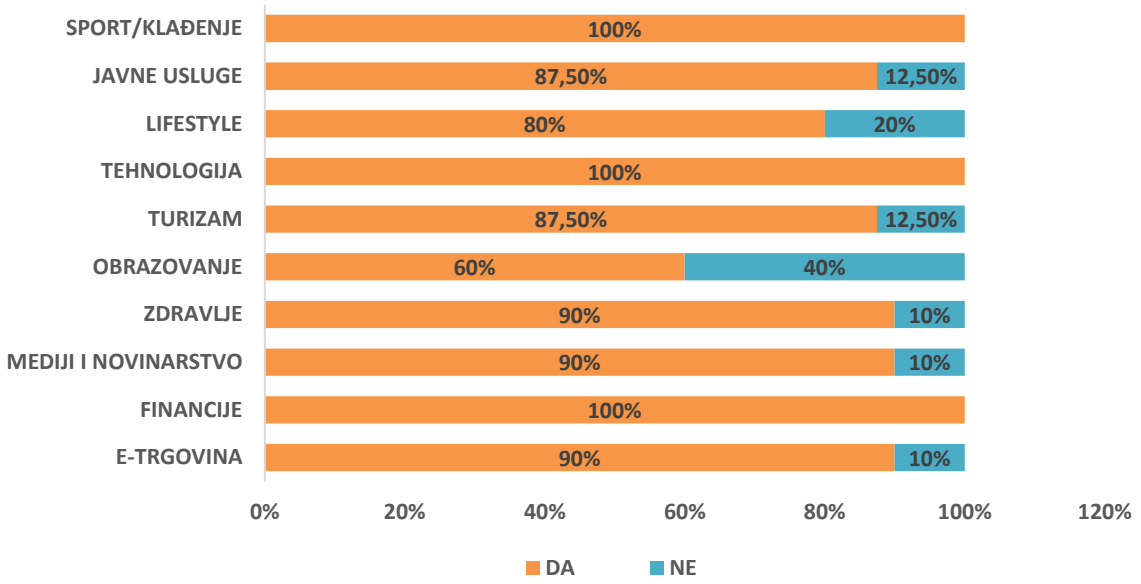
Agencija za zaštitu osobnih podataka (AZOP) navodi da je za dobivanje valjane privole pri obradi osobnih podataka putem kolačića potrebno pružiti najmanje sljedeće informacije:

- Identitet i kontakt podatke voditelja obrade;
- Svrhu svakog postupka obrade za koji se traži privola;
- Vrste osobnih podataka koji će se prikupljati i obrađivati;
- Pravo na povlačenje privole (koje mora biti jednostavno kao i njezino davanje);
- Primatelje ili kategorije primatelja (npr. kolačići treće strane);
- Razdoblje pohrane osobnih podataka ili kriterije za određivanje tog razdoblja;
- Informacije o korištenju podataka za automatizirano donošenje odluka prema članku 22. stavka 2. točka c), ako je primjenjivo;
- Moguće rizike povezane uz prijenos podataka.

Ove informacije obično se pružaju u dokumentu nazvanom „Politika privatnosti“, koji mora biti napisan jednostavnim i razumljivim jezikom te lako dostupan posjetiteljima web stranica (Obrada osobnih podataka putem kolačića, n.d.). Navedeno osigurava transparentnost i omogućava korisnicima da budu informirani o načinima na koje se koriste njihovi podaci. U zadnjoj analizi istraženo je jesu li politika privatnosti i kolačića lako dostupne na obavijesti o kolačićima. U analizi su uključene one web stranice koje nude obavijest o web kolačićima, odnosno, 91 web stranica. Analizom se utvrdilo da 82 web stranice od njih 91, omogućuje lako dostupnu politiku privatnosti i kolačića, čime zadovoljavaju propise o transparentnosti i informiranju korisnika, dok 9 web stranica od 91 ne nude (Grafički prikaz 41).

Grafički prikaz 41.

Politika privatnosti na analiziranim web stranicama



Izrada autorice

7.5. Osvrt na rezultate istraživanja

Rezultati istraživanja ukazuju da većina hrvatskih web stranica (91%) pruža jasne obavijesti o korištenju web kolačića. Nadalje, 89% web stranica pruža opciju odbijanja kolačića, što je u skladu s GDPR-om koji zahtijeva da privola bude dobrovoljna i da korisnik ima stvaran izbor. Ipak, evidentirani su značajni problemi u vezi s jednostavnošću odbijanja kolačića i dizajnom opcija za prihvaćanje i odbijanje. Naime, 49,38% hrvatskih web stranica nema opciju jednostavnog odbijanja kolačića, dok 75,3% hrvatskih web stranica koristi varljive dizajne koji naglašavaju gumb za prihvaćanje u odnosu na odbijanje. Ovi rezultati ukazuju na potrebu za poboljšanjem transparentnosti i jednostavnosti pristupa korisnicima u vezi s odbijanjem kolačića. Rezultati anketnog istraživanja također potvrđuju ove rezultate. Na uzorku od 224 ispitanika, njih 42% izjavilo je da bi napustilo web stranicu ako bi se suočili s obavijesti o kolačićima koja prikazuje opcije „Prihvati i zatvori“ i „Upravljanje opcijama“, gdje je opcija „Odbij“ skrivena. Međutim, samo 21,4% bi kliknulo na opciju upravljanja, što ukazuje na to da varljive taktike smanjenja vidljivosti opcija za odbijanje funkcioniraju, a korisnici nisu dovoljno informirani ili motivirani da pretražuju dodatne opcije. Jedan od iznenađujućih trendova jest visok postotak web stranica koje koriste unaprijed označene gumbe „Prihvaćam“, posebice u kategoriji „Lifestyle“ gdje je postotak 66,67%, što je u suprotnosti s načelima GDPR-a. Navedeni trend ukazuje na potrebu za strožom regulacijom i kontrolom prakse dobivanja privola. Dosljedni problem

identificiran u istraživanju jest nedostatak transparentnosti i jednostavnosti odbijanja kolačića. Prethodno anketno istraživanje potvrdilo je tu činjenicu, s obzirom da većina korisnika, njih 34,4%, često prihvaća uvjete bez puno razmišljanja.

Na temelju rezultata oba istraživanja preporučuje se:

- Promjena obavijesti o web kolačićima: većina analiziranih hrvatskih web stranica koristi alate koji ne zadovoljavaju kriterije zakonitog dobivanja privola. Privole moraju omogućiti korisnicima jednostavan i jasan način za odbijanje svih kolačića, te informacije o kolačićima moraju biti napisane jednostavnim i razumljivim jezikom, u skladu s člankom 12. GDPR-a. Potrebno je osigurati da opcije za odbijanje kolačića budu jednako vidljive i lako dostupne kao i opcije za prihvaćanje te time omogućiti korisnicima stvaran i informiran izbor.
- Proaktivna djelovanja regulatornih tijela: regulatorna tijela u Republici Hrvatskoj trebaju povećati svoju učinkovitost i jasno postaviti i postrožiti pravila kako bi proaktivno djelovali u zaštiti osobnih podataka korisnika. ovo uključuje redovne inspekcije i nadzore nad hrvatskim web stranica kako bi se osigurala usklađenost s regulativama.

7.6. Ograničenja istraživanja

Provedeno istraživanje pružilo je vrijedne uvide u prakse upotrebe web kolačića na hrvatskim web stranica, no postojala su određena ograničenja tijekom istraživanja koja treba uzeti u obzir prilikom interpretacije dobivenih rezultata. Procjena obavijesti o kolačićima može biti subjektivna jer su obavijesti različito konstruirane na svakoj web stranici. Stoga, iako su korišteni određeni kriteriji za ocjenu, subjektivnost i osobna interpretacija mogu utjecati na dosljednost tvrdnje „da“ ili „ne“. Iako je uzorak od 100 web stranica odabran s ciljem predstavljanja raznolikosti, veći uzorak bi pružio pouzdanije rezultate. Nadalje, istraživanje je provedeno u razdoblju od 03.06. do 09.06.2024. godine, što znači da rezultati predstavljaju stanje u tom specifičnom trenutku. S obzirom da web stranice često ažuriraju svoje obavijesti o kolačićima i politike privatnosti, navedeno može utjecati na dugoročnu relevantnost rezultata. Zadnje, ručna analiza koja je provedena u ovom istraživanju podložna je ljudskim pogreškama, stoga automatizirani alati mogli bi pružiti dosljedniju i objektivniju analizu velikog broja web stranica. Unatoč ograničenjima, navedeno istraživanje postavilo je temelje za buduća istraživanja koje mogu dodatno istražiti i adresirati identificirane probleme.

8. ZAKLJUČAK

Web kolačići su mali tekstualni podaci pohranjeni na korisničkim uređajima koji omogućuju web stranica prepoznavanje korisnika i prilagođavanje njihovog iskustva na internetu. Kroz povijest, razvoj web kolačića evoluirao je od jednostavnih alata za pamćenje proizvoda u košarici do složenih mehanizama za praćenje korisničkih aktivnosti i personalizaciju sadržaja. Rad je detaljno razmotrio različite vrste web kolačića prema njihovom porijeklu, trajanju i svrsi, naglašavajući njihovu važnost u suvremenom digitalnom okruženju. S obzirom na evoluciju web kolačića, pravni aspekti web kolačića pokazali su se ključnim za zaštitu privatnosti korisnika. Ključne regulative koje uređuju ovu oblast uključuju Opću uredbu o zaštiti podataka (GDPR), Direktiva o e-privatnosti i nadolazeću Uredbu o privatnosti i elektroničkim komunikacijama, koja bi zamijenila trenutnu Direktivu. Također, Zakon o elektroničkim komunikacijama u Republici Hrvatskoj dodatno definira pravila za korištenje web kolačića na hrvatskom teritoriju. Opća uredba o zaštiti podataka stupila je na snagu 2018. godine i time predstavlja ključni zakonodavni okvir za zaštitu osobnih podataka u Europskoj Uniji koja postavlja stroge zahtjeve za transparentnost i privolu korisnika pri prikupljanju i obradi osobnih podataka. Konkretno, članak 4. GDPR-a definira pojmove poput obrade, privole i povrede osobnih podataka, članak 5. definira osnovna načela obrade osobnih podataka, članak 6. definira u kojim slučajevima je obrada zakonita, dok članak 7. opisuje uvjete za davanje privole. Nova Uredba o privatnosti i elektroničkim komunikacijama, koja bi trebala zamijeniti Direktivu o e-privatnosti, očekuje se da će dodatno pooštriti regulative i uskladiti se s GDPR-om. Navedena Uredba naglašava važnost jačanja povjerenja korisnika u korištenju digitalnih usluga, strože kontrole nad web kolačićima i veću transparentnost u obradi osobnih podataka.

Sigurnosni rizici povezani s web kolačićima uključuju Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), napade korisničkih sjednica i krađu identiteta. Rad je detaljno analizirao ove rizike, pružajući uvid u scenarije u kojima napadači mogu iskoristiti web kolačiće za neovlašteni pristup osobnim podacima. Identifikacija i analiza ovih rizika naglašavaju važnost implementacije sigurnosnih mjera i kontinuirane edukacije korisnika kako bi se smanjile prijetnje.

Kroz diplomski rad provedena su dva istraživanja. Prvo istraživanje odnosilo se na provedenu anketu o svijesti korisnika o web kolačićima, i time otkrila značajan deficit u početnom znanju među korisnicima interneta. 224 ispitanika pokazala su nisku razinu razumijevanja funkcionalnosti i svrhe kolačiće, ali kroz edukaciju unutar ankete pokazali su povećanu svijest i razumijevanje. Na kraju istraživanja, većina ispitanika izrazila je zabrinutost za privatnost i prikupljanje osobnih podataka

putem web kolačića, naglašavajući potrebu za većom transparentnošću i regulacijom. Drugo istraživanje koje je provedeno odnosilo se na analizu 100 najpopularnijih web stranica sa hrvatskom domenom .hr. Analiza je pokazala da većina hrvatskih web stranica pruža na svojoj web stranici obavijest o korištenju web kolačića, međutim mnogi koriste varljive dizajne koji otežavaju odbijanje web kolačića. Otkriveno je da mnoge stranice, naročito u kategoriji „Lifestyle“, upotrebljavaju unaprijed označene gumbe za prihvaćanje, što je suprotno načelima GDPR-a. Povezivanjem rezultata oba istraživanja, može se uvidjeti da ispitanici često nisu dovoljno motivirani da pretražuju dodatne opcije za odbijanje web kolačića već često prihvate sve kolačiće jer je jednostavnije, što se i otkrilo analizom web stranica, da većina web stranica otežava odbitak kolačića, skrivajući navedenu opciju pod „Upravljanje opcijama“ ili pod opcijom „Saznajte više“, dok je „Prihvati i zatvori“ vidljivo istaknutija bojom, fontom i kontrastom. Rezultati istraživanja jasno ukazuju na potrebu za većom transparentnošću, boljim praksama u informiranju korisnika i strožom regulacijom kako bi se osigurala veća zaštita privatnosti korisnika. Proaktivna djelovanje regulatornih tijela u Republici Hrvatskoj trebala bi osigurati bolju usklađenost s GDPR-om i drugim relevantnim regulativama, uključujući redovne inspekcije i nadzore hrvatskih web stranica.

Kroz istraživanja, došlo se do sljedećih odgovora na postavljena istraživačka pitanja na početku rada:

- Web kolačići uistinu igraju ključnu ulogu u praćenju i personalizaciji korisničkog iskustva na internetu, omogućujući web stranicama prikupljanje podataka o korisnicima i time stvaranja prilagođenog oglašavanja na temelju njihovih interesa i navika.
- Svijest korisnika o prikupljanju osobnih podataka putem web kolačića je ograničena, međutim kroz edukaciju moguće je postići veću svjesnost o rizicima istih.
- Zakonodavstvo, posebice GDPR i Direktiva o e-privatnosti, imaju značajan utjecaj na praksu upotrebe web kolačića, ali postoje vidljivi izazovi u postizanju potpune usklađenosti i transparentnosti među web stranicama gdje mnogima nedostaje jasnoća svrhe obrade osobnih podataka, što naposljetku smanjuje povjerenje posjetitelja web stranica. Tehnike zaštite sigurnosti, poput redovitih sigurnosnih provjera, brisanju web kolačića sa uređaja, kontinuirane edukacije korisnika, mogu smanjiti rizike povezane s istima.

LITERATURA

Agencija Za Zaštitu Osobnih Podataka - AZOP (n.d.). *Obrada osobnih podataka putem kolačića i pružanje informacija ispitanicima vezano za obradu osobnih podataka*. Agencija za zaštitu osobnih podataka. Agencija Za Zaštitu Osobnih Podataka. https://azop.hr/obrada-osobnih-podataka-kolacici/

Agencija za zaštitu osobnih podataka (n.d.). *Vodič o obradi osobnih podataka putem kolačića. Agencija za zaštitu osobnih podataka (AZOP)*. https://azop.hr/vodic-o-obradi-osobnih-podataka-putem-kolacica/

Alfatec (2020). *Važnost „end-to-end" enkripcije*. https://www.alfatec.ai/hr/akademija/baza-znanja/vaznost-end-to-end-enkripcije (Datum pristupa: 01.09.2023).

All About Cookies (2023). *Privacy issues for computer cookies*. All About Cookies. https://allaboutcookies.org/privacy-issues-cookies (Datum pristupa: 01.10.2023)

Anchor Digital (2022). *The evolution of web Cookies - The future of Third-Party Cookies.* Anchor Digital. https://anchordigital.com.au/articles/the-evolution-of-web-cookies-the-future-of-third-party-cookies

Bennett, S.C. (2011*). Regulating Online Behavioral Advertising*. 44 J. Marshall L. Rev. 899 (2011)

Bollinger, D. (2021). *Analyzing Cookies Compliance with the GDPR* [Diplomski rad, ETH Zurich] ETH Zurich Research Collection

Cahn, A., Scott, A., Barford, P. & Muthukrishnan, S. (2016). *An Empirical Study of Web Cookies*. In Proceedings of the 25th International Conference on World Wide Web (WWW '16). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 891– 901. https://doi.org/10.1145/2872427.2882991

CARNet (2006). *Analiza XSS sigurnosnih propusta*. CCERT-PUBDOC-2006-05-157

CARNet (2007). *Napadi krađom korisničkih sjednica.* CCERT-PUBDOC-2007-03-185

CARNet (2008). *Provjera XSS i SQL Injection ranjivosti Exploit Me skupom alata*. CCERT-PUBDOC-2008-01-215

CARNet (2010). *CSRF napadi.* NCERT-PUBDOC-2010-04-297

Center For Democracy & Technology. (2009). *Simple Behavioral Advertising. Center for Democracy & Technology*. https://cdt.org/insights/simple-behavioral-advertising/

Center for Democracy and Technology. (2009). *Behavioral advertising across multiple sites - Center for Democracy and Technology*. https://cdt.org/insights/behavioral-advertising-across-multiple-sites/

Center for Democracy and Technology. (2009). *Privacy Impact - Center for Democracy and Technology*. https://cdt.org/insights/privacy-impact/

Cookie Law Info. (2023). *Cookieless future: What can we expect?* Cookie Law Info. https://www.cookielawinfo.com/cookieless-future/

Cookie Script (2022). *What are Different Types of Web Cookies*? CookieScript. https://cookie-script.com/web-cookie-types (Datum pristupa: 11.03.2024).

CookiePro. (2022). *What's the difference between first and Third-Party cookies?* CookiePro. https://www.cookiepro.com/knowledge/whats-the-difference-between-first-and-third-party-cookies/ (Datum pristupa: 05.01.2024).

CookieYes (2024). *All About Internet Cookies*. CookieYes. https://www.cookieyes.com/blog/internet-cookies/

CookieYes (2024). *What is CCPA: A Quick Guide to Compliance*. CookieYes. https://www.cookieyes.com/blog/what-is-ccpa/

CookieYes (n.d.). *What are session cookies? Do they need consent?* CookieYes. https://www.cookieyes.com/blog/session-cookies/

CookieYes (n.d.). *What is UK GDPR? A Complete Guide* [with Infographic]. CookieYes. https://www.cookieyes.com/blog/what-is-uk-gdpr/ (Datum pristupa: 14.03.2024).

Dodt, C. (2020). *Cookies: An overview of associated privacy and security risks*. INFOSEC https://resources.infosecinstitute.com/topics/general-security/cookies-an-overview-of-associated-privacy-and-security-risks/ (Datum pristupa: 20.09.2023.)

E. Aïmeur, E., Schőnfeld, D. (2011). *The ultimate invasion of privacy: Identity theft*. 2011 Ninth Annual International Conference on Privacy, Security and Trust, Montreal, QC, Canada, 2011, pp. 24-31, doi: 10.1109/PST.2011.5971959.

Espacenet (1998). *Persistent client state in a hypertext transfer protocol based client-server system*. US5774670A

European Commision (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. European Commision. https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

Europska komisija (n.d.). *Što su tijela za zaštitu podataka (TZP-ovi)?*. Europska komisija. https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_hr

Europski revizorski sud (2022). *Tematsko izvješće: sigurnost 5G mreža.* https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/hr/

Ferraresi, M. (2023). International: The evolution of the right to privacy and data protection. Data Guidance. https://www.dataguidance.com/opinion/international-evolution-right-privacy-and-data

Fisher, T. (2022). *Why Online Ads Follow You Around the Web*. Lifewire. https://www.lifewire.com/ads-online-why-are-they-following-you-around-the-web-4063788 (Datum pristupa: 06.01.2024).

GDPR Summary (n.d.). *GDPR Summary - An overview of the General Data Protection Act.* GDPR Summary. https://www.gdprsummary.com/gdpr-summary/

GDPR.EU (2019). *GDPR Small Business Survey*. https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf

Google for Developers. (n.d.). *Preparing for the end of third-party cookies | Privacy Sandbox* | Google for Developers. https://developers.google.com/privacy-sandbox/blog/cookie-countdown-2023oct

Gotze, M., Matic, S., Iordanou, C., Smaragdakis, G., Laoutaris, N. (2022). *Measuring Web Cookies in Governmental Websites*. In 14th ACM Web Science Conference 2022 (WebSci '22), June 26–29, 2022, Barcelona, Spain. ACM, New York, NY, USA 11 Pages. https://doi.org/10.1145/3501247.3531545

Helmond, A., Nieborg, D. B., & van der Vlist, F. N. (2017). *The Political Economy of Social Data: A Historical Analysis of Platform–Industry Partnerships*. In 8th International Conference on Social Media & Society: Social Media for Good or Evil: Toronto, Canada. Article 38 The Association for Computing Machinery. https://doi.org/10.1145/3097286.3097324

Information Commissioner's Office (ICO) (2012). *Guidance on the rules on use of cookies and similar technologies*. https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf

Jordan, K. (2018). *Degrees of Intrusion? A Survey of Cookies Used by UK Higher Education Institutional Websites and Their Implications*. DOI: http://dx.doi.org/10.2139/ssrn.3142312

Kesan, J., P., Shah, R., C. (2004). *Deconstructing Code*. 297-301 str. Dostupno putem SSRN: https://ssrn.com/abstract=597543

Khu-smith, V., Mitchell, C. (2001). *Enhancing the Security of Cookies*. 132-145. 10.1007/3-540-45861-1_11.

Klosowski, T. (2021). *The State of Consumer Data Privacy Laws in the US (And Why It Matters).* New York Times | Wirecutter. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Koch, R. (n.d.). *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.eu. https://gdpr.eu/cookies/

Kristol, D. M. (2001). *HTTP Cookies: Standards, privacy, and politics*. ACM Trans. Internet Technol. 1, 2 (November 2001), 151–198. DOI: https://doi.org/10.1145/502152.502153.

LaCroix, K., Loo, Y. L., Choi, Y. B. (2017). *Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen*, 2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, USA, 2017, pp. 20-24, doi: 10.1109/ICSSA.2017.9.

Lancefield, D., Ambler, M., Rauber, M. & Patel, R. (2011*). Research into consumer understanding and management of Internet cookies and the potential impact of the EU Electronic Communications Framework*. Department for Culture, Media & Sport (DCMS). https://assets.publishing.service.gov.uk/media/5a78bcc040f0b62b22cbc646/PwC_Internet_Cookies_final.pdf

Lopez, M. (2024). *The role of Blockchain in secure online transactions.* Devlane. https://www.devlane.com/blog/the-role-of-blockchain-in-secure-online-transactions (Datum pristupa: 14.04.2024).

Lord, N. (2017). *What is the Data Protection Directive? The Predecessor to the GDPR*. Digital Guardian. https://www.digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr (Datum pristupa: 14.03.2024).

Macbeth, S. (2016). *Tracking and Online Banking: A Survey*.

MDN Web Docs (2024). *An overview of HTTP - HTTP | MDN*. https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview (Datum pristupa: 01.12.2023).

MDN Web Docs (2024). *Using HTTP Cookies – HTTP | MDN. https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies* (Datum pristupa: 03.12.2023).

Monique. (2023). 10 Different types of web cookies and how are they used. Ubique Digital Solutions. https://ubiquedigitalsolutions.com/blog/10-different-types-of-web-cookies-and-how-are-they-used-for-tracking-user-behaviour/ (Datum pristupa: 10.03.2024)

Mustapha, R. (2023). *What Is HTTP? Protocol Overview for Beginners*. FreeCodeCamp.org. https://www.freecodecamp.org/news/what-is-http/ (Datum pristupa 10.11.2023).

Neumetric (2023). *Understanding the Consequences: Penalties for Violating GDPR.* Neumetric. https://www.neumetric.com/penalties-for-violating-gdpr/ (Datum pristupa: 14.03.2024).

O'Brien, C. (2024). *How AI is Changing Digital Marketing*. Digital Marketing Institute. https://digitalmarketinginstitute.com/blog/how-ai-is-changing-digital-marketing

Patel, V., Juric, R. (2001*). Internet users and online privacy: a study assessing whether Internet users' privacy is adequately protected*. Proceedings of the 23rd International Conference on Information Technology Interfaces, 2001. ITI 2001., Pula, Croatia, 2001, pp. 193-200 vol.1, DOI: 10.1109/ITI.2001.938018.

Pitofsky, R., Anthony, S.F., Thompson, M.W., Swindle, O., Leary, T.B. (2000). Online Profiling: A Report to Congress

Practical Law. (n.d.). *EU Data Protection Directive*. Practical Law. https://uk.practicallaw.thomsonreuters.com/6-501-7455?transitionType=Default&contextData=(sc.Default)&firstPage=true

Presido (2022). *Alternative kolačićima trećih strana*. https://presido.hr/blog/alternative-kolacicima- trecih-strana-138/ (Datum pristupa: 01.09.2023).

Privacy Sandbox. (n.d.). *The Privacy Sandbox: Technology for a more private web*. https://privacysandbox.com/

Rivero, N. (2021). *The Inventor of the Digital Cookie Has Some Regrets*. Quartz. https://qz.com/2000350/the-inventor-of-the-digital-cookie-has-some-regrets (Datum pristupa: 10.12.2023).

Rosner, G., Kenneally, E. (2018). *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*. UC Berkeley Center for Long-Term Cybersecurity/Internet of Things Privacy Forum. 5-13 str. https://ssrn.com/abstract=3320670

Schwartz, J. (2001). *Giving Web a Memory Cost Its Users Privacy*. The New York Times. https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html (Datum pristupa: 10.12.2023).

Simon. (2023). *Why are cookies called cookies? The history and inventor behind the name*. SimonStapleton.com. https://www.simonstapleton.com/wordpress/2023/12/16/why-are-cookies-called-cookies-the-history-and-inventor-behind-the-name/

Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća. *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)* (2016)

Usercentrics. (2024). *Data privacy regulation in 2024: what we're watching*. Consent Management Platform (CMP) Usercentrics. https://usercentrics.com/knowledge-hub/data-privacy-in-2024-what-we-are-watching/ (Datum pristupa: 15.04.2024).

Wagner, P. (2020). *Cookies: Privacy Risks, Attacks, and Recommendations*. DOI: http://dx.doi.org/10.2139/ssrn.3761967.

Wolford, B. (n.d.). What is GDPR, the EU's new data protection law? GDPR.EU. https://gdpr.eu/what-is-gdpr/

Yu, X., Samarasinghe, N., Mannan, M., Youssef, A. (2022). *Got Sick and Tracked: Privacy Analysis of Hospital Websites*. 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2022, pp. 278-286, doi: 10.1109/EuroSPW55150.2022.00034.

POPIS GRAFIČKIH PRIKAZA

PRILOZI

Web kolačići i privatnost korisnika: uloga, svjesnost i zaštita sigurnosti

Hvala Vam što sudjelujete u ovom istraživanju koji se provodi u svrhu izrade diplomskog rada na temu **"Web kolačići i privatnost korisnika: uloga, svjesnost i zaštita sigurnosti."**

Cilj ovog istraživanja je dobiti uvid u percepciju korisnika o web kolačićima, te kako razumiju i doživljavaju zaštitu svoje sigurnosti na internetu.

Osim prikupljanja mišljenja ispitanika, ova anketa također ima i **edukativni karakter**. Kroz zanimljive i korisne informacije nastoji se približiti koncept web kolačića i njihove svrhe.

Sudjelovanje u ovoj anketi je potpuno **anonimno** i **dobrovoljno**. Podaci prikupljeni ovim putem koristit će se isključivo u svrhu akademskog istraživanja.

* Označava obavezno pitanje

1. Spol *

Označite samo jedan oval.

- ◯ Muško
- ◯ Žensko

2. Dob *

Označite samo jedan oval.

- ◯ Manje od 18 godina
- ◯ 18-24 godine
- ◯ 25-34 godine
- ◯ 35-44 godine
- ◯ 45-54 godine
- ◯ 55-64 godine
- ◯ 65 godina ili više

3. Najveći stupanj obrazovanja *

Označite samo jedan oval.

- ◯ Osnovno obrazovanje
- ◯ Srednjoškolsko obrazovanje
- ◯ Preddiplomski studij
- ◯ Diplomski studij
- ◯ Doktorski studij
- ◯ Ostalo: _____

4. Koliko često koristite internet? *

Označite samo jedan oval.

- ◯ Svakodnevno (više sati dnevno)
- ◯ Nekoliko puta tjedno
- ◯ Jednom tjedno
- ◯ Nekoliko puta mjesečno
- ◯ Jednom mjesečno ili rjeđe
- ◯ Nikada

5. Kada koristite internet, koliko ste zabrinuti zbog svoje online privatnosti? *

Označite samo jedan oval.

- ◯ Vrlo sam zabrinut/a
- ◯ Donekle sam zabrinut/a
- ◯ Malo sam zabrinut/a
- ◯ Nisam uopće zabrinut/a
- ◯ Nisam siguran/a

6. Ocijenite svoj stupanj suglasnosti s navedenim tvrdnjama *

Označite samo jedan oval po retku.

	Potpuno se ne slažem	Ne slažem se	Neutralan/a	Slažem se	Potpuno se slažem
Preferiram personalizirano oglašavanje koje je prilagođeno mojim interesima	◯	◯	◯	◯	◯
Zabrinut/a sam zbog načina na koji tvrtke prikupljaju moje osobne podatke	◯	◯	◯	◯	◯

7. Jeste li upoznati s konceptom web kolačića? *

Označite samo jedan oval.

- ◯ Da, potpuno razumijem što su web kolačići
- ◯ Čuo/la sam za njih, ali ne znam točno što su
- ◯ Nisam siguran/na
- ◯ Ne, nikada nisam čuo/la za web kolačiće

8. Molimo označite odgovarajuću opciju za svaku izjavu o web kolačićima *

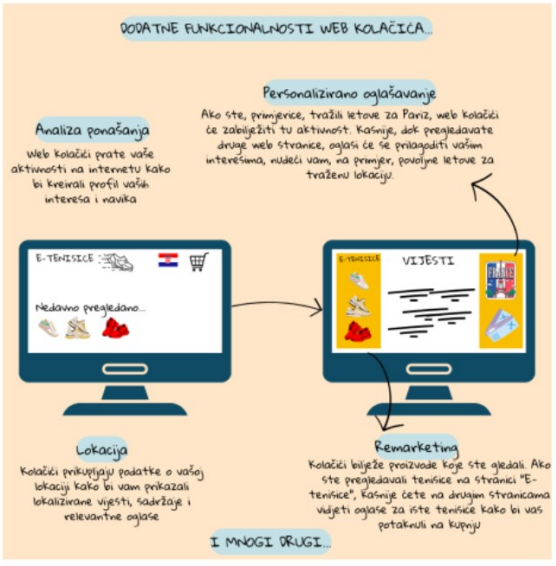
Označite samo jedan oval po retku.

	Točno	Netočno	Ne znam
Web kolačići su male datoteke koje se pohranjuju na mom računalu	◯	◯	◯
Web kolačići omogućuju brže prikazivanje web stranica	◯	◯	◯
Web kolačići mi omogućuju automatsku prijavu bez potrebe za ponovnim unošenjem lozinke	◯	◯	◯
Web kolačići omogućuju personalizirano oglašavanje na temelju mojih prethodnih aktivnosti	◯	◯	◯
Web kolačići se ne razlikuju od povijesti mog internetskog preglednika	◯	◯	◯

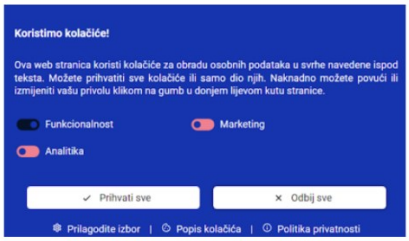
Osim već navedenih svrha, smatrate li da web kolačići imaju još neku dodatnu svrhu? Ako da, molimo vas da odaberete sve relevantne opcije *

Odaberite sve točne odgovore.

- [ ] Ne, mislim da su navedene sve svrhe kolačića
- [ ] Personalizirano oglašavanje
- [ ] Praćenje korisničkih navika
- [ ] Praćenje performansi web stranice
- [ ] Analitika za marketinške svrhe
- [ ] Remarketing (ponovno ciljanje korisnika s oglasima)
- [ ] Praćenje lokacije
- [ ] Praćenje aktivnosti na različitim uređajima i platformama
- [ ] Nisu mi poznate dodatne svrhe
- [ ] Ostalo: _____



Primjer obavijesti o web kolačićima na web stranici



10. Kako reagirate na obavijesti o web kolačićima na web stranicama? *

Označite samo jedan oval.

- ◯ Prihvaćam uvjete bez puno razmišljanja
- ◯ Ponekad ih pročitam prije nego što prihvatim/odbijem
- ◯ Ignoriram ih i nastavim dalje
- ◯ Uvijek tražim više informacija prije nego što prihvatim/odbijem

11. Po Vašem mišljenju, smatrate li navedenu suglasnost ispravnom? *

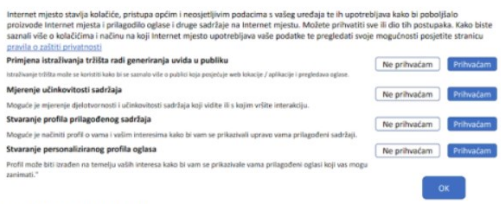
Označite samo jedan oval.

- ◯ Da
- ◯ Ne
- ◯ Nisam siguran/na

Primjer loše prakse obavijesti o prihvaćanju/ne prihvaćanju kolačića

Kada korisnik klikne na poveznicu za više informacija, otvara se stranica koja opisuje kolačiće i njihove svrhe, ali **ne nudi mogućnost odabira skupina kolačića** po funkcionalnosti. Korisnika se upućuje da postavke kolačića regulira kroz svoj preglednik, uz upute gdje pronaći daljnje informacije o podešavanju kolačića.

12. Kako ocjenjujete praksu unaprijed označene opcije "Prihvaćam" u obavijesti o kolačićima? *



Označite samo jedan oval.

- ◯ Ispravna
- ◯ Neispravna
- ◯ Nisam siguran/a

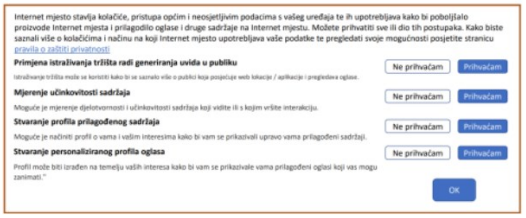
13. Koju biste opciju odabrali da Vam se ova suglasnost prikaže na web stranici? *

Odaberite sve točne odgovore.

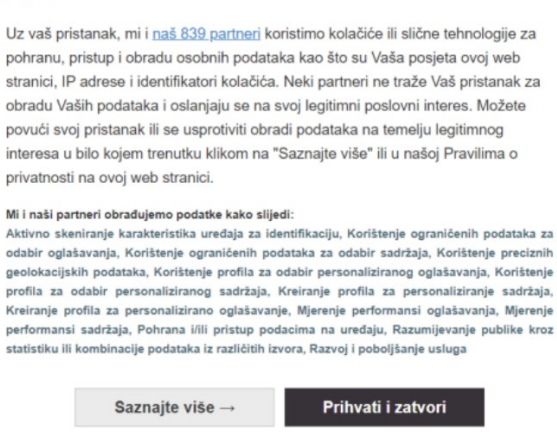
- ☐ Prihvaćam sve
- ☐ Ne prihvaćam sve
- ☐ Napuštanje web stranice
- ☐ Primjena istraživanja tržišta radi generiranja uvida u publiku
- ☐ Mjerenje učinkovitosti sadržaja
- ☐ Stvaranje profila prilagođenog sadržaja
- ☐ Stvaranje personaliziranog profila oglasa
- ☐ Kliknuo/la bih na "Pravila o zaštiti privatnosti"

Primjer loše prakse obavijesti o prihvaćanju/ne prihvaćanju kolačića

Pored svake grupe kolačića su gumb "Prihvaćam"/"Ne prihvaćam", pri čemu je **"Prihvaćam" unaprijed odabran**. Iako obavijest sadrži kratko objašnjenje koji se podaci prikupljaju i u koju svrhu, te nudi mogućnost izbora za svaku skupinu kolačića, **ovakva privola nije u skladu s europskim zakonodavstvom** jer je opcija "Prihvaćam" unaprijed odabrana. Zahtjevi za privolama ne smiju imati unaprijed odabrane opcije.



14. Kako biste postupili u situaciji da se suočite s ovom obavijesti na web stranici koju posjećujete? *



Označite samo jedan oval.

- ◯ Prihvatio/la bih i nastavio/la na web stranicu
- ◯ Kliknuo/la bih na "Saznajte više"
- ◯ Kliknuo/la bih na "naš 839 partneri"
- ◯ Napustio/la bih web stranicu

15. Kakvo je Vaše povjerenje prema web stranici koja Vam prikazuje ovu obavijest o web kolačićima? *

Označite samo jedan oval.

- ◯ Vrlo nisko
- ◯ Nisko
- ◯ Srednje
- ◯ Visoko
- ◯ Vrlo visoko

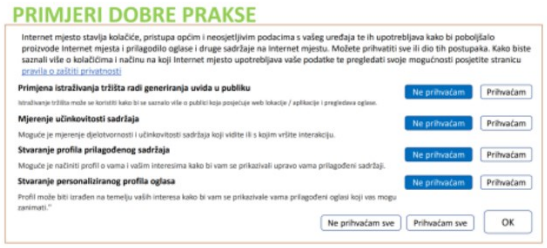
16. Po Vašem mišljenju, smatrate li navedenu suglasnost ispravnom? *

Označite samo jedan oval.

- ◯ Da
- ◯ Ne
- ◯ Nisam siguran/a

Primjer dobre prakse obavijesti o prihvaćanju/ne prihvaćanju kolačića

- Jasno objašnjeno koji podaci se prikupljaju i u koje svrhe;
- Detaljne informacije o obradi podataka dostupne su u Pravilima o zaštiti privatnosti;
- Korisnik sam odlučuje o pristanku za svaki opseg podataka;
- Nema unaprijed definiranih opcija pristanka.



17. Smatrate li da je transparentnost u vezi s web kolačićima važna za korisnike interneta? *

Označite samo jedan oval.

- ◯ Da, vrlo važna
- ◯ Da, važna je
- ◯ Neutralan/na
- ◯ Ne, nije toliko važna
- ◯ Ne, uopće nije važna

18. Koja je Vaša glavna briga u vezi s web kolačićima na internetu? *

Odaberite sve točne odgovore.

- ☐ Kolačići prikupljaju moje osobne podatke bez mog znanja ili dopuštenja
- ☐ Praćenje mojih online aktivnosti putem kolačića i stvaranja profila o meni bez mog pristanka
- ☐ Preopterećenost oglasa mi smeta jer kolačići omogućuju ciljanje oglasa na temelju mojih interesa
- ☐ Nedostatak jasnih informacija o kolačićima i njihovoj svrsi
- ☐ Ništa od navedenog
- ☐ Nisam siguran/a
- ☐ Ostalo: _____

19. Smatrate li da bi zakonodavstvo trebalo strože regulirati korištenje web kolačića na internetu radi zaštite privatnosti korisnika? *

Označite samo jedan oval.

- ◯ Da, apsolutno
- ◯ Da, ali u određenoj mjeri
- ◯ Ne, mislim da je postojeća regulativa dovoljna
- ◯ Nisam siguran/na

20. Koliko često brišete kolačiće s Vašeg uređaja? *

Označite samo jedan oval.

- ◯ Redovno
- ◯ Povremeno
- ◯ Rijetko
- ◯ Nikada

Uklanjanje kolačića

Uklanjanje kolačića s računala je prilično jednostavno. Potrebno je učiniti sljedeće:

- Otvorite postavke preglednika
- Idite na odjeljak "Privatnost i sigurnost"
- Odaberite "Brisanje podataka o pregledavanju" i unutar te opcije odaberite "Kolačići i ostali podaci o web lokacijama" i zatim odaberite opciju "Izbrišite".

21. Imajući detaljnije informacije o tome kako kolačići funkcioniraju, mijenja li to Vaš uobičajeni način reagiranja na obavijesti o kolačićima ubuduće?

Označite samo jedan oval.

- ◯ Da, potpuno mijenja
- ◯ Da, donekle mijenja
- ◯ Ne, ne mijenja
- ◯ Nisam siguran/a

22. Kako biste ocijenili svoje znanje o web kolačićima nakon sudjelovanja u ovoj anketi? *

Označite samo jedan oval.

- ◯ Vrlo dobro
- ◯ Dobro
- ◯ Osrednje
- ◯ Slabo
- ◯ Nedovoljno

KATEGORIJA	WEB STRANICE	P1	P2	P3	P4	P5	P6	P7
E-TRGOVINA	Njuškalo.hr	DA	DA	NE	NE	DA	NE	DA
E-TRGOVINA	Pevex.hr	DA	DA	DA	NE	DA	NE	DA
E-TRGOVINA	Jeftinije.hr	DA	NE	*	*	*	*	DA
E-TRGOVINA	Bauhaus.hr	DA	DA	NE	NE	DA	NE	NE
E-TRGOVINA	Notino.hr	DA	DA	DA	DA	DA	NE	DA
E-TRGOVINA	Aboutyou.hr	DA	DA	DA	DA	DA	NE	DA
E-TRGOVINA	Zalando.hr	DA	DA	DA	NE	DA	DA	DA
E-TRGOVINA	Ecipele.hr	DA	DA	NE	NE	DA	NE	DA
E-TRGOVINA	Mojekrpice.hr	DA	NE	*	*	*	*	DA
E-TRGOVINA	eKupi.hr	DA	DA	NE	NE	NE	*	DA
FINANCIJE	Zaba.hr	DA	DA	DA	DA	NE	*	DA
FINANCIJE	PBZ.hr	DA	DA	DA	DA	DA	NE	DA
FINANCIJE	Euroherc.hr	DA	NE	*	*	*	*	DA
FINANCIJE	OTPbanka.hr	DA	DA	DA	DA	DA	NE	DA
FINANCIJE	Erstebank.hr	DA	DA	DA	NE	DA	NE	DA
FINANCIJE	HNB.hr	DA	DA	DA	DA	DA	NE	DA
FINANCIJE	Crosig.hr	DA	DA	NE	NE	DA	NE	DA
FINANCIJE	Fina.hr	DA	DA	DA	NE	DA	NE	DA
FINANCIJE	RMF.hr	DA	DA	DA	NE	DA	NE	DA
FINANCIJE	HPB.hr	DA	DA	DA	DA	DA	NE	DA
MEDIJI I NOVINARSTVO	Index.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	Jutarnji.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	Vecernji.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	24sata.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	Slobodnadalmacija.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	Tportal.hr	DA	DA	NE	NE	DA	NE	NE
MEDIJI I NOVINARSTVO	Dnevnik.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	n1info.hr	DA	DA	NE	NE	DA	NE	DA
MEDIJI I NOVINARSTVO	telegram.hr	DA	DA	NE	NE	DA	DA	DA
MEDIJI I NOVINARSTVO	RTL.hr	DA	DA	NE	NE	DA	NE	DA
ZDRAVLJE	Roda.hr	DA	DA	DA	NE	NE	*	DA
ZDRAVLJE	Plivazdravlje.hr	DA	DA	NE	NE	DA	NE	DA
ZDRAVLJE	Adiva.hr	DA	DA	NE	NE	DA	NE	DA
ZDRAVLJE	Fitness.hr	DA	NE	*	*	DA	DA	DA
ZDRAVLJE	eljekarna24.hr	DA	DA	DA	NE	DA	NE	DA
ZDRAVLJE	najdoktor.hr	DA	DA	NE	NE	DA	DA	DA
ZDRAVLJE	vitamini.hr	DA	DA	DA	DA	DA	NE	DA
ZDRAVLJE	svkatarina.hr	DA	DA	DA	NE	DA	NE	DA
ZDRAVLJE	lupilu.hr	DA	DA	DA	NE	DA	NE	DA
ZDRAVLJE	kbscm.hr	DA	NE	*	*	*	*	NE
OBRAZOVANJE	ucitelji.hr	NE	*	*	*	*	*	*
OBRAZOVANJE	skole.hr	DA	DA	NE	NE	DA	DA	NE
OBRAZOVANJE	unizg.hr	NE	*	*	*	*	*	*
OBRAZOVANJE	srce.hr	DA	NE	*	*	*	*	DA
OBRAZOVANJE	aaiedu.hr	NE	*	*	*	*	*	*
OBRAZOVANJE	fer.hr	DA	NE	*	*	*	*	NE
OBRAZOVANJE	e-skole.hr	DA	DA	NE	NE	DA	NE	DA
OBRAZOVANJE	ffzg.hr	NE	*	*	*	*	*	*
OBRAZOVANJE	ncvvo.hr	NE	*	*	*	*	*	*
OBRAZOVANJE	unist.hr	DA	DA	DA	DA	DA	NE	DA
TURIZAM	crnojaje.hr	DA	NE	*	*	*	*	NE
TURIZAM	croatiaairlines.hr	DA	DA	DA	NE	DA	DA	DA
TURIZAM	adriatic.hr	DA	DA	DA	NE	DA	NE	DA
TURIZAM	blablacar.hr	DA	DA	DA	NE	DA	NE	DA
TURIZAM	putnikofer.hr	DA	DA	NE	NE	DA	DA	DA
TURIZAM	getbybus.hr	NE	*	*	*	*	*	*
TURIZAM	flixbus.hr	DA	DA	DA	NE	DA	NE	DA
TURIZAM	putoholičari.hr	DA	DA	NE	NE	DA	DA	DA
TURIZAM	zagreb-airport.hr	NE	*	*	*	*	*	*
TURIZAM	jadrolinija.hr	DA	DA	DA	DA	DA	NE	DA

TEHNOLOGIJA	Bug.hr	DA	DA	DA	DA	DA	DA	DA
TEHNOLOGIJA	A1.hr	DA	DA	NE	NE	DA	NE	DA
TEHNOLOGIJA	Hrvatskitelekom.hr	DA	DA	DA	DA	DA	NE	DA
TEHNOLOGIJA	Telemach.hr	DA	DA	DA	DA	DA	NE	DA
TEHNOLOGIJA	Sancta-domenica.hr	DA	DA	NE	NE	DA	NE	DA
TEHNOLOGIJA	links.hr	DA	DA	NE	NE	DA	NE	DA
TEHNOLOGIJA	ozone.hr	DA	DA	NE	NE	DA	DA	DA
TEHNOLOGIJA	hgspot.hr	DA	DA	NE	NE	DA	NE	DA
TEHNOLOGIJA	iskon.hr	DA	DA	DA	DA	DA	NE	DA
TEHNOLOGIJA	instar-informatika.hr	DA	DA	NE	NE	DA	DA	DA
LIFESTYLE	Gloria.hr	DA	DA	NE	NE	DA	NE	DA
LIFESTYLE	Journal.hr	DA	DA	NE	NE	DA	DA	DA
LIFESTYLE	Zenskirecenziraj.com	DA	DA	NE	NE	DA	DA	NE
LIFESTYLE	Story.hr	DA	DA	NE	NE	DA	NE	DA
LIFESTYLE	Coolinarika.com	DA	DA	DA	DA	DA	DA	DA
LIFESTYLE	ELLE.hr	DA	DA	NE	NE	DA	DA	DA
LIFESTYLE	forum.hr	DA	DA	NE	NE	DA	DA	DA
LIFESTYLE	Grazia.hr	DA	NE	*	*	*	*	NE
LIFESTYLE	Zadovoljna.hr	DA	DA	NE	NE	DA	NE	DA
LIFESTYLE	Cromoda.hr	DA	DA	NE	NE	DA	DA	DA
JAVNE USLUGE	hzz.hr	DA	DA	DA	NE	DA	NE	NE
JAVNE USLUGE	porezna uprava.hr	DA	NE	*	*	*	*	DA
JAVNE USLUGE	gov.hr	DA	DA	DA	DA	DA	NE	DA
JAVNE USLUGE	socskrb.hr	DA	DA	DA	DA	DA	NE	DA
JAVNE USLUGE	posta.hr	DA	DA	DA	NE	DA	NE	DA
JAVNE USLUGE	zakon.hr	DA	DA	NE	NE	DA	DA	DA
JAVNE USLUGE	mirovinsko.hr	DA	DA	DA	DA	DA	NE	DA
JAVNE USLUGE	oss.uredjenazemlja.hr	NE	*	*	*	*	*	*
JAVNE USLUGE	ZET.hr	NE	*	*	*	*	*	*
JAVNE USLUGE	HEP.hr	DA	DA	DA	DA	DA	NE	DA
SPORT/KLAĐENJE	supersport.hr	DA	DA	DA	NE	DA	NE	DA
SPORT/KLAĐENJE	lutrija.hr	DA	DA	DA	DA	DA	NE	DA
SPORT/KLAĐENJE	favbet.hr	DA	DA	DA	NE	DA	DA	DA
SPORT/KLAĐENJE	rizk.hr	DA	DA	NE	NE	DA	NE	DA
SPORT/KLAĐENJE	germaniasport.hr	DA	DA	DA	NE	DA	NE	DA
SPORT/KLAĐENJE	admiral.hr	DA	DA	NE	NE	DA	NE	DA
SPORT/KLAĐENJE	psk.hr	DA	DA	NE	NE	DA	DA	DA
SPORT/KLAĐENJE	germanijak.hr	DA	DA	DA	NE	DA	NE	DA
SPORT/KLAĐENJE	sportnet.hr	DA	DA	DA	NE	DA	NE	DA
SPORT/KLAĐENJE	arenacasino.hr	DA	DA	DA	NE	DA	NE	DA

SAŽETAK

Web kolačići su ključni elementi koji omogućuju personalizaciju korisničkog iskustva na internetu, omogućujući web poslužiteljima da pamte informacije o korisnicima. Male tekstualne datoteke pohranjuju se na korisničke uređaje, pomažući web stranicama da prepoznaju korisnike prilikom njihovog povratka na stranicu. Iako pružaju brojne pogodnosti, postavljaju značajne izazove i rizike za privatnost korisnika. Primjeri takvih rizika uključuju XSS i CSRF napade, koji mogu ugroziti sigurnost osobnih podataka. Ovi rizici ističu važnost primjene adekvatnih sigurnosnih mjera i korisničke svijesti o potencijalnim rizicima na webu. Pravne regulative, poput Opće uredbe o zaštiti podataka (GDPR) i Direktive o e-privatnosti, postavljaju stroge zahtjeve za transparentnost i privolu korisnika, čime se nastoji zaštititi privatnost i sigurnost osobnih podataka. Ove regulative zahtijevaju da web stranice jasno obavijeste svakog posjetitelja o korištenju web kolačića i zatraže privolu prije pohranjivanja kolačića na njihove uređaje. Unatoč regulativama, analiza 100 najpopularnijih web stranica s hrvatskom domenom pokazuje da mnoge web stranice ne poštuju u potpunosti pravila propisana GDPR-om. Mnoge web stranice ili ne pružaju jasne obavijesti o korištenju web kolačića ili otežavaju odbijanje kolačića kako bi korisnik bio prinuđen prihvatiti ih, što je protivno načelima GDPR-a. Ova praksa ukazuje na potrebu za strožim nadzorom i kontinuiranom regulacijom kako bi se osigurala zaštita osobnih podataka. Istraživanje provedeno anketnim upitnikom pokazalo je da postoji značajan nedostatak svijesti među korisnicima o tome kako web kolačići funkcioniraju. Mnogi korisnici automatski prihvaćaju web kolačiće bez razumijevanja njihovih implikacija, što naglašava potrebu za edukativnim kampanjama koje će korisnicima pružiti jasne informacije o sigurnosnim rizicima i mogućnostima zaštite. Poboljšanje transparentnosti obavijesti o kolačićima na web stranicama također je ključno za omogućavanje korisnicima donošenja informiranih odluka. Razmatrani su i budući trendovi u korištenju kolačića, uključujući razvoj novih tehnologija koje bi mogle zamijeniti kolačiće u svrhu praćenja korisnika i personalizacije sadržaja. Primjerice, tehnologije poput fingerprintinga mogu omogućiti praćenje korisnika bez potrebe za pohranjivanjem podataka na njihove uređaje. Takvi trendovi zahtijevaju stalno prilagođavanje kako bi se osigurala zaštita osobnih podataka u sve kompleksnijem digitalnom okruženju. Diplomski rad naglašava potrebu za kontinuiranim unaprjeđenjem sigurnosnih mjera, edukacijom korisnika interneta i transparentnošću u korištenju web kolačića, kako bi se očuvalo povjerenje korisnika i zaštitila njihova privatnost.

Ključne riječi: web kolačići, privatnost korisnika, GDPR

SUMMARY

Web cookies are essential elements that enable the personalization of user experiences on the internet by allowing web servers to remember information about users. These small text files are stored on users' devices, helping websites recognize users upon their return. Despite their numerous benefits, cookies pose significant challenges and risks to user privacy. Examples of such risks include XSS (Cross-Site Scripting) and CSRF (Cross-Site Request Forgery) attacks, which can compromise the security of personal data. These risks highlight the importance of implementing adequate security measures and raising user awareness about potential web risks. Legal regulations, such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive, impose strict requirements for transparency and user consent to protect the privacy and security of personal data. These regulations mandate that websites clearly inform visitors about the use of cookies and obtain their consent before storing cookies on their devices. However, despite these regulations, an analysis of the 100 most popular websites with Croatian domains reveals that many websites do not fully comply with GDPR rules. Many websites either fail to provide clear notifications about cookie usage or make it difficult for users to refuse cookies, effectively forcing users to accept them, which contravenes GDPR principles. This practice underscores the need for stricter oversight and continuous regulation to ensure the protection of personal data. A survey conducted through a questionnaire revealed a significant lack of awareness among users about how web cookies function. Many users automatically accept cookies without understanding their implications, emphasizing the need for educational campaigns that provide clear information about security risks and protection options. Improving the transparency of cookie notifications on websites is also crucial for enabling users to make informed decisions. Future trends in cookie usage were also considered, including the development of new technologies that could replace cookies for user tracking and content personalization. For instance, technologies like fingerprinting can enable user tracking without storing data on users' devices. Such trends necessitate continuous adaptation of legal frameworks to ensure the protection of personal data in an increasingly complex digital environment. This thesis highlights the need for ongoing improvement of security measures, user education, and transparency in the use of web cookies to maintain user trust and protect their privacy.

Keywords: web cookies, user privacy, GDPR