

Kolačići i personalizirano oglašavanje

Margetić, Marina

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:131:245644>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-06-26**



Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

[ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences](#)



SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2021./ 2022.

Marina Margetić

Kolačići i personalizirano oglašavanje

Diplomski rad

Mentor: dr.sc. Kristina Kocijan, izv. prof.

Zagreb 2022.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

(potpis)

Sadržaj

Izjava o akademskoj čestitosti	1
Sadržaj	3
1. Uvod	4
2. Kolačići	6
2.1. Povijest kolačića	6
2.2. Podjela kolačića	10
2.2.1. Sesijski kolačići	10
2.2.2. Trajni kolačići	11
2.2.3. Kolačići prve i treće strane	12
2.2.4. Neophodni kolačići	13
2.2.5. Kolačići za funkcionalnost.....	13
2.2.6. Kolačići za performanse	14
2.2.7. Kolačići za praćenje	14
2.3. Stvaranje kolačića	15
2.4. Zloupotreba kolačića.....	16
2.4.1 Fiksacija sesije	17
2.4.2 Usputno otimanje sesije	17
2.4.3 XSS napadi.....	17
2.4.4 Korištenje zlonamjernog softvera	17
2.5. Onemogućavanje kolačića	18
2.6. Zakonske odredbe i regulative	20
2.6.1 ePrivacy direktiva	21
2.6.2 Direktiva o pravima građana.....	21
2.6.3 GDPR (Opća uredba o zaštiti osobnih podataka)	22
2.6.4 Agencija za zaštitu osobnih podataka	22
3. Kolačići i personalizirani marketing	24
3.1. Personalizirano oglašavanje.....	24
3.1.1 Personalizacija publike	25
3.1.2. Personalizacija jedan-na-jedan.....	29
3.2. Postavke personalizacije oglasa	31
3.3. Blokatori oglasa	34
4. Istraživanje	37
4.1 Politika o kolačićima.....	38
4.2. Pristanak korisnika na korištenje kolačića	39
4.3 Pregled obavijesti	42
4.4 Oglasi	46
5.5 Analiza rezultata CookiePro alata.....	47
5. Zaključak	55
6. Literatura	56
Sažetak	59

1. Uvod

U današnje vrijeme većini populacije je teško zamisliti svakodnevni život bez interneta. Internet nam omogućava komunikaciju s ljudima diljem svijeta bez vremenskog odmaka te nam pruža gomilu novosti iz minute u minutu. Prilikom korištenja interneta za pretraživanje raznih informacija, uglavnom ne razmišljamo o svim procesima koji se odvijaju u pozadini već ih primijetimo onda kada nešto ne funkcionira kako bi trebalo. Uređaji koje koristimo za pretraživanje interneta koriste velike količine podataka koje ne vidimo, a neki od tih podataka su i mrežni kolačići (engl. *HTTP cookies*).

Mrežni kolačići su omogućili prikupljanje podataka o korisnicima te su tvrtke u tome vidjele dobru priliku za razvoj mrežnog marketinga. Jedan od glavnih dijelova mrežnog marketinga je oglašavanje, a kolačići omogućavaju da se to oglašavanje personalizira. Korištenjem prikupljenih podataka o korisnicima, tvrtkama je lako definirati interese svojih korisnika te prema tome stvarati oglase koji su namijenjeni određenoj skupini. Pomoću personaliziranih oglasa lakše je privući korisnike koji su već zainteresirani za neki proizvod te stvoriti bolje rezultate od prikazivanja oglasa bilo kojem korisniku. No, korištenje osobnih korisničkih podataka dovodi u pitanje našu privatnost. Stoga je bitno da korisnici znaju zašto i kako se prikupljaju njihovi osobni podaci te također tko ih koristi.

Naredno poglavlje ovog rada daje kompletan pregled kolačića, od samog nastanka pa do načina na koje se koriste danas. Napravljen je povijesni pregled kolačića te način na koji su nastali. Danas postoji puno različitih tipova kolačića koji se mogu podijeliti u nekoliko osnovnih skupina što je prikazano u poglavlju 2.2. Osim toga objašnjeno je i prikazano kodom kako se kolačići stvaraju, a u poglavlju 2.4. opisani su načini na koje se oni mogu zloupotrijebiti.

Kako bi se zloupotreba kolačića svela na najnižu razinu, reagirale su velike tvrtke te omogućile svojim korisnicima onemogućavanje kolačića koje je opisano u poglavlju 2.5. Nedugo nakon toga bilo je potrebno donijeti i zakonske odredbe i regulative koje će spriječiti narušavanje privatnosti korisnika. Pregled tih odredbi i regulativa napravljen je u poglavlju 2.6.

Načini na koje su kolačići pomogli u razvoju personaliziranog marketinga objašnjeni su u trećem poglavlju. Treće poglavlje sadrži pregled personaliziranog oglašavanja, ali i mogućnosti koje su ponuđene korisnicima u svrhu ograničavanja oglasa, kao što su postavke personalizacije i blokatori oglasa.

Kao glavni dio ovog rada napravljeno je istraživanje koje ispituje transparentnost mrežnih stranica u njihovom prikupljanju mrežnih kolačića, na koji se način koriste te također načine na koje korisnik može utjecati na prikupljanje mrežnih kolačića. Također, napravljen je i pregled rezultata dobivenih korištenjem alata za pregled kolačića korištenih na stranicama odabranim za istraživanje. Rezultati istraživanja prikazani su u poglavlju 4.

2. Kolačići

2.1. Povijest kolačića

90-ih godina jedan od najvećih problema prilikom korištenja interneta, odnosno mrežnih stranica, bio je taj da je svaki posjet određenoj stranici bio kao da korisnik stranicu posjećuje prvi put. Navedeno nije uvijek problem, ali to znači da se sve transakcije moraju obaviti odmah. Na primjer, korisnik nije mogao odabrati neke proizvode, spremiti ih u košaricu i zatvoriti stranicu te se nakon nekog vremena vratiti i završiti kupnju. Nije postojala tehnologija koja bi pamtila odabire korisnika te ih kao takve korisniku prikazala prilikom idućeg posjeta toj stranici (Kristol, 2001).

Ovom problemu odlučio je stati na kraj Lou Montulli u lipnju 1994. godine. Montulli je programer koji se 90-ih godina bavio razvojem HTTP-a i HTML-a. 1994. godine postao je jedan od prvih inženjera za tvrtku Mosaic Communications Corporation, koja je kasnije promijenila naziv u Netscape Communications. Kako i sam navodi na svojoj mrežnoj stranici, Montullija možemo "okriviti" za razvoj mrežnih kolačića (Montulli, „www – Lou“). Naime, tijekom rada u današnjem Netscape-u, zaprimili su od jednog korisnika zahtjev za razvojem tehnologije koja će im omogućiti pohranjivanje stanja određene stranice te je tako nastao kolačić. Tehnologija koju je Montulli razvio prvobitno se koristila za provjeru jesu li korisnici već posjetili Netscape mrežnu stranicu (Kukučka, 2021).

Naziv ove tehnologije nastao je od naziva čarobni kolačić (engl. *magic cookie*), koji je svoj naziv dobio od kolačića sreće (engl. *fortune cookie*) koji sadrži skrivenu poruku. Čarobni kolačići su paketi podataka koje program šalje i nepromijenjene zaprima te ih koriste Unix programeri. S obzirom na to da se radi o veoma sličnoj tehnologiji koja je primijenjena na web, Montulli je svojoj tehnologiji dao naziv kolačići (Schwartz, 2001).

Prije prihvaćanja Montullijeve specifikacije, 1995. je osnovan Istraživački fond kako bi se pronašlo rješenje za pohranu stanja na mrežnim stranicama. Kako navodi Kristol (2001), do kraja 1995. postojala su 3 prijedloga za implementaciju tehnologije koja će omogućiti pohranu stanja te je Larry Masinter, predsjednik HTTP radne grupe (engl. *HTTP*

Working Group), zatražio zainteresirane strane da okupe podgrupu koja će predložiti jedan od prijedloga ostatku radne grupe. Navedena podgrupa, koja je uključivala i Loua Montullija te još sedmero stručnjaka, odlučila je prihvatiti Netscape-ov prijedlog te pripremiti preciznu specifikaciju.

Nescape-ova specifikacija definira načine na koje se kolačići smiju dijeliti s drugim serverima te je prema tim pravilima radna podgrupa predvidjela 2 glavna problema. Prvi je taj da bi se kolačići mogli "preliti" u druge servere, a ne samo u one kojima su namijenjeni. Drugi problem je taj da bi neki od servera u domeni mogli namjerno ili slučajno izvesti tzv. DoS napad (engl. *denial-of-service attack*), odnosno napad uskraćivanja usluge gdje bi se mogli slati kolačići koji ometaju aplikaciju koja se nalazi na drugom serveru u toj domeni. Ovo se još naziva i "*cookie spoofing*" ili "*cookie hijacking*", odnosno otimanje sesije ili kolačića. Navedeno se izvodi s ciljem dobivanja pristupa informacijama ili uslugama u računalnom sustavu, točnije za pristup ranije spomenutom magičnom kolačiću koji sadrži podatke za autentifikaciju korisnika prilikom pristupa udaljenom serveru (OWASP, „Session hijacking attack“).

Kristol (2001) navodi kako je radna grupa, u veljači 1996. godine, otkrila značajnu prijetnju privatnosti korisnika. Navedenu prijetnju predstavljaju tzv. **kolačići treće strane** (engl. *third-party cookies*) koji su zapravo transakcije koje nije moguće potvrditi. Bitno je napomenuti kako je transakcije moguće potvrditi onda kada korisnik unaprijed može zaključiti gdje će one ići. Kolačići treće strane pojavljuju se prilikom prikazivanja reklama na mrežnim stranicama. Navedene reklame, odnosno slike, povlače se s drugih stranica te sa sobom donose i kolačiće. U tom slučaju preglednik "posjećuje" drugu mrežnu stranicu, putem transakcije koju nije moguće potvrditi, te s nje učitava reklamu i preuzima kolačiće (Kristol, 2001). Više o kolačićima treće strane bit će navedeno kasnije u ovom radu (poglavlje 2.2.3).

Zabrinutost oko kolačića treće strane navodi i sam Montulli u svom intervjuu za Quartz (Rivero, 2021) gdje opisuje kako su 1996. godine postali svjesni prijetnje te im je to bilo vrlo i iznenađujuće i alarmantno. Montulli dodatno opisuje tri opcije koje su razmatrali.

Prva opcija bila je zanemariti problem i dopustiti oglašivačima da koriste kolačiće treće strane kako žele. Druga opcija bila je u potpunosti blokirati korištenje kolačića treće strane, no treća opcija, ona koju su odlučili pokušati realizirati, je ta da stvore preciznije rješenje u kojemu vraćaju korisnicima kontrolu nad kolačićima, odnosno kontrolu nad načinom na koji oglašivači koriste kolačiće kako bi ih pratili. Kako bi realizirali odabranu opciju, u preglednike su ugradili mnoštvo raznih funkcionalnosti koje korisnicima omogućavaju uvid u kolačiće koji se koriste za prikupljanje podataka. Korisnici također imaju mogućnost odabira načina na koji će se koristiti prikupljeni podaci. Montulli u intervjuu navodi kako im opcija potpunog blokiranja kolačića treće strane nije odgovarala zato što je oglašavanje na mrežnim stranicama bio jedini način za stvaranje prihoda jer u to vrijeme koncept e-trgovine (engl. *e-commerce*) još nije bio toliko razvijen (Rivero, 2021).

Zabrinutost oko privatnosti korisnika nastavila je rasti, ali većina korisnika nije toga bila svjesna sve dok Financial Times 12. veljače 1996. nije izdao članak pod nazivom "*This bug in your PC is a smart cookie*". To je bio prvi članak koji je širu javnosti upozorio na opasnosti mrežnih kolačića. Autor članka, Tim Jackson, upozorava korisnike na neke opasnosti koje su vjerojatno previdjeli prilikom korištenja interneta. Jackson navodi kako je tehnologija kolačića dostupna već od verzije 1.2 Netscape-ovog preglednika te se sama specifikacija, napisana u lipnju 1995., može pročitati unutar preglednika. Također, navodi kako se kolačići koriste u svrhu personalizacije oglašavanja te čitatelja podsjeća na često korištenu izreku u marketingu koja kaže kako je pola uloženog novca u oglašavanje potraćeno, ali se nikada ne zna koja polovica. Na kraju članka, autor zaključuje kako je najgora stvar koja se može dogoditi ta da će tvrtke korisnicima pokušati prodati nešto (Jackson, 1996).

Iako je Radna skupina za razvoj interneta (engl. *Internet Engineering Task Force – IETF*) u samom početku korištenja kolačića u publikaciji RFC 2109 dala prijedlog za blokiranje kolačića treće strane, većina preglednika i tvrtki su odlučile ignorirati taj prijedlog. Kako bi stali na kraj glasinama koje su se počele širiti u javnosti, Savjetodavni odbor za računalne sigurnosne incidente (engl. *Computer Incident Advisory Capability – CIAC*), izdao

je priopćenje. U priopćenju navode kako kolačići ne uništavaju i ne kompromitiraju datoteke ili sustave te se koriste samo za identifikaciju korisnika, ali mogu se koristiti i za praćenje korisničkih navika pregledavanja sadržaja. Također, korisnicima daju prijedlog da onemoguće prikupljanje i korištenje kolačića unutar preglednika ili da koriste neke od paketa za blokiranje kolačića. CIAC napominje kako većina kolačića postoji samo dok korisnik koristi preglednik, osim trajnih kolačića koji imaju datum isteka. U navedenom priopćenju stoji kako informacije o stranicama koje korisnici koriste već postoje u zapisima mrežnih servera te se mogu koristiti za praćenje, a kolačići to samo olakšavaju (CIAC, 1998).

Nastavno na nove zabrinutosti oko sigurnosti korisničke privatnosti, 2000. godine izdana je nova RFC publikacija¹ koja detaljno opisuje kada i kako bi se određene vrste kolačića trebale koristiti. Time se pokušao olakšati rad preglednicima koji nisu bili prilagođeni prvoj RFC 2109 publikaciji, no nažalost i ove smjernice su se ubrzo zaboravile te su se kolačići i dalje nastavili koristiti ugrožavajući privatnost korisnika.

Kako su velike tvrtke nastavile prikupljati razne podatke o korisnicima, Europska Unija je 12. srpnja 2002. godine izdala Direktivu 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama). U njoj stoji kako *“dopunjujući Direktivu 95/46/EZ, ova Direktiva ima za cilj zaštititi temeljna prava fizičkih osoba, posebno njihovo pravo na privatnost, kao i legitimne interese pravnih osoba”* (Europski parlament i Vijeće Europske Unije, 2002). Više o navedenoj Direktivi bit će objašnjeno u poglavlju 2.6.

2011. godine je Europska Unija donijela novu direktivu koja je poznata kao Zakon o kolačićima (engl. *The Cookie Law*) koja je napokon stala na kraj mahnitom prikupljanju podataka korisnika putem kolačića. Navedena direktiva prihvaćena je od strane svih država članica u svibnju 2011. godine. Zakon o kolačićima navodi kako je protuzakonito

¹ RFC publikacija (engl. *Request for Comments*) je službeni dokument koji izdaje IETF (Internet Engineering Task Force) na temelju podataka o razvoju neke tehnologije

postavljati kolačiće trećih strana na uređaje korisnika bez njihovog pristanka (cookielaw, „The Cookie Law Explained“).

2.2. Podjela kolačića

Prema definiciji Hrvatske enciklopedije, mrežni kolačić je „*mala tekstovna datoteka s informacijama o aktivnostima i postavkama korisnika, koja se na njegov uređaj (računalo, mobitel i sl.) pohranjuje prigodom posjeta pojedinoj mrežnoj stranici*“.

Preglednici mogu sadržavati velike količine kolačića u takozvanoj kutiji za kolačiće (engl. *Cookie Jar*) no ne šalju ih svakoj stranici koju korisnik posjeti jer to ne bi bilo praktično niti sigurno. Preglednici šalju stranicama samo one kolačiće koji su relevantni za tu stranicu, na primjer kolačići stvoreni na stranici coca-cola.hr neće biti poslani na stranicu led.hr. Kada bi preglednici slali sve kolačiće svim stranicama to bi značajno usporilo rad preglednika te bi također dovelo to ugrožavanja privatnosti korisnika jer bi stranice kojima korisnik nije dozvolio pristup nekim kolačićima na taj način mogle doći do podataka koje pohranjuju (Gourley et al., 2002).

Kolačići se mogu podijeliti u tri grupe ovisno o svom trajanju (engl. *duration*), porijeklu (engl. *provenance*) i namjeni (engl. *purpose*). Svaka od navedenih grupa sadrži nekoliko različitih vrsti kolačića. Kolačići se prema trajanju mogu definirati kao sesijski i trajni kolačići. Prema porijeklu se razlikuju kolačići prve strane i kolačići treće strane, a prema namjeni razlikujemo neophodne kolačiće, kolačiće za funkcionalnost, kolačiće za performanse i kolačiće za praćenje („Cookies, the GDPR, and the ePrivacy Directive“, 2019). U nastavku ćemo reći nešto više o svakom navedenom kolačiću.

2.2.1. Sesijski kolačići

Sesijski kolačići (engl. *session cookies*) su tipovi mrežnih kolačića koji se pohranjuju samo privremeno, odnosno brišu se kada korisnik napusti stranicu. Ova vrsta kolačića omogućava pamćenje stanja košarice u internetskim trgovinama, bodova u igricama i sl.

Navedeno olakšava korisnicima korištenje stranice te isključuje potrebu za ponovnim upisivanjem podataka u obrascima ili punjenjem košarice. Većina stranica koristi sesijske kolačiće za bitne funkcionalnosti stranice (Gourley et al., 2002).

2.2.2. Trajni kolačići

Trajni kolačići (engl. *persistent cookies*) se pohranjuju na uređaju korisnika te sadrže informacije, postavke i korisničke podatke. Navedeni kolačići osiguravaju jednostavnije korištenje stranica jer pamte odabire korisnika vezano za boju i veličinu teksta na stranici, jezik te također pamte i korisničke podatke za prijavu na stranice te ih korisnik ne mora upisivati prilikom svake prijave (Gourley et al., 2002).

Name	V.	D	P.	Expires / Max-Age
INGRESSCOOKIE	W..	w...	/	Session
sid	m...	w...	/	Session
POD	8...	w...	/	Session
_gat_gtag_UA_92084236_1	1	/	2022-05-26T15:27:48.000Z
_gid	G...	/	2022-05-27T15:26:48.000Z
1P_JAR	2...	/	2022-06-25T15:26:47.552Z
_gcl_au	1...	/	2022-08-24T15:26:48.000Z
_fbp	f...	/	2022-08-24T15:26:49.000Z
AEC	A...	/	2022-11-22T15:26:45.021Z
NID	5...	/	2022-11-25T15:26:47.552Z
CONSENT	Y...	/	2024-05-25T15:26:47.055Z
_ga	G...	/	2024-05-25T15:26:48.000Z

Slika 1. Trajanje kolačića²

Slika 1 prikazuje trajanje kolačića koje prikuplja mrežna stranica kras.hr. Na slici su vidljiva tri kolačića, „INGRESSCOOKIE“, „sid“ i „POD“ kojima u polju „Expires / Max-Age“ kao datum isteka stoji „Session“. Navedeno predstavlja sesijske kolačiće koji će se, kao što je ranije navedeno, obrisati kada korisnik napusti stranicu. Ostali kolačići imaju definiran

² Ekranska slika napravljena na stranici <https://www.kras.hr/>

datum isteka, odnosno datum kada će se obrisati s korisnikovog uređaja te se prema tome definiraju kao trajni kolačići.

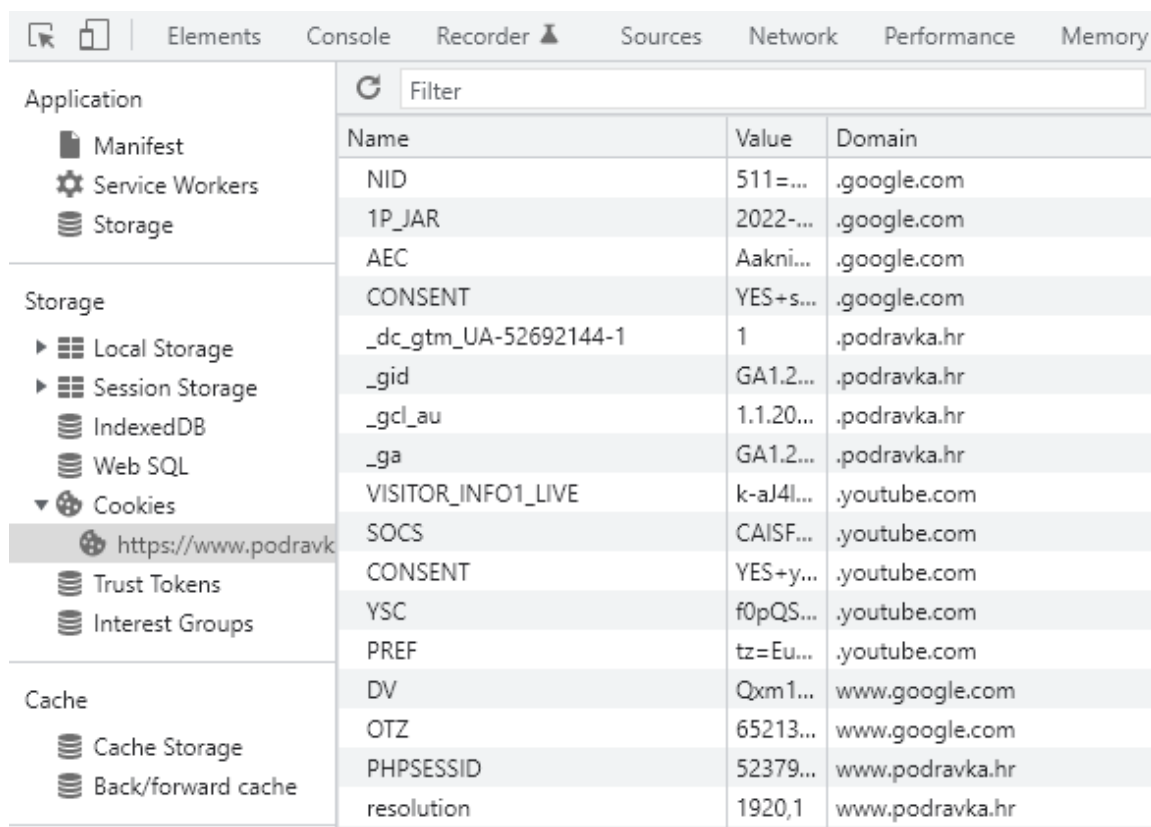
2.2.3. Kolačići prve i treće strane

Kao što je ranije navedeno, kolačići se prema porijeklu dijele na kolačiće prve strane (engl. *first-party cookies*) i kolačiće treće strane (engl. *third-party cookies*).

Kolačići prve strane su oni koje postavlja stranica na kojoj se korisnik nalazi. Oni se koriste za pohranu analitičkih podataka, podataka o odabirima korisnika i slično. Na stranici CookiePro je navedeno kako bez kolačića prve strane korisnici ne bi mogli kupiti više proizvoda odjednom jer bi se košarica internetske trgovine prilikom dodavanja novog proizvoda osvježila te bi se time obrisao ranije dodani proizvod (Kulyk et al., 2018).

Kolačići treće strane su kolačići koje na uređaj korisnika postavlja neka druga stranica od one koju je korisnik posjetio. Navedeni kolačići najčešće se koriste u svrhe oglašavanja te se postavljaju koristeći skripte (engl. *scripts*) i oznake (engl. *tags*). Kolačići treće strane omogućavaju oglašivačima praćenje korisnika po stranicama koje posjećuju. Kada korisnik posjeti neku stranicu ona postavi određene kolačiće. Nakon toga se učita reklama koja zapravo dolazi s neke druge stranice te se pomoću te reklame postavljaju kolačići treće strane, odnosno te druge stranice, na uređaj korisnika. Kolačići treće strane se sve manje koriste te ih je većina preglednika zabranila (Kulyk et al., 2018).

Na Slici 2 prikazani su kolačići koje prikuplja stranica podravka.hr. Svi kolačići koji kao domenu u polju „Domain“ imaju navedeno „podravka.hr“ smatraju se kolačićima prve strane te ih postavlja navedena stranica. Ostali kolačići su kolačići treće strane. U primjeru sa slike vidljivo je kako postoji nekoliko kolačića s domene „youtube.com“. Stranice koje postavljaju video zapise s platforme YouTube „pozivaju“ kolačiće treće strane na svoju stranicu. Naime, YouTube automatski postavlja kolačiće za praćenje u marketinške svrhe, ali korisnici nisu upitani za dozvolu te navedeno predstavlja kršenje GDPR-a.



Name	Value	Domain
NID	511=...	.google.com
1P_JAR	2022-...	.google.com
AEC	Aakni...	.google.com
CONSENT	YES+s...	.google.com
_dc_gtm_UA-52692144-1	1	.podravka.hr
_gid	GA1.2...	.podravka.hr
_gcl_au	1.1.20...	.podravka.hr
_ga	GA1.2...	.podravka.hr
VISITOR_INFO1_LIVE	k-aJ4l...	.youtube.com
SOCS	CAISF...	.youtube.com
CONSENT	YES+y...	.youtube.com
YSC	f0pQS...	.youtube.com
PREF	tz=Eu...	.youtube.com
DV	Qxm1...	www.google.com
OTZ	65213...	www.google.com
PHPSESSID	52379...	www.podravka.hr
resolution	1920,1	www.podravka.hr

Slika 2. Porijeklo kolačića³

2.2.4. Neophodni kolačići

Nadalje, neophodni kolačići (engl. *strictly necessary cookies*) su oni koje stanice moraju koristiti kako bi mogli korisniku pružiti određene funkcionalnosti. Neophodni kolačići koriste se za prijavu, zadržavanje proizvoda u košarici i slično. Oni su u većini slučajeva kolačići prve strane te su jedini kolačići koje svi zakoni dopuštaju.

2.2.5. Kolačići za funkcionalnost

Kolačići za funkcionalnost (engl. *Functionality cookies*) koriste se kako bi stranice mogle zapamtiti neke preferencije korisnika, kao što su regija ili jezik. Navedeni kolačići ne

³ Ekranska slika napravljena na stranici <https://www.podravka.hr/>

koriste se za praćenje korisnika već omogućavaju stranicama da korisniku ponudi personalizirani sadržaj kao što su na primjer lokalne vijesti. *Information Commissioner's Office* (ICO) navodi kako se kod korištenja kolačića za funkcionalnost može podrazumijevati pristanak korisnika.

2.2.6. Kolačići za performanse

Kolačići za performanse (engl. *performance cookies*) su kolačići koji se koriste za prikupljanje podataka o načinu na koji korisnici koriste određenu stranicu. Na primjer, ovi kolačići broje koliko puta je neki korisnik posjetio stranicu, koje je vrijeme učitavanja stranice ili koji je postotak korisnika koji otvore stranicu te ju odmah napuste. U većini slučajeva kolačići za performanse se koriste od strane stranice koju je korisnik posjetio i navedeni podaci se ne dijele s dugim stranama. Ova vrsta kolačića uglavnom spada pod trajne ili sesijske kolačiće.

2.2.7. Kolačići za praćenje

Kolačići za praćenje (engl. *tracking cookies*) su uzorci teksta koji se postavljaju na preglednik prilikom korištenja stranice. Navedeni kolačići mogu prikupljati podatke o aktivnosti korisnika na stranici, lokaciji korisnika, navike kupnje, povijest pregledavanja i slično. Za razliku od ostalih vrsta kolačića, kolačići za praćenje mogu pratiti korisnika preko raznih stranica i prikupljati podatke. Podatci koji se prikupe na ovakav način uglavnom se koriste u marketinške svrhe te je jedan od primjera korištenja i personalizirano oglašavanje. Od preglednika još jedino Google Chrome dozvoljava korištenje ovih kolačića te i svih ostalih kolačića treće strane. Među kolačiće za praćenje spada i tzv. Superkolačić (engl. *Supercookie*). Superkolačić je vrsta kolačića za praćenje koja se postavlja u HTTP zaglavlje od strane davatelja usluga interneta kako bi se pratile navike korisnika kod korištenja interneta te povijest pretraživanja.

2.3. Stvaranje kolačića

Prije samog stvaranja kolačića, potrebno je razumjeti kako kolačići funkcioniraju. Kod korištenja kolačića bitan je HTTP, odnosno *Hypertext Transfer Protocol*. Enciklopedija Britannica navodi kako je HTTP protokol na aplikacijskoj razini koji se koristi za prijenos datoteka na internetu. Mrežni preglednici su HTTP klijenti koji šalju zahtjeve mrežnim serverima koji onda obrađuju te zahtjeve putem HTTP servisa. Putem HTTP zahtjeva (engl. *HTTP request*) šalju se Set-Cookie zaglavlja (engl. *header*) s odgovorom od strane servera. Navedeno Set-Cookie HTTP zaglavlje šalje kolačiće od servera prema korisničkom klijentu (Barth, 2011).

Kolačići se mogu stvarati u raznim programskim jezicima, a u ovom poglavlju bit će objašnjeno stvaranje kolačića koristeći JavaScript.

```
document.cookie = newCookie;
```

Navedeni dio koda predstavlja stvaranje novog kolačića. "document.cookie" je svojstvo unutar JavaScript-a koje omogućava stvaranje kolačića. Na ovaj način se može stvarati ili ažurirati samo po jedan kolačić. Kao što je ranije navedeno, kolačići imaju domene te se prema tome razlikuje njihovo porijeklo. Kako bismo kolačiću dodali naziv i domenu, nastavno na gore prikazani dio koda potrebno je navesti atribute "name" i "domain", odnosno:

```
document.cookie = "name=linzer; domain='primjer.com'"
```

Na ovaj način se kolačiću definirala domena "primjer.com", a u slučaju da se domena ne postavi putem koda, tada se automatski postavlja domena od poslužitelja na kojemu se nalazi dokument.

Kolačićima možemo definirati vrijeme isteka te ih prema tome označiti kao sesijske ili trajne kolačiće. Kolačić koji ima definirano trajanje koristeći atribut "expires" smatra se trajnim kolačićem, a u slučaju da kolačiću ne postavimo datum isteka tada će se taj kolačić obrisati po zatvaranju stranice. Takav kolačić se smatra sesijskim kolačićem.

```
document.cookie = "name=linzer; domain='primjer.com';  
expires=Sun, 25 Dec 2022 23:59:59 GMT"
```

Na primjeru koda prikazan je kolačić kojemu je definiran datum isteka te će se prema tome kolačić obrisati 26. prosinca 2022. godine. Osim korištenja atributa "expires" možemo koristiti i atribut "max-age" te u sekundama upisati trajanje kolačića:

```
document.cookie = "name=linzer; domain='pimjer.com';  
max-age=" + (60 * 60 * 24 * 365) + ""
```

Nadalje, ako imamo stranicu koja se sastoji od nekoliko pod-domena, kolačiću možemo omogućiti da je vidljiv na svim tim pod-domenama dodajući mu atribut "path". Kada kao vrijednost navedenog atributa postavimo znak "/" znači da će kolačić biti dostupan na cijeloj stranici i svim pod-domenama.

```
document.cookie = "name=linzer; domain='primjer.com';  
expires=Sun, 25 Dec 2022 23:59:59 GMT; path=/"
```

Prikazanim kodom definiran je kolačić "linzer" koji se nalazi na domeni primjer.com te je dostupan na toj domeni i svim njenim pod-domenama, a traje do 26. prosinca 2022. godine kada će se obrisati.

2.4. Zloupotreba kolačića

Kao i u većini tehnologija koje su nastale, i kod kolačića je došlo do zlouporabe. S obzirom na to da određeni kolačići sadrže razne podatke o korisnicima, postali su zanimljivi hakerima koji su pronašli načine kako da ukradu i zlouporabe te podatke, odnosno kako da otmu sesije korisnika.

Otimanje sesije podrazumijeva iskorištavanje valjanje sesije korisnika radi dobivanja neovlaštenog pristupa određenim podacima ili servisima. Otimanje sesije može se postići koristeći četiri metode: fiksacija sesije, usputno otimanje sesije, XSS napadi i korištenje zlonamjernog softvera (Wagner, 2020) koje ćemo u nastavku ukratko opisati.

2.4.1 Fiksacija sesije

Fiksacija sesije (engl. *Session fixation*) je metoda otimanja sesije u kojoj napadač postavlja korisnički ID sesije putem kojeg će, nakon prijave korisnika, moći pristupiti podacima kojima korisnik inače ima pristup. Najčešće se korisnički ID sesije postavlja tako da napadač korisniku pošalje poveznicu koja sadrži taj ID putem e-maila.

2.4.2 Usputno otimanje sesije

Kod usputnog otimanja sesije (engl. *Session sidejacking*) napadač presreće i čita podatke iz mrežnog prometa između dvije strane te krađe sesijski kolačić. Pomoću sesijskog kolačića napadač se može lažno predstaviti kao korisnik kako bi dobio pristup podacima. Na ovakve vrste otimanja sesije su najranjivije nezaštićene Wi-Fi mreže jer omogućavaju da korisnici koji koriste tu mrežu čitaju podatke o mrežnom prometu.

2.4.3 XSS napadi

U XSS (*Cross site scripting*) napadima vrši se postavljanje zlonamjernih skripti unutar stranica koje su inače povjerljive. Napadači korištenjem mrežnih aplikacija pomoću skripti šalju zlonamjerne kodove korisnicima koji ne mogu znati da je to zlonamjerni kod koji bi im mogao naštetiti. Navedene skripte mogu pristupiti kolačićima, tokenima sesije i raznim drugim podacima koji se pohranjuju unutar preglednika a koriste na stranici na kojoj je postavljena skripta (Tirtea *et al.*, 2011).

2.4.4 Korištenje zlonamjernog softvera

Korištenjem zlonamjernog softvera (engl. *malware*) može se postići takozvano otimanje preglednika (engl. *Browser Hijacking*). Otimanje preglednika je modificiranje postavki preglednika bez dopuštenja korisnika u svrhu postavljanja neželjenih oglasa.

Prilikom otimanja preglednika napadač također može postaviti i softver za praćenje koji će prikupljati informacije o korisniku.

2.5. Onemogućavanje kolačića

Sve češćim korištenjem kolačića rasla je zabrinutost oko privatnosti korisnika te su samim time neke tvrtke odlučile poduzeti nešto kako bi spriječile narušavanje te privatnosti.

Prva tvrtka koja je odlučila stati na kraj neograničenom prikupljanju i korištenju korisničkih podataka pomoću kolačića bio je Apple. Naime, Apple je 2015. godine, u verziji 9 iOS-a donio nekoliko novosti, a među njima je bila i mogućnost korištenja blokatora sadržaja u pregledniku Safari. Navedeno je omogućilo korisnicima stvaranje i korištenje blokatora oglasa (engl. *Ad blocker*). Ove novosti od strane tvrtke Apple oglašivači nisu dobro prihvatili te je Google, 26. kolovoza 2015. godine, izdao savjete kako se mogu zaobići nova ograničenja u iOS-u 9 u članku naziva „Handling App Transport Security in iOS 9“. U članku navode kako korisnici mogu zaobići navedena ograničenja tako da dodaju iznimke koje dozvoljavaju prolazak HTTP zahtjevima te učitavanje nesigurnog sadržaja. Dan nakon, 27. kolovoza 2015. godine, objavili su dodatak navedenom članku u kojemu navode kako su dan ranije izdali navedene savjete jer su ih razvojni programeri zatražili izvore koji im stoje na raspolaganju za nadolazeći iOS 9. Također, napomenuli su kako bi se ovaj postupak trebao provoditi samo kada svi drugi pokušaji prilagodbe koji su sukladni *App Transport Security* (ATS) značajki ne uspiju.

Apple je odlučio 2017. godine otići još jedan korak dalje u prevenciji praćenja svojih korisnika te su izdali *Intelligent Tracking Prevention 2.0 (ITP 2.0)* značajku. *ITP 2.0* automatski dijeli kolačiće po domenama za koje je ustanovljeno da mogu pratiti korisnike te također otklanja mogućnost pristupanja kolačićima unutar 24 sata. Sukladno navedenom, tvrtke više ne mogu ponovo ciljati proizvode prema korisnicima čak ni unutar 24 sata od zadnjeg posjeta njihovoj stranici od strane korisnika. Također, nakon objave *ITP 2.1* i *2.2* kolačići prve strane su se počeli filtrirati prema funkcionalnosti, a analitički

kolačići su se brisali nakon 24 sata. Ovime je Apple zabranio korištenje kolačića treće strane te se time uvelike otežao rad oglašivača koji više nisu mogli kvalitetno analizirati i koristiti podatke korisnika iz Safari preglednika u svrhu personalizacije oglasa.

Firefox je 2018. godine počeo mijenjati svoju politiku privatnosti u korist korisnika tako što su omogućili korištenje blokatora kolačića treće strane i blokatora praćenja. U verziji 65.0 preglednika Firefox, objavljenoj 29. siječnja 2019. godine, izdana je poboljšana zaštita od praćenja. Navedeno je omogućilo korisnicima da sami odaberu na koji način će se kontrolirati praćenje te su im ponuđene tri opcije: standardna, stroga i prilagođena. Korisnici su s navedene tri opcije mogli odabrati koji će se kolačići blokirati te su tako mogli blokirati kolačiće treće strane, ali i sve kolačiće uključujući kolačiće prve strane. Nakon nekoliko narednih verzija Firefox preglednika, blokiranje kolačića treće strane postalo je automatsko.

Google Chrome je tek u kolovozu 2019. godine odlučio poduzeti nešto te su najavili *Privacy Sandbox*. Google je također naveo kako razumiju problem narušavanja privatnosti od strane kolačića treće strane, ali također smatraju kako blokiranje korištenja tih kolačića može dovesti do korištenja drugih tehnologija za praćenje, točnije takozvanoj *fingerprinting* tehnologiji. Navedena tehnologija je invazivnija od korištenja kolačića jer njom tvrtke stvaraju profile korisnika u kojima se pohranjuju svi podaci koji se prikupe od onih o hardware-u i software-u do nekih preferencija korisnika. Google, umjesto potpune zabrane korištenja kolačića treće strane, predlaže stvaranje novih standarda za web koji bi zaštitili privatnost korisnika, ali bi i omogućili zadržavanje određenih mogućnosti praćenja korisnika u svrhu personalizacije oglašavanja.

Sud Europske Unije je 1. listopada 2019. godine odlučio kako se unaprijed označene kućice za pristanak na prikupljanje kolačića ne smatraju pristankom te također kako podaci o kolačićima moraju sadržavati informaciju o trajanju kolačića te o tome imaju li treće strane pristup tim kolačićima.

Od ožujka 2020. godine kolačići treće strane automatski su blokirani unutar preglednika Safari te je time Apple ponovno bila prva tvrtka koja je poduzela daljnje

korake u zaštiti privatnosti svojih korisnika. Uz navedeno, unutar preglednika Safari tvrtka Apple je također blokirala korištenje ranije spomenute tehnologije *fingerprinting*.

Nakon nekih velikih koraka koje su poduzele druge tvrtke, Google je odlučio pokušati stvoriti alternativno rješenje kako ne bi morali potpuno ukinuti korištenje kolačića treće strane te su tako stvorili *Federated Learning of Cohorts* ili skraćeno FLoC.

FLoC je bio osmišljen kao tehnologija koja bi omogućila korisnicima da zadrže anonimnost, ali bi također ostavila priliku oglašivačima da ciljaju korisnike prema njihovim interesima. Korisnike bi se grupiralo prema tim interesima te se njihovi podaci ne bi dijelili s Google-om ili nekom drugom stranom. Većina preglednika nije prihvatila ovaj prijedlog alternativne tehnologije jer bi ona mogla dovesti do drugačijih napada na privatnost korisnika te je također postojala mogućnost da se korisnicima prikazuju diskriminirajuće reklame. S obzirom na zabrinutosti oko Google-ove nove tehnologije, Europska komisija je pokrenula protumonopolsku istragu kako bi se utvrdilo je li Google prekršio neke odredbe Europske Unije koristeći *FLoC*. Do siječnja 2022. tehnologija *FLoC* je u potpunosti odbačena od strane Google-a te su je zamijenili novom tehnologijom *Topics API*.

Topics API je tehnologija koja funkcionira na način da određenim stranicama dodijeli određene teme i prema tome se prikupljaju informacije o navikama pretraživanja korisnika. Najveća razlika između *FLoC* i *Topics API* tehnologija je ta da se u *Topics API* tehnologiji ne grupira korisnike te se na taj način sprječava identifikaciju pojedinog korisnika. Za sada još nije poznato hoće li se nova Google-ova tehnologija koristiti, ali već postoje određene zabrinutosti od strane manjih tvrtki koje imaju manje budžete.

Mozilla je također u veljači 2021. godine najavila potpunu zaštitu od kolačića u pregledniku Firefox. Osim kolačića za praćenje, svi ostali kolačići se održavaju zasebno te to osigurava da se korisnike ne može pratiti prilikom pregledavanja sadržaja na web-u.

2.6. Zakonske odredbe i regulative

Uz razvoj digitalnog marketinga i personaliziranog oglašavanja rasla je i zabrinutost korisnika oko njihove privatnosti na internetu. Osim tvrtki koje su poduzele razne korake

kako bi zaštitile svoje korisnike, prikupljanje podataka je bilo potrebno i zakonski regulirati kako bi korisnici imali dodatnu sigurnost.

2.6.1 ePrivacy direktiva

Prva direktiva Europske Unije koja se pozabavila korištenjem kolačića izdana je 2002. godine kao Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) koja je poznatija po skraćenom nazivu ePrivacy direktiva (ePD). U navedenoj direktivi stoji kako se korištenje kolačića treba dopustiti ako je namijenjeno legitimnoj svrsi no korisniku se mora pružiti jasna i precizna informacija o svrsi kolačića. Također, navedeno je kako korisniku mora biti ponuđena mogućnost odbijanja pohrane kolačića. Uz navedeno također je propisano da korisnicima treba biti ponuđeno što više jasnih informacija o načinima prikupljanja i korištenja kolačića. U ePD-u se također spominje i marketing te je navedeno kako se korisnicima treba ponuditi mogućnost zaštite protiv narušavanja privatnosti neželjenom komunikacijom u svrhu izravnog marketinga.

2.6.2 Direktiva o pravima građana

Iako je u ePrivacy direktivi pokriven velik dio zabrinutosti oko kolačića, direktivu je bilo potrebno dopuniti kako bi obuhvatila što je više moguće problematičnih aspekata korištenja podataka o korisnicima. Tako je, 2009. godine, ePD nadopunjena direktivom koja je poznata kao Direktiva o pravima građana (engl. *Citizens' Rights Directive*). U navedenoj direktivi stoji kako operateri moraju prijaviti incidente koji su se dogodili vezano za podatke korisnika kao što je, na primjer, krađa podataka. Također, navedeno je kako tvrtke moraju na svojim stranicama dobiti pristanak korisnika za prikupljanje i obradu kolačića. Ova direktiva kasnije je postala poznata kao Zakon o kolačićima (engl. *The Cookie Law*).

Zakon o kolačićima propisuje da stranice smiju postavljati kolačiće na uređaje korisnika nakon što korisniku daju jasne i precizne informacije o načinu korištenja podataka koji će se prikupiti s tim kolačićima. Korisnicima bi također trebala biti ponuđena mogućnost odbijanja kolačića na početku pregledavanja stranice te isto tako i u bilo kojem trenutku. Informacije koje se korisniku nude vezano za kolačiće moraju biti predstavljene na jednostavan način koji je prilagođen korisniku. Zakon o kolačićima isključuje kolačiće koji su neophodni za rad stranice ili za prijenos podataka u svrhu komunikacije.

2.6.3 GDPR (Opća uredba o zaštiti osobnih podataka)

Još jedan korak dalje napravljen je 2016. godine kada je uspostavljen takozvani GDPR (engl. *General Data Protection Regulation*), odnosno Opća uredba o zaštiti osobnih podataka. Navedena uredba u Hrvatskoj je na snazi od 25.05.2018. godine.

GDPR se primarno bavi zaštitom osobnih podataka korisnika te uz to propisuje i pravila prema kojima se podaci mogu koristiti. Također, navodi i kako korisnici moraju moći donijeti odluku o prihvaćanju načina na koje se njihovi podaci prikupljaju i koriste. U uredbi je spomenut i izravni marketing te je navedeno kako bi “korisnik trebao imati pravo prigovora na obradu osobnih podataka u tu svrhu” (Europski parlament i vijeće, 2016). Bitno je napomenuti da se GDPR ne odnosi samo na Europsku Uniju već i na treće zemlje, odnosno tvrtke i organizacije, koje obrađuju podatke stanovnika Europske Unije.

2.6.4 Agencija za zaštitu osobnih podataka

U Hrvatskoj je za provedbu nadzora nad korištenjem osobnih podataka zadužena Agencija za zaštitu osobnih podataka (AZOP) koja je osnovana temeljem Zakona o zaštiti osobnih podataka, a započela je s radom 2004. godine (AZOP, „Djelokrug“).

U Ustavu Republike Hrvatske (2010) navedeno je: „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te

nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.“ te se time vodi i AZOP prilikom obavljanja nadzora.

Ukratko, uredbe i direktive navedene u ovom poglavlju propisuju da:

- korisnik mora dati svoj pristanak na korištenje svih kolačića, osim onih neophodnih, kako bi se pomoću kolačića mogli prikupljati podaci
- korisniku moraju biti dostupne jednostavne, lako razumljive, specifične i ispravne informacije o kolačićima i podacima koje oni prikupljaju
- pristanak korisnika mora se pohraniti
- korisnik mora imati pristup uslugama čak i kada odbije korištenje određenih kolačića
- korisnik mora imati mogućnost na jednostavan način povući svoj pristanak na korištenje kolačića (Basart Dotras, 2021).

3. Kolačići i personalizirani marketing

Razvoj interneta doveo je i do razvoja digitalnog marketinga. Razni korisnici koriste internet te je to jedinstvena prilika oglašivačima da reklamiraju svoje proizvode i tako privuku nove kupce. Digitalni marketing podrazumijeva oglašavanje na raznim digitalnim kanalima, a neki od njih koriste i kolačiće. Kolačići su oglašivačima omogućili personalizaciju oglašavanja, odnosno biranje korisnika kojima će reklamirati svoje proizvode. Kako bi se znalo koji su prikladni korisnici, potrebno je imati i neke podatke o njima. Kolačići omogućavaju pristup upravo takvim podacima koji će oglašivaču dati informacije o interesima, navikama i povijesti kupovine, lokaciji i slično. Postoje razne vrste personaliziranog oglašavanja kao što su prilagođeni mailovi, ciljani popusti ili personalizirane reklame.

3.1. Personalizirano oglašavanje

Personalizirano oglašavanje postalo je popularan način oglašavanja na digitalnim kanalima jer korisnicima nudi proizvode povezane s onima koje su ranije pretraživali. Kolačići su omogućili prilagodbu oglasa prema određenim karakteristikama kupaca kao što su na primjer lokacija ili prethodne navike kupovine. Personalizirani marketing koristi se kampanjama koje su prilagođene korisnicima prema demografiji i interesima te ih je moguće vrlo ciljano usmjeriti na određene korisnike.

Prednosti personaliziranog marketinga su veće zadovoljstvo kupaca s iskustvom kupovine, povećana vjernost kupaca te veći povratak uloženog novca u oglašavanje. Naravno, kada se korisniku prikaže oglas povezan s nekim prijašnjim pretraživanjima, dolazi i do određene zabrinutosti korisnika oko njegove privatnosti. Zbog navedenog oglašivači trebaju biti oprezni te odabrati pravu mjeru u kojoj će koristiti prikupljene podatke korisnika u svrhu marketinga.

Kako navode Gourley i Totty (2002), mnoge stranice surađuju s dobavljačima treće strane koji upravljaju oglasima. Objašnjavaju kako se trajni kolačići, stvoreni prilikom

korisnikova posjeta određenoj stranici, ponovo koriste u slučaju da korisnik posjeti drugu stranicu koja surađuje s istim dobavljačem. U ovom slučaju se na više stranica koriste isti kolačići jer svi dolaze s iste domene, odnosno s domene dobavljača koji upravlja oglasima.

Prilagodba personaliziranog oglašavanja može se podijeliti u 2 grupe: personalizacija publike i personalizacija jedan-na-jedan. U navedene dvije grupe nalazi se nekoliko načina na koji se može prilagoditi sadržaj oglasa za korisnike.

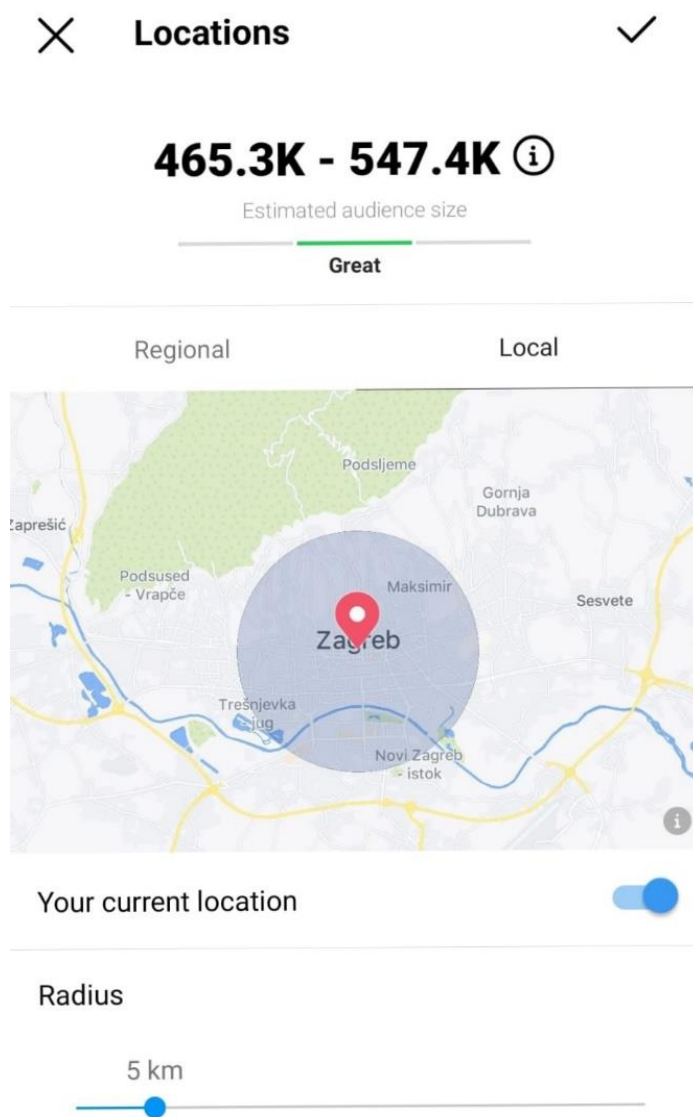
3.1.1 Personalizacija publike

Personalizacija publike (engl. *audience personalisation*) podrazumijeva prilagodbu oglašavanja na veći broj korisnika te se može postići korištenjem nekoliko metoda: prilagodba iskustva korisnika, zemljopisno ciljanje korisnika, ciljanje uređaja, demografsko ciljanje, istraživanje ponašanja, kontekstualno ciljanje, ciljanje proizvoda i ciljanje parametara.

Prilagodba iskustva korisnika (engl. *user journey targeting*) koristi tzv. karte putovanja (engl. *journey map*) koje prikazuju informacije o načinu na koji je korisnik saznao za određenu tvrtku ili proizvod te koje je sve korake prošao od tada do kupnje proizvoda. Ove karte oglašivačima daju uvid u potrebe i/ili zabrinutosti korisnika koje utječu na njihove odluke. U kartu putovanja korisnika spadaju proces kupovine korisnika, postupci korisnika, emocije, bolne točke i rješenja. Svi navedeni elementi su povezani te su tako, na primjer, negativne emocije kod korisnika, kao što je frustracija, uzrokovane nekom bolnom točkom koju bi tvrtka trebala promijeniti kako bi iskustvo korisnika na tom putovanju bilo što bolje. Negativne emocije mogu se pojaviti kod bilo kojeg koraka u samom procesu koji korisnik prolazi od otkrivanja proizvoda ili tvrtke do same kupnje.

Zemljopisno ciljanje korisnika (engl. *Geo-targeting*) koristi lokaciju korisnika kako bi korisnicima na određenim područjima bilo moguće prikazati oglase prilagođene za to područje (Ramchandani, Nagar, 2017). Primjer ove metode personalizacije oglasa je oglašavanje na društvenim mrežama *Instagram* i *Facebook*. Prilikom generiranja oglasa na navedenim društvenim mrežama, moguće je odabrati područje na kojemu će se

prikazati oglas. Na Slici 3. prikazana je mogućnost odabira područja na kojemu će se stvoreni oglas prikazati. Moguće je postaviti radijus oko trenutne lokacije ili odabrati drugu lokaciju te postaviti radijus oko nje. Također, prikazan je i predviđeni broj korisnika koji se nalaze na odabranoj lokaciji.



Slika 3. Prikaz odabira lokacije za oglas na Instagram-u

Ciljanje uređaja (engl. *Device targeting*) korisno je prilikom oglašavanja proizvoda koji su namijenjeni za određenu vrstu uređaja. Tako, na primjer, tvrtke koje proizvode aplikacije za *Apple* uređaje mogu odabrati da se njihovi proizvodi prikazuju samo korisnicima koji koriste *Apple* uređaje. Ovaj način ciljanja korisnika smanjuje negativne

reakcije do kojih može doći kada se korisniku koji ne koristi potreban uređaj za određene proizvode prikaže oglas namijenjen za njih.

Demografsko ciljanje (engl. *demographics targeting*) koristi se podacima o spolu, dobi, religiji, etničkoj pripadnosti, obrazovanju i slično. Google na stranici "About demographic targeting" navodi kako prikupljaju demografske podatke o korisnicima preko njihovih Google računa, a u slučaju da korisnik ne posjeduje Google račun tada pretpostave njegove demografske podatke ovisno o aktivnostima. Navode kako postoji mogućnost da će takvom korisniku postaviti identifikator unutar preglednika koristeći kolačiće te će pomoću tog identifikatora odrediti kojoj demografskoj skupini pripada kako bi mu mogli prikazati oglase prilagođene za tu skupinu.

Istraživanje ponašanja (engl. *Behavioral prospecting*) bavi se prikupljanjem podataka o korisnicima koji pretražuju ili su zainteresirani za specifične proizvode. Pomoću kolačića za praćenje određuje se mjesto na kojemu će se korisniku prikazati oglas te se također na taj način može stvoriti digitalni profil korisnika kako bi bilo lakše napraviti ciljane oglase. Kada se koristi navedeni način ciljanja korisnika tada će se različitim korisnicima prikazati različite verzije oglasa (E. Pottinger, 2019). Bitno je napomenuti kako je po nastanku GDPR-a znatno otežano korištenje ovog načina ciljanja korisnika jer sada korisnici moraju dati pristanak za korištenje kolačića za praćenje.

Kontekstualno ciljanje (engl. *Contextual targeting*) bavi se prilagodbom oglasa prema mjestu na kojima će se ti oglasi postaviti. Kod kontekstualnog ciljanja bitno je da je oglas povezan sa stranicom na kojoj se korisnik nalazi. Na primjer, korisnik koji pretražuje sadržaj vezan za vrtlarenje vjerojatno bi radije na toj stranici vidio oglas za tvrtku koja prodaje alat za vrtlarenje nego oglas od, na primjer, autosalona. Ovim načinom se privlači kupce koji su već zainteresirani za određene proizvode, ali možda još nisu odlučili gdje će ih kupiti. Kontekstualno ciljanje se koristi ključnim riječima na stranicama te također može koristiti tvrtkama i kod prilagodbe oglasa za određene stranice na kojima bi se htjele oglašavati.

Ciljanje proizvoda (engl. *Product targeting*) omogućava oglašivačima da korisnicima predlože proizvode koji su povezani s onima koje su već pretraživali. Na primjer, Amazon prilikom pretraživanja prijenosnih računala korisniku ponudi ostalu opremu koja mu je možda potrebna, kao što su monitor, miš i slično (Slika 4.) te također putem oglasa ponudi neki drugi model prijenosnog računala (Slika 5.).

Buy it with



Slika 4. Prikaz ponude opreme prilikom pretraživanja na Amazon-u



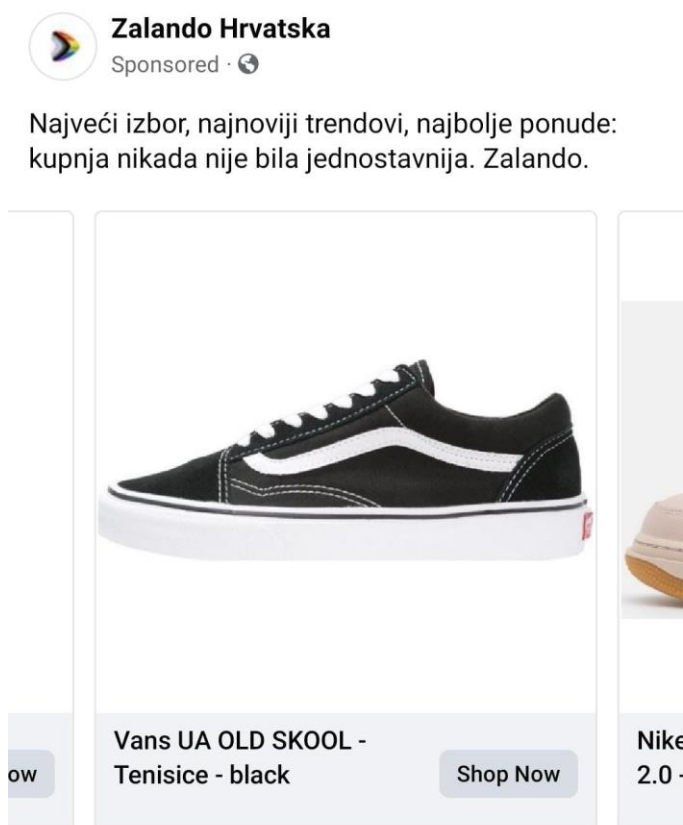
Slika 5. Prikaz oglasa prilikom pretraživanja na Amazon-u

Ciljanje parametara (engl. *Parameter targeting*) bazira se na korištenju vanjskih parametara koje nudi neka stranica. Ova metoda ciljanja korisnika prigodna je kada se radi o oglašavanju putem partnerskih stranica. Oglašavanje putem partnerskih stranica podrazumijeva prikazivanje oglasa jedne stranice na nekoj drugoj stranici. Svaka partnerska stranica ima određeni ID broj prema kojemu se prepoznaje te se putem tog ID broja može odabrati varijanta oglasa koja će se prikazati korisniku na stranici.

3.1.2. Personalizacija jedan-na-jedan

Personalizacija jedan-na-jedan (engl. *One-to-one personalisation*) fokusira se na stvaranje individualnog iskustva s korisnicima te se time pokušava povećati vjernost kupaca i osigurati vraćanje većeg dijela uloženog novca u marketing. Ovaj tip personalizacije postoji i prilikom kupnje uživo gdje će prodavač zapamtiti neke pojedinosti o kupcu, na primjer, kada konobar u kafiću zapamti kakvu kavu neki gost pije ili kada prodavač u cvjećarnici zapamti koje cvijeće kupac inače kupuje. Isti princip primjenjuje se i na digitalni marketing. Kod personalizacije jedan-na-jedan koriste se dvije metode: ponovno ciljanje proizvoda i dinamična kreativna optimizacija.

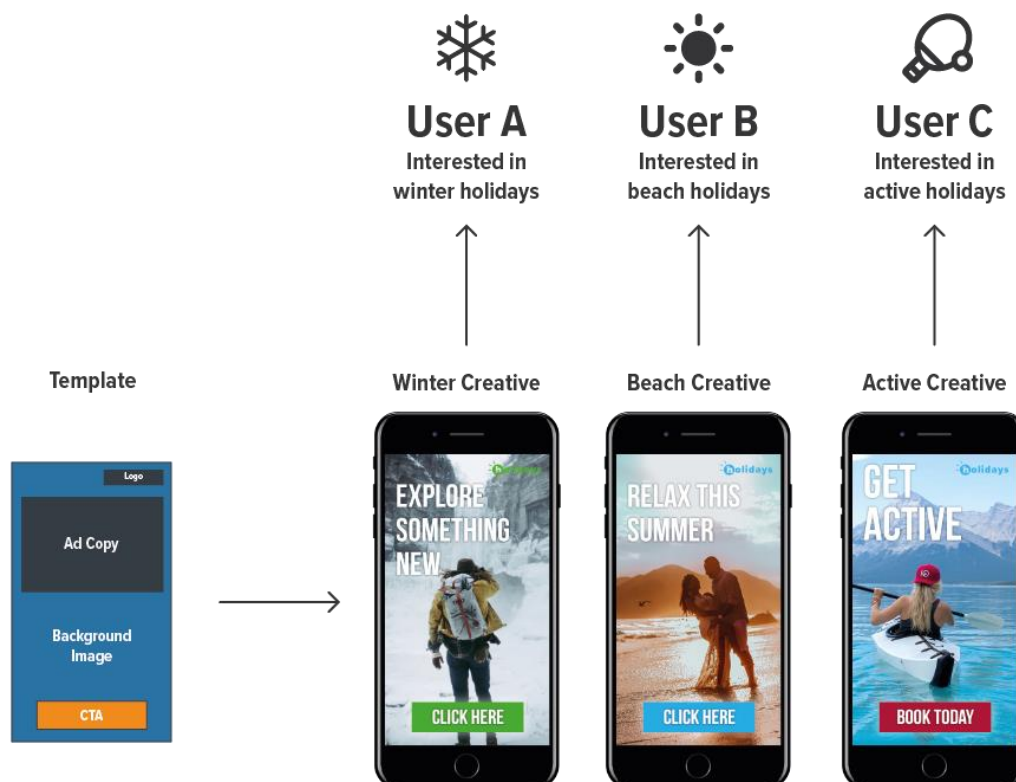
Ponovno ciljanje proizvoda slično je i kao ciljanje proizvoda no bazira se na jednom korisniku umjesto na skupini korisnika. Prilikom ponovnog ciljanja fokus je na proizvodima koje je korisnik pregledavao te koje je stavio u košaricu, ali ih nije kupio. Na slici 6. prikazan je primjer oglasa na kojemu je primijenjena metoda personalizacije jedan-na-jedan te se korisniku prikazuju proizvodi koje je već prije pregledavao.



Slika 6. Prikaz oglasa na Facebook-u

Dinamična kreativna optimizacija (engl. *Dynamic creative optimisation*) ili skraćeno DCO je najnapredniji način personalizacije oglasa. DCO se koristi trenutnim analitičkim podacima, velikim izvorima podataka te kreativnom optimizacijom u realnom vremenu.

Na slici 7. prikazan je primjer korištenja DCO metode personalizacije kod koje se stvara predložak oglasa koji će se mijenjati ovisno o korisniku kojemu se prikazuje. Razni korisnici imaju razne interese te se ponekad jedan oglas ne može primijeniti na sve. Kao što je prikazano na primjeru, korisniku koji više voli zimske aktivnosti prikazat će mu se oglas koji sadrži fotografiju napravljenu zimi dok će se korisniku koji preferira ljeto prikazati oglas s nekom ljetnom fotografijom. Na ovaj način će korisnik dobiti ono što želi vidjeti te će tvrtka koja je postavila oglas imati veću vjerojatnost da tom korisniku proda neki svoj proizvod.

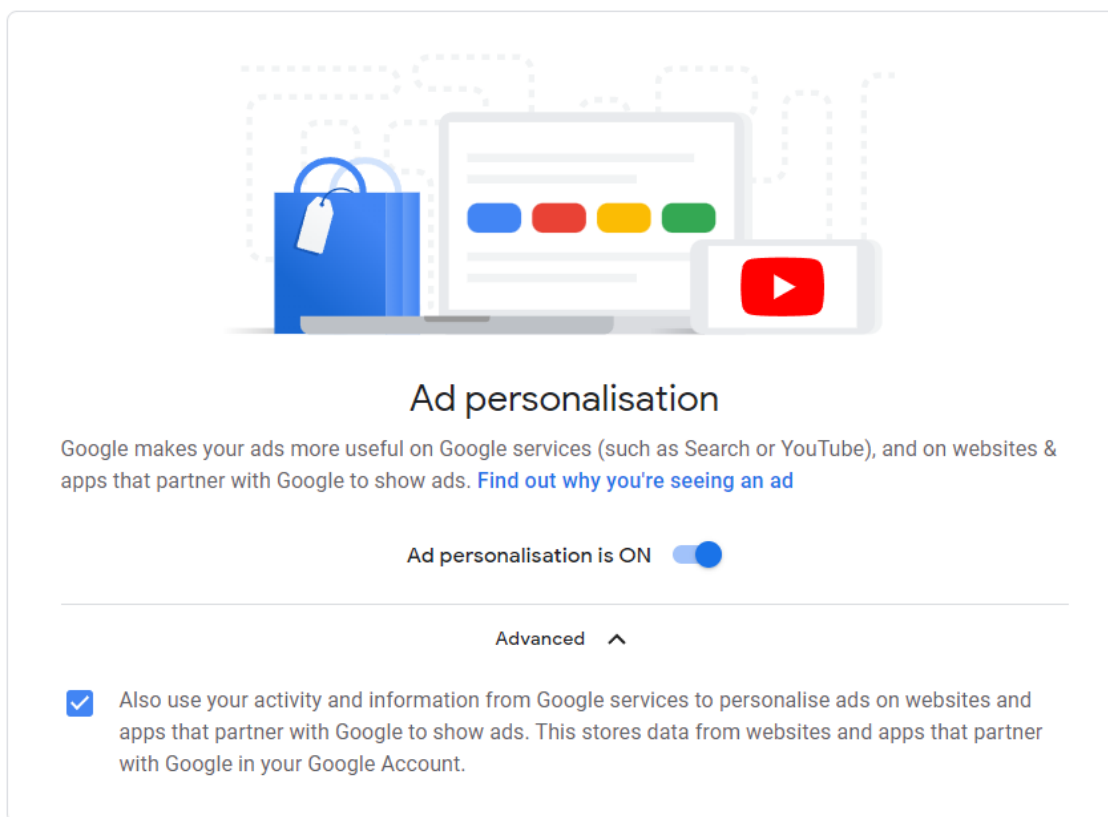
Slika 7. Primjer dinamične kreativne optimizacije⁴

3.2. Postavke personalizacije oglasa

Preglednici Google Chrome, Microsoft Edge i Safari nude svojim korisnicima podešavanje personalizacije oglasa. Unutar preglednika Mozilla Firefox za sada nije ponuđeno podešavanje personalizacije oglasa.

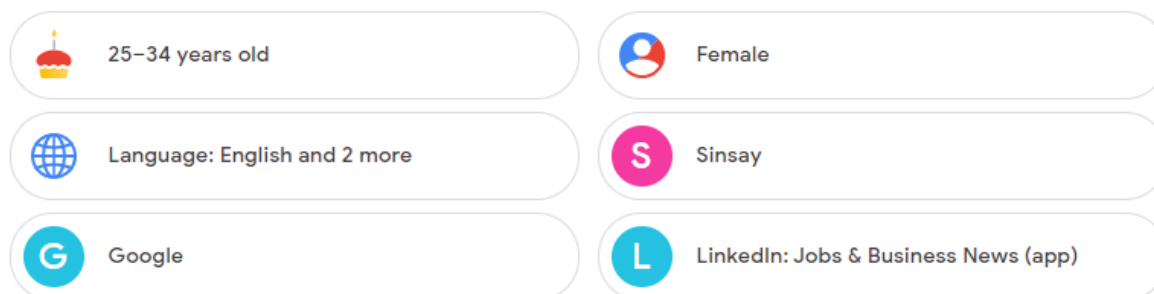
Na slici 8 prikazana je mogućnost podešavanja personalizacije oglasa u Google Chrome pregledniku. Google navodi kako za korisnike stvaraju korisnije oglase na Google servisima kao što je YouTube te na stranicama i aplikacijama koje surađuju s njima. Nadalje, u naprednim postavkama korisnici mogu omogućiti korištenje podataka o aktivnosti i ostalih informacija s Google servisa kako bi oglasi bili personalizirani.

⁴ slika preuzeta sa: <https://www.warroominc.com/institute-library/blog/dynamic-creative-optimization/>



Slika 8. Prikaz podešavanja personalizacije u Google Chrome pregledniku

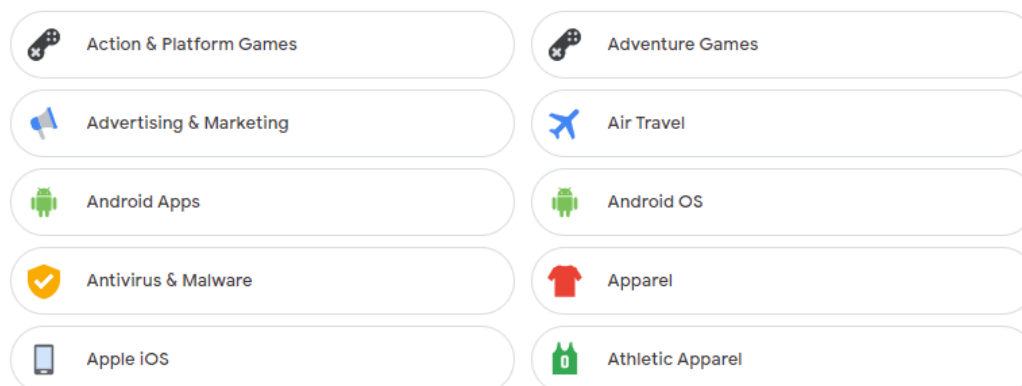
Na slici 9. vidljivi su podaci o korisniku koje Google koristi u svrhu personalizacije oglasa. Navedeno su podaci koje Google prikuplja putem korisničkog profila, na primjer spol, jezik i dob korisnika te podaci koje prikupljaju pomoću kolačića na stranicama koje korisnik posjećuje. U ovom primjeru to su kolačići sa stranica Sinsay, Google te iz aplikacije LinkedIn.



Slika 9. Prikaz podataka koje Google koristi za personalizaciju

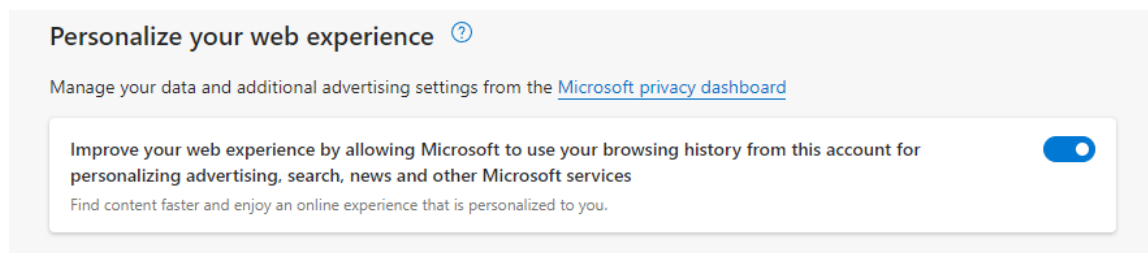
Na slici 10. prikazani su interesi korisnika koje Google uz podatke o korisnicima koristi za personalizaciju. Interese korisnika stvaraju također koristeći kolačiće sa stranica koje

korisnik posjećuje te ih svrstava u razne kategorije interesa kao što su Odjeća, Putovanja, Aplikacije, Igre i slično.



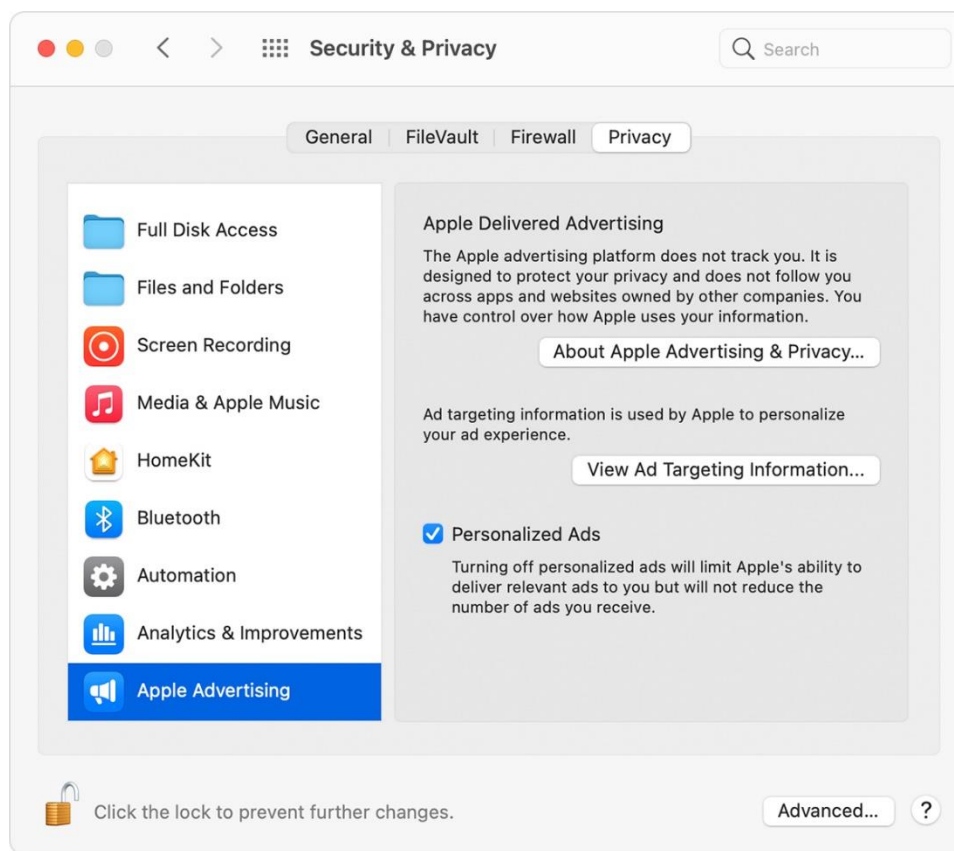
Slika 10. Prikaz interesa korisnika koje Google koristi za personalizaciju

Kao što je vidljivo na slici 11., Microsoft Edge ne nudi toliku količinu informacija o personalizaciji svojim korisnicima. Korisniku je ponuđeno omogućavanje opcije koja će omogućiti Microsoftu da poboljša njegovo iskustvo na web-u koristeći podatke o povijesti pretraživanja za personalizaciju oglasa, pretraživanja, vijesti te drugih Microsoft servisa.



Slika 11. Prikaz podešavanja personalizacije u Microsoft Edge pregledniku

Slika 12. prikazuje mogućnosti koje preglednik Safari nudi korisnicima u vezi personalizacije oglasa. Navedeno je da će onemogućavanje personalizacije oglasa ograničiti mogućnost Apple-a da korisniku ponudi relevantne oglase, ali neće smanjiti količinu oglasa koja će se prikazivati.



Slika 12. Prikaz podešavanja personalizacije u pregledniku Safari⁵

3.3. Blokatori oglasa

Osim što se razne tvrtke kao što su Apple i Mozilla trude sačuvati privatnost svojih korisnika, sami korisnici također mogu poduzeti neke korake kako bi spriječili prikupljanje svojih podataka. Korisnici mogu sami brisati kolačiće unutar preglednika ili koristiti anonimni način rada u kojemu nije omogućeno prikupljanje kolačića. Na ovaj način se također otežava rad oglašivačima u smislu personalizacije sadržaja koji prikazuju korisnicima, ali korisnici također imaju i opciju korištenja blokatora oglasa.

Blokatori oglasa (engl. *Ad blocker*) su dodaci koji se instaliraju unutar preglednika te blokiraju oglase koji će se korisnicima prikazivati prilikom pregledavanja sadržaja na mrežnim stranicama. Neki od najpoznatijih blokatora oglasa su *AdBlock* i *AdBlock Plus* koji

⁵ slika prezeta sa: <https://support.apple.com/en-us/HT202074>

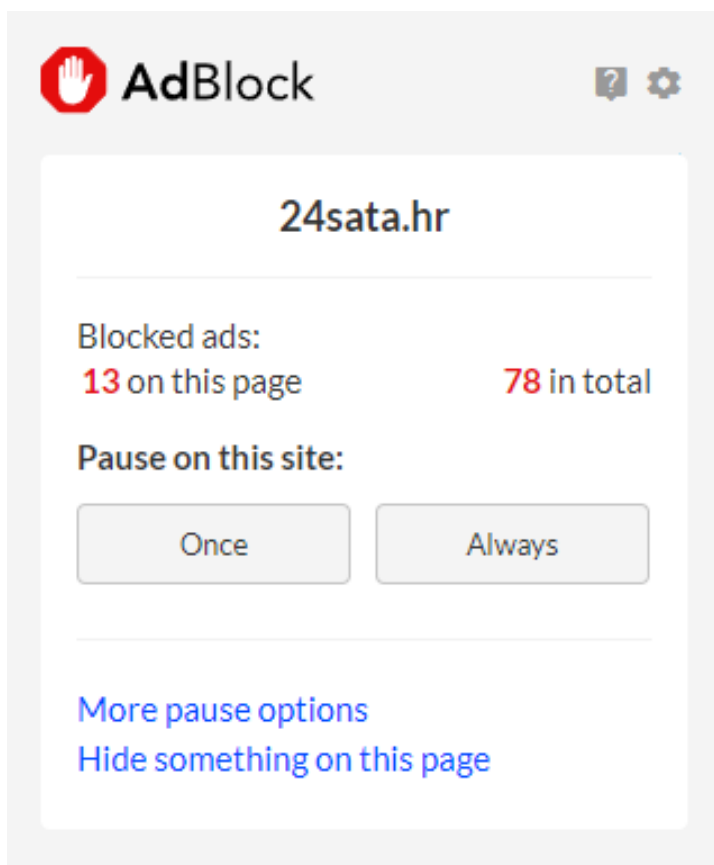
rade na način da pregledavaju pravila filtriranja prema kojima određuju koji sadržaj će se korisniku prikazati, a koji neće. Blokator oglasa uspoređuje sve HTTP zahtjeve s popisom filtera na koje je korisnik pretplaćen ili one koje je sam postavio te u slučaju da se URL web mjesta poklapa s onim unutar nekog filtera, taj HTTP zahtjev se blokira te se sadržaj neće učitati.

AdBlock na svom blogu, 2020. godine, u članku "How does AdBlock work?" navodi kako se kao jedan od najčešćih načina za prikazivanje oglasa koristi metoda kodiranja slike koristeći `data:image/png`. Navedena metoda ne pokreće normalan HTTP zahtjev te se oglasi koji se prikazuju na ovaj način ne mogu blokirati. Umjesto blokiranja takvih oglasa, *AdBlock* se koristi metodom postavljanja stilskih oblikovanja na svaku stranicu. Navedena stilska oblikovanja sadrže selektor koji je postavljen kao `display:none !important` te se na taj način sakrije oglas.

Ranije navedene liste filtera prema kojima se blokiraju oglasi nalaze se unutar velike kolekcije poznatih oglasa na engleskom jeziku, *EasyList*. Osim navedenog, korisnici se mogu pretplatiti i na druge filtere koji mogu blokirati oglase na drugim jezicima te također i neke druge sadržaje. Korisnici također mogu odabrati i da prihvaćaju neke nenametljive oglase.

Na slici 13. vidljiv je prikaz dodatka *AdBlock* na stranici portala 24sata. Samo na početnoj stranici navedenog portala *AdBlock* je blokirao 13 oglasa.

Blokatori oglasa stvaraju poteškoće oglašivačima i stranicama koje stvaraju prihod od prikazivanja oglasa. Naime, ako se određeni oglas ne prikaže korisniku, ta stranica neće stvoriti prihod od sesije tog korisnika.



Slika 13. prikaz broja blokiranih oglasa⁶

⁶ ekranska slika napravljena na stranici: <https://www.24sata.hr/>

4. Istraživanje

Za potrebe ovog rada napravljeno je istraživanje na stranicama pet tvrtki koje se bave proizvodnjom hrane i pića: Podravka, Kraš, Coca-Cola, Jamnica i Ledo, odnosno, njihovi mrežni sadržaji na stranicama. Odabrane su tvrtke koje se nalaze među top 10 tvrtki po poslovnim prihodima prema Mazars analizi industrije hrane i pića iz 2019. godine⁷. Navedene tvrtke odabrane su za ovo istraživanje kako bi smo dobili uvid kako tvrtke, koje su poznatije među širom hrvatskom populacijom, prikupljaju osobne podatke svojih korisnika te koji se od tih podataka mogu koristiti u svrhu personalizacije oglašavanja. Odabrane stranice za istraživanje su:

1. <https://www.podravka.hr/>
2. <https://www.kras.hr/>
3. <https://www.coca-cola.hr/>
4. <https://www.jamnica.hr/hr/naslovnica/>
5. <https://www.ledo.hr/>

Postavljene su dvije hipoteze u skladu s ciljevima istraživanja.

- H1: poznate tvrtke u Hrvatskoj prikupljaju neke od kolačića treće strane koji mogu biti korišteni za prilagodbu i personalizaciju oglasa
- H2: poznate tvrtke u Hrvatskoj imaju jasno izražene informacije o prikupljanju kolačića kako je i propisano zakonskim regulativama.

Istraživanje se temelji na pitanjima podijeljenima u tri kategorije:

1. Politika o kolačićima (engl. *Cookie Policy*)
 - P1. Postoji li upozorenje o prikupljanju kolačića?
 - P2. Postoji li objašnjenje kolačića?
 - P3. Jesu li navedeni tipovi kolačića koji se koriste?

⁷Mazars, "Analiza industrije hrane i

pića": <https://www.mazars.hr/content/download/953194/49862674/version//file/Analiza%20industrije%20hrane%20i%20pi%20C4%87a.pdf>

- P4. Je li navedeno korištenje kolačića treće strane?
- P5. Je li naveden razlog korištenja kolačića?
- P6. Je li navedeno kako korisnik može naknadno odustati od dopuštenja za korištenje kolačića?
- P7. Je li navedeno korištenje kolačića u svrhu personalizacije?
2. Pristanak korisnika na korištenje kolačića
- P8. Na koji se način traži pristanak korisnika (banner, pop-up)?
- P9. Koje su opcije (gumbi) ponuđene korisniku?
- P10. Jesu li neke opcije već označene? Koje?
3. Oglasi
- P11. Koliko je oglasa blokirano na stranici od strane AdBlock dodatka?

Za potrebe istraživanja također je korišten i alat CookiePro⁸ koji skenira svaku stranicu zasebno te pruža uvid u vrste kolačića koji se prikupljaju. Pregled rezultata skeniranja stranica bit će prikazan u drugom dijelu ovog poglavlja.

Na kraju istraživanja je napravljena i usporedba količine pronađenih trajnih i sesijskih kolačića prve i treće strane na stranicama odabranim za istraživanje.

4.1 Politika o kolačićima

Politika o kolačićima podrazumijeva informacije koje određena stranica nudi svojim korisnicima vezano za prikupljanje i korištenje kolačića.

Tablica 1. tablica odgovora za prvi blok pitanja (P1 – P7)

	P1	P2	P3	P4	P5	P6	P7
<i>Podravka</i>	+	+	-	-	+	+	+/-
<i>Kraš</i>	+	+	-	-	+	+	-
<i>Coca Cola</i>	+	+	+	+	+	+	+

⁸ <https://www.cookiepro.com/>

Jamnica	+	+	+	+	+	+	+
Ledo	+	+	+	+	+	+	+

Tablica 1. prikazuje odgovore na pitanja P1 do P7 iz prve grupe pitanja koja spadaju pod politiku o kolačićima. Kao što je vidljivo iz tablice, na većinu pitanja je odgovor pozitivan, odnosno zadovoljavajuć. Stranice tvrtki Coca Cola, Jamnica i Ledo ispunjavaju sve kriterije prvog bloka istraživanja te time svojim korisnicima daju potpune i jasne informacije o razlozima za prikupljanje kolačića, tipovima kolačića koje prikupljaju pa i o tome što su zapravo kolačići i o njihovom korištenju u svrhu personalizacije oglasa. Stranice tvrtki Podravka i Kraš ispunjavaju četiri od sedam kriterija u ovom bloku. Podravka i Kraš obavještavaju korisnike da se kolačići prikupljaju te daju njihovo objašnjenje, a također i navode razloge korištenja kolačića i korisnicima objašnjavaju kako da odustanu od korištenja kolačića. Ono što nedostaje na njihovim stranicama su popis tipova kolačića koji se koriste te napomena o korištenju kolačića treće strane. Također, Podravka objašnjava kako se određeni kolačići koriste u marketinške svrhe, no ne i da ih oni koriste dok Kraš ne navodi nikakvo korištenje kolačića u svrhu oglašavanja.

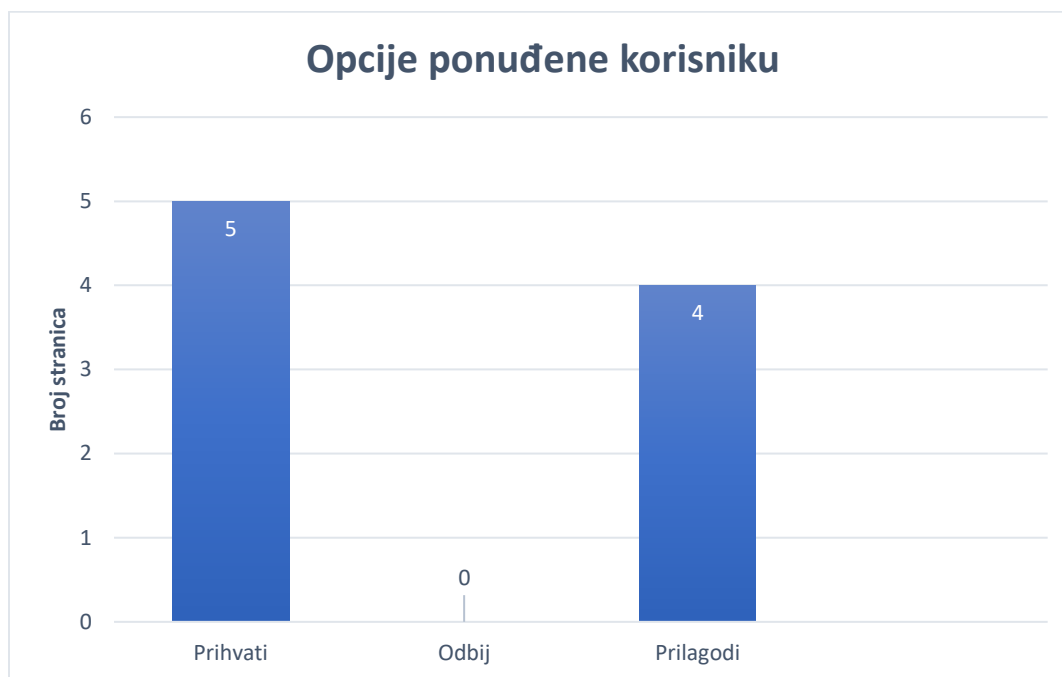
4.2. Pristanak korisnika na korištenje kolačića

Kao što je ranije u ovom radu objašnjeno, stranice moraju zatražiti dopuštenje od korisnika kako bi na njihove uređaje mogle postavljati kolačiće koje koriste u razne svrhe.



Dijagram 1. rezultati na temelju pitanja P8

Na dijagramu 1. vidljiv je omjer stranica koje korisniku prilikom pristupanja stranici prikazuju traku (engl. *banner*) i onih koji prikazuju skočni prozor (engl. *pop-up*) sa zahtjevom za dopuštenje korištenja kolačića. Razlika u ova dva načina je ta da je skočni prozor puno uočljiviji te na nekim stranicama čak i ometa rad korisnika sve dok korisnik ne napravi neku akciju, odnosno dok ne odbije ili dopusti korištenje kolačića. Od stranica koje su odabrane za ovo istraživanje, metodom prikazivanja skočnog prozora koriste se Podravka, Jamnica, Coca Cola i Ledo, dok Kraš koristi metodu prikazivanja trake koja se nalazi pri dnu stranice.



Dijagram 2. rezultati na temelju pitanja P9

Opcije koje se korisniku mogu ponuditi prilikom traženja dopuštenja za korištenje kolačića su „Prihvati“, „Odbij“ ili „Prilagodi“, odnosno postavke. Od 5 stranica sve imaju opciju za prihvaćanje korištenja kolačića, ali niti jedna korisnicima ne nudi odbijanje svih kolačića.

Za prilagodbu kolačića mogu se koristiti razne metode kao što je postavljanje poveznice na stranicu na kojoj korisnik može odabrati koje će kolačiće dopustiti ili metoda u kojoj se unutar skočnog prozora korisniku omogućiti odabir vrste kolačića koje će dopustiti. Druga metoda je i najjednostavnija za korisnike jer ne moraju izlaziti iz trenutne stranice kako bi postavili svoje preferencije o korištenju kolačića. Stranice tvrtki Coca Cola, Jamnica, Ledo i Podravka imaju jednu od dvije navedene opcije za prilagodbu dok na stranicama tvrtke Kraš takve opcije nisu ponuđene. Coca Cola i Ledo koriste metodu koja je najpristupačnija, odnosno korisniku u samom skočnom prozoru nude opciju odabira kolačića, dok Jamnica i Podravka korisniku nude poveznicu na kojoj navedeno mogu postaviti. Bitno je napomenuti kako se prilikom klika na poveznicu „Postavke kolačića“ unutar skočnog prozora na stranici tvrtke Jamnica ne dogodi ništa, odnosno korisnika se vodi ponovno na

početnu stranicu te mu se pojavljuje isti skočni prozor koji ne nudi prilagodbu korištenja kolačića.

S obzirom na to da samo dvije od ovdje korištenih stranica (Coca Cola i Ledo) korisnicima nude biranje kolačića koji će se koristiti, pitanje P10 se može odnositi samo na te dvije stranice. Tvrtka Coca Cola već ima unaprijed označene strogo potrebne kolačiće te ih nije moguće od-značiti dok su analitički kolačići i kolačići za personalizaciju onemogućeni dok ih korisnik sam ne omogući. Tvrtka Ledo već unaprijed omogućava nužne, odnosno tehničke kolačiće te ih korisnik može onemogućiti. I u ovom slučaju, analitički i marketinški kolačići nisu automatski omogućeni te ih korisnik posebno treba dopustiti.

4.3 Pregled obavijesti

Iako sve stranice odabrane za ovo istraživanje imaju neku vrstu obavijesti o korištenju kolačića, neke od njih nisu dovoljno pristupačne za korisnike te će u ovom dijelu rada biti objašnjeno zašto.

Poštujemo Vašu privatnost

Kako bi naša stranica radila ispravno i kako bismo stalno unaprjeđivali naše usluge koristimo kolačiće. U slučaju da želite onemogućiti korištenje kolačića, neki dijelovi stranice mogu postati nedostupni. Detaljnije pročitajte u [Uvjetima korištenja](#).

Vrste kolačića: Tehnički, Marketing

PRIHVATI SVE

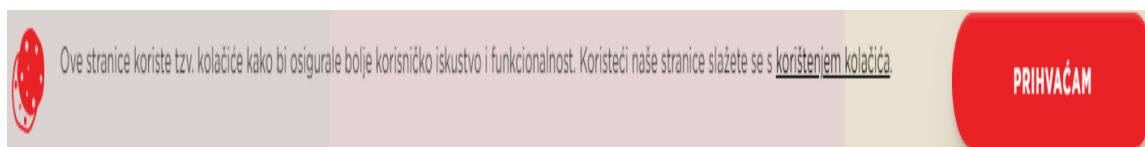
[Postavke](#)

Slika 14. prikaz obavijesti na stranici tvrtke Podravka⁹

Na slici 14. vidljiva je obavijest koja se korisnicima prikaže kada pristupe stranici tvrtke Podravka. Unutar obavijesti nalazi se kratko objašnjenje korištenja kolačića te poveznica

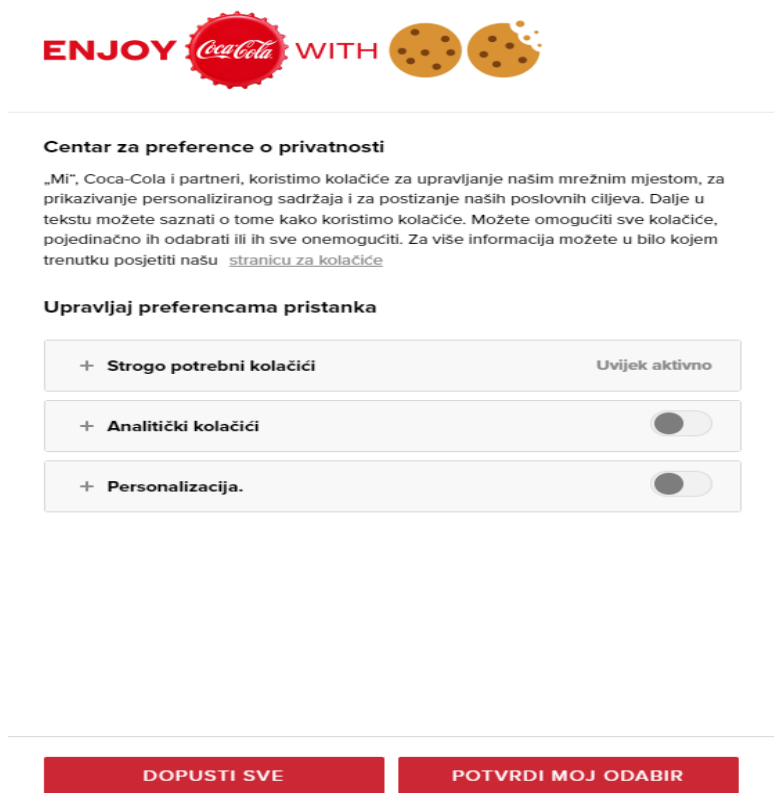
⁹ Ekranska slika napravljena na: <https://www.podravka.hr/>

na kojoj se nalaze detalji vezani za njih. Korisnik može samo prihvatiti sve kolačiće. Odabirom opcije „Postavke“ korisnika se vodi na stranicu na kojoj može prihvatiti i korištenje marketinških kolačića, ali ne može odbiti korištenje tehničkih kolačića.



Slika 15. prikaz obavijesti na stranici tvrtke Kraš

Obavijest koju tvrtka Kraš prikazuje posjetiteljima svoje stranice vidljiva je na slici 15. Navedena obavijest nudi jako malo informacija, te samo opciju za prihvaćanje kolačića i poveznicu na politiku o kolačićima. Korisniku nigdje nije omogućeno biranje kolačića koji će se koristiti pa čak niti u politici o kolačićima.



Slika 16. prikaz obavijesti na stranici tvrtke Coca Cola¹⁰

¹⁰ Ekranjska slika napravljena na: <https://www.coca-cola.hr/>

Na slici 16. vidljiv je prikaz skočnog prozora koji korisnicima nudi razne informacije o korištenju kolačića na stranicama tvrtke Coca Cola. Navedeno je primjer kvalitetne i pristupačne obavijesti koja je usmjerena na korisnika. Korisnik u obavijesti dobije informacije o prikupljanju kolačića, mogućnost biranja kolačića koji će se koristiti te također klikom na tip kolačića i informacije o tim kolačićima. Osim informacija koje se navode na skočnom prozoru, korisniku je ponuđena i poveznica na politiku o kolačićima gdje može saznati i detaljnije informacije.

Obavijest koja se prikazuje na stranici tvrtke Jamnica (Slika 17.) slična je onoj koja se prikazuje na stranicama tvrtke Podravka no sadrži nešto više informacija. Bitno je napomenuti kako ni u ovoj obavijesti nije ponuđen odabir kolačića koje korisnik želi dopustiti ili odbiti već je moguće samo prihvatiti. Uz navedeno je ponuđena i poveznica na politiku o kolačićima. Poveznica „Postavke kolačića“, kao što je i ranije navedeno, nije funkcionalna, odnosno korisnika vodi ponovo na istu stranicu s istom obavijesti.

Kolačići

Klikom na [Prihvati](#) i zatvori koristit ćemo alate na drugim internetskim stranicama da bismo vam pružili prilagođene informacije u marketinške svrhe putem partnera, uključujući one izvan naše web stranice. Njima se omogućuju prilagođeni mrežni oglasi i proširene mogućnosti analize i procjene koje se odnose na ciljnu skupinu i ponašanje korisnika. Također pristajete i na to da se podaci mogu prenositi i u treće zemlje izvan Europskog gospodarskog prostora bez odgovarajuće razine zaštite podataka (posebno SAD-a).

Klikom na [Postavke kolačića](#) možete pregledati sve opcije, uključujući kontrole za odbijanje upotrebe kolačića za prilagodbu i informacije o kontrolama na razini preglednika za odbijanje nekih ili svih kolačića za druge upotrebe.

Svoju privolu u bilo kojem trenutku možete odbiti ili povući u [Postavkama kolačića](#) na ovoj web stranici. Više o politikama privatnosti i kolačićima možete pročitati ovdje: [Politika privatnosti i Politika kolačića](#).

[Postavke kolačića](#)

[Prihvati i zatvori](#)

Slika 17. prikaz obavijesti na stranici tvrtke Jamnica¹¹

Na slikama 18. i 19. vidljiva je obavijest koju stranica tvrtke Ledo prikazuje svojim posjetiteljima. Navedena obavijest slična je obavijesti na stranicama tvrtke Coca Cola.

¹¹ Ekranska slika napravljena na: <https://www.jamnica.hr/hr/naslovnica/>

Razlika je u tome što unutar ove obavijesti korisnici pristupaju odabiru kolačića klikom na opciju „Postavke“ te se otvara drugi skočni prozor koji je prikazan na slici 19.

COOKIE POLICY

Da bi ova web-stranica mogla pravilno funkcionirati i da bismo unaprijedili vaše korisničko iskustvo, koristimo kolačiće kojima se pristupa općim i najosjetljivijim podacima na uređaju s kojeg pristupate ovoj web stranici. Za postavljanje određenih kolačića možete dati privolu u dijelu postavki, a više informacija o samim kolačićima i načinu prikupljanja potražite u našoj **Politici kolačića**.

Postavke ^

Prihvaćam sve

IZABERITE KOLAČIĆE NA STRANICI

Omogućite ili onemogućite web-stranici upotrebu funkcionalnih i/ili reklamnih kolačića opisanih u nastavku:

On

Nužni (tehnički) kolačići

Nužni kolačići omogućuju osnovne funkcionalnosti. Bez ovih kolačića, web-stranica ne može pravilno funkcionirati, a isključiti ih možete mijenjanjem postavki u svome web-pregledniku.

Off

Analitički kolačići

Analitički kolačići pomažu nam unaprijediti web-stranicu prikupljanjem i analizom podataka o njeziniu korištenju.

Off

Marketinški kolačići

Marketinške kolačiće koristimo radi povećanja relevantnosti oglasa koje primete.

Slike 18. i 19. prikaz obavijesti na stranici tvrtke Ledo¹²

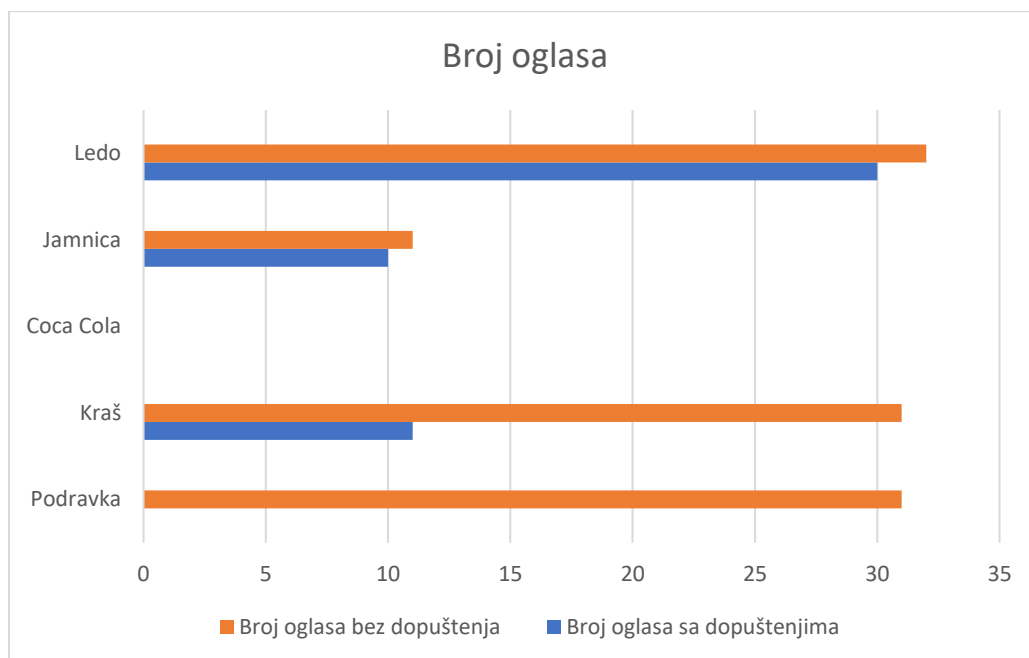
Iz navedenih prikaza može se zaključiti kako stranice tvrtki Coca Cola i Ledo imaju najkvalitetnije rješenje za obavještanje korisnika o korištenju kolačića. Svojim korisnicima nude bitne informacije koje su jasno i razumljivo napisane te također nude i odabir tipova kolačića za korištenje. Najlošije rješenje od prikazanih bilo bi ono tvrtke

¹² Ekranška slika napravljena na: <https://www.ledo.hr/>

Kraš. Naime, prema raspisanim uredbama, koje su objašnjene u poglavlju 2 ovog rada, tvrtke korisnicima moraju dati jasne, precizne i lako razumljive informacije o prikupljanju i korištenju kolačića te im također moraju ponuditi mogućnost odbijanja određenih tipova kolačića. Tvrtke Podravka i Jamnica korisnicima nude jasne i razumljive informacije, no nedostaje mogućnost odabira tipova kolačića kako bi obavijest bila potpuna. Ovim rezultatima nije moguće u potpunosti potvrditi hipotezu H2. Odnosno, hipotezu potvrđuju rezultati za stranice tvrtki Coca Cola, Ledo, Podravka i Jamnica dok rezultati za tvrtku Kraš ne potvrđuju hipotezu.

4.4 Oglasi

Za potrebe istraživanja koristila sam dodatak ADBlock koji je ranije spomenut u radu. U ovom dijelu rada korišten je za pregled broja oglasa koji se blokiraju na stranicama odabranim za istraživanje. Za rezultate se broje oglasi blokirani na početnoj stranici određene tvrtke te na još 10 nasumično odabranih podstranica na toj domeni.



Dijagram 2. rezultati na temelju korištenja ADBlock dodatka

Dijagram 2. prikazuje rezultate dobivene korištenjem dodatka *AdBlock* na stranicama odabranim za istraživanje. Napravljena je usporedba količine oglasa koja je blokirana kada je u postavkama dodatka dozvoljeno prikazivanje nekih nenametljivih oglasa te količine oglasa kada je ista opcija onemogućena. Nenametljivi oglasi su oni koji ne narušavaju korisničko iskustvo kao što to čine na primjer oglasi unutar skočnih prozora. Iz dijagrama 2. se može zaključiti kako tvrtka Coca Cola ne prikazuje oglase na svojim stranicama dok najviše nametljivih oglasa prikazuje tvrtka Ledo, njih čak 32, na nasumično odabranim podstranicama. Tvrtka Podravka ne prikazuje nenametljive oglase, ali nametljivih je prikazala 31. Na stranicama tvrtke Kraš prikazuje se gotovo tri puta više nametljivih oglasa nego nenametljivih. Točnije, prikazuje se 11 nenametljivih i čak 31 nametljiv oglas.

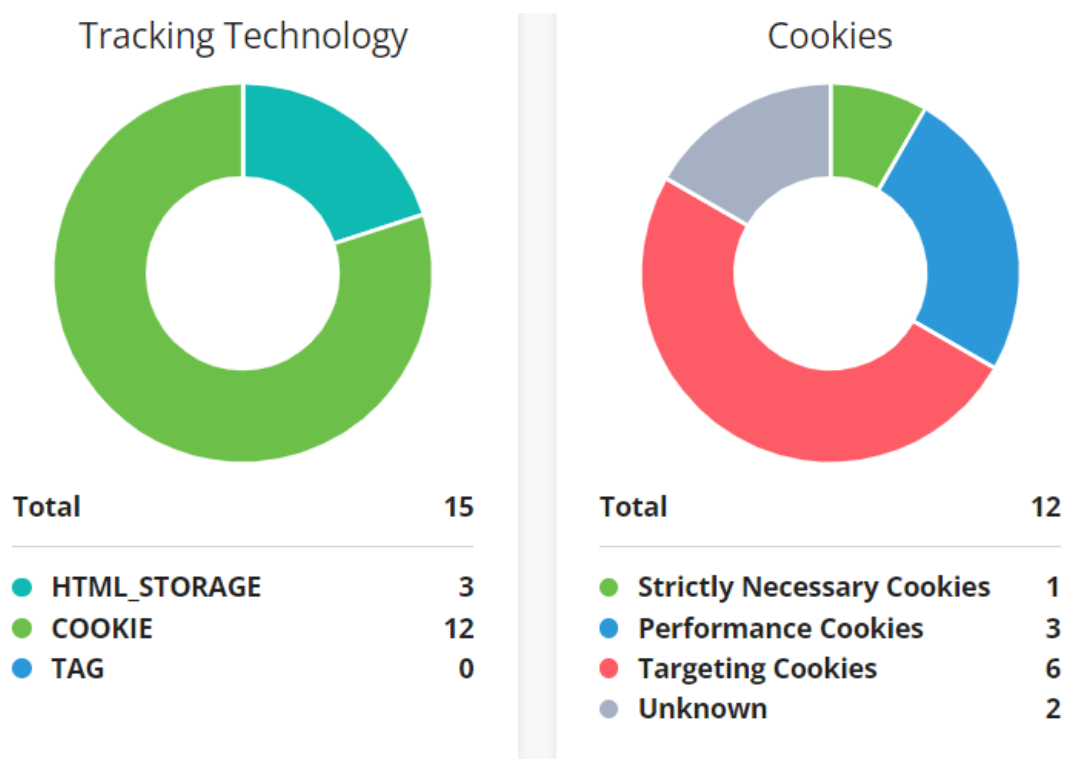
5.5 Analiza rezultata CookiePro alata

CookiePro je alat koji skenira stranice iste domene te broji količinu kolačića i svrstava ih u grupe po tipovima. Osim kolačića također pregledava koje tehnologije praćenja se koriste na stranicama te koje oznake i obrasci postoje. Za potrebe istraživanja bit će analizirani samo podaci koji su relevantni za ovaj rad, a to su podaci o kolačićima i tehnologijama za praćenje. Tehnologije za praćenje su zapravo kombinacija više elemenata pronađenih na stranici. Ti elementi su kolačići, objekti u HTML pohrani te oznake. Osim količine kolačića, alat *CookiePro* također napravi i popis kolačića koji su pronađeni na stranici te, ako je dostupno, ponudi i objašnjenje, trajanje te informacije o tome je li kolačić siguran i je li HTTP only.

Za sve stranice uključene u istraživanje podešene su jednake postavke, odnosno skeniranje se obavlja na najviše 100 podstranica domene te su geolokacijska obilježja postavljena na globalne korisnike i one na koje se odnosi GDPR.

Na slici 20. prikazani su rezultati skeniranja stranice **tvrtke Ledo** i podstranica na istoj domeni. Skeniranjem je pronađeno 15 tehnologija za praćenje od kojih su 12 kolačići. Među kolačićima nalazi se jedan neophodan kolačić, tri kolačića za performanse, šest

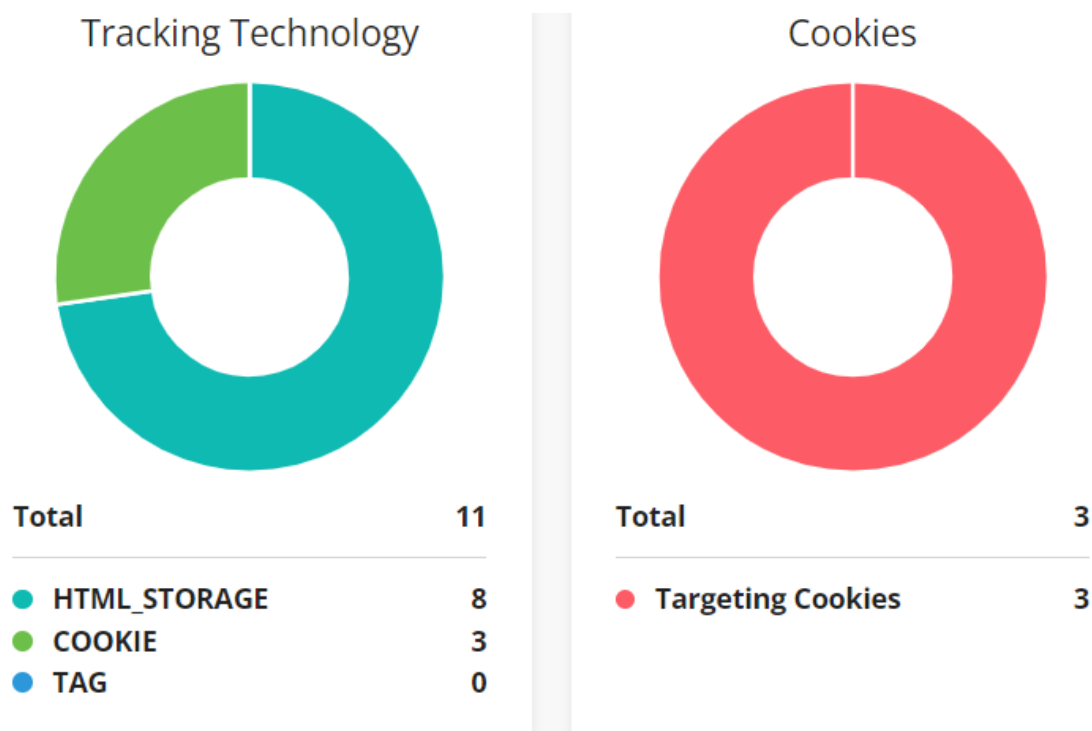
kolačića za ciljanje te dva nepoznata kolačića. Od pronađenih kolačića, za istraživanje, su značajni kolačići za ciljanje od kojih je pronađeno šest s domena adform.net, youtube.com i www.facebook.com. Od navedenih kolačića 2 su sesijska te se brišu kada korisnik napusti stranicu, a četiri su trajna od kojih kolačić naziva „CONSENT“ s domene youtube.com traje najdulje, odnosno dvije godine. Kolačić naziva „CONSENT“ prati kako korisnik koristi stranicu te provjerava koje je sve oglase korisnik vidio prije nego je posjetio stranicu. Kod stranice tvrtke Ledo bitno je obratiti pozornost na još dva kolačića, a to su „_fbp“ i „VISITOR_INFO1_LIVE!“. Kolačić naziva „_fbp“ dolazi s domene ledohr.hr te se zbog toga smatra kolačićem prve strane no koristi ga društvena mreža Facebook kako bi ponudila više oglasa od oglašivača treće strane. „VISITOR_INFO1_LIVE“ je kolačić treće strane koji dolazi s domene youtube.com te se postavlja od strane tvrtke YouTube kako bi se pratile preferencije korisnika putem ugrađenih videozapisa na stranicama.



Slika 20. rezultati za stranicu www.ledo.hr¹³

¹³ Ekranska slika napravljena na: app.cookiepro.com

Na stranicama **tvrtke Jamnica** pronađeno je manje kolačiće, točnije njih tri, kao što je i prikazano na slici 21. Sva tri kolačića koja su pronađena su kolačići za ciljanje te također spadaju pod kolačiće treće strane. Od tri pronađena kolačića, dva su trajna a jedan je sesijski. Kao i kod tvrtke Ledo, na stranicama tvrtke Jamnica koriste se kolačići „CONSENT“ i „VISITOR_INFO1_LIVE!“ postavljeni od strane domene youtube.com.

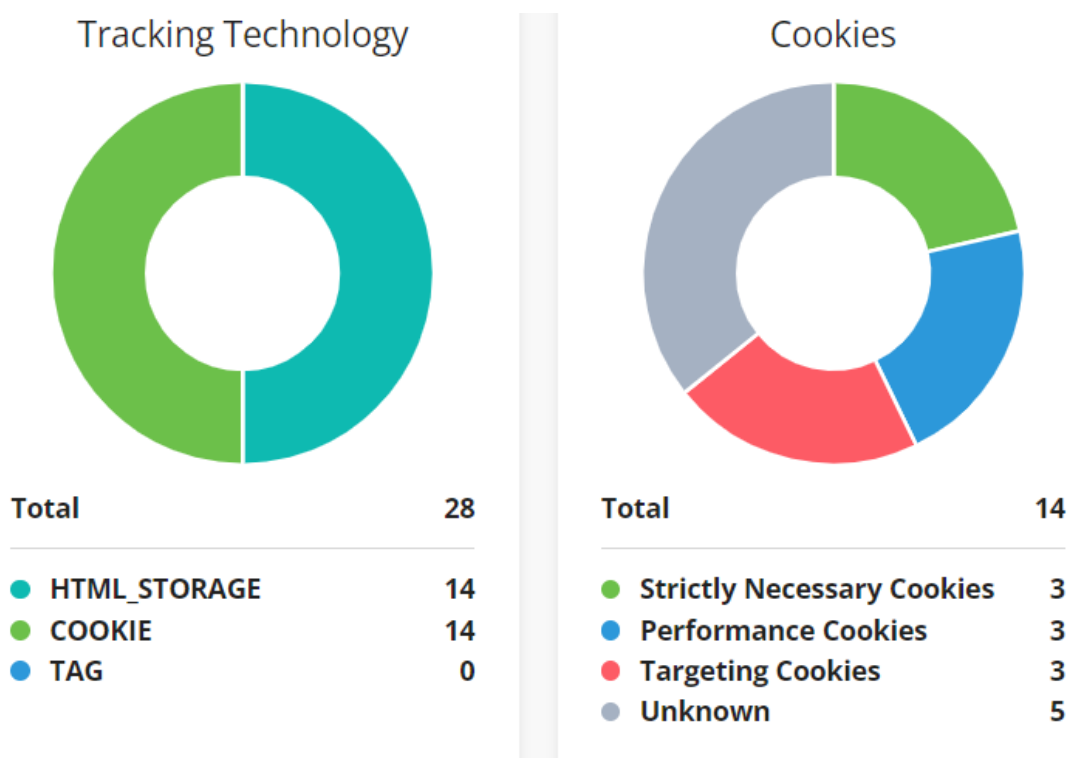


Slika 21. rezultati za stranicu www.jamnica.hr¹⁴

Stranice **tvrtke Coca Cola** koriste 28 tehnologija za praćenje od kojih je 14 kolačića te je navedeno prikazano na slici 22. Od pronađenih 14 kolačića tri su neophodna, tri su kolačića za performanse, tri kolačića za praćenje i pet je nepoznatih kolačića. Sva tri kolačića za praćenje ista su kao i kod prethodne dvije stranice analizirane u ovom poglavlju. Od nepoznatih kolačića bitno je spomenuti kolačić naziva „CONSENT“ koji dolazi

¹⁴ Ekrsanska slika napravljena na: app.cookiepro.com

s domene youtube-nocookie.com. Oznaka youtube-nocookie označava vrstu kolačića s domene youtube.com koji neće utjecati na iskustvo korisnika na platformi YouTube. To znači da ako korisnik pogleda neki videozapis na stranici tvrtke Coca Cola, na YouTube platformi mu se neće predlagati videozapisi povezani s tim videozapisom koji je pogledao.

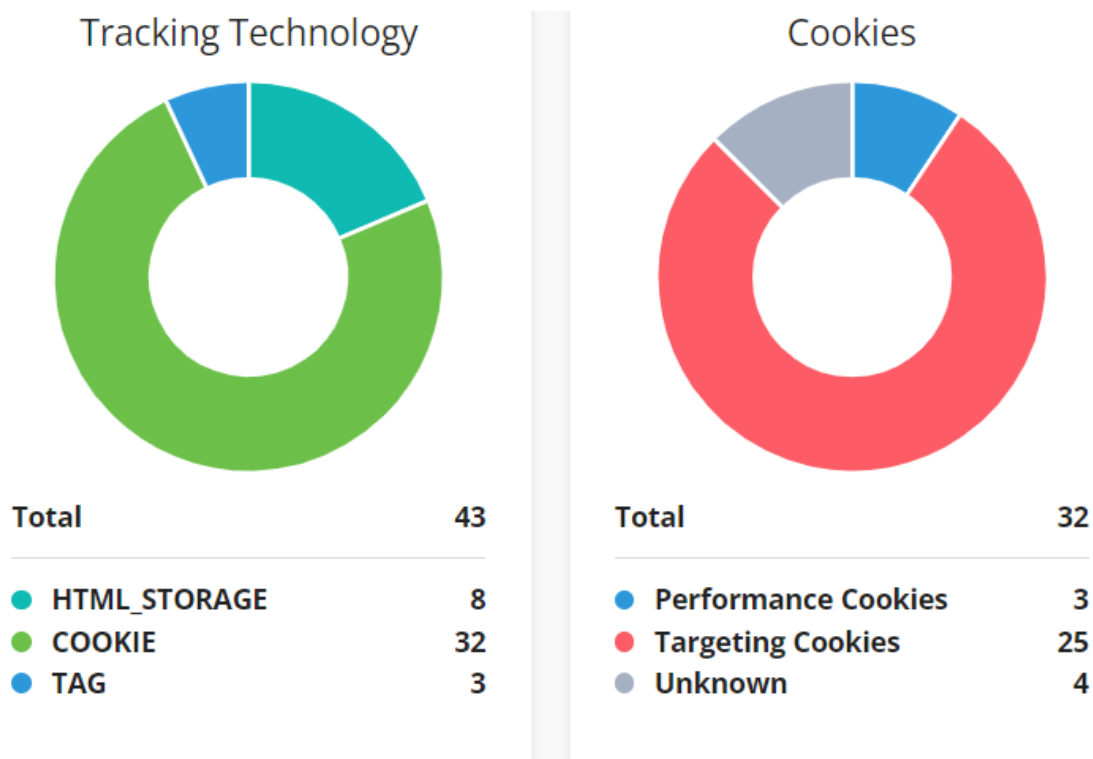


Slika 22. rezultati za stranicu www.coca-cola.hr¹⁵

Na rezultatima skeniranja stranice **tvrtke Kraš**, koji su prikazani na slici 23., vidljiva je razlika u količini pronađenih kolačića i općenito tehnologija za praćenje u odnosu na tri do sad analizirane stranice. Naime, na stranicama tvrtke Kraš pronađeno je 45 različitih tehnologija za praćenje od kojih su 32 kolačića. Od navedenih 32 kolačića, tri su kolačića za performanse, 25 je kolačića za ciljanje korisnika te su pronađena i četiri nepoznata kolačića. Od kolačića za ciljanje, 21 kolačić je prve strane te ih je četiri treće strane koji su isti kao i oni pronađeni na prethodne tri stranice. Među kolačićima prve strane nalazi se 19 kolačića istog naziva, „__sharethis_cookie_test__“, koji spadaju pod sesijske kolačiće

¹⁵ Ekranska slika napravljena na: app.cookiepro.com

te se koriste za praćenje dijeljenja stranica te tko ih dijeli. Osim navedenih koristi se još jedan kolačić Google Analytics usluge te kolačić koji je ranije spomenut, „_fbp“. Među nepoznatim kolačićima nalaze se tri kolačića za koja nije dostupan opis, ali je navedeno da su sesijski te također kolačić „__sharethis_cookie_test__“ no u ovom slučaju je to kolačić treće strane koji dolazi s domene platform-api.sharethis.com.¹⁶



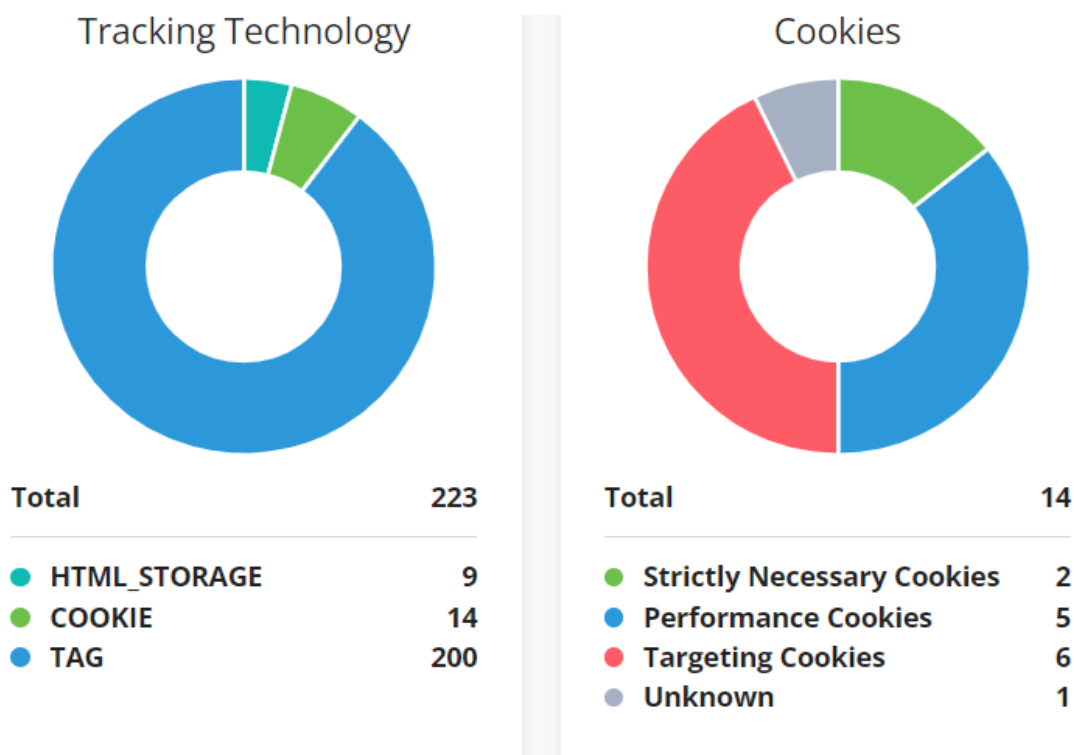
Slika 23. rezultati za stranicu www.kras.hr¹⁷

Posljednja stranica koja je skenirana alatom *CookiePro* za potrebe ovog istraživanja je ona **tvrtke Podravka** te su rezultati skeniranja prikazani na slici 24. Od 206 pronađenih tehnologija za praćenje, samo ih je 16 kolačića od kojih su dva neophodna, pet je kolačića za performanse, šest kolačića za ciljanje te jedan nepoznati kolačić. Stranice tvrtke Podravka također koriste kolačiće za ciljanje postavljene od strane domene youtube.com no uz njih koriste i kolačiće za koje je navedeno da su od strane tvrtke AppNexus, koja se

¹⁶ Domena stranice <https://sharethis.com/> koja nudi rješenja za personalizaciju oglašavanja i ciljanje korisnika

¹⁷ Ekranska slika napravljena na: app.cookiepro.com

dan danas naziva Xandr. Navedena tvrtka bavi se održavanjem platforme unutar oblaka koja omogućava programsko oglašavanje na internetu. Kolačići koji su postavljeni od strane domene adnxs.com koja je u vlasništvu tvrtke Xandr, su trajni kolačići kojima je trajanje 3 mjeseca te služe za provjeru ID broja kolačića za usporedbu sa zapisom u bazi prema čemu se može odrediti je li kolačić s tim ID brojem već povezan s platformom.



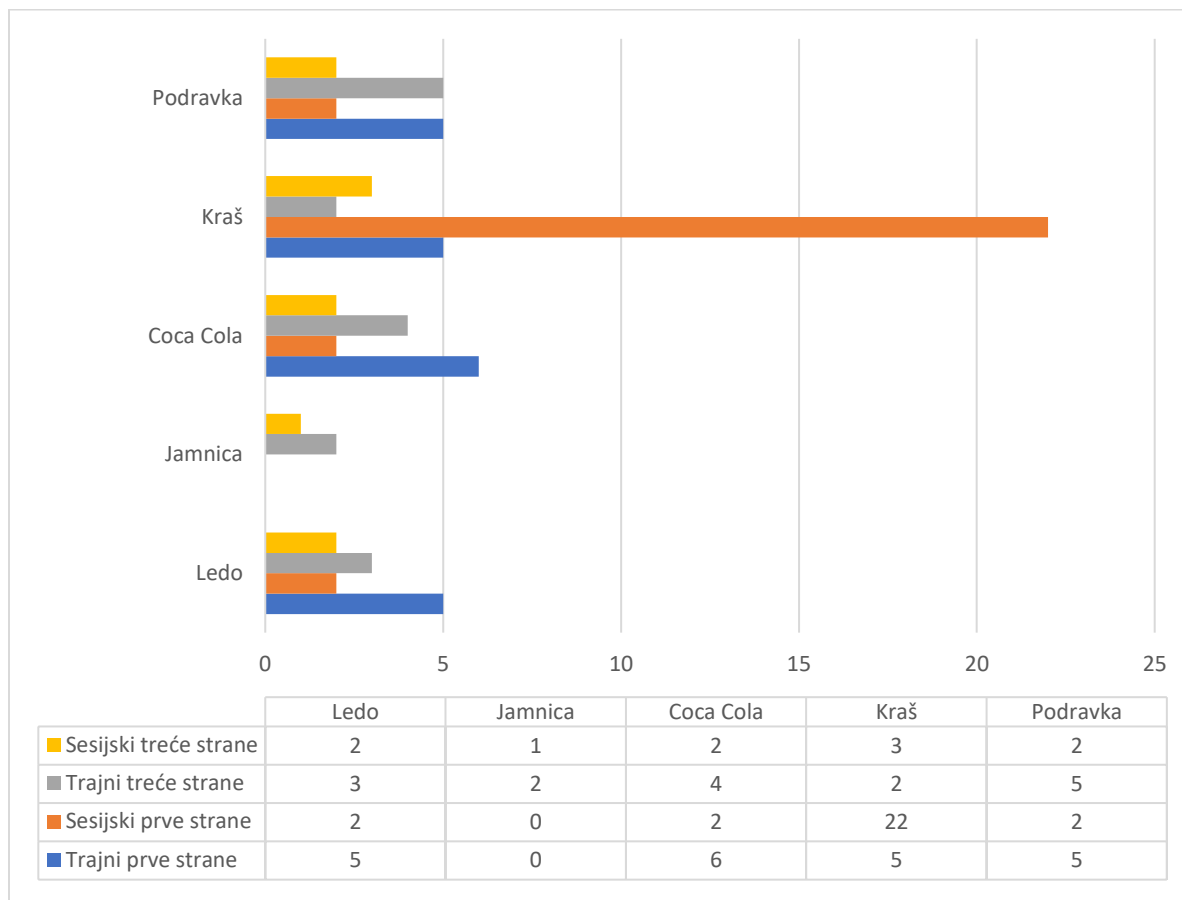
Slika 24. rezultati za stranicu www.podravka.hr¹⁸

Za kraj istraživanja napravljena je usporedba količine kolačića koji su pronađeni na stranicama tvrtki Ledo, Jamnica, Coca Cola, Kraš i Podravka. Rezultati su vidljivi na dijagramu 3 te uključuju trajne i sesijske kolačiće prve strane i trajne i sesijske kolačiće treće strane.

Prema dijagramu je vidljivo kako tvrtka Kraš na svojim stranicama koristi najviše sesijskih kolačića prve strane od svih stranica uključenih u analizu dok tvrtka Jamnica na svojim stranicama ne koristi sesijske kolačiće prve strane niti trajne kolačiće treće strane.

¹⁸ Ekranjska slika napravljena na: app.cookiepro.com

Najviše trajnih kolačića i prve i treće strane koristi tvrtka Coca Cola te se prema tome može zaključiti da Coca Cola prikuplja najviše podataka koji se mogu iskoristiti za personalizaciju oglašavanja.



Dijagram 3. rezultati na temelju analize alatom CookiePro

Rezultati prikazani u ovom dijelu istraživanja potvrđuju hipotezu H1 o prikupljanju kolačića treće strane. Dokazano je da sve od navedenih tvrtki na svojim stranicama prikupljaju barem neke kolačiće treće strane. Iz navedenih rezultata istraživanja prikazanog u ovom poglavlju može se zaključiti kako tvrtka Coca Cola ima najbolje razrađeno rješenje vezano za kolačiće za svoje korisnike. Uz kvalitetno postavljenu obavijest korisnicima, mogućnost odabira kolačića koji će se koristiti te detaljno raspisanu politiku privatnosti i politiku o kolačićima pokazuju kako im je stalo do korisnika koji će posjetiti njihovu stranicu. Među lošijim rješenjima je ono tvrtke Kraš jer su podbacili, kao

što je ranije prikazano u nekim segmentima (obavijest za korisnike i odabir kolačića koji će se koristiti), te imaju puno mjesta za poboljšanje.

5. Zaključak

Uz ubrzan razvoj tehnologije, svaki aspekt života korisnika tehnologije se također mijenja te su korisnici primorani prilagoditi se tome ili odustati od korištenja nekih dijelova tehnologije. Kao što je privatnost svakog čovjeka bitna u stvarnom svijetu, potrebno ju je štiti i od utjecaja tehnologije i interneta. Korištenje interneta je doprinijelo povredi privatnosti jer se na internetu koriste razne metode i tehnologije od kojih neke prikupljaju podatke korisnika u svrhu unaprjeđenja usluge.

Razni stručnjaci iz područja zaštite podataka već se dugi niz godina bore za zaštitu te stvaranje raznih zakona koji bi pomogli u zaštiti podataka. Prve velike korake prema zaštiti privatnosti svojih korisnika poduzele su neke od najvećih tvrtki u području tehnologije te su time započele eru zaštite korisnika. No, čak i nakon desetak godina od tih prvih koraka, određene tvrtke i dalje traže načine da iskoristavaju podatke korisnika, a sve u svrhu profita koji zarađuju oglašavanjem na svojim platformama.

U radu je dan pregled zakona koji su pomogli zaštititi privatnost korisnika na internetu te su propisali pravila prema kojima se tehnologije za praćenje korisnika, kao što su i kolačići, mogu koristiti. Za Hrvatsku je najbitnija Opća uredba o zaštiti osobnih podataka, poznatija kao GDPR, koja je u Hrvatskoj u primjeni od 25. svibnja 2018. godine.

Istraživanje provedeno u ovom radu dalo je uvid u mali uzorak stranica tvrtki koje se bave proizvodnjom hrane i pića u Hrvatskoj. Iz rezultata je vidljivo kako postoji još puno prostora za poboljšanje te također i kako je nekim tvrtkama više a nekima manje stalo do zaštite privatnosti svojih korisnika.

S obzirom na to da se do sada već uvelike ograničilo korištenje kolačića treće strane u svrhu praćenja korisnika, smatram kako će se uskoro oglašivači morati okrenuti alternativnim rješenjima za personalizaciju oglasa i za privlačenje korisnika. Naravno, u obzir se moraju uzeti i druge potencijalno opasne tehnologije koje bi mogle ugroziti privatnost korisnika čak i više nego što to rade kolačići. Svakako smatram da digitalni marketing neće propasti i da postoji način da se zaštiti privatnost bez većih gubitaka za oglašivače i tvrtke koje profitiraju od digitalnog marketinga.

6. Literatura

1. Barth, A. (2011). HTTP State Management Mechanism. RFC, 6265, 1-37. Basart Dotras, Meritxell. (2021). "Online privacy: Analyzing the use of cookies in web pages". <https://upcommons.upc.edu/handle/2117/360444> (15.12.2022.)
2. 'Djelokrug'. Agencija za zaštitu osobnih podataka, <https://azop.hr/djelokrug/>. (18.6.2022.)
3. E. Pottinger, Nicole. (2019) "Don't Forget to Subscribe: Regulation of Online Advertising Evaluated Through YouTube's Monetization Problem". <https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=5456&context=klj> (15.12.2022.)
4. EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE. Direktiva 2002/58/EZ Europskog Parlamenta i Vijeća Od 12. Srpnja 2002. o Obradi Osobnih Podataka i Zaštiti Privatnosti u Području Elektroničkih Komunikacija (Direktiva o Privatnosti i Elektroničkim Komunikacijama). Službeni list Europske unije, 31.7.2002, <https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=celex:32002L0058>. (25.5.2022.)
5. Europski parlament i vijeće. Opća Uredba o Zaštiti Podataka. Službeni list Europske unije, 27.4.2016, <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.
6. Gourley, Totty, Sayer, Aggarwal, Reddy. HTTP: The Definitive Guide. O'Reilly Media, Inc., 2002., 246-251, 257-260. (25.5.2022.)
7. Internet Cookies. CIAC, 12.3.1998. <https://packetstormsecurity.com/files/19214/ciac.i-034.internet.cookies.html>. (25.5.2022.)
8. Jackson, Tim. 'This Bug in Your PC Is a Smart Cookie'. Financial Times, 12 Feb. 1996, p. 32. <https://archive.org/details/FinancialTimes1996UKEnglish/Feb%2012%201996%2C%20Financial%20Times%2C%20%2312%2C%20UK%20%28en%29/page/n29/mode/2up?view=theater>. (25.5.2022.)

9. Kristol, David M. 'HTTP Cookies: Standards, Privacy, and Politics'. ACM Transactions on Internet Technology, vol. 1, no. 2, 1.11.2001, pp. 151–98, <https://doi.org/10.1145/502152.502153>. (25.5.2022.)
10. Kukuška M. 'What's Happening with Browser Cookies? Advertising Industry in the Face of Third-Party Cookie Phase-Outs.' NewProgrammatic Blog, 26.7.2021, <https://newprogrammatic.com/blog/third-party-cookies-in-programmatic-advertising-news/>. (25.5.2022.)
11. Kulyk, O., Hilt, A., Gerber, N., Volkamer, M. (2018). "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. Conference: 3rd European Workshop on Usable Security (EuroUSEC), London, England.
12. Mrežni Kolačić | Hrvatska Enciklopedija.
<https://enciklopedija.hr/Natuknica.aspx?ID=70676>. (12.7.2022.)
13. Ramchandani, Vinita. Nagar, Dhanashree. (2017). "GEO-TARGETING : TARGETING CUSTOMERS IN A BETTER WAY".
https://www.researchgate.net/publication/366289661_GEO-TARGETING_TARGETING_CUSTOMERS_IN_A_BETTER_WAY
(28.12.2022.)
14. Rivero, Nicolás. 'The Inventor of the Digital Cookie Has Some Regrets'. 25.4.2021. Quartz, <https://qz.com/2000350/the-inventor-of-the-digital-cookie-has-some-regrets/>. (25.5.2022.)
15. Schwartz, John. 'Giving Web a Memory Cost Its Users Privacy'. The New York Times, 4 Sept. 2001. NYTimes.com, <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html>. (25.5.2022.)
16. Session Hijacking Attack Software Attack | OWASP Foundation.
https://owasp.org/www-community/attacks/Session_hijacking_attack. (25.5.2022.)
17. 'The Cookie Law Explained'. CookieLaw, <https://www.cookie-law.org/the-cookie-law/>. (25.5.2022.)

18. Tirtea, R., Castelluccia, C., Ikonomou, D. (2011). "Bittersweet cookies. Some security and privacy considerations". The European Union Agency for Cybersecurity.
19. Ustav Republike Hrvatske - Zakon.Hr. <https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske>. (18.6.2022.)
20. Wagner, Paul. Cookies: Privacy Risks, Attacks, and Recommendations. 8.12.2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3761967. (12.7.2022.)
21. Www - Lou. <https://www.montulli.org/lou>. <https://www.montulli.org/lou>. (25.5.2022.)
22. 'Cookies, the GDPR, and the EPrivacy Directive'. GDPR.Eu, 9.5.2019, <https://gdpr.eu/cookies/>. (20.7.2022.)

Sažetak

Razvoj interneta doveo je do raznih promjena u svim aspektima života, pa tako i u oglašavanju. Najveći zadatak, kada se radi o oglašavanju, je kako privući što veći broj raznolikih kupaca ili korisnika. Mnoge tvrtke su rješenje tog problema pronašle upravo u mogućnostima koje internet nudi. U svrhu stvaranja personaliziranih oglasa tvrtke skupljaju određene podatke o korisnicima, a to rade upravo uz pomoć kolačića. U ovom radu je objašnjeno što su kolačići, kako su nastali te kako se i za što danas koriste. Objašnjeno je i personalizirano oglašavanje i kako mu kolačići pridonose. Rad također sadržava usporednu analizu nekoliko poznatih tvrtki u hrvatskoj u području proizvodnje hrane i pića, odnosno njihovog načina prikupljanja kolačića. Cilj istraživanja je prikazati koliko uspješno te tvrtke prikupljaju i koriste kolačiće u svrhu personaliziranog marketinga.

Ključne riječi: *mrežni kolačići, personalizirano oglašavanje, privatnost, digitalni marketing*

HTTP cookies and personalised advertising

Abstract

The development of Internet has led to various changes in everyday life, including advertising. One of the biggest challenges in marketing is attracting a large amount of diverse users and customers. Numerous companies have found a solution to this problem in the opportunities provided by the use of Internet. In an attempt to produce personalised advertisements, companies collect user data across the web and they do it with the use of cookies. This paper gives an insight into what HTTP cookies are, how they came into use and what they're being used for today, as well as the contribution cookies have in personalised advertising. The paper also contains a comparative analysis of popular food and beverage companies in Croatia in their collection and use of user cookies. The purpose of this analysis is determining how successfully these companies use the collected user cookies for personalised advertising.

Key words: *HTTP cookies, personalised advertising, privacy, digital marketing*