MARKETINŠKE IMPLIKACIJE ODNOSA PRIVATNOSTI I PERSONALIZACIJE NA INTERNETU

Kraljević, Marja

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

MARKETINŠKE IMPLIKACIJE ODNOSA PRIVATNOSTI I PERSONALIZACIJE NA INTERNETU

Mentor:
Doc. dr. sc. Dedić Goran

Student:
Marja Kraljević

Split, rujan, 2020

SADRŽAJ

1. UVOD

Za vrijeme u kojem živimo i radimo karakteristična je brzina razvoja tehnologije, široka i laka dostupnost informacija i veliki utjecaj marketinga na svakodnevnicu. Internetska era je najbrži tehnološki fenomen svih vremena, pojavom interneta došlo je do velikog preokreta kako u privatnom tako i u poslovnom životu svakog pojedinca.

S pojavom interneta informacije o ponudi usluga i proizvoda poslovnih subjekata postale su široko dostupne. Poslovni subjekti na internetu vide priliku za jednostavnim, brzim i relativno jeftinim oglašavanjem. Kako bi poslovni subjekt ostvario zadani cilj, koji je u pravilu vezan za ostvarenje određenog oblika razmjene, koristi se raznim alatima kao što su oglašavanje i prikupljanje osobnih podataka korisnika. Dobra marketinška strategija jedne tvrtke ili institucije mora biti utemeljena na etički prikupljenim podacima o svojim krajnjim korisnicima, zato veza između poslovnih subjekata i kupaca mora biti bazirana na objektivnoj i zdravoj razini personalizacije ponude. Ključ dobre veze s kupcem počiva u kvalitetnom balansu prilagodbe istome u pogledu stvaranja novih ili prilagodbi starih proizvoda.

Postavlja se pitanje u kolikoj mjeri su ljudi zapravo svjesni svojih aktivnosti na internetu odnosno koliko su svjesni stupnja izloženosti vlastite privatnosti. Dok svakodnevno koristimo internet kako bi zadovoljili određenu potrebu ljudi nisu u potpunosti svjesni rizika virtualnog svijeta. Pitanja koje bi si odgovorno i ozbiljno trebao postaviti svaki pojedinac jesu: Koliko privole, obrasci, profili na društvenim mrežama ili učestalost posjeta određenim sadržajima daju privatne i personalizirane informacije o meni, mojim životnim navikama, potrebama preferencijama i stavovima?

Kada govorimo o pojmovima kao što su privatnost i personalizacija na internetu treba jasno naglasiti kako postoji razlika između onih podataka koje svjesno svojom voljom putem različitih obrazaca i privola dajemo nekom poslovnom subjektu ili instituciji i onih podataka koji se mogu iščitati iz različitih e-aktivnosti te upotrijebiti u više svrhe. Kroz ovu tematiku proteže se definicija etičnosti koja treba biti vodilja svakog ponašanja u poslovnom svijetu, a nepoštivanjem iste dovodi se mnoge u rizik od zloupotrebe pa tako i u marketinške svrhe.

1.1 Definicija problema

Problem istraživanja u ovom radu predstavlja etičnost kod prikupljanja korisničkih podataka i njihova implementacija u marketinške svrhe. Marketinška etika podrazumijeva sve principe, vrijednosti i standarde ponašanja koje moraju slijediti marketinški stručnjaci pri tome je zadaća marketinga da usvoji moralne i etičke vrijednosti i svoje ponašanje uskladi s njima.

1.2 Cilj rada

Cilj ovog Završnog rada je objasniti odnos privatnosti i personalizacije na internetu te što korištenje osobnih podataka nudi s marketinške strane, cilj je ujedno istražiti i analizirati percepciju korisnika o rizicima i koristima kojima se izlažu u virtualnom svijetu podataka.

1.3 Metode rada

U ovom Završnom radu prisutna je kombinacija različitih znanstvenih metoda sa svrhom postizanja istraživačkih ciljeva. Sekundarni podaci korišteni su iz internetskih izvora. Provedena je metoda analize pomoću koje su razni pojmovi na jednostavniji način definirani i objašnjeni. Također korištena je i metoda sinteze kojom su različiti elementi rada povezani u jednu cjelinu. Metodom dedukcije i indukcije izvodili su se krajnji sudovi, dok su se pomoću empirijske metode prikupljali primarni podaci o stavovima korisnika kada je riječ o svjesnosti rizika kojem su izloženi dijeljenjem vlastitih podataka. Nadalje, u mnogim dijelovima rada korištena je deskriptivna metoda kako bi se opisale opće karakteristike privatnosti i personalizacije, ali i one na internetu. Također, deskriptivna metoda se koristila i prilikom interpretacije rezultata dobivenih provođenjem anketnog upitnika.

1.4 Struktura rada

Struktura ovog rada sastoji se od 5 primarnih poglavlja. Prvo poglavlje predstavlja uvod u kojem je objašnjena definicija problema, cilj rada, metode i struktura rada. Drugo poglavlje odnosi se na privatnost i personalizaciju na internetu, u ovom poglavlju je jasno prikazana problematika privatnosti na internetu u suvremenom svijetu. Također objašnjeni su pojmovi poput GDPR-a i odnosa etičnosti te prikupljanja podataka u marketinške svrhe. U trećem poglavlju detaljno su objašnjeni procesi hipertargetiranja i trgovine podacima te su dani prikladni primjeri iz prakse. Definiran je i paradoks privatnosti. Četvrto poglavlje posvećeno je empirijskom dijelu ovog rada u kojem su analizirani i definirani rezultati istraživanja. Peto

poglavlje obuhvaća zaključak nakon kojeg slijedi popis korištene literature, popis slika i tablica te sažetak na hrvatskom i stranom odnosno engleskom jeziku.

2. PRIVATNOST I PERSONALIZACIJA NA INTERNETU

2.1 Problematika privatnosti u suvremenom svijetu

Kako je navedeno u radu Boban (2012) pravo na privatnost nalazimo i u stranoj terminologiji kao *„Right to privacy"* na engleskom, „*Droit au respect de la vie"* na francuskom i na njemačkom pod pojmom *„Recht auf Privatheit"*. Pravo na privatnost prema Boban (2012) kako je navedeno u radu Šimundić (2017) možemo definirati kao temeljno pravo svakog pojedinca koje ima svoju međunarodnu, ustavno-pravnu i civilno-pravnu važnost. Takvo pravo pojedincu osigurava zaštitu od svakog neprikladnog, nezakonitog i zlonamjernog ponašanja, općenito osigurava mu zaštitu svake sfere njegove privatnosti.

Privatnost pojedinca Boban (2012) dijeli na:

- Prostornu
- Informacijsku
- Komunikacijsku

Prostorna privatnost odnosi se na životni prostor pojedinca, ona je ustavno zaštićena putem građanskog prava koje nalaže da je dom nepovrediv. Prostorna privatnost prezentira fizičku domenu te kao takva pojedincu omogućava uvjeta za osobni rast i razvoj.
Za *informacijsku privatnost* karakteristična je uska veza s razvojem informacijskih tehnologija. Ovaj tip privatnosti ogleda se kroz pojmove prikupljanja osobnih podataka, upravljanja i korištenje istih. Prema Boban (2012) kako Buble (1993) u svom radu navodi: „Informacija ima cijeli niz definicija prema kojima: predstavlja temelj donošenja organizacijske i upravljačke odluke svakog uspješnog menadžera".
Komunikacijsku privatnost pak definiramo kao vrstu privatnosti koja se odnosi na različite osobne zapise kao što je dopisivanje ili neki drugi oblik komuniciranja.

Prema CERT.hr (2017) u današnjem svijetu privatnost kao temeljno ljudsko pravo nije dovoljno shvaćena i kao takva je često narušavana pogotovo u virtualnom svijetu. Iako je prirodna potreba da se neki segmenti života i neke osobne informacije zadrže dalje od javnosti, prosječni korisnici u pravilu nisu svjesni opsega osobnih informacija koje korištenjem različitih e-usluga daju na uvid trećim stranama.

CERT.hr (2017) navodi kako je veoma čest slučaj da korisnici tvrtkama na raspolaganje daju vlastite podatke putem ispunjavanja raznih privola i prihvaćanja uvjeta poslovanja, tvrtke podatke evaluiraju s ciljem unaprjeđivanja poslovanja i maksimiziranja profita. Zapravo istinska zaštita ljudskih i građanskih prava trebala bi podrazumijevati jasno i nedvosmisleno upoznavanje korisnika s činjenicom da će se npr. njihovi zdravstveni podaci prodavati osiguravajućim kućama koje će na osnovu toga određivati cijenu police osiguranja. Pravno gledajući korisnik je slobodan odbiti uvjete i odreći se usluge, no to bi značilo odbiti veliki broj usluga na internetu te odreći se tehnoloških dobara koja su danas postala nužna.

S obzirom na tehnološki napredak, kojem svakodnevno svjedočimo, jasno je da smo sve više izloženi riziku manipulacije koja proizlazi uslijed uvida koje naši podaci pružaju, u ostalom oni su nerijetko odraz naše osobnosti i stila života. Suvremene tvrtke, institucije ili stranke danas, a u budućnosti posebice, bez premca će nastojati u svojem naumu da si u što većoj mjeri stvore gotovo savršeni profil klijenta, potrošača, pobornika ili možda čak i glasača te s obzirom na analizirane profile kreirati prilagođenu kampanju te na koncu ostvariti određenu korist koja je u najvećem broju slučajeva financijska. Problem privatnosti u suvremenom svijetu sa sobom nosi mnoštvo zanimljivih pitanja od kojih je zapravo najvažnije pitanje svjesnosti pojedinca različitih rizika koje nosi virtualni svijet.

2.1.1 Što je GDPR?

Slika 1: GDPR

Izvor: Vlastita izrada autorice

Opća uredba o zaštiti podataka (GDPR), koja se primjenjuje u svim državama članicama EU od 25. svibnja 2018., predstavlja značajan korak u razvoju europskog okvira privatnosti. Novi zakon obuhvaća zaštitu osobnih podataka svih stanovnika EU-a, bez obzira na mjesto obrade. Osobni podaci su podaci koji, izravno ili neizravno, mogu identificirati pojedinca, a posebno uključuju internetske identifikatore poput IP adrese, kolačiće i digitalni otisak prsta te podatke o lokaciji.

Osobni podaci prema (Uredba EU 2016/679) moraju biti:

- Zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika
- Prikupljeni u zakonski prihvatljive svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama
- Primjereni, relevantni i ograničeni na ono što je nužno
- Točni i redovno ažurirani
- Čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju
- Obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene obrade te od slučajnog gubitka, uništenja ili oštećenja

Gosh (2018) postavlja pitanje kako će i u kolikoj mjeri zapravo ova uredba EU promijeniti tržište digitalnog marketinga. Također govori kako će GDPR prisiliti poslovne subjekte da se odreknu većine svoje ovisnosti o prikupljanju podataka o ponašanju s obzirom na to najveću ugrozu njihovom poslovanju predstavlja nova formulacija za pristanak pojedinca na prikupljanje i obradu podataka. Digitalni trgovci znaju da korisnici internetskih usluga poput Snapchat-a, Facebooka i Googlea tehnički samom prijavom daju pristanak na uvjete usluge tih kompanija. Stoga je upitno je li korisnik voljan da se njegovi osobni podaci prikupljaju u digitalnom, fizičkom i svijetu izvan platforme te koriste li se ti podaci za izradu profila ponašanja u svrhe digitalnog marketinga.

2.2 Privatnost i personalizacija na Internetu

Prethodno, **privatnost** smo definirali kao temeljno ljudsko i ustavno pravo na zaštitu svakog segmenta privatnosti života pojedinca, pa tako i onog na internetu. Tako nam preostaje definirati pojam personalizacije.

Personalizacija je prema Montgomery i Smith (2009) usko povezana s idejom interaktivnog marketinga i odnosi se na prilagođavanje nekih elemenata marketinškog miksa na individualnu razinu. Na primjer, klijent koji naručuje određene dijelove za mikroračunalo od Della, bio bi primjer prilagođavanja, međutim kada Dell pred-instalira individualizirani softverski paket za koji očekuje da bi određeni korisnik želio kupiti predstavlja dobar primjer personalizacije. Dakle, personalizacija je usko povezana s tehnologijom i aplikacijama za koje je namijenjena.

Personalizacija na internetu, okruženju koje je bogato informacijama i dobro prilagođeno interaktivnosti Montgomery i Smith (2009) odvija se putem:

- Tražilica,
- Preporuka i
- Cijena i promocija

Tražilice funkcioniraju tako da podudaraju ključne riječi ili izraze koje opisuju što korisnik pretražuje prema indeksu web stranica. Cilj personalizacije u ovom kontekstu je prilagodba rezultata pretraživanja na temelju prethodnih pretraga korisnika, a potencijalno njihovih baza podataka i preferencija.

Preporuke s aspekta personalizacije na internetu funkcioniraju na način da se korisniku prikazuju preporuke formirane s obzirom na njegova prethodna pretraživanja, gledanja i

označavanja sadržaja sa „sviđa mi se“. Dobar primjer je Netflix-ov sustav preporuka koji unaprijed može procijeniti hoće li se korisniku svidjeti film.

Cijena i promocija je zasnovana na personaliziranoj cjenovnoj ponudi i promociji na temelju povijesti korisnika i iskazanih preferencija, međutim ova vrsta personalizacije zahtijeva iznimno veliku bazu podataka prethodnih cijena za izradu predviđanja budućih.

Primjer uspješne integracije strategije personalizacije:

Progresivna strategija personalizacije vidljiva je kod svjetski poznate tvrtke Amazon. Amazon kao najpoznatiji e-trgovac na svojoj web stranici pruža više različitih oblika personalizacije, a neki od najistaknutijih su *Vaš Amazon, današnje ponude, darovi i popisi želja, preporuke po kategorijama, Vaša povijest pregledavanja, Vaši popisi* i *Vaš profil*. S obzirom na stupanj prisutnosti personalizacije u poslovanju tvrtke Amazon može se zaključiti kako im kupac sa svim svojim preferencijama predstavlja središte poslovanja.

Strah od narušavanja privatnosti sveprisutan je u ljudskoj populaciji koja koristi nove komunikacijske tehnologije činjenica je da taj strah treba otkloniti i težiti kontinuiranom stvaranju povjerenja i sigurnosti u elektroničku infrastrukturu. Zaštita privatnosti igrala je i nastavit će igrati važnu ulogu u razvoju novih informacijskih tehnologija poglavito zbog zabrinutosti potrošača radi narušavanja privatnosti koja potiče mnogobrojne reakcije vlada, poduzeća i udruga potrošača.

U prethodnom ulomku spomenuli smo pojam *„narušavanje privatnosti na internetu“*, no na koje načine je sve ona zapravo narušena?

Navesti ćemo neke od njih, a prema CERT.hr (2017) to su:

1. Kolačići
2. Praćenje otiska Web preglednika
3. Detaljno praćenje korištenja stranice
4. Narušavanje privatnosti putem pametnih telefona

1. Kolačići

“Koristimo kolačiće! To znači da korištenjem web stranice pristajete na uporabu tih datoteka i koristite sve funkcionalnosti podržane tom tehnologijom. Molimo vas da prihvatite uvjete korištenja”

S gore navedenom obavijesti gotovo smo više puta dnevno suočeni prilikom ulaska na neku web stranicu, no sigurno je da malo tko zapravo zna što su kolačići i koja im je svrha.

All about cookies navodi slijedeće: „Kolačići su male tekstualne datoteke s danim ID oznakama koje se pohranjuju u direktorij korisnikovog preglednika ili podmape podataka programa“. Prilikom posjeta određenoj web stranici, uz prihvaćanje, kolačić se šalje na korisnikov internet preglednik kako bi pamtio što radi, npr. gdje klika i što dodaje u košaricu prilikom kupnje. Primarna svrha kolačića je da povezuju određene podatke s određenim posjetiteljem.

Koji sve tipovi kolačića postoje?

Kolačić prve strane (first party cookie) dolazi s internetske stranice koju korisnik pregledava, a mogu biti privremeni ili stalni. Na taj način, internetske stranice pohranjuju podatke koji će korisniku olakšati korištenje pri svakom novom posjetu.

Jednokratni kolačić (session cookie) postoji samo u trenutnoj memoriji kada korisnik pregledava neku web-stranicu. Web-preglednici obično izbrišu ovaj tip kolačića kada korisnik zatvori web-preglednik.

Trajni kolačić (persistent cookie) ostaje na korisnikovom tvrdom disku sve dok ih ne izbriše ili dok ne isteknu. Koliko dugo kolačić ostaje u pregledniku, ovisi o tome koliko je posjećena web stranica programirala da kolačić traje.

Kolačići treće strane (third party cookie) na računalo dolaze s drugih web mjesta koje se nalaze na internetskoj stranici koja se pregledava. Riječ je o tzv. pop-up oglasima, a kolačići imaju ulogu praćenja posjećenosti internetskih stranica u oglašivačke svrhe.

Superkolačić (supercookie) može biti potencijalno opasan za sigurnost korisnika i često ih preglednik sam blokira.

Kolačići se prema Marker.hr-u (2017) najčešće koriste u svrhu:

- praćenja broja posjetitelja na web stranicama
- praćenja vremena koje svaki posjetitelj provede na određenoj stranici
- optimizacije oglašavanja
- optimizacije web stranice

S obzirom na temu rada posebno je zanimljiva optimizacija oglašavanja pomoću trajnih kolačića. Oglašivači i agencije mogu prikupiti podatke o navikama i interesima korisnika te na taj način prikazivati oglase koje smatraju relevantnima odnosno privlačnima određenoj skupini korisnika. Kolačići se mogu i onemogućiti npr. pretraživanjem u anonimnim prozorima te upotrebljavanjem raznih alata za dodatnu zaštitu preglednika. Onemogućavanjem kolačića oglasi će se i dalje prikazivati samo neće biti prilagođeni navikama korisnika, odnosno bit će manje personalizirani.

2. Praćenje otiska Web preglednika

CIS.hr (2012) navodi: „Otisak web preglednika je tehnika prikupljanja i obrade informacija koje se mogu prikupiti iz web preglednika na način da se pokuša stvoriti jedinstvena slika tog preglednika. Cilj takve tehnike je prepoznavanje i praćenje korisnika. Kada korisnik jednom pristupi Internet stranici ona uzima njegov otisak, te ga pomoću tog otiska može prepoznati kada se vrati idući puta“.

3. Detaljno praćenje korištenja stranice

CERT.hr (2017) tvrdi da se na ovaj način snima sve što korisnik radi na web stranicama pomoću JavaScript koda. Također na ovaj način moguće je u potpunosti prikazati kako je korisnikovo korištenje web stranice izgledalo, odnosno kako ono trenutno izgleda. Kako bi što bliže objasnili ovaj tip narušavanja privatnosti možemo navesti bliski primjer s društvenim mrežama, kada se korisnik odlučio napisati određeni status npr. na Facebooku i napiše ga, ali se ipak predomisli i izbriše, odnosno ne objavi ga – Facebook ga je ipak „zapamtio“.

4. Narušavanje privatnosti putem pametnih telefona

Narušavanje privatnosti putem pametnih telefona odvija se kroz aplikacije koje prikupljaju brojne podatke unatoč tome što oni zapravo nisu potrebni za njihovu temeljnu funkcionalnost. Takav tip aplikacija traži tzv. dopuštenja za pristup datotekama, kameri, lokaciji, pozivima itd.

„Primjerice, aplikacija AccuWeather za iOS uređaje je između ostaloga prikupljala GPS koordinate korisnika te podatke o Wi-Fi mrežama i Bluetooth uređajima koji se nalaze u blizini te je iste podatke prodavala trećoj strani – tvrtki Reveal Mobile“ (CERT.hr, 2017).

2.2.1 Kako zaštititi privatnost na internetu?

Ubrzani tempo života svakodnevno plasira nove izazove s kojima se moramo nositi, život u suvremenom svijetu prvenstveno znači prilagodbu na novonastale tehnološke promjene, s time i pristanak na kompromise. Kompromisi u e-svijetu znače količinu korisnikove spremnosti da podnese svoju privatnost u rizik, a za uzvrat dobije traženu informaciju, uslugu ili proizvod. Na kraju, postoje kompromisi na koje korisnik jednostavno mora pristati jer mu određene mogućnosti na internetu neće biti dostupne, no ipak postoji prostor za određeni osobni doprinos kojim možemo barem malo više zaštititi svoj privatni životni segment.

Kako se zaštititi? (CERT, 2017)

1. Razumijevanje rizika
2. Ispravno podešavanje postavki postojećih alata
3. Korištenje dodatnih alata za zaštitu privatnosti
4. Virtual Private Network (VPN)

1. Razumijevanje rizika

CERT.hr (2017) navodi: „Briga o privatnosti na Internetu prije svega je odgovornost samog korisnika a razumijevanje rizika kojima je privatnost izložena uporabom interneta prvi je korak u njenoj zaštiti“. Danas veliki broj tvrtki koriste popularni poslovni model pružanja usluga koje ne moramo platiti, no za uzvrat ipak moramo pristati na određeni kompromis odnosno dati im potrebne osobne podatke. S obzirom na navedeno postaje jako teško sačuvati privatnost, a ujedno se neograničeno koristiti svim mogućnostima koje nam internet pruža na svim svojim platformama.

2. Ispravno podešavanje postavki postojećih alata

Jedan od ključnih koraka u zaštiti privatnosti na internetu prema CERT.hr-u (2017) je i ispravno podešavanje postojećih alata koje podrazumijeva onemogućavanje upotrebu kolačića trećih strana kojim eliminiramo rizik praćenja korisnika. Isto tako dobro je obratiti pozornost na popis tzv. dozvola koje zahtijevaju određene aplikacije na pametnim telefonima te onemogućiti one dozvole koje nisu nužno potrebne za njihovu primarnu funkciju.

3. Korištenje dodatnih alata za zaštitu privatnosti

Razvijeni su brojni dodaci za web preglednike koji uvelike povećavaju razinu zaštite kao što su prema CERT.hr-u (2017) :

a) uBlock Origin - blokira web oglase, skripte za praćenje korisnika te web adrese koje su poznati izvori zlonamjernih programa

b) Signal Private Messenger - utemeljen na sigurnom komunikacijskom protokolu koji omogućuje šifriranje s kraja na kraj (eng. end to end encryption), čime se onemogućuje čitanje sadržaja trećim stranama

c) Tor Browser - građani zemalja u kojima država regulira sadržaj mrežnog prometa mogu koristiti Tor Browser kako bi anonimno i privatno mogli pregledavati web sadržaj i zaobišli cenzure.

4. Virtual Private Network (VPN)

U VPN vezi stvara se tzv. virtualni tunel u kojem je sva komunikacija šifrirana i nerazumljiva trećim stranama koje bi je mogle presresti na javnim mrežama.

2.3 Odnos etičnosti i prikupljanja podataka u marketinškoj praksi

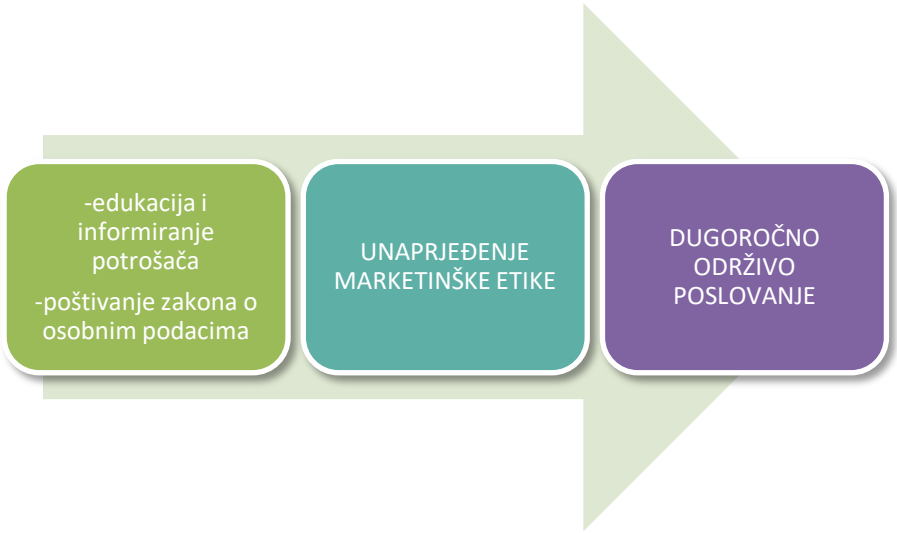
„Etika je filozofska disciplina koja istražuje i bavi se ciljevima i smislom moralnih htijenja, temeljnim kriterijima moralnih činova kao i općenitim zasnovanostima i izvorima morala“ (Karpati, 2001).

Brajković (2016) navodi kako Aristotel *ethos* povezuje uz pojmove dobrog djelovanja, dobre osobine i karaktera tako i uz pojmove efikasnosti i ekonomičnosti.

„Etika u istraživanju marketinga je skup načela i smjernica koje reguliraju cjelokupni proces istraživanja, od njegovog ugovaranja, preko provođenja samog istraživanja do prezentacije rezultata i postupanja sa dobivenim podacima. Samo jasna istraživačka etika kao i njena dosljedna i nedvosmislena primjena omogućuju povjerenje javnosti u istraživanje tržišta i ispitivanje javnog mnijenja, kao i u subjekte koji ih provode“ (Babić ,2014)

Etičke dileme prema Brajković (2016) nastaju u trenutku kada bez znanja dozvole klijenta marketinški odjel određene tvrtke privremeno posudi, kupi ili razmijeni informacije o klijentu. Dvije najznačajnije dileme postavljaju pitanje: tko ima pravo vidjeti sve privatne podatke klijenta i ima li klijent pravo znati tko traga za njegovim podatcima, te ima li pravo onemogućiti pristup istima?

Postoje dvije vrste prikupljanje korisnikovih ili potrošačevih podataka, prva je ona kada korisnik svjesno i svojom voljom daje osobne podatke za određenu njemu znanu svrhu, dok s druge strane postoji i ona pasivna vrsta bez znanja korisnika. Zapravo problem etičnosti i prikupljanja podataka u marketinškoj praksi počiva na dilemi je li korisnik točno zna u koju svrhu će se upotrijebiti njegovi podaci, tko sve zapravo smije imati uvid u osobne i personalizirane podatke te na koncu može li onemogućiti manipulaciju istima.



Slika 2: Model za unaprjeđenje marketinške etike u poslovanju

Izvor: Vlastita izrada autorice

3. POSLOVNI MODELI IT KORPORACIJA I MARKETINŠKE IMPLIKACIJE

3.1 Hipertargetiranje

Neprestani razvoj reklamnih sustava i algoritama osigurava brzo i efikasno pronalaženje potencijalnih kupaca. Hipertargetiranje prema Semeradov-i i Weinlich-u (2017) predstavlja upotrebu detaljnih podataka o klijentima i marketinšku automatizaciju za isporuku visoko ciljanih i personaliziranih poruka na velikom broju kanala. Marketinške kampanje zasnovane na ovakvom tipu dizajnirane su tako da privuku određene segmente ljudi i/ili kupaca. Današnja inovativna tehnologija ima mogućnost obrade velike količine podataka te upravo mogućnost predstavlja temelj za ciljanje javnosti na sasvim inovativan način.

Maksimiziranje profita predstavlja središte poslovanja svake tvrtke u suvremenom svijetu. Kako bi ostvarile taj cilj tvrtke su neprestanoj potrazi za novim i efikasnim modelima koji podrazumijevaju kvalitetan marketinški pristup. Oglašivačke platforme, poput Facebooka i Google Ads-a, pružaju mnogo opcija za ciljanje i oblikovanje baze korisničkih podataka koje omogućuju oglašivačima da eksperimentiraju.

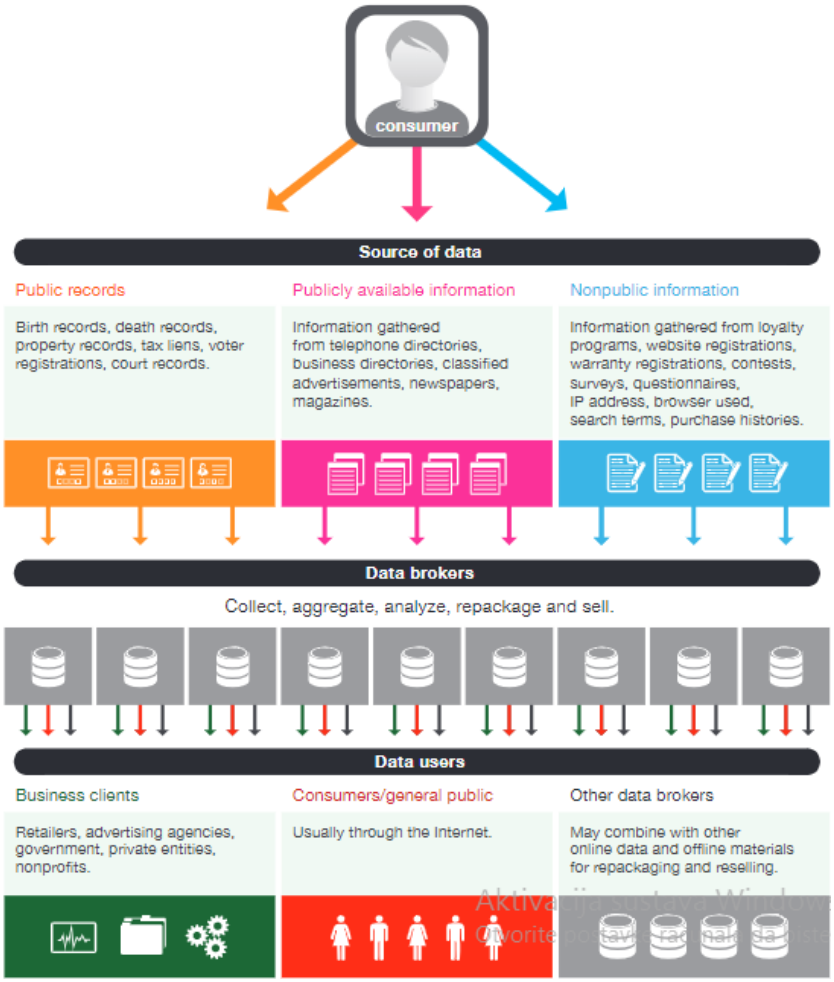
Cilj formiranja personaliziranih profila korisnika prema Jovanović i Ercegovac (2013) predstavlja uspostavljanje logičkih veza u ponašanju korisnika; npr. definiranje individualnih razlika u kognitivnim procesima. To mogu biti: pažnja, kapacitet radne memorije, opća inteligencija, motoričke i jezične sposobnosti. Osnova psihološkog prilagođavanja je u nastojanju za promjenom ponašanja, stavova i motivacije korisnika. Usprkos skepticizmu prakse, empirijski podaci pokazuju da psihološko prilagođavanje čini oko 10% hipertargetiranja. Također činjenica je da informacija kreirana u skladu s potrebama ciljanog segmenta potrošača zapravo povećava mogućnost za promjenu stava i ponašanja potrošača. „Emocionalno personalizirana informacija o proizvodu može biti fokusirana na: stvaranje trenutnog i primitivnog emocionalnog odgovora, kreiranje raspoloženja i indirektno utjecati na sekundarne efekte emocija i raspoloženja kao što su pažnja, pamćenje, performanse i zaključci, a rezultat je trenutna on-line kupovina ili kasnija kupovina zasnovana na pamćenju poruke“ (Jovanović, Ercegovac, 2013).

U svijetu oglašavanja postoje različite tehnike hipertargetiranja, no svaka ima primarne uvjete: web stranicu, potencijalnog korisnika koji će posjetiti stranicu, oglasni sadržaj i specifične alate za personalizaciju. Tehnike targetiranja razlikuju se samo u segmentu načina prikupljanja podataka, pa tako postoje one u kojima korisnik svjesno sudjeluje i one u kojima

korisnik nesvjesno sudjeluje dajući široki spektar personalizirajućih podatka. Osnovne metode targetiranja prema Jovanović i Ercegovac (2013) baziraju se na prikupljanju: IP adresa sa kojih se pristupa određenom sadržaju, dobu dana kada se sadržaj otvara, prikupljanjem informacija o e-aktivnostima korisnika, prikupljanju podataka iz povijesti pretraživanja, kao i na prikupljanju svjesno unesenih podataka o kulturi, stavovima, preferencijama, interesima, političkoj orijentiranosti, omiljenim sadržajima i sl.

3.2 Trgovina podacima

Prikupljanje podataka o ponašanju korisnika na internetu, u cilju postizanja veće preciznosti u ciljanju internetskih oglasa, predstavlja uobičajenu praksu. Jedno od glavnih sredstava monetizacije, odnosno sredstava za postizanje profita putem internetskog oglašavanja, jest izgradnja što većeg broja profila korisnika s pripadajućim podacima kako bi se što preciznije moglo predvidjeti njihovo ponašanje kada su izloženi hiper-ciljanom oglašavanju. Tijek kojim informacije o internet korisnicima fluktuiraju je posebice zanimljiv s aspekta privatnosti iz razloga što se svi podaci koje korisnik svjesno i nesvjesno podijeli na intrenetu pa tako i na društvenim mrežama aktivno akumuliraju i evidentiraju. Ti podaci su interesantni tzv. „data brokerima“ koji ih prikupljaju, analiziraju i prodaju poslovnim subjektima u svrhu kvalitetnijeg oglašavanja i maksimalizacije profita ili drugim „data brokerima“.



Slika 3: Model upravljanja podacima

Izvor: Communications of the ACM (2015)

3.2.1 Trgovina podacima u političke svrhe

Narušavanje privatnosti podataka, identifikacija zlouporabe istih i druge vrste napada na zaštitu privatnosti na internetu postali su sveprisutni u digitalnoj globalnoj ekonomiji koja se temelji na podacima.

Prema Kozlowskoj (2018) profesor psihologije s Cambridge sveučilišta dr. Aleksander Kogan 2013. godine stvorio je aplikaciju pod nazivom „*this is your digital life*“. Ova aplikacija je plasirana putem društvene mreže Facebook te je korisnicima omogućila pristupanje testu osobnosti. Aplikacija bi netom nakon preuzimanja započela prikupljanje osobnih podataka korisnika kao što su podaci o profilu i Facebook aktivnosti (npr. koju vrstu sadržaja je označio sa "sviđa mi se"). Aplikaciju je preuzelo oko 300 000 ljudi, no to nije bio kraj prikupljanju podataka. Budući da je aplikacija također prikupljala podatke o prijateljima tih korisnika, kojima su postavke privatnosti profila to dopuštale, aplikacija je prikupljala podatke od oko

87 milijuna ljudi. Dr. Kogan je prikupljene podatke putem aplikacije proslijedio Strateškim komunikacijskim laboratorijima (SCL) čiji je vlasnik Cambridge Analytica (CA) politička konzultantska tvrtka koja koristi podatke za određivanje osobina i ponašanja birača na izborima. Podaci su se koristili pri kreiranju kampanja u svrhu što preciznijeg ciljanja mrežnih oglasa i poruka prema određenom segmentu birača. Prijenosom podataka s dr. Kogana na treće strane poput CA-a dr. Kogan je prekršio Facebook-ove uvjete pružanja usluge, koji zabranjuju prijenos ili prodaju podataka bilo kojoj oglasnoj mreži, posredniku podataka ili drugom oglašavanju ili unovčavanju usluga. Psihometrija je samo jedna metoda hiper-ciljanja koja je iz komercijalne sfere svojim djelovanjem prešla u sferu javnih i demokratskih procesa, korištena je kao analitički model u naporima za prikupljanje i obradu podataka tvrtke Cambridge Analytica. Kampanje Teda Cruza i Donalda Trumpa iz 2016. godine također su zapošljavale CA koja je ujedno bila povezana i s „Leave“ kampanjom koja se odnosila na referendum o Brexitu u Velikoj Britaniji.

Psihometrijsko mjerenje odnosno testiranje osobnosti u svrhe oglašavanja i uvjeravanja javnosti može otkriti nešto o korisniku što mu ni samom do tada nije bilo poznato. Također ono može otkriti i osjetljive podatke koje korisnik vjerojatno ne bih izravno podijelio s drugima. Ova tematika će biti sve aktualnija u budućnosti s obzirom da smo sredstvima hiper-ciljanja sve više izloženi u svakodnevnom životu.

3.2.2 Facebook Lookalike audiencies

Broj oglašivača koji koriste Facebook kao platformu za oglašavanje svojih proizvoda i usluga kontinuirano raste, prema Semeradovoj i Weinlichu (2019) u prvom tromjesečju 2019. godine zabilježeno je u prosjeku 7 miliona mjesečno aktivnih oglašivača. U današnje vrijeme kada je konkurencija sve jača tvrtke ulažu sve veći trud u što kreativniji i inovativniji pristup kod sastavljanja oglasa kako bi ostvarile optimizaciju oglasa, a ujedno i minimalizaciju troškova. 2015. godine Facebook je predstavio koncept tzv. prilagođene publike (custom audiences CA), omogućavajući oglašivačima da stvore segmente vlastitog specifičnog kupca izravno u njihovom Facebook Ads Manageru bez potrebe za izdvajanjem podataka i njihovom dodatnom analizom. 2016. godine CA koncept je nadograđen poboljšanim algoritmima podudaranja i oglašivačima je isporučena prva verzija nazvana Lookalike Audiences (LA).

CA i LA rade na principu konstantne procjene sličnosti kupaca izračunate pomoću algoritma za podudaranje. Lookalike Audiencies pomaže tvrtkama da pronađu što veći broj potencijalnih kupaca koji imaju slične karakteristike već postojećih kupaca, posjetitelja

njihove web stranice ili postojećih Facebooka i Instagram pratitelja. Facebook posjeduje tzv. kod za praćenje, nazvan Facebook pixel, koji se može generirati izravno s računa tvrtke koja oglašava. Facebook pomoću tog koda uvozi cjelokupni popis e-mail adresa trenutnih kupaca tvrtke i na temelju njihovih karakteristike izvodi LA. Također Semeradova i Weinlich (2019) navode kako se predviđanje publike na temelju sličnosti izračunava pomoću tajnog Facebook algoritma koji neprestano uspoređuje do 9 milijuna kriterija. Algoritam je dizajniran da potencijalnim kupcima pruži personalizirano iskustvo i sadržaj koji preferiraju. Facebook evidentira sve aktivnosti svojih korisnika odnosno prikuplja i klasificira sve dostupne podatke. Na primjer, algoritam može otkriti s koje vrsta uređaja se korisnik povezuje na društvenu mrežu te dodatne informacije kao što su one o obrazovanju, zanimanju, mjestu gdje korisnik ili potencijalni kupac provodi godišnji odmor itd.

3.3 Paradoks privatnosti

Napredak digitalne tehnologije je sasvim sigurno pokrenuo velik broj pitanja o privatnosti i sigurnosti na internetu. Nesklad između visoke zabrinutosti za privatnost na internetu i istovremenog kontradiktornog ponašanja kojim se iskazuje nebriga za privatnost prema Pavuni (2018) nazivamo **paradoks privatnosti**.

Iz definicije parodoksa privatnosti možemo zaključiti kako se radi o situaciji u kojoj korisnici tvrde da su vrlo zabrinuti o svojoj privatnosti, ali čine vrlo malo da zaštite svoje osobne podatke. Mnoga istraživanja pokazuju kako se korisnici na upite vezane o privatnosti na internetu deklariraju kao da su svjesni svih rizika, manipulacija i zlouporabe te istovremeno iskazuju nezadovoljstvo s obzirom na rizik kojem su izloženi. Bez obzira na njihovu očitu zabrinutost ne ponašaju se u skladu s istom što znači da i dalje bez dodatnih provjera ispunjavaju razne obrasce i privole s vlastitim privatnim i personaliziranim podacima, bez povećanog opreza objavljuju osobne informacije, stavove i preferencije putem društvenih mreža i sl. Riječ paradoks označava proturječnost koju jasno možemo uočiti u ranije navedenoj definiciji kao i u Sokratovom paradoksu: *„Znam da ništa ne znam“*. Bit paradoksa privatnosti je u tome da internet korisnici znaju za rizik i zabrinuti su, ali se ponašaju kao da ne znaju i kao da gotovo ne postoji.

Barth i Jong (2017) u svom radu navode 35 različitih teorija paradoksa privatnosti koje dijele na dvije glavne kategorije, prva kategorija je ona u kojoj se odluke donose na temelju *izračuna rizika i koristi* koje korisnici dobivaju svjesnim izlaganjem svojih podataka dok druga kategorija predstavlja donošenje odluke na temelju *prevladavajućih koristi s niskom ili nikakvom procjenom rizika*. Ljudsko racionalno razmišljanje opravdava ovakvo paradoksalno

ponašanje, budući da se odluke pažljivo razmatraju svjesno-analitičkim izračunima gubitka i dobiti. Korisnici na taj način svjesno zanemaruju nedostatke koji potencijalno mogu ugroziti privatnost u odnosu na uočene koristi koje dobivaju zauzvrat. Donošenje takve odluke može se ilustrirati primjerom kada korisnik odluči instalirati određenu aplikaciju na svom mobilnom uređaju, u trenutku preuzimanja korisnik je istovremeno suočen s koristi koju dobiva i rizikom potencijalne upotrebe podataka od strane trećih strana. Nakon preuzimanja aplikacije kod korisnika se javlja zadovoljenje potrebe i , kako je Barth i Jong (2017) nazivaju, optimistična pristranost odnosno stanje u kojem korisnici biraju pogodnosti i ignoriraju rizike misleći da se posljedice rizika neće manifestirati na njima. Isto se događa i kada web mjesto koje pruža korisne podatke može zahtijevati od korisnika da se registrira kako bi pristupio informacijama.

Rizik možemo definirati kao nesigurnost koja proizlazi iz mogućnosti negativnog ishoda, a na procjenu rizika utječe vjerojatnost nastanka negativnog događaja kao i percipirana važnost istog. Zabrinutost potrošača zasigurno je uzrokovana percepcijom rizika koju bi organizacije mogle znatno umanjiti uspostavljanjem povjerljivog i etičnog odnosa. Uspostavljanjem međusobnog povjerenja mogao bi se značajno skratiti postupak donošenja odluka o otkrivanju podataka. S obzirom na navedeno možemo zaključiti kako i percepcija povjerenja utječe na korisnikovu sliku o privatnosti u kojoj više povjerenja dovodi do manje brige za privatnost. Prema Barth i Jongu (2017) pojedinci imaju tendenciju podcjenjivati vlastiti rizik od narušavanja privatnosti, istovremeno precjenjujući vjerojatnost da će i drugi doživjeti štetne posljedice. Zaključno takvo razmišljanje dovodi do uvjerenja da njihova privatnost nije ugrožena, što može zauzvrat na kraju rezultirati povećanom izloženošću riziku.

U prvoj kategoriji, u kojoj se odluke donose s obzirom na izračun rizika i koristi, pojedinci nastoje maksimizirati korisnost i minimizirati rizik racionalnom računicom kao odgovor na unutarnja i vanjska ograničenja. Barth i Jong (2017) kako je navedeno u radu Culnana i Armstronga (1999) objašnjavaju kako danas u svijetu opažene koristi često premašuju opažene rizike, što dovodi do zanemarivanja zabrinutosti za privatnost što rezultira davanjem podataka u zamjenu za društvenu ili ekonomsku korist. Unutar ovog izračuna, ekonomske i društvene koristi te koristi iz personalizacije imaju tendenciju negirati negativnu stranu uočenih rizika (Barth i Jong, 2017 navedeno u radu Wilson i Valacich, 2012). U većini ljudske populacije, a pogotovo mlađem dijelu iste prisutna je upotreba društvenih mreža na svakodnevnoj razini. S obzirom na učestalost uporabe možemo je nazvati ritualnom praksom koja nam osigurava povezanost s cijelom mrežom drugih korisnika, također mnogima osigurava i izvor prihoda (influenceri). Ritual odnosno navika, s obzirom na koristi koje npr. u

ovom slučaju aktivno korištenje društvenih mreža nudi, dovodi do prekida veze između brige o privatnosti i krajnjeg ponašanja.

Drugu kategoriju predstavlja donošenje odluke u kojima pojedinci poznaju malo ili nimalo čimbenika koji mogu ugroziti njihovu privatnost, poput one kod kojih postizanje cilja poništava sva druga razmatranja. Prema Bartu i Jongu (2017) takve situacije rezultiraju značajno opaženim koristima popraćenim zanemarivim ili nikakvim rizikom. Primjer za takvu situaciju može biti trenutak kada pri i preuzimanju mobilne aplikacije prihvaćamo sva pravila o privatnosti koja je aplikacija postavila unatoč zabrinutosti zbog izloženosti naših podataka trećim stranama. Takvo ponašanje dovodi do zaključka kako je pojedinac u stanju prihvatiti apsolutno sve uvjete privatnosti (koji su često oskudno napisani) samo da može koristiti aplikaciju zauzvrat. Ljudi su često svjesni kako se unatoč određenoj politici privatnosti neke tvrtke njihova privatnost ugrožava, no ta svijest ne proizvodi stvaran osjećaj straha jer posjedovanje određene mobilne aplikacije ili mogućnost pristupanja određenim web sadržajima nadilazi sve moguće posljedice koje bi zloupotreba podataka mogla uzrokovati. Korisnici možda nisu svjesni osjetljivosti podataka koje otkrivaju i kakve su posljedice otkrivanja osobnih podataka te upravo zbog toga potencijalni rizici ne mogu biti pravilno procijenjeni.

Na kraju postavlja se pitanje postoji li način kojim problem paradoksalnog ponašanja postaje rješiv? Zapravo kao djelomično rješenje, bar što se tiče preuzimanja aplikacija na mobilne uređaje, možemo navesti pojednostavljenje mogućnosti ograničavanja dozvola za pristup podacima tijekom instalacije. Napredak u ponašanju biti će vidljiv tek onda kada korisnici shvate da se radi o osjetljivim podacima koji su isključivo njihovo vlasništvo, tada će i razina percipiranog rizika porasti.

3.3.1 Podaci i personalizacija

Kako u teoriji tako i u praksi postoji jedan osnovni preduvjet koji mora biti ispunjen kako bi se proces personalizacije uopće započeo, a to je otkrivanje osobnih podataka. Taj preduvjet je sasvim logičan s obzirom da sustavi za personalizaciju funkcioniraju na način da prilagođavaju sadržaj oglasa pojedinačnim interesima. Zapravo radi se o kompletnom paketu prilagođenih karakteristika prema određenom segmentu potrošača koji su njegovi konačni korisnici.

Marketinškim i drugim stručnjacima ekonomskih znanosti, osobni podaci uglavnom predstavljaju *ekonomsku vrijednost* dok ta ista vrijednost za pojedinca predstavlja *privatnost*

te *intimu*. Svi podaci nisu jednako osjetljivi i ne predstavljaju jednaku važnost korisnicima. U konačnici, korisnici kada se nađu u situaciji da moraju odlučiti hoće li dati na korištenje svoje određene personalizirane podatke suočavaju se s nizom čimbenika prema kojima donose odluku. Sasvim je sigurno kako je jedan od tih čimbenika i osjetljivost podataka kao što to npr. mogu biti politički stavovi i preferencije, no među ostale bitne čimbenike također se ubrajaju i rizik te potencijalne koristi koje korisnik dobiva zauzvrat. Prema, Martin, Wadle i Ziegler (2019) kako je navedeno u radu Culnan i Armstrong (1999) namjera otkrivanja osobnih podataka proizlazi iz „*racionalnog vaganja*" međusobno potencijalnih rizika i koristi. S obzirom na veličinu potencijalnog rizika i veličinu koristi koju dobiva, korisnik donosi konačnu odluku. Fenomen paradoksa privatnosti i dalje otežava razumijevanje na koji način ljudi odlučuju hoće li otkriti svoje privatne podatke ili ne s obzirom da se njihove namjere razlikuju od stvarnog ponašanja.

Odluka o davanju osobnih podataka uglavnom se provodi procjenom potencijalnih rizika dok je stvarno ponašanje pod većim utjecajem ocjene povjerenja u organizaciju kojoj se podaci daju. U tom slučaju korisnik će radije ostaviti podatke na web stranici organizacije s kojom nije imao nikakva negativna korisnička iskustva i kojoj već duže vremena poklanja svoje povjerenje, bez obzira na činjenicu da rizik uvijek postoji. Prema Martin, Wadle i Ziegler (2019) ne otkrivanje podataka zbog nedostatka povjerenja može proizaći iz činjenice da su danas korisnici često suočeni s opcijom *sve* ili *ništa* u politikama privatnosti. Pozitivno korisničko iskustvo paralelno dovodi do povećanja namjere za otkrivanje osobnih podataka. Do takvog korisničkog iskustva dolazi se rješavanjem osnovnih potreba korisnika, kao što je npr. sustavno dizajniranje interaktivnih proizvoda ili usluga u kojim i sami korisnici na neki način sudjeluju te time dobivaju osjećaj pripadnosti.

Wadle, Martin i Ziegler (2019) u svojem radu *„The Trade-off between Data Disclosure and Personalization Benefit"* proveli su istraživanje kojim su htjeli dokazati kako odluka o davanju privatnih i personaliziranih podataka na uvid ovisi o koristi koja bi uslijedila nakon davanja podataka na raspolaganje za određenu svrhu. Dokazali su kako namjera otkrivanja osobnih podataka ovisi o *vrsti kategorije podataka* i *pogodnosti* ili koristi obećane personalizacijom. Prema autorima istraživanja sudionici procjenjuju postoji li razumna veza između kategorije podataka i koristi (npr. otkrivanje financijskih podataka je vjerojatnije kada je u pitanju korist financijske prirode). Rezultati njihovog istraživanja sugeriraju da se interakcija između vrste podataka i obećane koristi od personalizacije svakako mora uzeti u obzir pri dizajniranju procesa personalizacije.

4. EMPIRIJSKO ISTRAŽIVANJE O PRIVATNOSTI NA INTERNETU

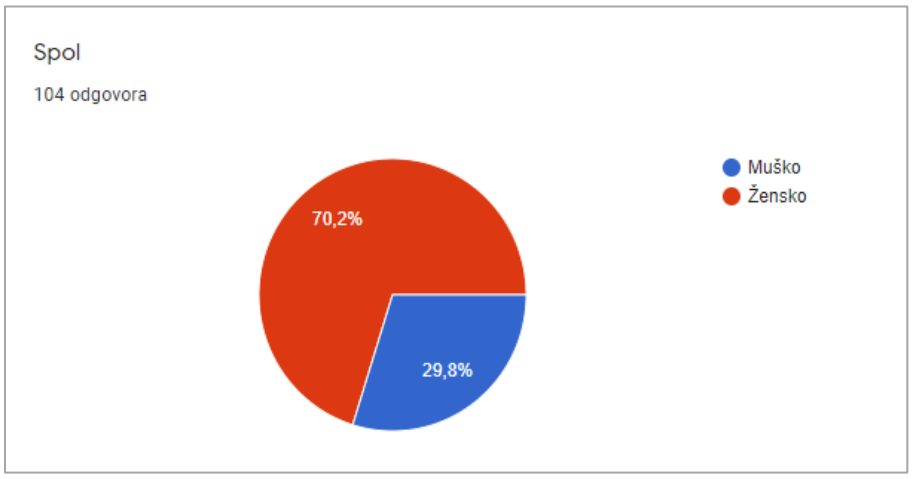
4.1 Uzorak i metoda istraživanja

Empirijski dio u ovom radu temelji se na proučavanju koliko zapravo ispitanici percipiraju rizik od narušavanja njihove privatnosti na internetu. Također cilj je istražiti koliko su ispitanici upoznati i koliko koriste dostupne alate za zaštitu privatnosti na internetu. Istraživanje je provedeno na prigodnom uzorku od 104 ispitanika putem online anketnog upitnika. Anketni upitnik se distribuirao putem *WhatsApp* aplikacije u razdoblju od 2 dana u rujnu 2020.godine, odnosno 11.9.2020.-12.9.2020. Anketni upitnik sastoji se od 16 pitanja pomoću kojih želimo ispitati slijedeće hipoteze:

H1: Ispitanici digitalne usluge doživljavaju kao izvor rizika od narušavanja privatnosti.

H2: Ispitanici su upoznati i koriste alate za zaštitu privatnost na internetu.

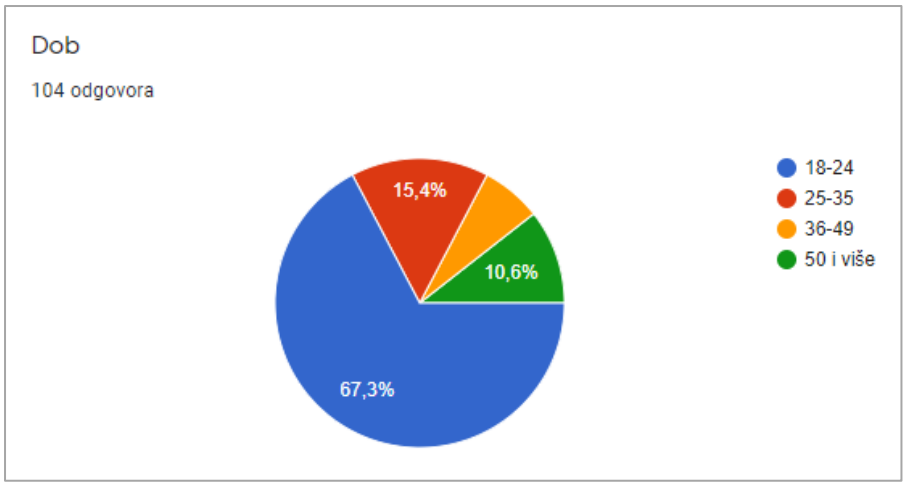
4.2 Rezultati istraživanja



Slika 4: Spol ispitanika

Izvor: Vlastita izrada autorice

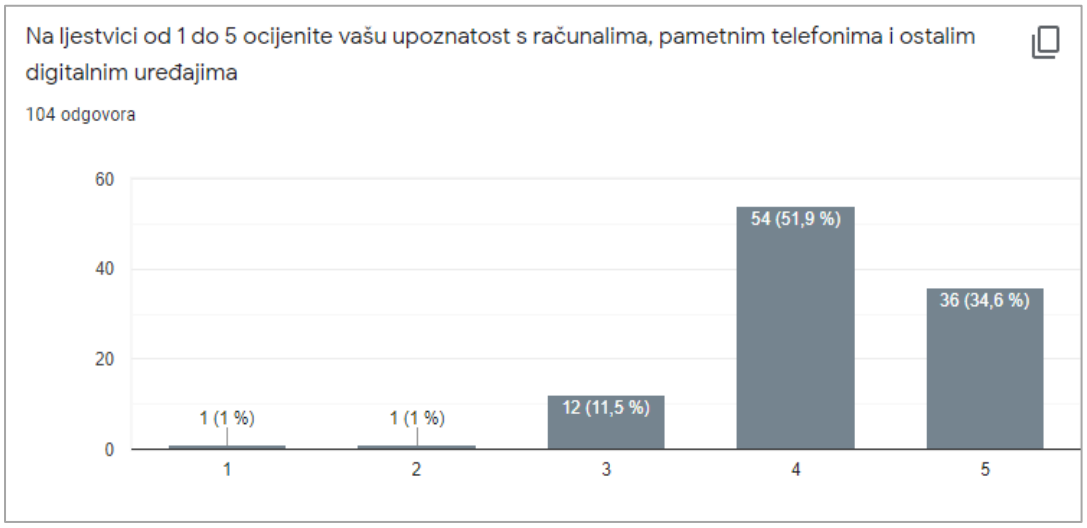
Slika 4 prikazuje kako na uzorku od 104 ispitanika prevladavaju osobe ženskog spola, u postotku žene obuhvaćaju 70,2% uzorka dok muškarci 29,8%.



Slika 5: Dob ispitanika

Izvor: Vlastita izrada autorice

Dob ispitanika podijeljena je na mlađu, srednju i stariju dob. U mlađu dob pripadaju ispitanici od 18 do 24 i od 25 do 35 godina starosti te zajedno obuhvaćaju 82,7% uzorka. Srednjoj dobi pripadaju ispitanici od 36 do 49 godina u postotku obuhvaćaju 6,7% uzorka, starijoj dobi pripadaju svi ispitanici koji imaju 50 i više godina i tako čine 10,6% ispitanika.

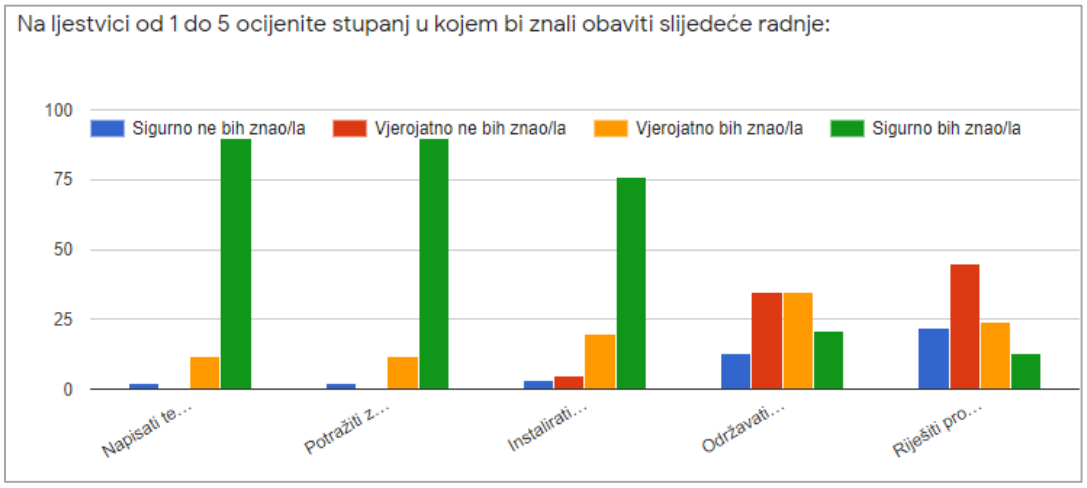


Slika 6: Upoznatost ispitanika s digitalnim uređajima

Izvor: Vlastita izrada autorice

Slika 6 prikazuje ljestvicu u kojoj ocjena 1 znači da ispitanici nisu upoznati i ne koriste digitalne uređaje dok ocjena 5 znači da su ispitanici izvrsno upoznati s digitalnim uređajima te su ujedno i napredni korisnici istih. Većina ispitanika odnosno 51,9% izjasnilo se kako su vrlo dobro upoznati s računalima, pametnim telefonima i ostalim digitalnim uređajima dok je

34,6% ispitanika svoju upoznatost ocijenilo s ocjenom 5. S obzirom na ovakve rezultate može se zaključiti kako je velika većina ispitanih osoba upoznata s digitalnim uređajima.



Slika 7: Stupanj znanja ispitanika za obavljanje radnji na digitalnim uređajima

Izvor: Vlastita izrada autorice

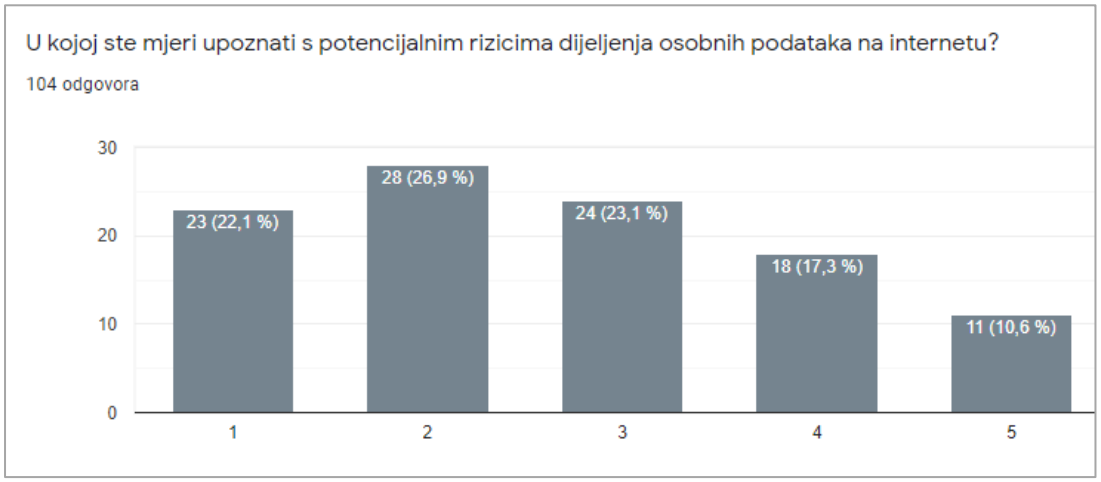
Na slici 7 dan je prikaz korisnikovih znanja u vezi upravljanja digitalnim uređajima. U anketnom upitniku ispitanici su trebali odrediti stupanj u kojem bi znali obaviti radnje od onih osnovnih pa sve do onih naprednijih. Osnovne radnje uključuju: znanje pisanja teksta na računalu, pametnom telefonu ili drugom digitalnom uređaju, pretragu značenja riječi ili neke druge potrebne informacije. Malo napredniju radnju predstavlja instalacija programa ili aplikacije na uređaj dok se pod iznimno napredne radnje smatraju: održavanje web stranice ili bloga i rješavanje kvara na uređaju. Analizom rezultata dolazimo do zaključka kako bih većina ispitanika (86,5%) sigurno znala obavljati osnovne radnje i malo napredniju kao što je instalacija programa ili aplikacije (73%). Ispitanici su naveli kako vjerojatno ne bih znali obaviti naprednije radnje na uređajima.

Tablica 1: Rješavanje problema/kvara na uređaju s obzirom na spol ispitanika

Spol	Riješiti problem/kvar na uređaju				Ukupno
	Sigurno ne bih znao/la	Vjerojatno ne bih znao/la	Vjerojatno bih znao/la	Sigurno bih znao/la	
Muško	4	10	8	9	31
Žensko	18	35	16	4	73
Ukupno	22	45	24	13	104

Izvor: Vlastita izrada autorice

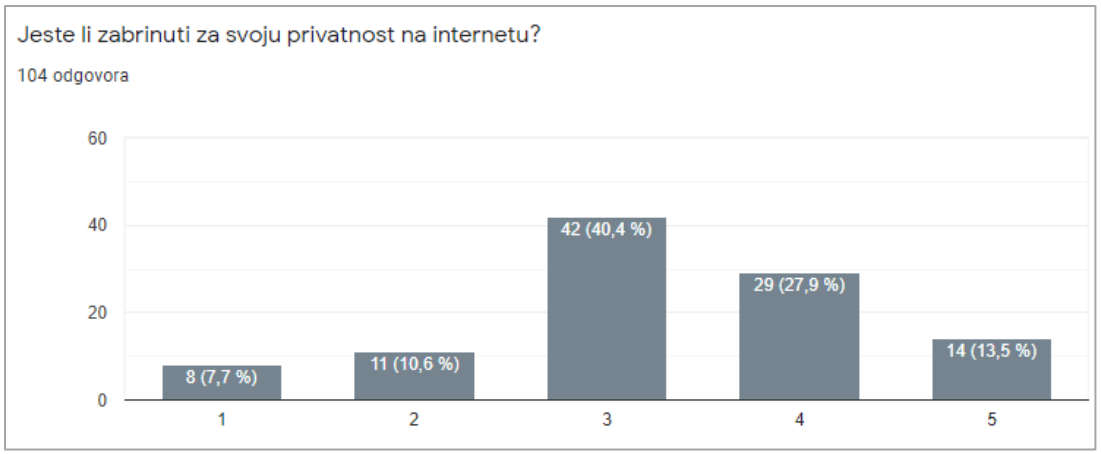
Tablica 1 prikazuje odnos stupnja u kojem su ispitanici spremni riješiti problem ili kvar na uređaju s obzirom na spol. Stavljanjem u odnos te dvije varijable došli smo do zaključka kako se čak 72,6% žena izjasnilo kako sigurno ili vjerojatno ne bih znale riješiti problem ili kvar na računalu dok se isto tako izjasnilo samo 45% ispitanika muškog spola. Rezultat dokazuje kako se muškarci češće izjašnjavaju kao spol koji zna riješiti određeni problem na uređajima.



Slika 8: Prikaz stupnja korisnikove upoznatosti s potencijalnim rizicima dijeljenja osobnih podataka na internetu

Izvor: Vlastita izrada autorice

Kako je vidljivo na slici 8 ispitanici su u anketnom upitniku trebali ocijeniti stupanj svoje upoznatosti s potencijalnim rizicima kojima se izlažu tijekom dijeljenja svojih osobnih podataka. Stupanj 1 označava jako dobro poznavanje rizika dok stupanj 5 označava nikakvo razumijevanje rizika. Tijekom analize rezultata korištena je statistička funkcija Mod koja označava najčešću vrijednost u nizu, odnosno u ovom slučaju najčešći odabrani stupanj upoznatosti. Vrijednost Moda iznosi 2 što znači da se većina ispitanika izjasnila da vrlo dobro poznaju rizike.



Slika 9: Stupanj zabrinutosti ispitanika za svoju privatnost na internetu

Izvor: Vlastita izrada autorice

Prilikom analize rezultata ovog pitanja također je korišten Mod kao najčešća vrijednost u nizu. Ispitanici su najčešće izabirali vrijednost 3 u nizu gdje 1 označava da nisu uopće zabrinuti dok 5 označava izrazitu zabrinutost za svoju privatnost na internetu. Čak 40,4% ispitanika je izabrala vrijednost 3 odnosno neutralnu poziciju u nizu koja nam govori kako ispitanici nisu niti zabrinuti niti ne zabrinuti. U usporedbi sa slikom 8 nailazimo na zanimljivost gdje je Mod vrijednost iznosila 2 dok na slici 9 iznosi 3 što navodi na zaključak kako su ispitanici u većini vrlo dobro upoznati s potencijalnim rizicima koji mogu narušiti njihovu privatnost na internetu, no i dalje se ne deklariraju kao zabrinuti.

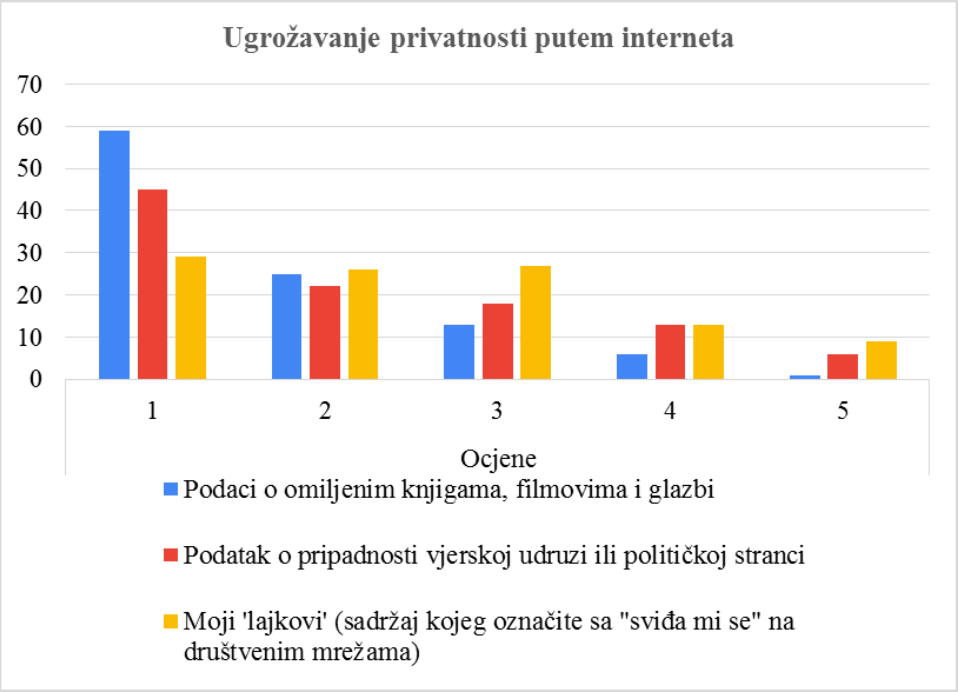
Tablica 2: Prikaz veze između stupnja upoznatosti s potencijalnim rizicima i čitanja uvjeta korištenja

Upoznatost s potencijalnim rizicima	**Čitanje uvjeta korištenja**		
	Da	Ne	Ukupno
1	6	17	23
2	4	24	28
3	5	19	24
4	6	12	18
5	6	5	11
Ukupno	27	77	104

Izvor: Vlastita izrada autorice

U Tablici 2 vidljiv je prikaz odnosa dvije varijable točnije; mjere upoznatosti s potencijalnim rizicima i čitanja uvjeta korištenja. S obzirom da mjera 1 označava dobro poznavanje potencijalnih rizika, a mjera 5 nikakvo poznavanje rizika, analizom rezultata može se zaključiti kako oni koji su označili svoju upoznatost s rizicima s mjerom 1 i 2 u velikoj većini

tj. njih 80,3% ne čita uvjete korištenja pri kreiranju računa na različitim stranicama (društvene mreže, forumi, trgovine i sl.). Takav rezultat možemo interpretirati kroz visoki stupanj neopreznosti koji se javlja u ponašanju ispitanika premda dobro poznaju rizike.

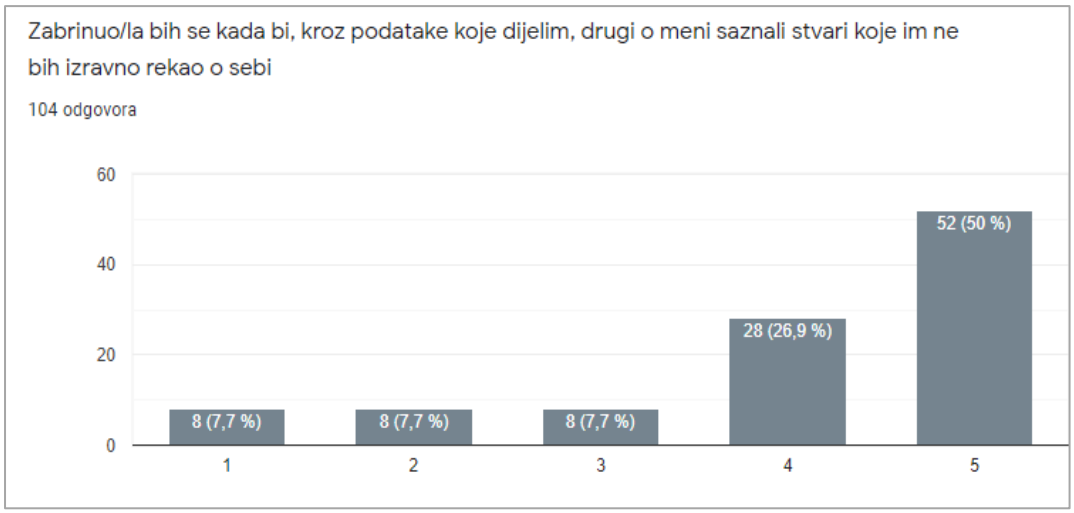


Slika 10: Stupanj potencijalnog narušavanja privatnosti na internetu s obzirom na vrstu podataka

Izvor: Vlastita izrada autorice

U anketnom upitniku također se nalazi pitanje prilikom kojeg su ispitanici trebali ocijeniti stupanj potencijalnog narušavanja privatnosti na internetu s obzirom na vrstu podataka koje izlažu. Vrstu podataka podijelili smo na podatke o: imenu, prezimenu i adresi stanovanja, e-mail adresi, broju telefona ili mobitela, omiljenim knjigama, filmovima i glazbi, pripadnosti vjerskoj udruzi ili političkoj stranci, sadržaju koji je označen sa „sviđa mi se“, povijesti pretraživanja i na podatke o web kolačićima. Ocjena 1 označava da određena vrsta podatka uopće ne ugrožava dok ocjena 5 označava da jako ugrožava korisnikovu privatnost na internetu. Na grafikonu na slici 10 posebno su analizirani podaci kod kojih su se ispitanici u velikoj većini izjasnili da uopće ne ugrožavaju njihovu e-privatnost. Zanimljivo je kako se čak 55,7% ispitanika izjasnilo kako podaci o omiljenim knjigama, filmovima i glazbi uopće ne ugrožavaju njihovu privatnost, također 43,3% ispitanika podacima o pripadnosti vjerskoj udruzi ili političkoj stranci daje ocjenu 1. Za sadržaj koji korisnici označavaju sa „sviđa mi se“ 28% ispitanika smatra kako uopće ne ugrožava njihovi privatnost na internetu i

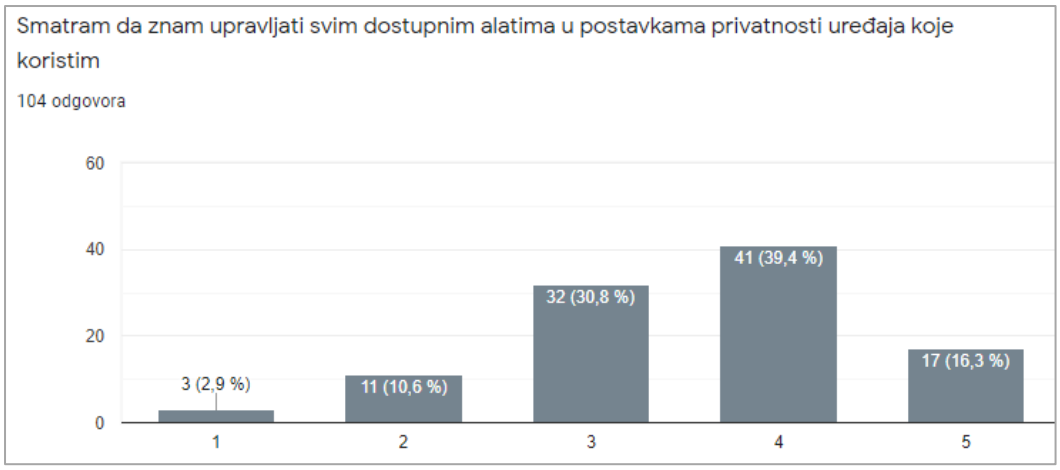
označavaju ga ocjenom 1. S obzirom na temu rada, u kojem se proteže definicija personalizacije korisnika na internetu, vrlo je zanimljiva činjenica da ispitanici ne obraćaju pažnju koliko zapravo ranije navedeni podaci mogu otkriti o njima, a da nisu ni svjesni te da se isti mogu upotrijebiti u treće svrhe odnosno svrhe kreiranja personaliziranog profila korisnika.



Slika 11: Stupanj zabrinutosti ispitanika s obzirom na podatke koje dijele i okolinu

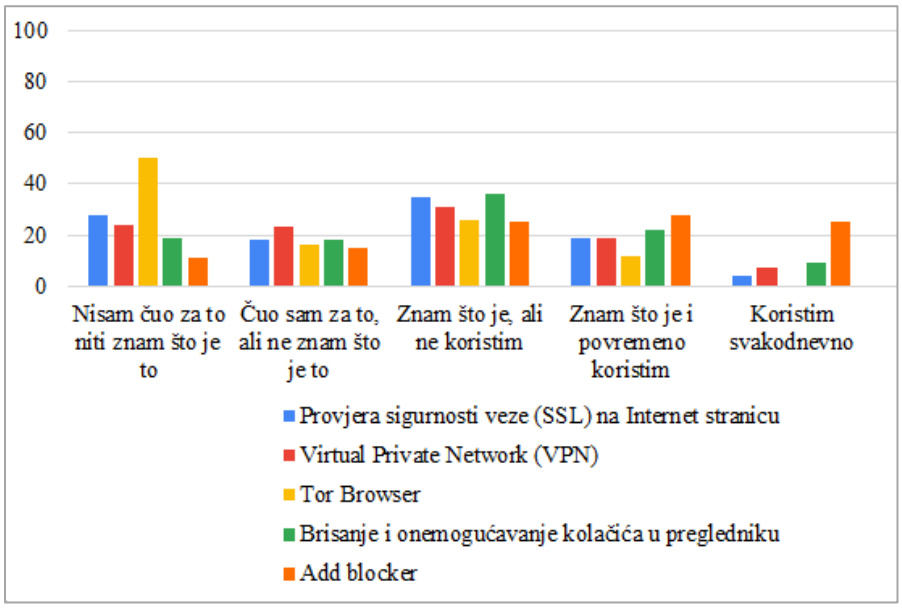
Izvor: Vlastita izrada autorice

Na slici 11 jasno se može iščitati kako je ukupno 76,9% ispitanika dalo ocjenu 4 i 5, u nizu u kojem ocjena 1 označava potpuno neslaganje dok ocjena 5 označava potpuno slaganje s tvrdnjom. Prethodni grafikon na slici 10 pokazao je kako korisnici u većini smatraju da tzv. banalni podaci (o omiljenim knjigama, omiljenom sadržaju i pripadnosti vjerskoj udruzi ili političkoj stranci) uopće ne predstavljaju ugrozu njihovoj privatnosti na internetu. Unatoč tom podatku zanimljivo je kako se ispitanici i dalje izjašnjavaju kao zabrinuti u slučaju kada bi ti podaci otkrili nešto o njima što inče ne bih izravno podijelili s okolinom.



Slika 12: Znanje ispitanika o upravljanju alatima za zaštitu privatnosti

Izvor: Vlastita izrada autorice

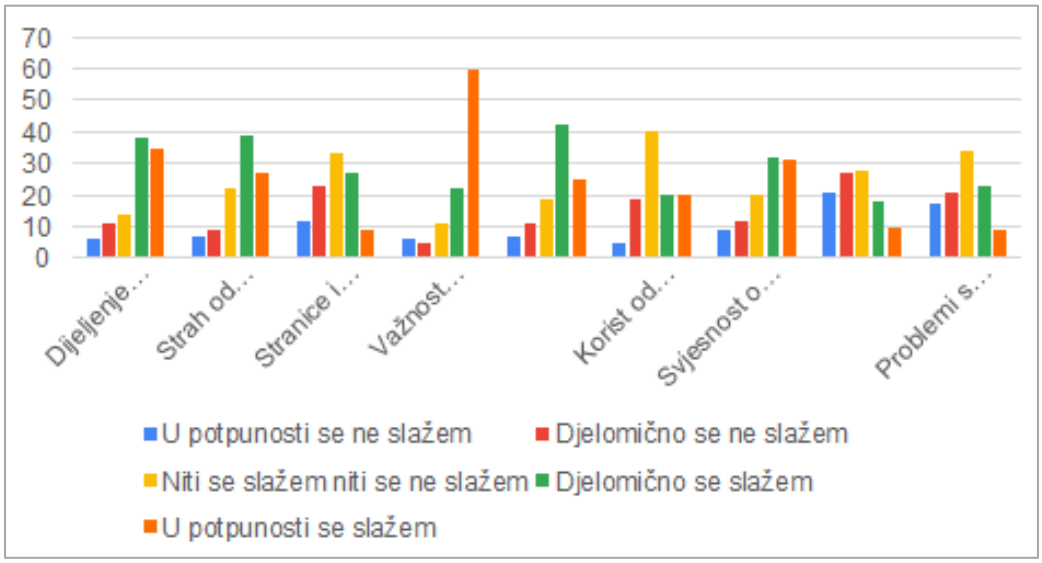


Slika 13: Poznavanje i redovno korištenje alata za zaštitu privatnosti na internetu kod ispitanika

Izvor: Vlastita izrada autorice

Najčešće izabrana ocjena na slici 12 jest 4 u nizu u kojem ocjena 1 označava uopće ne slaganje dok ocjena 5 označava potpuno slaganje s navedenom tvrdnjom. Zaključno, većina ispitanika odnosno njih 55,7% se djelomično i u potpunosti slaže s tvrdnjom da znaju upravljati svim dostupnim alatima u postavkama privatnosti na svojim uređajima. Pomoću pitanja na slici 13 cilj je bio saznati koje alate ispitanici poznaju i redovno koriste. Kod analize odgovora posebno su se promatrali alati koji su se pokazali manje poznatim ispitanicima (SSL, VPN, Tor Browser, brisanje, onemogućavanje kolačića u pregledniku i Ad blocker). Zapravo riječ je o naprednijim alatima za zaštitu privatnosti na internetu, čak 48%

ispitanika nikada nije čulo niti zna što je Tor Browser. U kategoriji „znam što je i povremeno koristim“ sa 26,9% dominira alat Ad blocker te sa 21,1% alat brisanja i onemogućavanja kolačića u pregledniku.



Slika 14: Čimbenici koji utječu na percepciju rizika

Izvor: Vlastita izrada autorice

U anketnom upitniku ispitanici su navedenim tvrdnjama trebali dodijeliti stupanj osobnog slaganja s istima. Redom, kako je grafički prikazano na slici 14 tvrdnje su glasile:

1) Dijeljenje osobnih podataka putem različitih privola i obrazaca na internetu predstavlja rizik za moju privatnost
2) Bojim se da bi moji osobni podaci mogli biti zloupotrijebljeni
3) Stranice i aplikacije koje traže moje podatke zauzvrat nude dobre usluge
4) Važno mi je imati povjerenja u organizaciju kojoj dajem svoje osobne podatke na internetu
5) Smatram da svoju privatnost na internetu uspješno držim pod kontrolom
6) Korist od besplatnih usluga kojima pristupam putem interneta su veće od rizika dijeljenja osobnih podataka koje im dajem
7) Potpuno sam svjestan/na koje podatke dijelim putem interneta
8) Radije ću ustupiti neke svoje podatke nego platiti korištenje usluge na internetu
9) Problemi s privatnošću na internetu uglavnom pogađaju druge ljude

Pomoću navedenih tvrdnji cilj je bio dokazati kako postoje čimbenici koji utječu na percepciju rizika ispitanika o zaštiti privatnosti na internetu. Prilikom obrade rezultata, kako bi što jednostavnije i preciznije mogli utvrditi postojanost čimbenika, zbrojeni su odgovori

ispitanika koji su se izjasnili da se u potpunosti i djelomično slažu s tvrdnjama. Tvrdnje 1) i 7) označavaju *svjesnost*, kada uzmemo rezultate obje tvrdnje u obzir u prosjeku se čak 65% ispitanika složilo s tvrdnjama da dijeljenje njihovih podataka predstavlja potencijalnu ugrozu i da su svjesni koje podatke dijele. Tvrdnja 2) označava *strah,* 63,5% ispitanika izjasnilo se kako se boje zloupotrebe svojih privatnih podataka. Posebice je zanimljiva činjenica da su se ispitanici prilikom ocjenjivanja tvrdnji 3) i 6) većinom opredijelili za neutralno stajalište kada je u pitanju *korist* koja bi trebala proizaći nakon dijeljenja podataka. No ipak kada uzmemo u obzir sve kategorije odgovora nakon dominante neutralne većine slijede ispitanici koji se slažu s tvrdnjama. Tvrdnja 4) označava *povjerenje*, čak 78,8% ispitanika se složilo kako je izuzetno bitno imati povjerenje u organizaciju kojoj daju svoje podatke. Tvrdnja 5) označava *kontrolu,* te je 64,3% ispitanika izjavilo kako smatraju da svoju privatnost na internetu uspješno drže pod kontrolom. Tvrdnja 8) nema posebno obilježje, no zanimljivo je kako se većina niti ne slaže niti slaže kako bi radije svoje podatke dali na upotrebu prije nego bi platili određenu uslugu na internetu. Također ovu neutralnu većinu slijede oni ispitanici koji se ne slažu s tvrdnjom stoga rezultati ukazuju na optimizam.

4.3 Rasprava o rezultatima

Ispitanici su putem anketnog upitnika trebali odabrati koje od uređaja, društvenih mreža i internet usluga redovito koriste i u koje svrhe. Pomoću ovakvog tipa pitanja cilj je bio definirati prosječan profil ispitanika. Prosječni ispitanik od digitalnih uređaja redovno koristi android „pametni“ telefon i laptop putem kojih najčešće koristi usluge Google tražilice i Gmail-a. Također putem istih uređaja u najvećoj mjeri koristi Facebook i Instagram, što potvrđuje podatak da se internet koristi najčešće u svrhu zabave i razonode (81,7%).

H1: Ispitanici digitalne usluge doživljavaju kao izvor rizika od narušavanja privatnosti.

Analizom rezultata dolazimo do zaključka kako ispitanici percipiraju rizik od narušavanja njihove privatnosti na internetu. Dokaz tome je činjenica da se najveći broj ispitanika (26,9%) izjasnio kako vrlo dobro poznaju rizike kojima se izlažu dijeljenjem privatnih podataka. Također stupanj slaganja s tvrdnjama 1) i 7) na slici 14 dokazuje kako ispitanici u većini smatraju da su svjesni potencijalnih rizika i opasnosti po svoju e-privatnost. Ispitanici su naveli kako je dijeljenje podataka poput IP adrese (32,7%), imena, prezimena i adrese stanovanja (28,8%) u najvećoj mjeri ugroženo. Zaključno, ispitanici doživljavaju izvor rizika od narušavanja privatnosti na internetu te ovu hipotezu možemo potvrditi.

S obzirom da je u H1 naglasak na riziku potrebno je definirati čimbenike koji utječu na percepciju rizika kod ispitanika. Pomoću ocjenjivanja stupnja ispitanikovih slaganja s tvrdnjama (slika 14) čimbenici koji utječu na percepciju rizika od narušavanja privatnosti putem dijeljenja podataka su:

- Svjesnost
- Strah
- Korist
- Povjerenje i
- Kontrola

H2: Ispitanici su upoznati i koriste alate za zaštitu privatnosti na internetu

55,7% ispitanika se izjasnilo kako vrlo dobro ili odlično upravljaju sa svim dostupnim alatima u postavkama privatnosti uređaja koje koriste. Potvrdnost ove hipoteze također dokazuje i podatak da je 66,3% ispitanika upoznato s postojanjem Agencije za zaštitu podataka. Zaključak je kako ispitanici povremeno ili svakodnevno najčešće koriste alate kao što su brisanje povijesti pretraživanja, pregledavanje sadržaja u anonimnom načinu i blokiranje reklama u pregledniku. Ispitanici su većinom upoznati sa svim ponuđenim alatima, osim s Tor Browser-om koji pripada skupini naprednijih alata.

5. ZAKLJUČAK

Činjenica je kako je u današnjem svijetu, u kojem je virtualna sfera života zauzela dobar dio one stvarne, postalo iznimno teško sačuvati vlastitu privatnost unutar razumnih granica intime. S obzirom da se sva ljudska bića razlikuju i da su svojevrstan unikat tako postoji bezbroj različitih stavova i razmišljanja oko različitih tematika. Svaki pojedinac na drukčiji način mjeri npr. potencijalni rizik ili opasnost i korist ili zabrinutost. Tako je i kada govorimo o odnosu privatnosti i personalizacije na internetu koji projicira određene marketinške implikacije. Ubrzani tempo života koji svakodnevno postavlja nove zahtjeve i prepreke nas tjera na prilagodbu i suživot s tehnologijom. Taj suživot je prepun potencijalnih rizika po našu privatnost na internetu, no ipak ga odabiremo jer nam s druge strane nudi bezbroj koristi. Svjesnost, informiranost i budnost pojedinca predstavlja određenu garanciju za zaštitu privatnosti. Cilj ovog rada bio je progovoriti o ugroženosti privatnosti na internetu i načinu implementacije personalizacije kroz procese hipertargetiranja i trgovine podacima. Svi korisnici različitih internetskih usluga trebaju znati kome i u koju svrhu daju svoje podatke, također moraju biti svjesni da se oni mogu iskoristiti u treće njima često nepoznate svrhe. Podaci koje dijelimo o sebi na direktan ili indirektan način određenim tvrtkama ili organizacijama mogu osigurati olakšani proces kreiranja profila korisnika pomoću kojeg prilagođavaju svoje poslovanje. Dijeljenje osobnih podataka posljedično može dobiti marketinški okvir kroz personalizirane kampanje i ponude. U ovom radu provedeno je istraživanje pomoću anketnog upitnika koji se sastojao od pitanja povezanih s privatnosti na internetu. Obradom rezultata došli smo do zaključka kako ljudi percipiraju važnost osobne privatnosti na internetu, također ispitanici doživljavaju i poznaju potencijalne izvore rizika te redovno koriste neke od alata za zaštitu svoje online privatnosti. Provedeno istraživanje ima i svoja određena ograničenja. Najveća ograničenja predstavljaju kanal distribuiranja anketnog upitnika i mali uzorak ispitanika u kojem je većina njih pripada mlađoj populaciji. U ovom istraživanju odabrani kanal distribucije bila je WhatsApp aplikacija što znači da potencijalni ispitanici koji je ne posjeduju nisu bili u mogućnosti ispuniti anketni upitnik. Kada je riječ o ovoj istraživačkoj temi preporuka budućim istraživanjima svakako je ispitivanje većeg uzorka populacije s ravnomjernim udjelom svih dobnih skupina kako bi se dobili puno precizniji i relavantniji rezultati. Svakako bi bilo zanimljivo dodatno istražiti koji sve čimbenici utječu na odluku o dijeljenju osobnih podataka i korisnikovu percepciju o upotrebi njihovih podataka u treće svrhe.

LITERATURA

All about cookies.org. 2020. *What Is A Cookie? - All About Cookies*. [Internet] Raspoloživo na: <https://www.allaboutcookies.org/cookies/> [pristup 5.8.2020].

Babić, M., 2014. [Internet] Sors.ba. Raspoloživo na: <http://sors.ba/UserFiles/file/SorS/SORS%202014/Zbornik%20PDF-ovi/03%20Babic.pdf> [pristup 7.8.2020].

Barth, S. and de Jong, M., 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), str.1038-1058. [Internet] Raspoloživo na: <https://doi.org/10.1016/j.tele.2017.04.013> [pristup 27.8.2020].

Boban, M., 2012. Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu: *Zbornik radova Pravnog fakulteta u Splitu*, str. 575.- 598., [Internet] Raspoloživo na: <https://hrcak.srce.hr/file/129212> [pristup 4.8.2020].

Brajković, T., 2016. *Uloga poslovne etike u marketingu.* Završni rad. Sveučilište u Splitu, Ekonomski fakultet, Split

CERT.hr. 2017. Osnove privatnosti na Internetu. [Internet] Raspoloživo na: <https://www.cert.hr/wpcontent/uploads/2017/12/osnove_privatnosti_na_Internetu_0.pdf> [pristup 4.8.2020].

CIS.hr. 2012. Otisak web preglednika. : <https://www.cis.hr/dokumenti/5568-otisak-web-preglednika.html> [Internet] Raspoloživo na: [pristup 12.8.2020].

Ercegovac, I., Jovanović, D. 2013. *Hipertargetiranje i personalizacija mas medija* Međunarodni skup „Moć komunikacije 2013“, Apeiron, Beograd, str. 124.-138.

Eurlex.europa.eu., 2016. EUR-Lex 2016/679 od 27. travnja 2016. *Službeni list Europske unije, L 119*, [Internet] Raspoloživo na: https://eurlex.europa.eu/eli/reg/2016/679/oj [pristup: 5.8.2020].

Ghosh, D. 2018. How GDPR Will Transform Digital Marketing. [Internet] Raspoloživo na: <https://scholar.harvard.edu/files/dipayan/files/how_gdpr_will_transform_digital_marketing.pdf> [pristup 5.8.2020].

Karpati, T., 2001. *Etika u gospodarstvu*. Osijek: Ekonomski fakultet u Osijeku, Grafika, str. 5-6

Kozlowska, I., 2018. The Henry M. Jackson School of International Studies University of Washington: Facebook and Data Privacy in the Age of Cambridge Analytica, [Internet] Raspoloživo na: <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/ > [pristup: 25.8.2020].

Marker.hr., 2017. Kolačići. [Internet] Raspoloživo na: <https://marker.hr/blog/kolacici-cookies-sto-su-kako-obavijestiti-posjetitelje-473/> [pristup: 6.8.2020].

Martin, N., Wadle, L., Ziegler, D., 2019. Privacy and Personalization: The Trade-off between Dana Disclosure and Personalization Benefit, UMAP, [Internet] Raspoloživo na: <https://doi.org/10.1145/3314183.3323672> [pristup: 9.9.2020].

Montgomery, A., Smith, M., 2009. Prospects for Personalization on the Internet. *Journal of Interactive Marketing br.23*, str. 130–137, [Internet] Raspoloživo na: <https://doi.org/10.1016/j.intmar.2009.02.001> [pristup 6.8.2020].

Pavuna, A., 2018. Paradoks privatnosti: empirijska provjera fenomena. *Politička misao: Časopis za politologiju Vol.56 No.1 2019* str. 132-162, [Internet] Raspoloživo na: <https://doi.org/10.20901/pm.56.1.05> [pristup 25.8.2020].

Semerádová, T., Weinlich, P., 2019. Computer Estimation of Customer Similarity with Facebook Lookalikes: Advantages and Disadvantages of Hyper-targeting, [Internet] Raspoloživo na: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8877755> [pristup: 9.8.2020].

PRILOZI

Slike:

Tablice:

SAŽETAK

Obzirom da je tehnološki napredak iz dana u dan sve veći, mi korisnici internet usluga postali smo sve više izloženi riziku od narušavanja privatnosti na internetu. Svaka naša online aktivnost izložena je svojevrsnoj ugrozi, a posebice dijeljenje osobnih podataka. U ovom radu promatrali su se aspekti odnosa privatnosti i personalizacije na internetu te njihove marketinške implikacije. Rad sadrži i empirijski dio, čiji rezultati navode na činjenicu da ispitanici percipiraju izvor rizika od narušavanja privatnosti te da poznaju i redovno koriste pojedine alate za zaštitu iste. Posljednji dio rada posvećen je zaključnim razmatranjima i preporukama.

Ključne riječi: privatnost, personalizacija, internet

SUMMARY

As technological advances increase day by day, we, Internet service users have become increasingly at risk of violating online privacy. Each of our online activities is exposed to a kind of threat, especially the sharing of personal data. In this paper, aspects of the relationship between privacy and personalization on the Internet and their marketing implications were observed. The paper also contains an empirical part, the results of which lead to the fact that respondents perceive the source of the risk of privacy violations and that they know and regularly use certain tools to protect it. The last part of the paper is devoted to concluding remarks and recommendations.

Keywords: privacy, personalization, Internet