UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VLOGA ZASEBNOSTI V ODNOSU UPORABNIKOV DO SPLETNE PERSONALIZACIJE

Ljubljana, september 2023 TJAŠA KOKALJ

IZJAVA O AVTORSTVU

Podpisana Tjaša Kokalj, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom »Vloga zasebnosti v odnosu uporabnikov do spletne personalizacije«, pripravljenega v sodelovanju s svetovalko izr. prof. dr. Matejo Kos Koklič

I Z J A V L J A M

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

11. da sem preverila verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 21.9.2023 Podpis študentke: _____

KAZALO

1 UVOD 1

2 SPLETNA PERSONALIZACIJA 3

2.1 Opredelitev spletne personalizacije 3

2.2 Oblike spletne personalizacije 5

2.3 Izvedba spletne personalizacije 7

2.4 Prednosti in slabosti spletne personalizacije za podjetja in uporabnike 8

3 ZBIRANJE IN OBDELAVA PODATKOV O UPORABNIKIH 10

3.1 Vrste podatkov o uporabnikih 10

3.2 Načini zbiranja podatkov o uporabnikih 11

3.3 Spletna analitika 13

4 ZASEBNOST UPORABNIKOV 15

4.1 Opredelitev zasebnosti 16

4.2 Merjenje zaskrbljenosti uporabnikov glede zasebnosti 18

4.3 Pripravljenost uporabnikov za razkrivanje osebnih podatkov 19

4.4 Tehnike uporabnikov za zaščito zasebnosti 20

4.5 Paradoks zasebnosti 22

5 EMPIRIČNA RAZISKAVA VLOGE ZASEBNOSTI V ODNOSU UPORABNIKOV DO SPLETNE PERSONALIZACIJE 25

5.1 Namen in cilji kvantitativne raziskave 25

5.2 Raziskovalne hipoteze 26

5.3 Metodologija kvantitativne raziskave 29

5.4 Analiza rezultatov 31

5.4.1 Predstavitev vzorca 31

5.4.2 Opisne statistike 32

5.4.3 Preverjanje raziskovalnih hipotez 40

5.5 Interpretacija ugotovitev 48

5.6 Omejitve raziskave in priporočila za nadaljnje raziskave 51

5.7 Implikacije za podjetja 52

6 SKLEP 54

LITERATURA IN VIRI 55

PRILOGE 65

KAZALO TABEL

Tabela 1: Pogostost uporabe tehnik za zaščito zasebnosti (n = 306) 40
Tabela 2: Povzetek rezultatov Mann-Whitneyevega U testa 42
Tabela 3: Povezanost med zaskrbljenostjo glede zasebnosti in pripravljenostjo za deljenje podatkov 43
Tabela 4: Aritmetične sredine zaskrbljenosti glede zasebnosti po starostnih skupinah 44
Tabela 5: Povezanost posameznih trditev glede koristi spletne personalizacije in pripravljenosti za deljenje podatkov 45
Tabela 6: Povezanost zaznanih koristi in pripravljenosti za deljenje podatkov 46
Tabela 7: Opisna statistika pripravljenosti za deljenje posameznega podatka v zameno za personalizirane spletne vsebine 46
Tabela 8: Povzetek rezultatov Wilcoxonovega signed rank testa 47
Tabela 9: Povezanost med zaskrbljenostjo glede zasebnosti in verjetnostjo uporabe tehnik za zaščito zasebnosti 47
Tabela 10: Rezultati preverjanja hipotez 48

KAZALO SLIK

Slika 1: Večstopenjski proces izvedbe personalizacije 7
Slika 2: Starostna struktura anketirancev (n = 306) 31
Slika 3: Najvišja dosežena formalna izobrazba anketirancev (n = 306) 32
Slika 4: Prosti čas, ki ga anketiranci dnevno preživijo na spletu (n = 306) 32
Slika 5: Pogostost srečevanja z različnimi oblikami personalizacije (n = 306) 33
Slika 6: Stališče anketirancev do spletne personalizacije (n = 306) 34
Slika 7: Trditve o koristih spletne personalizacije (n = 306) 35
Slika 8: Splošna pripravljenost anketirancev za deljenje svojih podatkov (n = 306) 35
Slika 9: Pripravljenost anketirancev za deljenje različnih vrst podatkov (n = 306) 36
Slika 10: Trditve o zaskrbljenosti anketirancev glede zasebnosti (n = 306) 37
Slika 11: Trditve o zaupanju spletnim stranem (n = 306) 38
Slika 12: Tveganja za uporabnike spletnih strani, ki omogočajo spletno personalizacijo (n = 306) 39
Slika 13: Verjetnost samozaščitnega vedenja anketirancev (n = 306) 39
Slika 14: Primerjava odgovorov na 7. vprašanje pri podpovprečno in nadpovprečno zaskrbljenih anketirancih 42

KAZALO PRILOG

Priloga 1: Anketni vprašalnik 1
Priloga 2: Aritmetične sredine in standardni odkloni preučevanih konstruktov 6
Priloga 3: SPSS izpis za preverjanje 1. hipoteze 7
Priloga 4: SPSS izpis za preverjanje 2. hipoteze 8
Priloga 5: SPSS izpis za preverjanje 3. hipoteze 10
Priloga 6: SPSS izpis za preverjanje 4. hipoteze 11
Priloga 7: SPSS izpis za preverjanje 5. hipoteze 15
Priloga 8: SPSS izpis za preverjanje 6. hipoteze 16
Priloga 9: SPSS izpis za preverjanje 7. hipoteze 17

SEZNAM KRATIC

angl. – angleško
AS – aritmetična sredina
EU – (angl. European Union); Evropska unija
SD – standardni odklon

1 UVOD

Razvoj na področju informacijskih tehnologij je v številnih pogledih spremenil svet trženja. Med drugim je prinesel nove trženjske pristope, s katerimi lahko podjetja učinkovito komunicirajo s porabniki in z njimi gradijo tesne in dolgoročne odnose. Prav tako so se podjetja pričela odmikati stran od tradicionalnega masovnega trženja in se usmerila v bolj fokusirane trženjske programe, s katerimi je mogoče nagovoriti manjše skupine porabnikov in zadovoljiti njihove potrebe (Kotler in drugi, 2019). Podjetja lahko tako v svojih trženjskih strategijah kot enega izmed pristopov uporabijo personalizacijo, s katero elemente trženjskega spleta prilagajajo potrebam posameznih porabnikov glede na zbrane informacije o njih (Arora in drugi, 2008). Prilagajanje ponudbe porabnikom v trženju sicer ni nič novega, vendar nove tehnologije danes omogočajo, da lahko podjetja prilagoditve svoje ponudbe in storitev učinkovito izvajajo tudi na množični ravni (Kotler in drugi, 2019). Priložnosti, ki jih ponuja personalizacija, so prepoznala številna podjetja, kar potrjuje tudi raziskava podjetja Twilio (2022), ki je pokazala, da personalizacija v kar 82 % podjetij predstavlja pomemben del trženjske strategije.

Na področju digitalnega trženja in elektronskega poslovanja se uporablja tudi izraz spletna personalizacija, saj tehnologija igra eno izmed ključnih vlog v procesu prilagajanja ponudb in posredovanja le-teh preko različnih kanalov (Fan in Poole, 2006). Prilagojene ponudbe lahko zajemajo prilagoditve vsebin, rezultatov iskanja, posameznih spletnih strani, komunikacije in interakcij z uporabniki (Adomavicius in Tuzhilin, 2005). Pogosto se pojavljajo tudi v obliki priporočil za izdelke ali storitve, s katerimi predvsem spletni trgovci poskušajo olajšati odločitve svojim kupcem in zagotoviti, da bodo svoj nakup opravili v njihovi spletni trgovini (Schafer in drugi, 2001). Cilj podjetij je, da s pomočjo personalizacije posamezniku zagotovijo čim bolj relevantno vsebino, priporočilo ali drugo prilagojeno ponudbo, ki bo ustrezala njegovim potrebam in željam (Adomavicius in drugi, 2008; Isinkaye in drugi, 2015). Na ta način bodo lahko izboljšala njegovo izkušnjo in odnos s podjetjem, kar se bo odražalo v zadovoljstvu porabnika, njegovi nakupni nameri in zvestobi podjetju (Ball in drugi, 2006; Kalyanaraman in Sundar, 2006; Lee in Park, 2009).

Spletna personalizacija temelji na podatkih, ki jih podjetja zbirajo o svojih uporabnikih. Napredek na področju informacijskih tehnologij omogoča, da lahko podjetja ob vsaki interakciji z uporabniki hitro in enostavno pridobijo podrobnejše podatke o njih in njihovih preferencah, s katerimi lahko izpopolnijo njihove uporabniške profile (Gao in drugi, 2010; Kotler in drugi, 2019). Prav tako lahko spremljajo njihovo vedenje na spletnih straneh, kot na primer katere vsebine obiskujejo, koliko časa se zadržijo na določeni spletni strani ali kdaj najpogosteje dostopajo do določene vsebine (Zheng in Peltsverger, 2015). Vse te podatke lahko podjetja analizirajo z različnimi analitičnimi orodji, s katerimi pridobijo pomembne informacije o svojih uporabnikih, ki jih lahko nato uporabijo pri odločanju in poslovanju (Bekavac in Garbin Praničević, 2015). Napredek na področju umetne

inteligence, podatkovnega rudarjenja in strojnega učenja podjetjem omogoča, da s pomočjo kompleksnih analiz še bolje spoznajo svoje uporabnike in njihove potrebe. Prav tako jih lahko s pomočjo teh tehnologij v realnem času učinkovito nagovorijo in jim ponudijo prilagojeno izkušnjo (Chaffey in Ellis-Chadwick, 2019).

Čeprav spletna personalizacija prinaša številne koristi za uporabnike in jo mnogi celo pričakujejo s strani podjetij, se morajo tržniki vseeno zavedati, da z zbiranjem in obdelavo podatkov posegajo v zasebnost posameznikov (Quach in drugi, 2022; Salesforce, 2022). Dojemanje zasebnosti se med posamezniki razlikuje in je odvisno od številnih dejavnikov, kot so spol, osebnost, kultura, predhodne izkušnje in situacija, v kateri se posameznik nahaja (Smith in drugi, 2011). Nekateri lahko tako ravnanje podjetij razumejo kot grožnjo, saj s tem izgubijo nadzor nad svojimi podatki in nad tem, kdo in na kakšen način z njimi ravna (Malhotra in drugi, 2004). Različna tveganja in možne negativne posledice pri posameznikih povečajo zaskrbljenost glede njihove zasebnosti (Norberg in drugi, 2007). Raziskava, ki jo je izvedlo podjetje Norton (2023), je pokazala, da je skoraj 80 % anketirancev zaskrbljenih glede zasebnosti svojih podatkov. Zaskrbljenost posameznikov se lahko odraža v njihovi nepripravljenosti za razkrivanje svojih podatkov (Smith in drugi, 2011). Poleg tega se lahko pred tveganji zaščitijo z uporabo različnih orodij ali drugih tehnik, na primer z brisanjem piškotkov, uporabo varnostne programske opreme ali orodij za blokiranje sledenja (Baruh in drugi, 2017; Quach in drugi, 2022). Njihova zaskrbljenost negativno vpliva tudi na zaupanje podjetju, stališča do blagovne znamke in nakupno namero (Castañeda in Montoro, 2007; Swani in drugi, 2021; Taylor in drugi, 2009). Prav tako lahko ti negativni občutki negativno vplivajo na učinkovitost spletne personalizacije, saj posamezniki pričnejo s podjetji deliti napačne podatke ali pa se poskušajo izogibati personaliziranim ponudbam (Chen in drugi, 2022; Kaniewska-Sejba in Pilarczyk, 2014).

Namen magistrskega dela je celovito preučiti vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije. Tako nameravam povezati dosedanja teoretična spoznanja s področja spletne personalizacije in zasebnosti ter s pomočjo empirične raziskave ugotoviti, kako je zasebnost uporabnikov povezana z njihovimi stališči do spletne personalizacije in pripravljenostjo za deljenje podatkov. Spoznanja iz literature in ugotovitve empirične raziskave bodo tržnikom služila kot pomoč pri razumevanju uporabnikov in njihovega vedenja na spletu ter pripomogla k zagotavljanju učinkovitih in uporabniku prijaznih personaliziranih spletnih izkušenj.

Cilj magistrskega dela je ugotoviti, ali obstaja povezava med zasebnostjo uporabnikov in njihovim odnosom do spletne personalizacije. Prav tako želim ugotoviti, kako zaskrbljenost uporabnikov vpliva na njihova stališča in vedenjske namere. Preveriti želim, ali različni dejavniki vplivajo na pripravljenost posameznikov za deljenje osebnih podatkov na spletu. Poleg tega želim ugotoviti, na kakšen način poskušajo uporabniki zaščititi svojo zasebnost v primeru spletne personalizacije.

Magistrsko delo je sestavljeno iz dveh delov. V teoretičnem delu, ki obsega prva tri poglavja, bom sprva opredelila koncept spletne personalizacije in predstavila različne oblike spletne personalizacije, proces njene izvedbe ter prednosti in slabosti, ki jih prinaša za podjetja in uporabnike. V drugem poglavju bom predstavila področje zbiranja in obdelave podatkov, kjer bom opisala različne vrste podatkov, načine zbiranja le-teh in spletno analitiko. V tretjem poglavju bom predstavila koncept zasebnosti in zaskrbljenosti uporabnikov glede zasebnosti. Prav tako se bom v tem poglavju osredotočila na posledice zaskrbljenosti uporabnikov in na koncu predstavila tudi koncept paradoksa zasebnosti. Četrto poglavje predstavlja empirični del magistrskega dela. V tem poglavju bom predstavila metodologijo in analizo rezultatov kvantitativne raziskave, s katero sem preučevala vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije. Na koncu sledijo še ključne ugotovitve kvantitativne raziskave in njene omejitve, priporočila za nadaljnje raziskave ter implikacije za podjetja.

2 SPLETNA PERSONALIZACIJA

Informacijske tehnologije podjetjem omogočajo, da pridobijo številne podatke o svojih kupcih in si tako ustvarijo jasnejšo sliko o njihovih preferencah in vedenju. Na ta način lahko za vsakega posameznika ustvarijo prilagojeno izkušnjo, kar bo pozitivno vplivalo na njegovo zadovoljstvo in odnos s podjetjem (Deloitte, 2020). Personalizacija različnih elementov trženjskega spleta tako prinaša številne prednosti, zaradi česar je postala eden izmed ključnih elementov strategij digitalnega trženja v podjetjih (Twilio, 2022). Prednosti spletne personalizacije so prepoznali tudi porabniki, ki od podjetij vse bolj pričakujejo, da bodo razumela njihove potrebe in pričakovanja ter jim ponudila personalizirane ponudbe (Salesforce, 2022).

2.1 Opredelitev spletne personalizacije

Zaradi številnih možnosti uporabe na različnih področjih se v literaturi pojavljajo različne opredelitve spletne personalizacije, ki ta proces obravnavajo iz različnih zornih kotov. Na področju trženja in elektronskega poslovanja se spletna personalizacija obravnava predvsem kot način upravljanja odnosov s strankami, ki omogoča ustvarjanje dodane vrednosti za vsakega posameznika, saj mu lahko na ta način podjetja zagotovijo ponudbo, vsebino ali izkušnjo v skladu z njegovimi potrebami (Fan in Poole, 2006). V tem procesu ima zelo pomembno vlogo tehnologija, s pomočjo katere podjetja zbirajo in obdelujejo podatke ter tako pridejo do pomembnih spoznanj o svojih strankah, na podlagi katerih lahko pripravijo personalizirane ponudbe (Chaffey in Ellis-Chadwick, 2019).

Spletna personalizacija predstavlja eno izmed vrst personalizacije, pri kateri podjetja z uporabo različnih tehnologij posameznemu uporabniku zagotovijo ustrezno vsebino ob pravem času (Tam in Ho, 2006). Zajema prilagajanje procesov v spletnem okolju, pri čemer se lahko izvaja na spletnih straneh, preko priporočilnih sistemov ali preko drugih digitalnih

kanalov, kjer posamezniki pridejo v stik s podjetjem (Adomavicius in drugi, 2008). Če se ta proces nanaša na spletne strani, jo lahko opredelimo kot »proces prilagajanja vsebine in strukture spletne strani specifičnim in individualnim potrebam vsakega uporabnika z izkoriščanjem uporabnikovega navigacijskega vedenja« (Eirinaki in Vazirgiannis, 2003, str. 3). Po drugi strani jo lahko obravnavamo tudi bolj splošno, kjer lahko uporabimo opredelitev Fana in Poola (2006), ki pravita, da je spletna personalizacija proces, pri katerem lahko podjetja prilagajajo vsebino, uporabniški vmesnik, dostop do informacij ali funkcionalnosti informacijskega sistema, s čimer postanejo bolj relevantna za posameznika ali skupino uporabnikov. Adomavicius, Huang in Tuzhilin (2008) so izpostavili, da lahko pri opredelitvah spletne personalizacije kljub razlikam najdemo kar nekaj skupnih točk, saj gre v vseh primerih za prilagajanje ponudbe na podlagi znanja o uporabnikih in posredovanje teh ponudb preko različnih vmesnikov ali kanalov.

Znotraj koncepta spletne personalizacije lahko najdemo tudi podrobnejše razdelitve. Tam in Ho (2006) na primer razlikujeta med različnimi vrstami spletne personalizacije glede na to, kdo vodi ta proces. Razlago podata na primeru spletne strani, kjer lahko uporabniki aktivno sodelujejo in vnaprej določajo želeno postavitev spletne strani. Po drugi strani pa lahko sistem avtomatsko prilagaja vsebino in postavitev glede na predhodne interakcije. Kot tretjo možnost izpostavita kontekstno personalizacijo, kjer se sistem v realnem času prilagaja uporabnikom na podlagi njihovih preferenc. Na podoben način sta eno izmed razdelitev opredelila tudi Fan in Poole (2006), ki različne prakse personalizacije delita glede na stopnjo avtomatizacije procesa. Tako v primeru eksplicitne personalizacije uporabnik sam podaja informacije za prilagoditev sistema, v primeru implicitne personalizacije pa sistem sam pridobi informacije in prilagoditev izvede samodejno. V tem kontekstu lahko izpostavimo še delitev na reakcijsko in proaktivno personalizacijo, ki sta jo predstavila Zhang in Sundar (2019). Pri prvi se personalizacija izvede šele, ko uporabnik izrazi željo po tem, na primer ob vnosu iskalnega niza, medtem ko se pri proaktivni personalizaciji prilagoditve izvedejo brez interakcije uporabnika. S tem se uporabnika ne moti med njegovim obiskom spletne strani, saj se vse prilagoditve izvedejo avtomatsko na podlagi predhodno zbranih podatkov o uporabniku in njegovem vedenju. Po drugi strani pa lahko ta način pri uporabnikih vzbudi občutke pomanjkanja nadzora, saj se ne morejo izogniti personalizaciji ali zbiranju podatkov oziroma ne morejo tega procesa prekiniti, ko bi to želeli.

V povezavi s personalizacijo se pogosto pojavlja tudi izraz »prilagajanje« (angl. customization), vendar si raziskovalci glede uporabe izrazov niso enotni, saj nekateri izraza uporabljajo kot sinonima, drugi pa izpostavljajo, da gre za dva različna koncepta (Arora in drugi, 2008). Sundar in Marathe (2010) pravita, da se koncepta med seboj razlikujeta glede na to, kdo ta proces spodbudi ali izvaja. Pri personalizaciji gre za avtomatiziran proces, pri katerem sistem uporabnikom ponudi primerne in relevantne vsebine na osnovi predhodno zbranih podatkov o njih, medtem ko ima pri prilagajanju uporabnik veliko bolj aktivno vlogo, saj sam odloča glede sprememb vsebine (Arora in drugi, 2008; Sundar in Marathe, 2010). Če pokažemo na primeru spletnih strani, bi personalizacija pomenila, da sistem

avtomatsko prikaže izbor relevantnih vsebin na določeni strani, ki so v skladu s predhodnim vedenjem uporabnika ali njegovimi izraženimi interesi. Prilagajanje pa bi v tem primeru pomenilo, da uporabnik sam izbira med različnimi vrstami pisave ali barvami uporabniškega vmesnika ali pa si z uporabo različnih filtrov sam prilagodi izbor vsebin na strani (Eirinaki in Vazirgiannis, 2003).

2.2 Oblike spletne personalizacije

Podjetja lahko v okviru svoje strategije digitalnega trženja uporabljajo različne oblike spletne personalizacije, s katerimi vzdržujejo in krepijo odnose s svojimi strankami. S pomočjo personalizacije izven spletne strani, na primer v obliki e-poštnega trženja ali ciljanega oglaševanja, lahko podjetja med drugim pridobijo pozornost potencialnih uporabnikov in jih pripeljejo na svojo spletno stran (Ansari in Mela, 2003). Po drugi strani pa lahko podjetja personalizacijo uporabljajo na svoji spletni strani, pri čemer avtomatsko ali na pobudo uporabnika prilagajajo funkcionalnosti, vsebino in izgled spletne strani (Riemer in Totz, 2003).

Enega izmed načinov personalizacije vsebin na spletni strani predstavljajo priporočilni sistemi, ki jih uporabljajo predvsem spletni trgovci, s katerimi svojim uporabnikom ponudijo prilagojen izbor relevantnih izdelkov in jim tako poskušajo olajšati proces odločanja med nakupovanjem (Schafer in drugi, 2001). Priporočilni sistemi na podlagi zbranih podatkov o uporabnikih, njihovih preferencah ali predhodnem vedenju oblikujejo priporočila za posameznega uporabnika (Vafopoulos in Oikonomou, 2013). Z njihovo pomočjo podjetja poskušajo zmanjšati preobremenjenost uporabnikov z informacijami, saj celotno ponudbo zmanjšajo na zgolj nekaj izdelkov ali vsebin, za katere obstaja velika verjetnost, da bodo všeč uporabnikom (Isinkaye in drugi, 2015). Če podjetja uspejo pravilno povezati svojo ponudbo s preferencami uporabnikov, s tem povečajo možnost, da bo uporabnik opravil nakup na njihovi spletni strani. Prav tako lahko ustrezna priporočila pripomorejo k zadovoljstvu uporabnikov, kar poveča možnost, da se bodo na to spletno stran vrnili ali opravili ponoven nakup v spletni trgovini (Schafer in drugi, 2001).

Podjetja lahko za pripravo priporočil uporabljajo različne tehnike filtriranja, s pomočjo katerih izberejo tiste izdelke, ki jih želijo ponuditi uporabniku (Schafer in drugi, 2001). Najpogosteje se uporabljajo naslednje tehnike filtriranja:

- *Vsebinsko filtriranje* zajema algoritme, ki pripravljajo priporočila s pomočjo primerjave profila uporabnika in značilnosti posameznih izdelkov. Algoritem oblikuje priporočila za nove izdelke tako, da se vsebinsko ujemajo z izdelki, ki si jih je uporabnik v preteklosti ogledal ali jih je kupil. Izdelke tako primerja na podlagi podobnosti med značilnostmi izdelkov ali ključnimi besedami, ki so dodeljene izdelkom v podatkovni bazi (Isinkaye in drugi, 2015).

- *Skupinsko filtriranje* omogoča oblikovanje priporočil za nove izdelke oziroma vsebine na podlagi podobnosti med uporabniki (Gao in drugi, 2010). Sistem deluje na predpostavki, da obstaja velika verjetnost, da bodo uporabniku všeč enake vsebine, ki so všeč njemu podobnim uporabnikom (Isinkaye in drugi, 2015). Eden najbolj znanih primerov, ki deluje na principu skupinskega filtriranja, je funkcija »Ljudje, ki so kupili ta izdelek, so kupili tudi te izdelke« v Amazon spletni trgovini (Schafer in drugi, 2001).
- *Kombinirani oz. hibridni sistemi* poskušajo ponuditi najbolj optimalna priporočila s pomočjo kombiniranja vsebinskega in skupinskega filtriranja tako, da izkoristijo prednosti in odpravljajo pomanjkljivosti posameznih pristopov (Gao in drugi, 2010). Dober primer hibridnega sistema predstavlja Netflix, ki pri oblikovanju priporočil video vsebin uporablja tako primerjavo vedenja podobnih uporabnikov kot tudi informacije o video vsebini, ki jo je uporabnik v preteklosti ocenil oziroma si jo je ogledal (Mansur in drugi, 2017).

Čeprav so priporočilni sistemi pogosto obravnavani s tehničnega vidika z namenom izboljšanja algoritmov in točnosti priporočil, imajo pomembno vlogo tudi z vidika trženja, saj lahko pripomorejo k doseganju trženjskih ciljev (Vafopoulos in Oikonomou, 2013). S pomočjo priporočilnih sistemov lahko tržniki pridobijo podrobnejše informacije o svojih uporabnikih, izboljšajo modeliranje njihovega vedenja in preferenc ter izboljšajo njihovo zadovoljstvo. Ker priporočilni sistemi omogočajo avtomatizirano prilagajanje ponudb vsakemu posameznemu uporabniku, lahko tržniki tako dosežejo trženje ena na ena na množični ravni (Vafopoulos in Oikonomou, 2013).

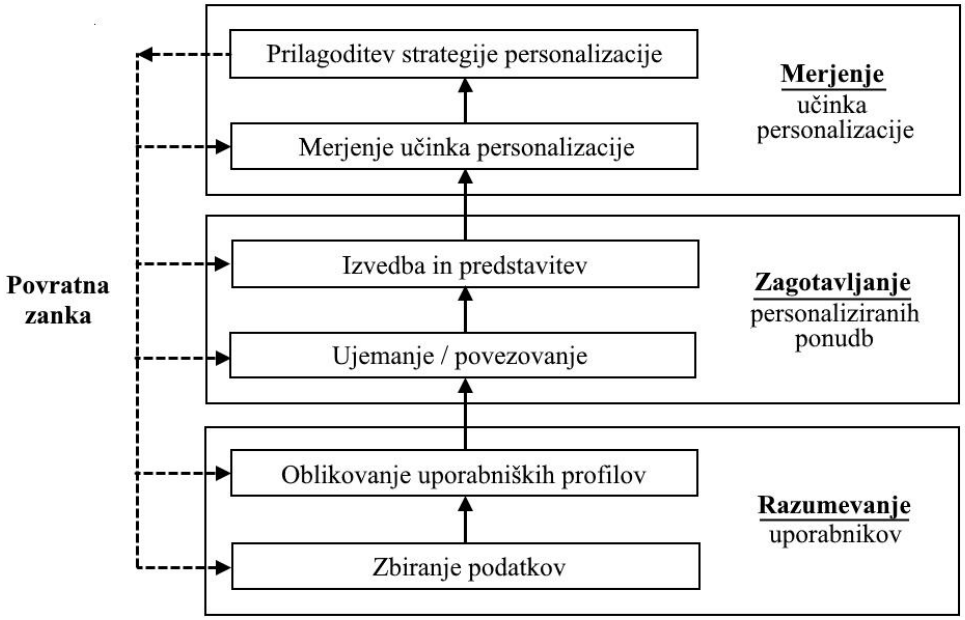
Poleg priporočilnih sistemov se personalizacija na spletu uporablja tudi za druge namene. Da bi uporabnikom čim hitreje ponudila informacije, ki jih iščejo, so podjetja pričela uporabljati personalizacijo rezultatov iskanja (Yoganarasimhan, 2020). Tako lahko uporabnikom ponudijo čim bolj natančne informacije, ki so razvrščeni po ustreznosti na podlagi poizvedbe uporabnika in predhodnega vedenja (Cai in drugi, 2017). Čeprav to vrsto personalizacije najpogosteje uporabljajo spletni iskalniki, jo lahko posamezna podjetja uporabijo tudi na lastnih spletnih straneh in tako uporabnikom omogočijo učinkovito iskanje informacij, navigacijo po strani ali hitrejše opravljanje transakcij (Yoganarasimhan, 2020).

Podjetja lahko za vsakega uporabnika predvidijo tudi lastno ceno izdelka ali storitve, s čimer razlikujejo med uporabniki glede na njihovo trenutno ali potencialno vrednost. Prav tako lahko oblikujejo tudi personalizirane programe zvestobe, s katerimi uporabnike nagradijo za redno uporabo njihovih storitev (Riemer in Totz, 2003). Ponudijo jim lahko tudi različne cene na podlagi njihove lokacije. Poleg tega lahko glede na lokacijo prilagodijo tudi rezultate iskanja, izdelke ali storitve in promocijske kampanje (Toch in drugi, 2012).

2.3 Izvedba spletne personalizacije

Tržniki morajo poznati in razumeti različne korake, ki jih je potrebno izvesti za zagotavljanje uspešne spletne personalizacije. Adomavicius in Tuzhilin (2005) sta personalizacijo predstavila kot večstopenjski proces, ki je prikazan na sliki 1 in je sestavljen iz pridobivanja in analize podatkov o uporabnikih, prilagajanja trženjskega spleta na podlagi teh podatkov ter merjenja in vrednotenja celotnega procesa. Opozarjata tudi, da je potrebno celoten proces obravnavati kot ponavljajočo povratno zanko, kjer ob vsaki ponovitvi s pomočjo povratnih informacij poskušamo izboljšati posamezne dele procesa.

Slika 1: Večstopenjski proces izvedbe personalizacije



Prirejeno po Adomavicius in Tuzhilin (2005).

Proces personalizacije se prične z zbiranjem podatkov o uporabnikih preko različnih kanalov. Z namenom čim boljšega razumevanja uporabnikov podjetja oblikujejo uporabniške profile, ki vsebujejo osnovne demografske podatke, podatke o njihovih predhodnih interakcijah s podjetjem (npr. predhodne transakcije ali nakupi), podatke o njihovi lokaciji in času interakcije in podatke o njihovih interesih (Adomavicius in Tuzhilin, 2005; Gao in drugi, 2010). Prav tako lahko podjetja v teh profilih hranijo podatke o vedenju uporabnikov na spletni strani, ki jih pridobijo z uporabo bolj naprednih tehnik modeliranja in podatkovne analitike (Gao in drugi, 2010).

V drugi fazi podjetja oblikujejo personalizirane ponudbe na podlagi zbranih podatkov o uporabnikih in jih uporabnikom ponudijo preko svojih kanalov (Adomavicius in Tuzhilin, 2005). Tako morajo zagotoviti, da se bodo prilagojene ponudbe čim bolj ujemale z zbranimi podatki. Za ta namen podjetja uporabljajo različne sisteme, ki na podlagi statističnih metod in napovednih modelov uporabnike povežejo s primernimi izdelki, vsebinami ali drugimi prilagojenimi ponudbami (Adomavicius in Tuzhilin, 2005).

Riemer in Totz (2003) sta v okviru sistema za izvedbo personalizacije predstavila različne načine, kako lahko podjetja personalizirajo elemente trženjskega spleta. V osrednjem delu sistema se nahaja izdelek, pri katerem lahko podjetja posameznemu uporabniku omogočijo, da si po svojih željah prilagodi posamezne komponente ali karakteristike. Prav tako lahko podjetja omogočijo prilagoditev spremljajočih dodatnih storitev, kot sta dostava ali vzdrževanje. Uporabnikom lahko ponudijo tudi prilagojene ponudbe v obliki priporočil ali prilagojenih cen in popustov (Riemer in Totz, 2003).

Poleg izdelka se podjetja pogosto odločajo tudi za prilagoditev svoje spletne strani, pri čemer glede na potrebe uporabnikov spreminjajo vsebino, izgled, uporabniški vmesnik in navigacijo na strani (Riemer in Totz, 2003). Pri tem gre lahko za vizualne prilagoditve, na primer barvnih shem, pisav ali postavitve vsebin, ki jih lahko uporabniki posredno ali neposredno prilagajajo. Po drugi strani pa gre tudi za prilagoditve informacij in navigacijske strukture, ki omogočajo lažji dostop do vsebin, ki so za uporabnike najprimernejše (Desai, 2019). Nazadnje lahko podjetja personalizirajo tudi svojo komunikacijo z uporabniki, pri čemer lahko prilagodijo vsebino in prejemnike sporočil, kanale in medije ter frekvenco in čas pošiljanja prilagojenih sporočil (Riemer in Totz, 2003).

V tretji fazi podjetja merijo učinek in uspešnost procesa personalizacije in na podlagi ugotovitev poskušajo izboljšati predhodne korake. Povratne informacije s strani uporabnikov omogočajo, da lahko podjetja ocenijo, kako točne in zanesljive so bile prilagoditve njihovih ponudb (Adomavicius in Tuzhilin, 2005). Pri ocenjevanju uspešnosti lahko analizirajo različne metrike, kot sta stopnja klikov in stopnja konverzije. Prav tako lahko opazujejo, v kolikšni meri in na kakšen način posamezniki uporabljajo personalizirane storitve in ali se to odraža v povečanju prodaje in prihodkov oziroma pripomore k doseganju drugih zastavljenih poslovnih ciljev (Zanker in drugi, 2019). Na podlagi ugotovitev nato podjetja poskušajo prepoznati, ali je potrebno katerega od predhodnih korakov izboljšati. Tako morajo znotraj posamezne stopnje ugotoviti vzroke za težave in prilagoditi svoje aktivnosti, kar jim v nadaljevanju omogoča doseganje boljših rezultatov (Adomavicius in Tuzhilin, 2005).

2.4 Prednosti in slabosti spletne personalizacije za podjetja in uporabnike

Spletna personalizacija podjetjem prinaša številne prednosti. Raziskava McKinsey navaja, da lahko podjetja z uporabo spletne personalizacije povečajo svoje prihodke med 10 in 15 odstotki (Arora in drugi, 2021). Podjetja lahko na ta način krepijo odnose s svojimi uporabniki, zaradi česar so bolj pripravljeni opraviti ponovni nakup pri teh podjetjih ali jih priporočiti svojim znancem (Arora in drugi, 2021). Prav tako lahko podjetja s pomočjo informacij o svojih strankah razširijo svojo ponudbo in si tako zagotovijo konkurenčno prednost (Murthi in Sarkar, 2003). Podjetja lahko s pomočjo spletne personalizacije vplivajo na zadovoljstvo svojih strank. Natančneje, Kalyanaraman in Sundar (2006) pravita, da personalizacija pozitivno vpliva na zadovoljstvo uporabnikov, saj z njeno pomočjo prejmejo

relevantne informacije. Relevantnost teh informacij bo prav tako pozitivno vplivala na zanimanje uporabnikov, zaradi česar bodo bolj pripravljeni uporabljati sisteme, ki ponujajo personalizirane vsebine. Pravita tudi, da spletna personalizacija pozitivno vpliva na uporabnikov odnos do spletnega portala. To pozitivno mnenje se lahko kasneje odraža v njihovem vedenju, saj jih lahko spodbudi, da bodo ta portal ponovno obiskali (Kalyanaraman in Sundar, 2006). Tudi Chang in Chen (2008) sta ugotovila, da lahko zadovoljstvo uporabnikov s spletno stranjo pozitivno vpliva na zvestobo uporabnikov. Prav tako sta izpostavila, da se morajo podjetja osredotočiti na oblikovanje spletne strani, ki bo uporabniku olajšala iskanje informacij in zagotovila pozitivno uporabniško izkušnjo. Na ta način bodo spletno stran zaznavali kot bolj kakovostno, kar se bo odražalo v njihovem zadovoljstvu in zvestobi (Chang in Chen, 2008).

Spletna personalizacija prinaša koristi tudi za uporabnike, saj omogoča, da prejmejo ponudbe, ki so prilagojene njihovim potrebam (Tam in Ho, 2006). Tako se uporabniki lahko osredotočijo zgolj na relevantne ponudbe, ki ustrezajo njihovim zahtevam (Murthi in Sarkar, 2003). Ob tem se bodo počutili bolj povezani s podjetji, saj bodo imeli občutek, da jih ta dobro poznajo (Arora in drugi, 2021). Zmanjšan obseg prilagojenih ponudb ali vsebin pripomore tudi k zmanjšanju preobremenjenosti uporabnika z informacijami. Uporabniki so lahko na ta način bolj učinkoviti v procesu odločanja, saj imajo na voljo manj alternativ, ki jih morajo upoštevati (Liang in drugi, 2006). Poleg že navedenih koristi spletna personalizacija omogoča tudi bolj materialne koristi za uporabnike. Podjetja pogosto uporabnike spodbujajo k razkrivanju osebnih podatkov tako, da jim v zameno ponudijo kupone, popuste, nagrade ali brezplačne vzorce (Strycharz in drugi, 2019).

Čeprav spletna personalizacija prinaša številne koristi, morajo biti podjetja vseeno pozorna, da bodo pri pripravi personaliziranih ponudb pravilno uporabila podatke o svojih uporabnikih in tako oblikovala ponudbe, ki so dejansko relevantne za njih (Kaniewska-Sejba in Pilarczyk, 2014). Prav tako morajo pred implementacijo preveriti, ali lahko ta proces tako s tehničnega kot s finančnega vidika sploh uspešno izvedejo (Adomavicius in drugi, 2008). Arora in drugi (2008) opozarjajo, da morajo imeti podjetja za uspešno izvedbo personalizacije dostop do primerne baze podatkov in ustrezne programske opreme, kar lahko predstavlja velik strošek.

Glavni izziv pri učinkoviti izvedbi spletne personalizacije predstavljajo zaznana tveganja v povezavi z zasebnostjo. Spletna personalizacija lahko pri uporabniku spodbudi zaskrbljenost glede možne zlorabe osebnih podatkov, ki jih delijo za ta namen (Chellappa in Sin, 2005). Strycharz in drugi (2019) so v svoji raziskavi ugotovili, da spletna personalizacija pri uporabnikih vzbuja številne negativne občutke. Ugotovili so, da lahko uporabniki spletno personalizacijo zaznavajo kot vsiljivo in nadležno. Prav tako lahko čutijo, da podjetja s personalizacijo premočno posegajo v njihova življenja ter vplivajo na njihovo vedenje in odločitve. Posledično lahko vsi ti negativni občutki privedejo do negativnih reakcij uporabnikov, ki se pričnejo izogibati uporabi personaliziranih ponudb (Kaniewska-Sejba in Pilarczyk, 2014). Cai in Mardani (2023) sta pokazala, da lahko zbiranje osebnih podatkov

za namen personalizacije privede do negativnih občutkov, kot sta jeza in razočaranje, ki se odražajo v vedenju posameznikov. Ti bodo lahko razvili odklonilen odnos do spletne personalizacije, se pričeli izogibati personaliziranim ponudbam ali prenehali kupovati izdelke pri ponudnikih, ki uporabljajo personalizirano trženje (Cai in Mardani, 2023).

3 ZBIRANJE IN OBDELAVA PODATKOV O UPORABNIKIH

Uporabniki ob brskanju po spletu za seboj puščajo številne osebne podatke, ki so postali dragocena dobrina v digitalnem trženju, saj ob ustrezni obdelavi podjetjem omogočajo boljše razumevanje svojih obstoječih in potencialnih strank. Če znajo podjetja pravilno izkoristiti pridobljene podatke, lahko oblikujejo prilagojene ponudbe in si tako zagotovijo konkurenčno prednost (Murthi in Sarkar, 2003). Na podlagi podatkov o uporabnikih in njihovih interesih tržniki pripravljajo prilagojena sporočila, spletne strani, promocijske kampanje in priporočila za izdelke, vsebine ali storitve (Adomavicius in Tuzhilin, 2005). Za uspešno izvajanje teh aktivnosti morajo sprva pridobiti točne, zanesljive in relevantne podatke o svojih uporabnikih. Poleg tega morajo pri zbiranju in obdelavi podatkov upoštevati veljavno zakonodajo. V Evropski uniji predpise na tem področju opredeljuje Splošna uredba EU o varstvu podatkov, ki med drugim določa, da morajo podjetja s strani uporabnika pridobiti eksplicitno soglasje za zbiranje in obdelavo osebnih podatkov (Jesus in Mustare, 2019). Prav tako morajo uporabnikom podati podrobnejše informacije o tem, kateri podatki, na kakšen način in zakaj bodo uporabljeni. Poleg ravnanja v skladu z zakonodajo morajo podjetja pri obdelavi podatkov delovati čim bolj transparentno in etično, saj tako varujejo podatke o svojih uporabnikih in zmanjšujejo njihovo zaskrbljenost glede zasebnosti na spletu (Edquist in drugi, 2022).

3.1 Vrste podatkov o uporabnikih

Informacijske tehnologije podjetjem omogočajo zbiranje različnih vrst podatkov o svojih uporabnikih. Tako lahko med drugim pridobijo tudi osebne podatke, na podlagi katerih je mogoče določiti identiteto posameznega uporabnika (Liu in drugi, 2023). Splošna uredba EU o varstvu podatkov osebni podatek opredeljuje kot »katero koli informacijo v zvezi z določenim ali določljivim posameznikom […], ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika« (Uredba (EU) 2016/679, 4. člen, str. 33). Osebni podatki tako ogrožajo anonimnost uporabnikov in jih izpostavljajo različnim tveganjem, zaradi česar so jih posamezniki manj pripravljeni razkrivati (Liu in drugi, 2023).

Belen Saglam in drugi (2022) so na podlagi pregleda zakonodaj o varstvu osebnih podatkov iz tridesetih držav opredelili pet kategorij osebnih podatkov:

- *Demografski podatki* – rojstni podatki, podatki o državljanstvu, izobrazbi in poklicu, rasnem in etničnem poreklu, veroizpovedi, političnem mnenju, itd.
- *Osebni identifikacijski podatki* – kontaktni podatki posameznika, uradne identifikacijske številke, identifikatorji na spletu, biometrični podatki, itd.
- *Zdravstveni podatki* – zdravstveno stanje posameznika in njegovih družinskih članov, predhodne in trenutne bolezni, diagnoze in zdravljenja, itd.
- *Finančni podatki* – kreditna sposobnost posameznika, podatki o izpolnjevanju finančnih obveznosti, podatki o bančnem računu, itd.
- *Sodni podatki* – podatki o izrečenih kaznih, prekrških, kazenskih ovadbah, itd.

Določeni zgoraj omenjeni podatki, kot so na primer podatki o veroizpovedi ali biometrični podatki, spadajo v kategorijo občutljivih podatkov, ki jih Splošna uredba EU o varstvu podatkov in druge zakonodaje na tem področju obravnavajo ločeno, saj bi njihovo razkritje ali zloraba škodilo posamezniku. Po drugi strani pa lahko posamezniki tudi druge podatke dojemajo kot občutljive, predvsem ko bi njihova obdelava lahko imela negativen vpliv na njihovo življenje (Belen Saglam in drugi, 2022). Raziskava, ki jo je izvedel Pew Research Center, je pokazala, da anketiranci menijo, da so podatki iz vsebin njihovih telefonskih pogovorov enako občutljivi kot podatki o njihovem zdravstvenem stanju. Prav tako se jim zdijo ti podatki bistveno bolj občutljivi kot na primer podatki o veroizpovedi, saj jih je le 22 % anketirancev ocenilo kot občutljive, medtem ko je podatke iz telefonskih pogovorov kot občutljive označilo 54 % anketirancev (Madden, 2014).

Poleg osebnih podatkov lahko podjetja zbirajo tudi druge podatke o svojih uporabnikih. Ob interakcijah uporabnikov s spletnim mestom lahko tako pridobijo podatke o njihovem vedenju na spletni strani, kot so na primer premikanje po določeni strani ali kliki na posamezne elemente (Zheng in Peltsverger, 2015). Prav tako lahko s pomočjo orodij za spletno analitiko preučijo, katere vsebine posamezniki pogosto obiskujejo ali koliko časa preživijo na posamezni strani. Na podlagi vseh teh podatkov lahko s pomočjo spletnega rudarjenja prepoznajo interese in preference svojih uporabnikov, s katerimi lahko oblikujejo ali izpopolnijo uporabniške profile in uporabnikom tako ponudijo prilagojene vsebine (Eirinaki in Vazirgiannis, 2003).

3.2 Načini zbiranja podatkov o uporabnikih

Podjetja lahko do podatkov o svojih uporabnikih pridejo na več različnih načinov. Uporabnike lahko neposredno vprašajo po podatkih, ki jih potrebujejo. To lahko naredijo na primer z uporabo anketnih vprašalnikov ali prijavnih obrazcev. Ti podatki bodo verjetno bolj zanesljivi in točni, saj jih uporabniki prostovoljno delijo s podjetjem, zato obstaja manjša verjetnost, da bi uporabljali napačne podatke (Gozman, 2022). V zameno za deljenje podatkov uporabnikom pogosto ponudijo nekaj koristnega ali dragocenega. Raziskava, ki jo je izvedla Columbia Business School, je na primer pokazala, da je 77 % anketirancev

pripravljenih deliti osebne podatke, kot sta e-poštni naslov ali telefonska številka, v zameno za darilne bone ali kupone (Quint in Rogers, 2015).

Po drugi strani pa lahko podjetja podatke zbirajo, ne da bi se uporabniki tega zavedali. Različni digitalni sistemi, ki analizirajo spletno vedenje uporabnikov, omogočajo, da podjetja podatke o uporabnikih zbirajo, ne da bi motila njihovo spletno izkušnjo. Kljub temu lahko prikrito zbiranje podatkov pri uporabnikih vzbudi občutke pomanjkanja nadzora nad osebnimi podatki, pri čemer se poveča njihova zaskrbljenost glede zasebnosti (Norberg in drugi, 2007; Zhang in Sundar, 2019). Najpogosteje podjetja za sledenje uporabnikov uporabljajo piškotke, poleg teh pa so se v zadnjih letih vzpostavili tudi drugi inovativni in bolj invazivni pristopi, s katerimi podjetja poskušajo zaobiti mehanizme za varovanje zasebnosti, ki so jih uvedli določeni spletni brskalniki (Bujlow in drugi, 2017).

Piškotki so majhne, praviloma do 4 kB velike tekstovne datoteke, ki se naložijo na računalnik uporabnika ob prvem obisku določene spletne strani. Ko jo uporabnik ponovno obišče, brskalnik pridobi informacijo o naloženem piškotku in tako prepozna uporabnika (Bujlow in drugi, 2017). Piškotki se uporabljajo za zagotavljanje boljše uporabniške izkušnje in določenih funkcionalnosti spletne strani, prav tako pa se lahko uporabljajo za spremljanje prometa in beleženje vedenja uporabnikov (Kulyk in drugi, 2021). Poznamo različne vrste piškotkov. Sejni piškotki se izbrišejo vsakič, ko uporabnik zapre svoj brskalnik, medtem ko se trajni piškotki shranijo na računalnik uporabnika in so aktivni do izteka veljavnosti (Bujlow in drugi, 2017). Razlikujemo tudi med lastnimi piškotki in piškotki tretjih oseb. Lastne piškotke določi spletno mesto, na katerem se uporabnik nahaja. Uporabljajo se predvsem za zagotavljanje funkcionalnosti spletnega mesta, spremljanje analitike in shranjevanje osnovnih podatkov za enostavnejšo uporabo spletnega mesta, kot so jezikovne preference ali podatki za prijavo v uporabniški račun (Adobe, 2021). Piškotki tretjih oseb pa so ustvarjeni s strani drugih spletnih mest kot je tisto, ki jo trenutno uporabnik obiskuje. Uporabljajo se za sledenje uporabnika na različnih spletnih mestih in zbiranje podatkov o njegovem vedenju. Ti podatki se uporabljajo predvsem za ciljano in personalizirano oglaševanje ter ponovno ciljanje na različnih spletnih mestih (Adobe, 2021).

V luči vse strožjih ukrepov na področju varstva osebnih podatkov in vse večje zaskrbljenosti uporabnikov glede spletnega sledenja so brskalniki, kot sta Firefox in Safari, pričeli ukinjati podporo piškotkom tretjih oseb (Adobe, 2021). Pri Googlu so opustitev piškotkov tretjih oseb prestavili na konec leta 2024, saj želijo pridobiti dodaten čas za razvoj in testiranje nove tehnologije Privacy Sandbox, ki bo nadomestila uporabo teh piškotkov (Love, 2022). Ta tehnologija bo omogočala, da bodo oglaševalci še vedno lahko dostopali do podatkov o uporabnikih in jih učinkovito nagovorili s svojimi oglasi, vendar na način, ki uporabnikom omogoča več zasebnosti kot do sedaj (Google, brez datuma b). Tehnologija temelji predvsem na združevanju uporabnikov na podlagi njihovih interesov, ki bodo predstavljali osnovo za prikazovanje ustreznih oglasov. Prav tako bodo te informacije shranjene znotraj brskalnika in ne na zunanjem strežniku, s čimer bodo omejili deljenje informacije med različnimi stranmi (Google, brez datuma c).

Postopno opuščanje piškotkov tretjih oseb je podjetja prisililo k iskanju novih načinov za zbiranje podatkov o uporabnikih. Tako se morajo podjetja bolj osredotočiti na zbiranje podatkov preko lastnih kanalov, kot sta spletna stran ali mobilna aplikacija (Ahuja in drugi, 2022). Podjetja lahko podatke pridobijo tudi s pomočjo kontaktnih obrazcev, anketnih vprašalnikov, kvizov in drugih interaktivnih orodij, kjer uporabnik prostovoljno deli določene podatke (Gozman, 2022). Prav tako se lahko podjetja povezujejo z različnimi partnerji, s katerimi si delijo podatke in jih uporabijo pri svojih trženjskih aktivnostih (Ahuja in drugi, 2022). Poleg omenjenih strategij pa se nekatera podjetja poslužujejo tudi bolj spornih načinov zbiranja podatkov, ki še vedno temeljijo na sledenju uporabnika. Identifikacija prstnega odtisa brskalnika (angl. browser fingerprinting) je strategija, s katero podjetja prepoznavajo uporabnika, na podlagi zbranih informacij o njegovem brskalniku ali napravi (Bujlow in drugi, 2017). Tako lahko uporabniku sledijo po različnih straneh, zbirajo podatke o njegovem spletnem vedenju in mu nato na primer ponudijo prilagojene oglase.

3.3 Spletna analitika

Zheng in Peltsverger (2015) sta spletno analitiko opredelila kot »proces merjenja, zbiranja, analiziranja in poročanja o podatkih, ki jih uporabniki ustvarjajo ob obisku spletnih strani«. Spletna analitika se lahko uporablja za spremljanje vedenja in stališč potencialnih uporabnikov ter primerjalno analizo s konkurenti. Uporablja pa se predvsem za spremljanje vedenja uporabnikov na določeni spletni strani. Tako lahko podjetja s pomočjo različnih metrik preučujejo delovanje svojih spletnih strani in interakcije uporabnikov z njimi (Kumar in Ogunmola, 2019).

Na podlagi ugotovitev, pridobljenih z analizo podatkov spletnega prometa, lahko podjetja optimizirajo delovanje svojih spletnih strani, izboljšajo izgled, vsebino in funkcionalnosti spletnih strani ter tako izboljšajo uporabniško izkušnjo (Kumar in Ogunmola, 2019; Zheng in Peltsverger, 2015). Prav tako lahko ta spoznanja uporabljajo za merjenje uspešnosti trženjskih kampanj ter optimizirajo svoje elektronsko poslovanje in tako dosegajo zastavljene poslovne cilje, kot so povečanje nakupov izdelkov, zbiranje kontaktov ali povečanje obiska na strani (Duncan, 2010; Zheng in Peltsverger, 2015).

Za uspešno izvedbo spletne analitike morajo podjetja sprva določiti cilje in ključne kazalnike uspešnosti, ki morajo biti razumljivi, dosegljivi, uporabni, enostavni in relevantni (Kaushik, 2009; Kumar in Ogunmola, 2019). Nato sledita merjenje in zbiranje podatkov, ki se lahko pridobijo iz strežniških dnevnikov ali oznak spletnih strani (Bekavac in Garbin Praničević, 2015). Podatki, ki jih podjetja zbirajo, so lahko kvantitativni ali kvalitativni. Kvantitativni podatki, kot so število obiskov strani ali čas na strani, povedo predvsem, kaj uporabniki počnejo na spletni strani, medtem ko s pomočjo kvalitativnih podatkov poskušamo ugotoviti, zakaj in kako se uporabniki vedejo na spletni strani. Kvalitativne podatke lahko pridobimo s pomočjo anketnih vprašalnikov na spletni strani ali testiranja uporabnosti spletnega mesta (Kaushik, 2009). Proces spletne analitike vključuje tudi poročanje, kjer s pomočjo poročil

prikazujemo določen izbor agregiranih podatkov (Sapateiro in Gomes, 2017). Poročila lahko podjetja prilagodijo svojim potrebam in zbrane podatke na pregleden in razumljiv način predstavijo v obliki tabel ali grafikonov.

Zbrane podatke je potrebno analizirati, da lahko iz njih pridobimo spoznanja o uporabnikih, njihovih interesih in preferencah. Zheng in Peltsverger (2015) sta izpostavila naslednje vrste analiz:

- *Dimenzijska analiza* – najbolj osnovna analiza, s katero podatke združujemo na podlagi različnih dimenzij, npr. demografski podatki, lokacija, kanal prihoda, naprava, itd.
- *Analiza trendov* – opazujemo, kako se določena metrika spreminja v nekem izbranem časovnem obdobju.
- *Analiza porazdelitve* – prikazujemo deleže znotraj posameznih dimenzij, npr. kolikšen delež uporabnikov je do spletne strani dostopal preko mobilnega telefona, namiznega računalnika in tablice.
- *Analiza vedenja in aktivnosti uporabnikov* – preučujemo interakcije uporabnikov s spletno stranjo, npr. katere in koliko strani je uporabnik obiskal v eni seji, kako pogosto se uporabniki vračajo na našo stran, koliko časa preživijo na posamezni strani, itd. Prav tako lahko spremljamo pot uporabnika po posamezni strani, premikanje miške in klike ter ugotovitve predstavimo v obliki toplotne karte (angl. heatmap).
- *Analiza konverzije* – analiziramo podatke v povezavi z doseganjem vnaprej določenih ciljev ter faktorje, ki pripomorejo k povečanju stopnje konverzije. Ta vrsta analize se uporablja predvsem v elektronskem poslovanju.

Za izvedbo zgoraj naštetih analiz uporabljamo orodja za spletno analitiko. Podjetja morajo biti pozorna pri izbiri pravega orodja, preučiti funkcionalnosti posameznih orodij in ugotoviti, ali izbrano orodje ustreza njihovim zahtevam in namenom uporabe (Bekavac in Garbin Praničević, 2015; Kaushik, 2009). Google Analytics je najpogosteje uporabljeno orodje za spletno analitiko, ki ga uporablja več kot 58 % spletnih strani (W3Techs, 2023). Priljubljeno je za uporabo, saj je na voljo brezplačno, je enostavno za uporabo in omogoča pregled nad podrobnejšimi statistikami o spletnem prometu, kar zadostuje potrebam večine podjetij (Plaza, 2009). Poleg teh orodij lahko podjetja uporabljajo tudi orodja za analitiko družbenih omrežjih, orodja za eksperimente in testiranje ter druga orodja, ki omogočajo analizo uporabniške izkušnje, povratnih informacij uporabnikov, itd. (Bekavac in Garbin Praničević, 2015; Kaushik, 2009).

Zbrane podatke s pomočjo orodij za spletno analitiko prikazujemo v obliki metrik, s katerimi opisujemo aktivnosti uporabnikov na spletni strani (Kaushik, 2009). Vsako podjetje oblikuje svoj sistem metrik, ki so prilagojene njihovim potrebam, digitalni strategiji in poslovnim ciljem (Järvinen in Karjaluoto, 2015). Vseeno pa obstajajo določene standardne metrike, ki jih uporablja večina podjetij. Med standardne metrike spadajo (Kaushik, 2009):

- *Obiski strani* predstavljajo interakcije uporabnika s spletnim mestom od trenutka, ko prvič odpre spletno stran do takrat, ko jo zapusti. Pogosto se za beleženje obiska uporablja tudi izraz *seja*, ki lahko obsega enega ali več ogledov strani in se prekine, če uporabnik več kot 30 minut ni aktiven na spletnem mestu ali ga zapusti.
- *Edinstveni obiskovalci* predstavljajo število različnih posameznikov, ki obiščejo spletno mesto v določenem obdobju. Vsak uporabnik je vštet le enkrat, tudi če v tem obdobju spletno mesto obišče večkrat.
- *Čas na strani* predstavlja čas, ki ga uporabnik preživi na določeni strani, ali celotni čas, ki ga preživi na spletnem mestu v okviru enega obiska oziroma seje.
- *Stopnja odboja* predstavlja odstotek uporabnikov, ki spletno mesto zapustijo po ogledu le ene strani. Google je v svoji najnovejši različici Google Analytics 4 stopnjo odboja nadomestil s *stopnjo vpletenosti* (angl. engagement rate), ki predstavlja odstotek sej, ki so trajale več kot 10 sekund, med katerimi se je zgodila vsaj ena konverzija ali znotraj katere je uporabnik obiskal vsaj 2 strani (Google, brez datuma a).
- *Delež izhodov* predstavlja odstotek uporabnikov, ki zapustijo spletno mesto na določeni strani.
- *Stopnja konverzije* predstavlja razmerje med uporabniki, ki so izpolnili vnaprej določen akcijski cilj, in vsemi uporabniki. Ti cilji so lahko nakup, izpolnitev kontaktnega obrazca, prijava na e-novice, prenos gradiva, itd. (Haden, 2012).

Proces spletne analitike bo privedel do pozitivnih učinkov le v primeru, da podjetja pridobljeno znanje uporabijo v procesu odločanja (Kemppainen in drugi, 2022). Prav tako lahko različni dejavniki privedejo do tega, da podjetja ne morejo v celoti izkoristiti celotnega potenciala, ki ga spletna analitika ponuja. Pomanjkanje sredstev in podpore vodstva ter nizka prioriteta teh aktivnosti v primerjavi s preostalimi trženjskimi aktivnostmi lahko privedejo do neučinkovite uporabe spletne analitike v podjetjih (Chaffey in Patron, 2012). Colas in drugi (2014) so ugotovili, da imajo podjetja pogosto težave zaradi nizke kvalitete podatkov, uporabe neustreznih orodij za analizo podatkov in pomanjkanja analitičnih znanj in sposobnosti. Podobno izpostavljata tudi Chaffey in Patron (2012), ki pravita, da se podjetja pogosto ukvarjajo zgolj s poročanjem podatkov namesto, da bi poskušala razumeti, kaj jim podatki povedo o uporabnikih in kakšni so razlogi za njihove spremembe. Ghasemaghaei in drugi (2018) so ugotovili, da lahko izboljšanje in razvijanje kompetenc povezanih s podatkovno analitiko privede do boljše uspešnosti pri sprejemanju odločitev, kar zagotavlja učinkovitejšo uporabo spletne analitike v praksi.

4 ZASEBNOST UPORABNIKOV

Napredek na področju informacijskih tehnologij podjetjem omogoča, da lahko nenehno zbirajo podatke o svojih uporabnikih in njihovem spletnem vedenju. Prav tako lahko sedaj hitro in učinkovito obdelujejo večje količine različnih podatkov in si tako ustvarijo podrobno sliko o svojih uporabnikih. Uporabniki lahko tako prekomerno zbiranje in obdelavo podatkov razumejo kot vdor in grožnjo za njihovo zasebnost (Quach in drugi, 2022).

Raziskava, ki sta jo izvedla podjetje Quantcast in Univerza Južne Kalifornije, je pokazala, da je večina anketirancev, ki uporabljajo digitalne storitve, nekoliko ali zelo zaskrbljenih glede zasebnosti svojih podatkov (Statista, 2019). Raziskava, ki jo je izvedel Pew Research Center, je pokazala, da je 79 % anketirancev zelo ali nekoliko zaskrbljenih glede načinov in namenov uporabe njihovih podatkov (Auxier in drugi, 2019). Prav tako 81 % anketirancev meni, da nimajo nadzora na tem, kako podjetja uporabljajo njihove podatke. Podjetja se morajo zavedati, da s svojimi aktivnostmi posegajo v zasebnost svojih uporabnikov. Prav tako se morajo odzvati na skrbi uporabnikov, saj njihovi odzivi neposredno vplivajo na uspešnost aktivnosti podjetij (Quach in drugi, 2022).

4.1 Opredelitev zasebnosti

Čeprav so številni raziskovalci z različnimi pristopi izboljšali razumevanje zasebnosti in upravljanja z njo, se je izkazalo, da je zasebnost zelo težko enovito opredeliti (Solove, 2006). Razumevanje zasebnosti je pogosto odvisno od področja, ki jo preučuje (Xu in drugi, 2008). V pravu se zasebnost obravnava predvsem v kontekstu pravice do zasebnosti, medtem ko se v psihologiji in filozofiji raziskovalci ukvarjajo predvsem z omejitvijo dostopa do posameznika. Na področju informacijskih tehnologij se zasebnost najpogosteje obravnava v povezavi z nadzorom osebnih podatkov pri interakciji z informacijskimi sistemi (Xu in drugi, 2008). Poleg tega so prepričanja in stališča posameznikov glede zasebnosti odvisna od številnih dejavnikov, kot so spol, osebnost, kultura ali predhodne izkušnje, in se tako razlikujejo v različnih situacijah (Smith in drugi, 2011). Prav zato je zasebnost dinamičen in večdimenzionalen koncept, ki ga je težko enovito opredeliti (Xu in drugi, 2008). Kot pravi Solove (2006), je potrebno zasebnost razumeti kot »krovni izraz, ki združuje skupek različnih, a povezanih stvari«.

Konec 19. stoletja sta Warren in Brandeis (1890, str. 195) zasebnost opredelila kot »pravico posameznika, da ga pustijo na miru«. Do te opredelitve je prišlo zaradi pojava Kodak fotoaparata, ki je omogočal fotografiranje obnašanja oseb v javnosti in deljenje teh fotografij z drugimi, kar sta Warren in Brandeis razumela kot močan poseg v zasebnost posameznika. Z napredkom na področju računalniške tehnologije pa se je pojavila potreba po razširitvi te opredelitve, ki bi obsegala tudi področje zbiranja in obdelave osebnih podatkov (Mulligan in drugi, 2016). V drugi polovici 20. stoletja je Westin (1967, str. 7) zasebnost opisal kot »zahtevo posameznikov, skupin ali institucij, da sami določijo kdaj, kako in v kakšnem obsegu se informacije o njih komunicirajo z drugimi«. Ta opredelitev izpostavlja predvsem pomen nadzora v povezavi z zasebnostjo, pri čemer so posamezniki tisti, ki sami odločajo o svojih osebnih podatkih in imajo nadzor nad njimi (Tavani in Moor, 2001). Ta vidik se odraža na primer tudi v trenutni evropski zakonodaji o varstvu osebnih podatkov, ki poskuša povečati nadzor posameznikov nad osebnimi podatki in jim tako pomaga pri zagotavljanju večje zasebnosti na spletu (Ke in Sudhir, 2022).

Zasebnost so raziskovalci obravnavali tudi s socialno-psihološkega vidika, kjer se za razumevanje zasebnosti najpogosteje uporablja opredelitev Altmana (1975, str. 11), ki pravi, da je zasebnost »selektiven nadzor nad dostopom do samega sebe«. Altman zasebnost obravnava kot dinamičen proces postavljanja mej, s katerimi posameznik nadzoruje interakcije z drugimi. Na podlagi te opredelitve je Petronio (2002) razvila teorijo upravljanja komuniciranja zasebnosti (angl. communication privacy management theory), kjer je obravnavala zasebnost v povezavi s samorazkrivanjem. Petronio (2002) pravi, da posamezniki razkrivajo informacije o sebi na podlagi pravil, ki določajo meje, ko je posameznik še pripravljen deliti svoje informacije z drugimi. Ta pravila so odvisna od različnih dejavnikov, kot so kultura, spol, motivacija, razmerje med koristmi in tveganji ter kontekst situacije.

V današnjem času zasebnost povezujemo predvsem z nevarnostmi na področju osebnih podatkov, ki jih prinaša razvoj informacijske tehnologije. Čeprav lahko uporabniki svoje osebne podatke enostavno delijo v zameno za določeno korist, na ta način izgubijo nadzor nad njimi in se izpostavijo tveganjem za zlorabo osebnih podatkov. S tem žrtvujejo tudi del svoje zasebnosti, ki jo imenujemo informacijska zasebnost. Obstajajo različne opredelitve informacijske zasebnosti, ki jim je v večini skupno to, da vključujejo nadzor nad morebitno uporabo osebnih podatkov (Belanger in Crossler, 2011). Po drugi strani pa Tavani in Moor (2001) trdita, da nadzor nad osebnimi podatki predstavlja način upravljanja zasebnosti, medtem ko lahko posamezniki dosežejo informacijsko zasebnost, če omejijo dostop drugih oseb do njihovih osebnih podatkov. Med novejšimi opredelitvami informacijske zasebnosti se je uveljavila tudi teorija kontekstualne integritete, ki informacijske zasebnosti ne opredeli na osnovi nadzora ali omejitev dostopa do informacij, ampak kot pravico do ustreznega pretoka osebnih podatkov (Nissenbaum, 2004). Zbiranje in deljenje podatkov je omejeno z informacijskimi normami, ki opredeljujejo, na kakšen način se informacije posredujejo med različnimi deležniki in katere informacije je primerno razkriti v določenem kontekstu. Nissenbaum (2004) poda primer, da pacienti delijo svoje zdravstvene podatke s svojim osebnim zdravnikom in ne s svojim delodajalcem, prav tako pa pričakujejo, da bodo te informacije ostale zaupne in ne bodo deljene z drugimi osebami. Posamezniki tako nimajo nujno izrecnega nadzora nad svojimi osebnimi podatki in vseeno ohranijo informacijsko zasebnost, ampak le pod pogojem, da te informacijske norme niso kršene (Nissenbaum, 2004).

V kontekstu personalizacije se zasebnost povezuje predvsem s tveganji, ki jih prinašata zbiranje in obdelava velike količine podatkov za namen prilagajanja spletne uporabniške izkušnje. Z deljenjem osebnih podatkov lahko posameznik izgubi nadzor nad svojimi podatki in je tako bolj izpostavljen kršitvam zasebnosti. Na primer, prilagajanje vsebine glede na lokacijo uporabnika ogroža njegovo varnost, saj lahko pride do deljenja ali razkritja njegove lokacije nepooblaščenim osebam (Toch in drugi, 2012). Prav tako lahko pride do zlorabe ali kraje podatkov, če pride do vdora v podatkovno bazo (Featherman in drugi,

2010). Posledično se pri posamezniku povečajo skrbi glede zasebnosti (Chellappa in Sin, 2005).

4.2 Merjenje zaskrbljenosti uporabnikov glede zasebnosti

Skrb glede zasebnosti (angl. privacy concern) je koncept, ki se uporablja za merjenje prepričanj in stališč posameznikov glede njihove zasebnosti (Martin in Murphy, 2017). V spletnem kontekstu se ta koncept pogosto nanaša na to, kako posamezniki zaznavajo svojo zaskrbljenost glede ravnanja spletnih strani z njihovimi osebnimi podatki (Hong in Thong, 2013). Različne študije so oblikovale inštrumente za merjenje tega koncepta. Smith in drugi (1996) so razvili lestvico Skrb glede informacijske zasebnosti (angl. »Concern for Information Privacy«), ki predstavlja enega izmed prvih teoretičnih okvirjev za merjenje skrbi posameznikov glede informacijske zasebnosti. Obsega štiri dimenzije, ki opredeljujejo skrbi posameznikov glede na različne vrste morebitne zlorabe osebnih podatkov. Skrb pri posameznikih se lahko pojavi zaradi zbiranja in shranjevanja večjih količin osebnih podatkov, preko katerih je mogoče posameznika identificirati. Prav tako se lahko zaskrbljenost pojavi zaradi potencialne uporabe osebnih podatkov za druge, prikrite namene ali zaradi deljenja teh podatkov z drugimi osebami brez dovoljenja posameznika. Pojavi se lahko tudi skrb glede dostopa do osebnih podatkov s strani nepooblaščenih oseb in glede ustreznosti osebnih podatkov, pri čemer se skrbi nanašajo predvsem na prakse podjetij, s katerimi preprečujejo shranjevanje napačnih podatkov o posameznikih (Smith in drugi, 1996).

Malhotra in drugi (2004) so to lestvico prilagodili za spletni kontekst in razvili lestvico Skrb glede informacijske zasebnosti internetnih uporabnikov (angl. »Internet users' information privacy concerns«), ki je sestavljena iz treh dimenzij. Prva dimenzija se nanaša na zbiranje osebnih podatkov, pri čemer Malhotra in drugi (2004) izpostavijo, da je skrb uporabnikov odvisna od koristi, ki jih prejmejo v zameno za zbrane podatke. Druga dimenzija se nanaša na nadzor nad osebnimi podatki, pri čemer so posamezniki manj zaskrbljeni, če lahko nadzirajo proces zbiranja osebnih podatkov ali imajo možnost, da se temu izognejo. Tretja dimenzija pa se nanaša na ozaveščenost posameznikov glede praks, ki jih podjetja uporabljajo za varovanje njihove zasebnosti. Tako bodo posamezniki, ki so seznanjeni s praksami podjetij, imeli boljši pregled nad uporabo svojih osebnih podatkov.

Raziskovalci so v okviru svojih študij preučevali tudi različne dejavnike, ki vplivajo na zaskrbljenost posameznikov glede zasebnosti na spletu. Smith in drugi (2011) so na primer ugotovili, da bodo posamezniki, ki imajo negativne izkušnje glede zasebnosti oziroma so bili v preteklosti žrtve zlorabe osebnih podatkov, bolj zaskrbljeni glede svoje zasebnosti. Prav tako so ugotovili, da se zaskrbljenost pojavi, ko se posamezniki pričnejo zavedati, da podjetja zbirajo in uporabljajo njihove osebne podatke brez dovoljenja.

Demografske razlike med posamezniki imajo prav tako pomembno vlogo pri zaskrbljenosti glede zasebnosti, vendar nasprotujoče ugotovitve različnih študij ne podajo dokončnega

odgovora glede njihovih vplivov (Bergström, 2015). Raziskovalci si niso enotni pri odgovoru, ali spol sploh vpliva na skrbi glede zasebnosti. Tiste študije, ki pa so dokazale statistično značilen vpliv spola, so pokazale, da so ženske na splošno bolj zaskrbljene glede zasebnosti in običajno ne razkrivajo občutljivih osebnih podatkov (Lee in drugi, 2019). Podobno velja tudi za vpliv starosti, kjer raziskave prav tako prihajajo do različnih zaključkov. Hoofnagle in drugi (2010) so na primer ugotovili, da ne prihaja do razlik v zaskrbljenosti med različnimi starostnimi skupinami, medtem ko so na primer Paine in drugi (2007) ugotovili, da so starejši ljudje bolj zaskrbljeni glede svoje zasebnosti na spletu. Po drugi strani pa so Blank in drugi (2014) ugotovili, da bodo mlajši posamezniki bolj verjetno upravljali s svojimi nastavitvami zasebnosti in se tako zavarovali pred tveganji. V povezavi s stopnjo izobrazbe so Blank in drugi (2014) ugotovili, da so posamezniki z višjo stopnjo izobrazbe bolj zaskrbljeni glede svoje zasebnosti in se bodo bolj verjetno posluževali različnih načinov za zaščito svoje zasebnosti.

Li (2014) predstavi tudi vpliv osebnostnih lastnosti posameznika, pri čemer izpostavi naravnanost posameznika, da ceni zasebnost (angl. disposition value to privacy). Ta lastnost posameznika predstavlja njegovo splošno skrb glede zasebnosti in težnjo po ohranitvi nadzora nad svojimi osebnimi podatki. Prav tako ta lastnost vpliva tudi na zaskrbljenost posameznika v določeni situaciji. Li (2014) to predstavi na primeru interakcije s spletnimi stranmi. Tako se bo pri posameznikih, ki so že na splošno bolj zaskrbljeni glede svoje zasebnosti, tudi ob interakciji s spletnim mestom pojavila višja stopnja zaskrbljenosti, saj zaznavajo večje tveganje za izgubo nadzora nad svojimi osebnimi podatki.

4.3 Pripravljenost uporabnikov za razkrivanje osebnih podatkov

Zaskrbljenost posameznikov glede zasebnosti predstavlja pomemben dejavnik, ki vpliva na njihova stališča in vedenje, saj se posamezniki zaradi povečanih skrbi lahko odločijo, da svojih podatkov ne bodo delili (Smith in drugi, 2011). Zaskrbljenost posameznikov je prav tako tesno povezana z različnimi tveganji, saj obstaja verjetnost, da bodo podjetja neprimerno ravnala z njihovimi podatki in jih delila z drugimi deležniki brez dovoljenja posameznikov (Dinev in Hart, 2006).

Ko se posamezniki odločajo, ali so pripravljeni deliti svoje osebne podatke, med seboj primerjajo tveganja ob izgubi zasebnosti in zaznane koristi, ki jih bodo ob tem pridobili. Če so zaznane koristi enake ali večje od pričakovanih tveganj, bodo posamezniki svoje podatke pripravljeni deliti (Dinev in Hart, 2006). Podjetja lahko uporabnike spodbudijo k razkrivanju osebnih podatkov tako, da jim v zameno ponudijo denarne nagrade ali popuste, personalizirane ponudbe, podrobnejše informacije o izdelkih ali storitvah ter brezplačen dostop do dodatnih vsebin. Na ta način bodo uporabniki bolj pripravljeni deliti svoje podatke, saj bodo koristi pomagale ublažiti pričakovana tveganja (Bol in drugi, 2018; Fernandes in Pereira, 2021).

Po drugi strani pa lahko ravnanje podjetij povečuje tveganja za njihove stranke, predvsem v primeru razkrivanja ali prodaje njihovih podatkov tretjim osebam, slabega nadzora nad dostopom ali kraje teh podatkov (Smith in drugi, 2011). Featherman in drugi (2010, str. 220) so tveganje za izgubo zasebnosti (angl. privacy risk) opredelili kot »porabnikovo subjektivno oceno morebitnih izgub zasebnosti zaupnih osebnih podatkov, ki vključuje oceno možne zlorabe teh informacij, ki lahko povzroči krajo identitete.« Porabniki tako ocenjujejo tudi verjetnost in obsežnost negativnih posledic razkritja osebnih podatkov (Smith in drugi, 2011). Dinev in Hart (2006) sta pokazala, da se bo višja stopnja zaznanega tveganja za zasebnost odražala v višji stopnji zaskrbljenosti posameznikov glede zasebnosti. Prav tako sta pokazala, da bodo zato posamezniki manj pripravljeni razkrivati svoje osebne podatke.

Pripravljenost posameznikov je odvisna tudi od vrste osebnih podatkov, ki jih podjetja želijo pridobiti. Phelps in drugi (2000) so ugotovili, da so posamezniki najbolj pripravljeni deliti svoje demografske podatke (npr. zakonski stan ali zadnji zaključeni letnik izobraževanja) in podatke o življenjskem slogu (npr. najljubši hobiji ali revije). Po drugi strani pa večina porabnikov ni pripravljena deliti podatkov o svojem letnem zaslužku, kreditnih karticah ali številki socialnega zavarovanja. V povezavi z osebnimi podatki so raziskovalci preučevali tudi povezavo med občutljivostjo teh informacij in pripravljenostjo posameznikov za razkrivanje le-teh. Metzger (2007) je ugotovila, da so posamezniki bolj pripravljeni zadržati občutljive informacije, kot so številka kreditne kartice, številka socialnega zavarovanja, kontaktni podatki ali podatki o svojih preferencah. Prav tako je ugotovila, da obstaja večja verjetnost, da bodo namesto teh podatkov uporabili izmišljene podatke.

Poleg zaznanih koristi sta Dinev in Hart (2006) izpostavila tudi pomen zaupanja, saj bodo posamezniki bolj pripravljeni deliti svoje osebne podatke, če so prepričani, da se podjetja ne bodo vedla oportunistično in bodo poskrbela za ustrezno varnost njihovih osebnih podatkov. Podjetja morajo tako najti načine, da povečajo zaupanje svojih uporabnikov (Swani in drugi, 2021). To lahko storijo na primer z uporabo pečatov zasebnosti (angl. privacy seals), kot so TRUSTe, WebTrust ali BBBOnline. Ti služijo kot dokazilo, da so spletne strani in uveljavljene prakse zasebnosti v skladu z zahtevami podeljevalca certifikata (Moores, 2005). Prav tako pa delujejo kot signal za uporabnike, da so te strani vredne zaupanja. Podjetja lahko oblikujejo tudi politiko zasebnosti, s katero uporabnikom pojasnijo, kateri osebni podatki in za kakšne namene bodo zbrani in obdelani. Hkrati pa jih na ta način tudi seznanijo z vsemi ukrepi, s katerimi zagotavljajo varnost njihovih osebnih podatkov (Wu in drugi, 2012).

4.4 Tehnike uporabnikov za zaščito zasebnosti

Zaskrbljenost posameznikov se lahko odraža tudi v njihovem vedenju, saj zaradi prevelikih skrbi ne delijo svojih osebnih podatkov in na ta način ohranjajo nadzor nad njimi (Baruh in drugi, 2017). Po drugi strani pa napredna tehnologija podjetjem omogoča, da podatke zbirajo brez zavedanja uporabnikov. Priprava priporočil, personalizacija vsebin ali druge

prilagoditve spletne izkušnje pogosto temeljijo na vedenjskih podatkih, ki jih uporabniki nezavedno delijo ob uporabi spletnih strani (Zhang in drugi, 2014). Tako nimajo izbire, da bi te podatke lahko zadržali zase, saj so zbrani avtomatsko in ne zahtevajo izrecnega vnosa v sistem (Zhang in drugi, 2014). V tem primeru se uporabniki lahko zaščitijo tudi z uporabo različnih tehnik za zaščito zasebnosti, ki bodo predstavljene v nadaljevanju.

Milne in drugi (2009, str. 450) so zaščitno vedenje opredelili kot »specifična računalniška dejanja, ki jih porabniki izvedejo, da ohranijo svoje osebne podatke na varnem«. Pri tem gre lahko za enostavnejša dejanja, na primer blokiranje piškotkov ali brskanje v anonimnem načinu, ki jih uporabniki sicer pogosto uporabljajo, vendar ne nudijo tako močne zaščite, predvsem v primeru bolj invazivnih metod spletnega sledenja (Boerman in drugi, 2021; Bujlow in drugi, 2017). Po drugi strani pa se uporabniki poslužujejo tudi bolj naprednih zaščitnih metod, na primer šifriranja svojih podatkov, povezav ali komunikacije, ki zagotavljajo višjo stopnjo zaščite zasebnosti, vendar zahtevajo tudi več računalniškega znanja (Boerman in drugi, 2021; Quach in drugi, 2022).

Posamezniki lahko uporabljajo različne tehnike za zaščito svoje zasebnosti na spletu. Quach in drugi (2022) so samozaščitno vedenje posameznikov razdelili v štiri kategorije. V prvo kategorijo spadajo odzivne informacijske strategije, s katerimi si poskušajo uporabniki zagotoviti zasebnost preko upravljanja z vsebinami. Tako lahko brišejo že objavljene informacije ali pa se poskušajo izogniti potrebi po deljenju osebnih podatkov. Prav tako se lahko zaščitijo z uporabo napačnih oziroma izmišljenih informacij. Raziskava, ki jo je izvedlo angleško podjetje RSA, je pokazala, da je 41 % anketirancev že namerno uporabljalo lažne osebne podatke, pri čemer je najpogosteje šlo za podatke o telefonski številki, rojstnem datumu in e-poštnem naslovu (Tan, 2018). V drugo kategorijo spadajo proaktivne informacijske strategije, s katerimi uporabniki poskušajo prikriti svoje osebne podatke ali jih zadržati zase (Quach in drugi, 2022). Uporabniki poskušajo karseda zmanjšati obseg deljenih informacij, pri čemer uporabljajo tehnologije za šifriranje komunikacije ali pa prenehajo z uporabo tehnologije in svoje zadeve urejajo izven spleta.

V tretjo kategorijo spadajo odzivne strategije, ki se jih uporabniki poslužujejo v situacijah, ko so že podali dovoljenje za dostop do svojih informacij, vendar ga želijo kasneje preklicati (Quach in drugi, 2022). Uporabniki pogosto poskušajo pridobiti nazaj del svoje zasebnosti tako, da izbrišejo piškotke, predpomnilnik brskalnika ali zgodovino brskanja. Prav tako lahko uporabljajo razširitve za brskalnike, kot so AdBlock, Ghostery, uBlock, Privacy Badger in Disconnect, ki preprečujejo odpiranje oglasov in blokirajo spletno sledenje (Mehrnezhad in drugi, 2022). Uporabniki lahko podjetja tudi prosijo za izbris svojih podatkov, izbris iz baze kontaktov ali za odstranitev z liste za obveščanje (Quach in drugi, 2022). V zadnjo kategorijo spadajo strategije, s katerimi uporabniki z bolj naprednim tehnološkim znanjem proaktivno nadzirajo dostop do svojih osebnih podatkov. To počnejo tako, da spreminjajo nastavitve zasebnosti, spremljajo protokole spletnih strani ali nameščajo različne protivirusne programe, ki omogočajo visoko stopnjo zaščite zasebnosti. Med te strategije spada tudi uporaba navideznega zasebnega omrežja, s pomočjo katerega

uporabniki ne razkrijejo IP naslova računalnika ter se tako obvarujejo pred invazivnimi metodami spletnega sledenja kot je na primer zajemanje prstnega odtisa naprave (Bujlow in drugi, 2017).

Za boljše razumevanje razlogov, zakaj se posamezniki odločajo za zaščito zasebnosti na spletu, so se raziskovalci poskušali opirati na različne teorije. Metzger (2007) je poskušala vedenje posameznikov razložiti s pomočjo teorije upravljanja komuniciranja zasebnosti. Pravi, da posamezniki oblikujejo meje, s katerimi urejajo dostop do svojih osebnih podatkov. Te meje nato prilagajajo na podlagi vrste in občutljivosti osebnega podatka ter zaznanega tveganja, ki nastane ob deljenju le-tega. Če je zaznano tveganje nizko, potem bodo te meje bolj prepustne in bodo tako razkrili več informacij o sebi (Metzger, 2007). Druga teorija, ki se uporablja za razlago vedenja posameznikov, je varnostno-motivacijska teorija (angl. protection motivation theory). Kot pravi Rogers (1983), je zaščitno vedenje odvisno od dveh dejavnikov: ocenjevanja ogroženosti in ocenjevanja obvladovanja. Posameznikova ocena ogroženosti je odvisna od zaznane resnosti grožnje, zaznane dovzetnosti za tveganja in nagrad ob samozaščitnem ravnanju. Posameznikova ocena obvladovanja je odvisna od zaznane samoučinkovitosti oziroma sposobnosti za spoprijemanje z grožnjo, učinkovitosti samozaščitnega odziva in stroškov, ki nastanejo ob tem odzivu. V primeru, da sta obe grožnji zaznani kot visoki, se bodo posamezniki odzvali s samozaščitnim vedenjem (Rogers, 1983). Boerman in drugi (2021) so s pomočjo te teorije poskušali izboljšati razumevanje vedenja za zaščito zasebnosti na spletu. Ugotovili so, da posamezniki zbiranje in obdelavo osebnih podatkov na spletu ocenjujejo kot ravnanje, ki prinaša visoko stopnjo ogroženosti. Prav tako so ugotovili, da zaznana resnost grožnje in učinkovitost samozaščitnega odziva predstavljata pozitivna napovedovalca samozaščitnega vedenja. Bolj kot bodo posamezniki zbiranje in obdelavo osebnih podatkov zaznali kot resno grožnjo s kritičnimi posledicami za njihovo zasebnost, bolj verjetno bodo poskušali svojo zasebnost zaščititi. Prav tako se posamezniki zavedajo, da obstajajo učinkoviti načini za zaščito lastne zasebnosti na spletu in prav to prepričanje jih bo spodbudilo k samozaščitnem vedenju (Boerman in drugi, 2021).

4.5 Paradoks zasebnosti

Nekatere raziskave so skrbi glede zasebnosti in pripravljenost posameznikov obravnavale kot indikator vedenja posameznikov (Dinev in Hart, 2006). Po drugi strani pa so Norberg in drugi (2007) ugotovili, da se namere posameznika ne odražajo v njihovem vedenju, saj so posamezniki v praksi bolj pripravljeni razkrivati svoje podatke kot nameravajo. Prav tako so posamezniki v zameno za določeno korist pripravljeni deliti svoje osebne podatke kljub poznanim tveganjem (Kokolakis, 2017). Ta neskladja med vedenjem posameznikov in njihovimi prepričanji opisuje paradoks zasebnosti.

Wilson in Valacich (2012) pravita, da prihaja do dveh vrst neskladij. Pri posameznikih lahko prihaja do razlik med izraženo zaskrbljenostjo glede zasebnosti in dejanskim vedenjem. V svoji raziskavi so Boerman in drugi (2021) ugotovili, da posamezniki zbiranje in obdelavo

podatkov vidijo kot skrb vzbujajočo grožnjo z negativnimi posledicami za njihovo zasebnost. Po drugi strani pa so odgovorili, da posamezniki svojo zasebnost le redko varujejo in da uporabljajo zgolj osnovne zaščitne ukrepe, ki niso tako učinkoviti pri varovanju zasebnosti. Drugo vrsto neskladij pa predstavljajo razlike med izraženimi namerami in dejanskim razkrivanjem osebnih podatkov na spletu (Wilson in Valacich, 2012). Norberg in drugi (2007) so izvedli eksperiment, v katerem so sprva študente vprašali o njihovih namerah povezanih z razkrivanjem različnih osebnih podatkov, čez dvanajst tednov pa so bili študenti pozvani naj te iste podatke dejansko delijo s podjetjem. Na podlagi eksperimenta so dokazali, da stopnja dejanskega razkrivanja podatkov močno presega predhodne namere posameznikov.

Želja po razumevanju nasprotujočega vedenja posameznikov je spodbudila številne raziskovalce, da bi s svojimi raziskavami poskušali razložiti, zakaj prihaja do teh neskladij. Prav tako je razumevanje vedenja posameznikov ključnega pomena za podjetja, saj osebni podatki o njihovih strankah predstavljajo temelj za številne spletne aktivnosti (Chellappa in Sin, 2005). Podobno kot pri raziskavah o zasebnosti in z njo povezano zaskrbljenostjo tudi v tem primeru raziskovalci niso prišli do enotnih ugotovitev. V nadaljevanju bom predstavila nekatere razlage za pojav paradoksa zasebnosti, ki se pojavljajo v literaturi, kot tudi nekatere razloge, zakaj prihaja do razlik pri obrazložitvah tega vedenja.

Kot sem izpostavila že v prejšnjih poglavjih, nekateri raziskovalci proces odločanja posameznikov glede razkrivanja svojih osebnih podatkov obravnavajo kot primerjavo zaznanih koristi in tveganj. Posameznik ob primerjavi tako ravna racionalno in se odloči za deljenje svojih osebnih podatkov, če zaznane koristi odtehtajo vsa zaznana tveganja (Dinev in Hart, 2006). Kokolakis (2017) pravi, da je lahko ta proces navzven nerazumljiv, saj lahko posamezniki pri svojem odločanju upoštevajo tudi bolj neoprijemljive koristi, ki jim pripisujejo velik pomen, in tako izničijo vpliv zaskrbljenosti drugih tveganj. Prav tako na posameznika in njegov proces odločanja vplivajo različni situacijski dejavniki. Če podjetja uspejo zmanjšati zaznana tveganja svojih uporabnikov in jih obenem uspejo prepričati o prednostih razkrivanja svojih podatkov, bodo bolj uspešna pri pridobivanju teh podatkov (Wilson in Valacich, 2012).

Čeprav so predhodno omenjeno razlago sprejeli številni avtorji, se nekateri raziskovalci ne strinjajo, da se lahko posamezniki v tem primeru vedejo povsem racionalno. Acquisti in Grossklags (2005) pravita, da posamezniki v procesu odločanja nimajo celovitih informacij o vseh koristih in tveganjih ter razsežnostih njihovih posledic, da bi lahko sprejeli ustrezno odločitev. Prav tako prihaja do asimetrije informacij, pri čemer posamezniki pogosto sploh niso v celoti seznanjeni z načini zbiranja njihovih osebnih podatkov in nameni, za katere bodo uporabljeni. Zaradi nepopolnih informacij lahko tako pripisujejo previsoko ali prenizko vrednost zaznanim koristim ali tveganjem in se zato odločijo za razkrivanje svojih osebnih podatkov kljub zaskrbljenosti glede svoje zasebnosti (Acquisti in Grossklags, 2005).

Tudi v primeru, da bi posamezniki imeli na voljo vse potrebne informacije, ne bi bili sposobni predelati tako velike količine informacij in vseh scenarijev, ki vključujejo možne posledice njihovih dejanj (Acquisti in Grossklags, 2005). Tako je v primerih, ko se posamezniki odločajo o razkrivanju svojih osebnih podatkov, njihova racionalnost omejena, zato se pričnejo zanašati na različne hevristike in kognitivne pristranskosti, s katerimi si olajšajo obdelavo vseh informacij in sprejemanje končne odločitve. Sundar in drugi (2020) so na primer ugotovili, da ugled in prepoznavnost podjetja ter transparentnost njihovih praks za zagotavljanje zasebnosti na spletu posameznikom zagotavljajo občutek varnosti glede njihovih osebnih podatkov, zaradi česar so lažje in hitreje pripravljeni razkrivati svoje podatke. Poleg tega lahko podjetja z različnimi signali spodbudijo uporabo hevristik. Tako lahko na primer preko izgleda svojih spletnih strani, kjer prikazujejo varnostne certifikate ali ocene in izkušnje drugih uporabnikov, izkazujejo svojo verodostojnost in zanesljivost, s čimer vplivajo na proces ocenjevanja zaznanih koristi in tveganj (Sundar in drugi, 2020). Prav tako pa lahko tudi posameznik sam pride do neracionalnih odločitev zaradi kognitivnih pristranskostih. Acquisti in Grossklags (2007) pravita, da lahko pride do razkrivanja osebnih podatkov, ker posamezniki dajejo prednost takojšnjim koristim in zanemarijo kasnejša tveganja. Hkrati se lahko odločijo za deljenje svojih osebnih podatkov, ker mislijo, da se negativne posledice, kot sta na primer kraja identitete ali zloraba osebnih podatkov, njim ne morejo zgoditi (Acquisti in Grossklags, 2007).

Po drugi strani pa nekateri avtorji v svojih člankih izražajo dvom v obstoj paradoksa. Solove (2020) trdi, da paradoks zasebnosti sploh ne obstaja, ampak je posledica prevelikega posploševanja pri oblikovanju ugotovitev empiričnih raziskav. Pravi, da je vedenje posameznikov močno odvisno od konteksta situacije, v kateri se posameznik v tistem trenutku nahaja. Tako bo v določeni situaciji bolj zadržan pri deljenju svojih osebnih podatkov, medtem ko bo v drugi situaciji razkril več informacij o sebi, kar pa ne pomeni, da posameznik zato nima skrbi glede svoje zasebnosti (Solove, 2020). Posamezniki morda prav tako ne bodo izrazili zaskrbljenosti glede zasebnosti, saj se njihovo pojmovanje zasebnosti razlikuje od tistega, ki je predstavljeno v raziskavi. Prav tako ne bodo nujno izrazili skrbi glede svoje zasebnosti, ker že uporabljajo različne tehnike za varovanje zasebnosti in se jim zato njihova zasebnost zdi manj ogrožena (Colnago in drugi, 2023).

Kokolakis (2017) opozarja, da lahko do razlik v ugotovitvah prihaja tudi zaradi razlik v metodoloških pristopih. Številni raziskovalci kot metodo za empirično raziskovanje paradoksa zasebnosti pogosto uporabljajo ankete, ki niso najbolj zanesljiva metoda za preučevanje spreminjajočega vedenja. Prav tako lahko posamezniki v anketah nepravilno poročajo o svojem vedenju, ki ne odraža njihovega vedenja v realnih situacijah (Solove, 2020). Nekateri raziskovalci so v svojih raziskavah izvedli eksperimente, ki pa vseeno ne morejo odpraviti težav s posploševanjem rezultatov. Poleg tega pa je tudi pri eksperimentih težko poustvariti situacije, v katerih bi se posamezniki vedli točno tako kot v realnih situacijah (Kokolakis, 2017).

5 EMPIRIČNA RAZISKAVA VLOGE ZASEBNOSTI V ODNOSU UPORABNIKOV DO SPLETNE PERSONALIZACIJE

Številne dosedanje raziskave na področju zasebnosti so poskušale predstaviti in pojasniti njeno vlogo v interakciji porabnikov in podjetij na spletu. Tako so poskušale razložiti preplet različnih dejavnikov, povezanih z zaskrbljenostjo uporabnikov, ki vplivajo na njihova stališča in odnos do različnih spletnih trženjskih aktivnosti in na spletno vedenje uporabnikov. Raziskave, ki so preučevale vlogo zasebnosti v povezavi s spletno personalizacijo, so se osredotočale predvsem na personalizirano oglaševanje, medtem ko je vloga zasebnosti pri ostalih oblikah spletne personalizacije manj raziskana. Na podlagi teoretičnih in empiričnih spoznanj iz literature o spletni personalizaciji in zasebnosti tako v nadaljevanju opredelim namen in cilje kvantitativne raziskave, zastavim raziskovalne hipoteze in oblikujem strukturiran anketni vprašalnik, s pomočjo katerega poskušam ugotoviti, kakšna je vloga zasebnosti v odnosu uporabnikov do spletne personalizacije. Na koncu predstavim ključne ugotovitve, omejitve kvantitativne raziskave, priporočila za nadaljnje raziskave in implikacije za podjetja.

5.1 Namen in cilji kvantitativne raziskave

Namen kvantitativne raziskave je preučiti vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije in ugotoviti, na kakšen način zaskrbljenost uporabnikov vpliva na njihova stališča in pripravljenost za deljenje osebnih podatkov za pripravo personaliziranih vsebin. S pomočjo kvantitativne raziskave bom tako preverila, ali ugotovitve dosedanjih raziskav na področju zasebnosti veljajo tudi v primeru spletne personalizacije. Ugotovitve kvantitativne raziskave bodo tržnikom v pomoč pri razumevanju uporabnikov in njihovih stališč. Tako bodo lahko oblikovali učinkovitejše in uporabnikom prijaznejše personalizirane spletne izkušnje.

Cilj kvantitativne raziskave je raziskati, ali obstaja povezava med zasebnostjo uporabnika in njegovim odnosom do spletne personalizacije. Ugotoviti želim, ali prihaja do razlik v stališču do spletne personalizacije pri posameznikih z različno stopnjo zaskrbljenosti glede zasebnosti. Prav tako želim preveriti, ali prihaja do razlik v stopnji zaskrbljenosti glede zasebnosti pri uporabnikih iz različnih starostnih skupin. V okviru kvantitativne raziskave se navežem tudi na pripravljenost uporabnikov za deljenje svojih podatkov, pri čemer želim ugotoviti, katere podatke so uporabniki pripravljeni deliti v zameno za personalizirane vsebine. Ugotoviti želim tudi, ali zaznane koristi in zaskrbljenost uporabnikov vplivajo na njihovo pripravljenost za deljenje svojih podatkov. Na koncu se navežem še na tehnike za zaščito zasebnosti, pri čemer želim ugotoviti, ali obstaja povezava med verjetnostjo uporabe teh tehnik in zaskrbljenostjo uporabnikov.

5.2 Raziskovalne hipoteze

Na podlagi dosedanjih raziskav in teoretičnih spoznanj iz znanstvene in strokovne literature sem oblikovala sedem hipotez, ki se nanašajo na zastavljene cilje kvantitativne raziskave. V nadaljevanju so zapisane utemeljitve zastavljenih hipotez.

Zaskrbljenost glede zasebnosti predstavlja osrednjo tematiko številnih raziskav, ki so se ukvarjale z vlogo zasebnosti v trženju. Phelps in drugi (2000) so na primer ugotovili, da je večina porabnikov zaskrbljenih glede tega, kako podjetja uporabljajo njihove podatke, in da si želijo, da bi imeli večji nadzor nad zbiranjem in uporabo svojih osebnih podatkov. Strycharz in drugi (2019) so ugotovili, da zaskrbljenost glede zasebnosti predstavlja najpogostejše tveganje, ki so ga posamezniki zaznali v povezavi s personaliziranim oglaševanjem. Zaskrbljenost posameznikov v povezavi z zbiranjem in obdelavo podatkov so pokazale tudi številne javnomnenjske ankete (Auxier in drugi, 2019; Statista, 2019). Ker zbiranje in uporaba podatkov predstavljata enega izmed ključnih elementov pri oblikovanju personaliziranih ponudb, bodo podjetja ob pripravi le-teh posegala v zasebnost uporabnikov. Tako predpostavljam, da bo ta poseg v zasebnost tudi v primeru spletne personalizacije privedel do negativnih občutkov in zaskrbljenosti glede zasebnosti.

Hipoteza 1: Uporabniki so na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije.

Podjetja v procesu spletne personalizacije posegajo v zasebnost posameznikov, saj morajo za pripravo personaliziranih ponudb zbirati in obdelovati njihove osebne podatke. Tako se lahko pri posameznikih pojavi zaskrbljenost glede zasebnosti, saj nimajo več nadzora nad svojimi osebnimi podatki (Smith in drugi, 2011). Hkrati se na ta način izpostavijo različnim tveganjem za zlorabo svojih osebnih podatkov, saj bi lahko podjetja te podatke brez dovoljenja delila z drugimi osebami (Dinev in Hart, 2006). Poleg neprimernega ravnanja podjetij s podatki lahko pride tudi do drugih negativnih posledic, kot je na primer kraja podatkov v primeru vdora v podatkovno bazo podjetja (Featherman in drugi, 2010). Poleg predhodno omenjenih tveganj so Toch in drugi (2012) prepoznali še druga tveganja, ki se pojavijo v primeru spletne personalizacije. Podjetja lahko tako zbrane podatke uporabijo za številne druge namene, na primer v različnih personaliziranih ponudbah ali trženjskih aktivnostih, kar lahko pri uporabnikih vzbudi negativne občutke. Prav tako za namen personalizacije zbirajo podatke o lokaciji uporabnika, kar ogroža njegovo varnost, saj lahko nepooblaščene osebe pridejo do teh podatkov in jih izkoristijo (Toch in drugi, 2012). Na podlagi ugotovitev iz preteklih raziskav predpostavljam, da bodo posamezniki, ki so bolj zaskrbljeni glede svoje zasebnosti, prepoznali tveganja, kar se bo negativno odražalo v njihovem stališču do spletne personalizacije.

Hipoteza 2: Uporabniki, ki so bolj zaskrbljeni glede zasebnosti, imajo bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni.

Po drugi strani pa lahko negativne posledice in zaskrbljenost uporabnikov glede visoke verjetnosti negativnih posledic odvrnejo od deljenja informacij za pripravo personaliziranih ponudb. Dinev in Hart (2006) sta ugotovila, da je zaskrbljenost posameznikov negativno povezana z njihovo pripravljenostjo za razkrivanje svojih osebnih podatkov, saj se želijo posamezniki na ta način izogniti negativnim posledicam in tveganjem, kot so na primer zloraba osebnih podatkov, prost dostop do teh podatkov brez njihovega zavedanja ter prodaja teh podatkov drugim deležnikom. Podobno pravita tudi Chellappa in Sin (2005), ki sta ugotovila, da zaskrbljenost posameznikov glede zasebnosti anonimnih, nedoločljivih in določljivih osebnih podatkov negativno vpliva na njihovo pripravljenost za deljenje teh podatkov za namen personalizacije. Na podlagi teh ugotovitev tako predlagam naslednjo hipotezo:

Hipoteza 3: Zaskrbljenost uporabnikov je negativno povezana z njihovo pripravljenostjo za deljenje svojih osebnih podatkov za namen spletne personalizacije.

Raziskovalci so v svojih raziskavah preučevali različne dejavnike, ki vplivajo na zaskrbljenost posameznikov glede zasebnosti. Med te dejavnike spadajo tudi demografske značilnosti posameznikov. Raziskovalci so tako na primer preučevali vpliv starosti na zaskrbljenost posameznikov glede svoje zasebnosti. Paine in drugi (2007) so v okviru svoje raziskave ugotovili, da prihaja do razlik v stopnji zaskrbljenosti med uporabniki različnih starosti, pri čemer so ugotovili, da so starejši uporabniki bolj zaskrbljeni glede svoje zasebnosti. Podobno so ugotovili tudi Lee in drugi (2019), saj je njihova raziskava pokazala, da se pri porabnikih stopnja zaskrbljenosti povečuje s starostjo. Po drugi strani pa so ugotovili, da pri porabnikih nad petdesetim letom stopnja zaskrbljenosti prične padati s starostjo, kar so pripisali temu, da starejši ljudje manj pogosto ali v manjšem obsegu uporabljajo spletne storitve. Na podlagi ugotovitev iz preteklih raziskav predlagam naslednjo hipotezo:

Hipoteza 4: Uporabniki različnih starostnih skupin so različno zaskrbljeni glede zasebnosti v primeru spletne personalizacije.

Spletna personalizacija prinaša koristi tako za podjetja kot za uporabnike. Podjetja lahko na podlagi zbranih podatkov o svojih uporabnikih in njihovem spletnem vedenju oblikujejo prilagojene ponudbe, ki ustrezajo njihovim potrebam in željam (Murthi in Sarkar, 2003). Prav tako jim lahko ponudijo priporočila za izdelke ali vsebine, ki bi jih utegnili zanimati (Adomavicius in drugi, 2008). Obenem pa s pomočjo spletne personalizacije podjetja zmanjšajo obseg informacij, ki jih morajo uporabniki upoštevati, zato lahko slednji hitreje in učinkoviteje sprejemajo svoje odločitve (Liang in drugi, 2006). Zaznane koristi predstavljajo pomemben dejavnik v procesu odločanja uporabnikov glede razkrivanja svojih osebnih podatkov. Uporabniki pri odločanju tako primerjajo zaznana tveganja in koristi in se odločijo za razkrivanje svojih podatkov, če zaznane koristi odtehtajo vsa tveganja, ki se jim v tem primeru izpostavijo. Bol in drugi (2018) so v svoji raziskavi potrdili, da bodo posamezniki, ki pričakujejo več koristi, bolj verjetno razkrivali svoje podatke. Podobno sta

dokazala tudi Fernandes in Pereira (2021), saj sta ugotovila, da tako utilitarne koristi (npr. dostop do popustov) kot tudi hedonistične koristi (npr. dostop do zabavnih vsebin) pozitivno vplivajo na pripravljenost uporabnikov za deljenje svojih osebnih podatkov. Na podlagi literature tako oblikujem naslednjo hipotezo:

Hipoteza 5: Zaznane koristi so pozitivno povezane s pripravljenostjo uporabnikov za deljenje svojih podatkov za namen spletne personalizacije.

Podjetja s pomočjo naprednih tehnologij in digitalnih sistemov pridobijo dostop tako do osebnih podatkov, ki omogočajo identifikacijo posameznih uporabnikov, kot tudi do podatkov o njihovem spletnem vedenju, preferencah in interesih (Liu in drugi, 2023; Zheng in Peltsverger, 2015). Raziskovalci so v preteklih raziskavah ugotovili, da se pripravljenost posameznikov za deljenje podatkov razlikuje tudi glede na vrste podatkov, ki jih podjetja želijo pridobiti. Metzger (2007) je v svoji raziskavi ugotovila, da so posamezniki najbolj pripravljeni deliti določene osebne identifikacijske podatke, kot sta ime in zvezna država, iz katere prihajajo. Fernandes in Pereira (2021) sta v svoji raziskavi izpostavila, da je pripravljenost posameznikov povezana z občutljivostjo določene vrste osebnega podatka, saj so posamezniki bolj zaskrbljeni glede negativnih posledic razkrivanja le-teh. Metzger (2007) je v svoji raziskavi ugotovila, da posamezniki podatek o svojem imenu zaznavajo kot enega izmed najmanj občutljivih podatkov. Na podlagi teh ugotovitev predpostavljam, da bodo uporabniki najbolj pripravljeni deliti svoje ime tudi za namen spletne personalizacije. Prav tako personalizacija na podlagi imena predstavlja eno izmed bolj osnovnih vrst personalizacije, ki ne posega pretirano v zasebnost uporabnika, saj ime uporabniki v večini primerov zavestno delijo s podjetjem.

Hipoteza 6: Uporabniki so najbolj pripravljeni deliti podatek o svojem imenu v zameno za personalizirane ponudbe.

Uporabniki se lahko pred negativnimi posledicami zaščitijo tudi z uporabo različnih tehnik za zaščito svoje zasebnosti na spletu. Spletna personalizacija, predvsem v obliki priporočil izdelkov ali vsebin, temelji tudi na vedenjskih podatkih, ki jih uporabniki posredno in nezavedno delijo s podjetji ob uporabi priporočilnih sistemov ali premikanju po spletnih straneh (Zhang in drugi, 2014). Uporabniki se lahko tako z uporabo tehnik zaščitijo pred morebitnim zbiranjem osebnih podatkov ali pa z njihovo pomočjo poskušajo pridobiti nazaj nadzor nad njimi. To lahko storijo na primer z brisanjem piškotkov ali brisanjem zgodovine brskanja (Quach in drugi, 2022). Baruh in drugi (2017) so na podlagi metaanalize različnih študij v povezavi z zasebnostjo na spletu ugotovili, da obstaja pozitivna povezava med zaskrbljenostjo uporabnikov in zaščitnim vedenjem. Podobno je v svojem preglednem članku izpostavila tudi Kokolakis (2017). Na podlagi teh ugotovitev predlagam naslednjo hipotezo:

Hipoteza 7: Zaskrbljenost uporabnikov glede zasebnosti je pozitivno povezana z njihovo stopnjo verjetnosti uporabe tehnik za zaščito svoje zasebnosti.

5.3 Metodologija kvantitativne raziskave

V okviru empirične raziskave sem se odločila za kvantitativno raziskavo, pri čemer sem primarne podatke zbirala s pomočjo spletne ankete. Izbrana metoda ustreza namenu in zastavljenim ciljem raziskave, saj želim med drugim preučevati povezave med spremenljivkami in primerjati skupine uporabnikov z različnimi značilnostmi, kar zahteva večji vzorec porabnikov. Ta metoda je ena izmed najbolj priljubljenih metod za zbiranje primarnih podatkov, saj omogoča hiter in enostaven način zbiranja podatkov, ki jih je nato mogoče analizirati s statističnimi testi in rezultate posplošiti na širšo populacijo. Prav tako lahko s pomočjo spletne ankete hitro dosežemo posameznike na širšem geografskem območju ter jim omogočimo, da anketo rešijo takrat, ko jim to najbolj ustreza. Metoda prinaša prednosti tudi za raziskovalce, saj je mogoče anketne vprašalnike enostavno prilagoditi potrebam raziskave in zastavljenim ciljem. Prav tako lahko zbrane podatke hitro in učinkovito analizirajo. Po drugi strani pa se moramo zavedati tudi slabosti spletnih anket, kot so na primer visoka verjetnost napačnih odgovorov, težave pri doseganju določenih skupin porabnikov, nizke stopnje odzivanja, itd. (Malhotra, 2013).

Za raziskovalni inštrument sem uporabila strukturiran spletni anketni vprašalnik, ki vsebuje 15 vprašanj zaprtega tipa. Vprašanja so razporejena v 6 sklopov. Posamezna vprašanja sem oblikovala na podlagi pregleda literature in zastavljenih hipotez. Kjer je bilo mogoče, sem uporabila preverjene merske lestvice iz preteklih raziskav in jih prilagodila, da so ustrezale namenu moje raziskave. Anketni vprašalnik je priložen v Prilogi 1.

Prvi sklop vprašanj zajema dve splošni vprašanji. Prvo se navezuje na prosti čas, ki ga uporabniki preživijo na spletu. Z drugim vprašanjem pa sem želela preveriti, kako pogosto se uporabniki srečujejo z različnimi oblikami personalizacije, ki sem jih našla v literaturi. Uporabila sem petstopenjsko lestvico pogostosti (od »nikoli« do »vsak dan«).

Drugi sklop vprašanj se navezuje na stališča uporabnikov glede spletne personalizacije in koristi, ki jih ta prinaša uporabnikom. Pri vprašanjih o spletni personalizaciji sem se pri oblikovanju vprašanj osredotočila na spletne strani in personalizirane spletne vsebine, zato da so vprašanja bolj razumljiva, saj si anketiranci tako lažje predstavljajo, na kaj se spletna personalizacija nanaša. Pri tretjem vprašanju sem za merjenje stališč uporabnikov uporabila petstopenjsko lestvico, pri kateri so lahko z odgovorom izrazili, kako jim je všeč, če jim spletna stran ponudi personalizirane vsebine. Lestvica obsega pet odgovorov, od »sploh mi ni všeč« do »zelo mi je všeč«. Pri četrtem vprašanju me je zanimalo, v kolikšni meri se anketiranci strinjajo s trditvami o koristih spletne personalizacije. Uporabila sem petstopenjsko Likertovo lestvico (od 1 - Sploh se ne strinjam do 5 – Popolnoma se strinjam), ki sem jo priredila po Bol in drugi (2018), da je ustrezala kontekstu spletne personalizacije.

Tretji sklop vprašanj se nanaša na pripravljenost uporabnikov za deljenje svojih podatkov. Pri petem vprašanju sem s pomočjo petstopenjske lestvice želela preveriti pripravljenost uporabnikov za deljenje podatkov v zameno za personalizirane spletne vsebine. Anketiranci

so lahko podali odgovore od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a«. Pri šestem vprašanju sem želela preveriti, katere vrste podatkov so uporabniki pripravljeni deliti v zameno za personalizirane spletne vsebine. Možne odgovore sem črpala iz raziskav Metzger (2007) in Kaniewska-Sejba in Pilarczyk (2014), pri čemer sem izbrala tiste podatke, ki se lahko uporabijo za personalizacijo vsebin.

Četrti sklop vprašanj se nanaša na zaskrbljenost uporabnikov glede zasebnosti na spletu. Pri sedmem vprašanju sem merila zaskrbljenost uporabnikov glede zasebnosti v primeru spletne personalizacije. Uporabila sem petstopenjsko Likertovo lestvico, ki sem jo prilagodila od Xu in drugi (2008) in Dinev in Hart (2006). Ti dve raziskavi sta svoje merske lestvice oblikovali glede na lestvico Skrb glede informacijske zasebnosti, ki so jo oblikovali Smith in drugi (1996). Osmo vprašanje se je nanašalo na zaupanje uporabnikov glede ravnanja spletnih strani, ki uporabljajo njihove podatke za spletno personalizacijo. Pri tem sem prilagodila petstopenjsko Likertovo lestvico avtorjev Bol in drugi (2018). Deveto vprašanje se je nanašalo na tveganja, povezana z zasebnostjo, pri čemer sem trditve prilagodila po Dinev in Hart (2006). Anketiranci so lahko izbirali med tremi odgovori in sicer, »nizko tveganje«, »srednje tveganje« in »visoko tveganje«.

Peti sklop vprašanj se nanaša na samozaščitno vedenje v primeru spletne personalizacije in tehnike za zaščito zasebnosti na spletu. Z desetim vprašanjem sem želela preveriti, kako verjetno se bodo uporabniki odločili za zaščito svojih podatkov v primeru spletne personalizacije. Uporabila petstopenjsko lestvico verjetnosti (od »zelo malo verjetno« do »zelo verjetno«). Pri oblikovanju tega vprašanju sem se zgledovala po Boerman in drugi (2021). Z enajstim vprašanjem sem želela preveriti pogostost uporabe različnih tehnik za zaščito zasebnosti. Uporabila sem petstopenjsko lestvico pogostosti (od »nikoli« do »vsak dan«). Možne odgovore sem črpala iz raziskave Boerman in drugi (2021) in pregledane literature.

Zadnji sklop vprašanj obsega štiri sociodemografska vprašanja: spol, starost, stopnja izobrazbe in trenutni status.

Pred izvedbo raziskave sem anketni vprašalnik testirala na 10 anketirancih, ki sem jih prosila, da podajo svoje komentarje glede jasnosti in razumljivosti vprašanj ter opozorijo na možne težave pri izpolnjevanju vprašalnika. Na podlagi njihovih odgovorov sem prilagodila anketni vprašalnik in ga objavila na spletnem portalu 1ka.si. Anketni vprašalnik je bil na portalu objavljen od 10. do 18. julija 2023. Povezavo do vprašalnika sem objavila na družbenem omrežju Facebook in različnih forumih, saj sem želela zajeti čim širši vzorec anketirancev. Prav tako sem povezavo delila s prijatelji in znanci preko elektronskih sporočil. Za namen kvantitativne raziskave sem tako uporabila neverjetnostno obliko vzorčenja, in sicer priložnostno vzorčenje, ki ne omogoča, da je vzorec reprezentativen in da bi rezultate raziskave lahko posplošili na celotno populacijo.

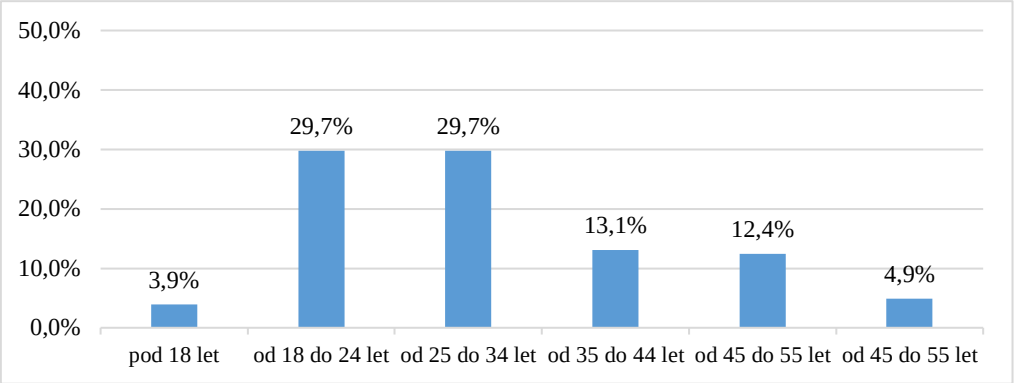
5.4 Analiza rezultatov

Zbrane podatke sem analizirala s pomočjo programa SPSS, s katerim sem izračunala frekvenčne porazdelitve in opisne statistike ter izvedla statistične teste za preverjanje zastavljenih hipotez. Pri pripravi in čiščenju podatkov ter vizualizaciji rezultatov sem si pomagala s programom Microsoft Excel. V nadaljevanju bom najprej predstavila vzorec, nato opisne statistike in na koncu še rezultate preverjanja zastavljenih hipotez.

5.4.1 Predstavitev vzorca

Anketni vprašalnik je pričelo izpolnjevati 376 anketirancev, vendar ga 70 oseb ni izpolnilo v celoti. Nepopolno izpolnjeni vprašalniki so bili v celoti izločeni, zato je vzorec za nadaljnjo analizo in preverjanje hipotez obsegal 306 oseb. Vzorec sestavlja 57,8 % moških (n = 177) in 34,0 % žensk (n = 104). 25 anketirancev (8,2 %) ni želelo podati odgovora glede spola. Slika 2 predstavlja starostno strukturo anketirancev, pri čemer sta najbolj zastopani starostni skupini od 18 do 24 let in od 25 do 34 let (vsaka 29,7 %). Sledita starostna skupina od 35 do 44 let (13,1 %) in od 45 do 55 let (12,4 %). Najmanjši delež anketirancev spada v starostno skupino nad 55 let (4,9 %) in pod 18 let (3,9 %). 19 anketirancev (6,2 %) ni želelo podati odgovora glede starosti.

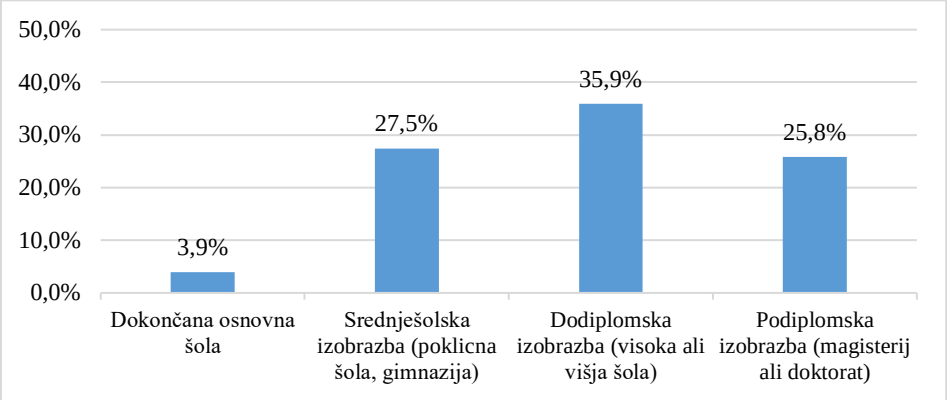
Slika 2: Starostna struktura anketirancev (n = 306)



Vir: lastno delo.

Kot je prikazano na sliki 3, ima največji delež anketirancev (35,9 %) dokončano dodiplomsko izobrazbo, sledijo tisti, ki imajo dokončano srednješolsko izobrazbo (27,5 %) in podiplomsko izobrazbo (25,8 %). Najmanjši delež predstavljajo anketiranci z dokončano osnovo šolo (3,9 %). Na to vprašanje ni želelo odgovoriti 21 anketirancev (6,9 %).

Slika 3: Najvišja dosežena formalna izobrazba anketirancev (n = 306)



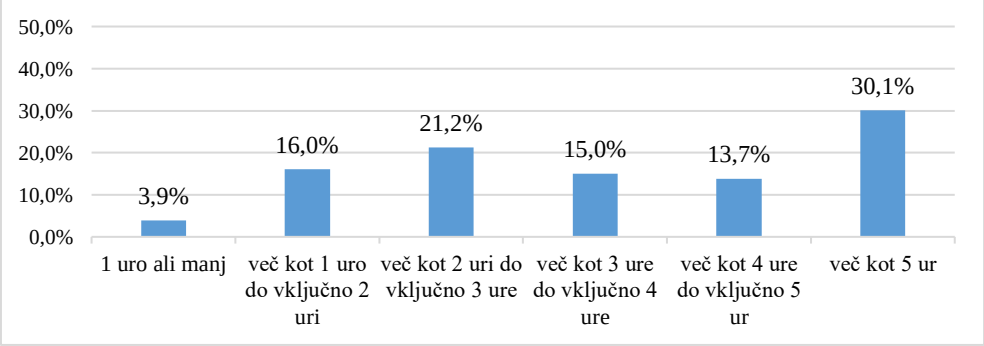
Vir: lastno delo.

Zadnje izmed sociodemografskih vprašanj se nanaša na trenutni status anketirancev, pri čemer največji delež vzorca predstavljajo zaposleni (51,6 %). Nato sledijo študenti, ki predstavljajo 29,7 % vseh anketirancev. Ostale skupine so precej manj zastopane in sicer, 6,2 % anketirancev je dijakov, 3,9 % anketirancev je brezposelnih in 1,0 % anketirancev je upokojenih. 7,5 % anketirancev ni želelo podati svojega odgovora na to vprašanje.

5.4.2 Opisne statistike

S prvim vprašanjem sem želela ugotoviti, koliko prostega časa v dnevu anketiranci preživijo na spletu. Več kot polovica anketirancev (58,8 %) dnevno preživi na spletu več kot 3 ure svojega prostega časa. Kot je razvidno s slike 4, največji odstotek anketirancev (30,1%) dnevno na spletu preživi več kot 5 ur svojega prostega časa. 21,2 % anketirancev pa na spletu dnevno preživi več kot 2 uri do vključno 3 ure svojega prostega časa. Sledijo tisti, ki na spletu preživijo več kot 1 uro do vključno 2 uri (16,0 %) ter tisti, ki preživijo več kot 3 ure do vključno 4 ure (15,0 %). 13,7 % anketirancev na dan preživi na spletu več kot 4 ure do vključno 5 ur. Precej manj, in sicer 3,9 % anketirancev, na dan preživi 1 uro ali manj na spletu.

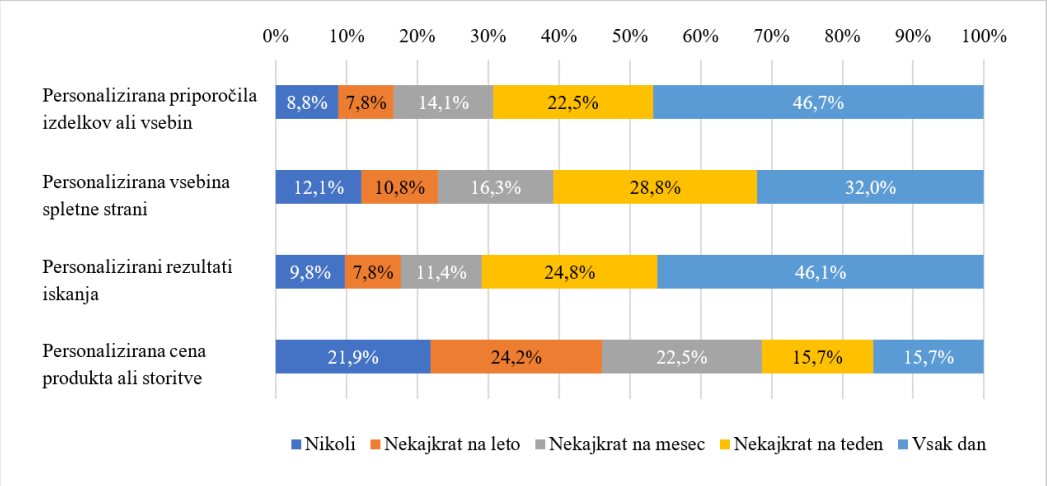
Slika 4: Prosti čas, ki ga anketiranci dnevno preživijo na spletu (n = 306)



Vir: lastno delo.

Z drugim vprašanjem sem želela ugotoviti, kako pogosto se anketiranci srečujejo s posameznimi oblikami spletne personalizacije. Kot je razvidno s slike 5, se največji delež anketirancev pogosto srečuje s personaliziranimi rezultati iskanja, saj se skoraj 71 % anketirancev s to obliko personalizacije srečuje vsaj nekajkrat na teden. Prav tako se anketiranci pogosto srečujejo tudi s personaliziranimi priporočili za izdelke, pri čemer je 46,7 % anketirancev odgovorilo, da se s to obliko personalizacije srečujejo vsakodnevno, medtem ko se 22,5 % anketirancev s personaliziranimi priporočili srečuje nekajkrat na teden. V primeru personalizirane vsebine spletnih strani se 32,0 % anketirancev s to obliko personalizacije srečuje vsakodnevno in 28,8 % nekajkrat na teden. V primerjavi s prejšnjima dvema oblikama personalizacija se s personalizirano vsebino spletnih strani redkeje srečuje večji delež anketirancev, saj je vse preostale tri odgovore (»nekajkrat na mesec«, »nekajkrat na leto« in nikoli«) v tem primeru izbralo največ anketirancev. S personaliziranimi cenami izdelka ali storitve se pogosto srečuje najmanjši delež anketirancev, saj je 15,7 % anketirancev izbralo odgovor »vsak dan« in 15,7 % odgovor »nekajkrat na teden«. Prav tako je med vsemi oblikami personalizacije največji delež anketirancev v primeru personaliziranih cen izbral odgovor »nikoli« in sicer 21,9 %. Ob tem naj poudarim, da je pri tem vprašanju šlo za anketirančevo zaznavanje izpostavljenosti, ne objektivno merjenje izpostavljenosti spletni personalizaciji.

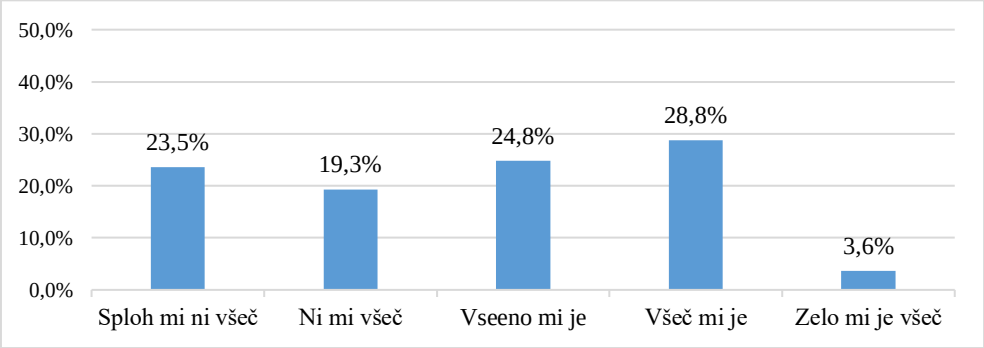
Slika 5: Pogostost srečevanja z različnimi oblikami personalizacije (n = 306)



Vir: lastno delo.

Tretje vprašanje se navezuje na stališča uporabnikov glede spletne personalizacije, pri čemer sem želela ugotoviti, ali je anketirancem všeč, če jim spletne strani ponudijo personalizirane vsebine glede na njihove interese. Kot je razvidno s slike 6, je največ anketirancev (28,8 %) odgovorilo, da jim je všeč, če jim spletne strani ponudijo personalizirane vsebine. Po drugi strani pa lahko vidimo, da ima večji delež anketirancev bolj negativno stališče do personaliziranih vsebin, saj je 42,8 % anketirancev izbralo odgovor »sploh mi ni všeč« ali »ni mi všeč«, medtem ko je 32,4 % anketirancev izbralo odgovor »všeč mi je« ali »zelo mi je všeč«. Skoraj četrtina anketirancev pa ima do spletne personalizacije nevtralno stališče.

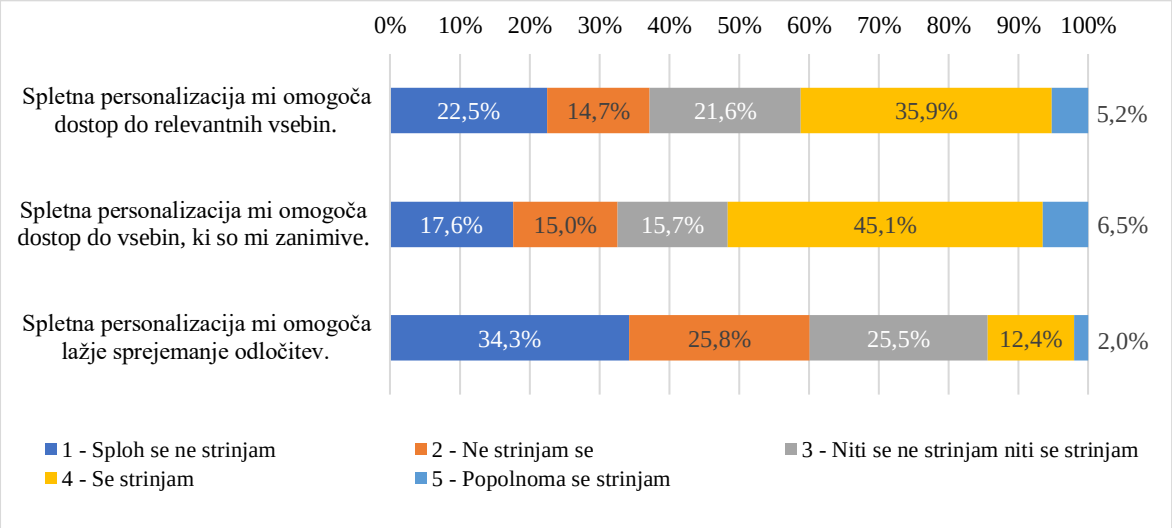
Slika 6: Stališče anketirancev do spletne personalizacije (n = 306)



Vir: lastno delo.

Pri naslednjem vprašanju so anketiranci izrazili, v kolikšni meri se strinjajo s trditvami glede koristi, ki jih zanje prinaša spletna personalizacija. Anketiranci so svoje odgovore podali na lestvici od 1 (sploh se ne strinjam) do 5 (popolnoma se strinjam). Slika 7 prikazuje porazdelitve odgovorov anketirancev po posameznih trditvah. Pri prvi trditvi se je največji delež anketirancev (35,9 %) strinjal, da spletna personalizacija omogoča dostop do relevantnih vsebin. Sledijo tisti, ki se s trditvijo sploh ne strinjajo (22,5 %) ter tisti, ki se s trditvijo niti ne strinjajo niti strinjajo (21,6 %). 14,7 % anketirancev se s trditvijo ne strinja. Med anketiranci je najmanjši delež (5,2 %) tistih, ki se s trditvijo popolnoma strinjajo. Pri drugi trditvi se prav tako največji delež anketirancev (45,1 %) strinja, da spletna personalizacija omogoča dostop do zanimivih vsebin. Sledijo tisti, ki se s trditvijo sploh ne strinjajo (17,6 %), ter tisti, ki se s trditvijo niti ne strinjajo niti strinjajo (15,7 %). 15,0 % anketirancev je odgovorilo, da se s trditvijo ne strinjajo, medtem ko je najmanj anketirancev (6,5 %) odgovorilo, da se s trditvijo popolnoma strinjajo. Pri zadnji trditvi je največ anketirancev (34,3 %) odgovorilo, da se popolnoma ne strinjajo, da spletna personalizacija omogoča lažje sprejemanje odločitev. Sledijo tisti, ki se s to trditvijo ne strinjajo (25,8 %) ter tisti, ki se s to trditvijo niti ne strinjajo niti strinjajo (25,5 %). 12,4 % anketirancev se s to trditvijo strinja, medtem ko se zgolj 2,0 % anketirancev s to trditvijo popolnoma strinja. Na podlagi odgovorov anketirancev sem za vsako trditev izračunala tudi aritmetično sredino (AS) in standardni odklon (SD). Rezultati kažejo, da se anketiranci v povprečju ne strinjajo z zadnjo trditvijo glede olajšanja sprejemanja odločitev (AS = 2,22, SD = 1,108), medtem ko so v povprečju nevtralni glede trditve, da jim spletna personalizacija omogoča dostop do relevantnih vsebin (AS = 2,87, SD = 1,267) in trditve, da jim spletna personalizacija omogoča dostop do zanimivih vsebin (AS = 3,08, SD = 1,252). Skupno povprečje vseh trditev znaša 2,72 s standardnim odklonom 1,079, kar kaže, da so anketiranci v povprečju nevtralni glede zaznanih koristi spletne personalizacije. Povzetek izračunanih aritmetičnih sredin in standardnih odklonov se nahaja v tabeli 1 v Prilogi 2.

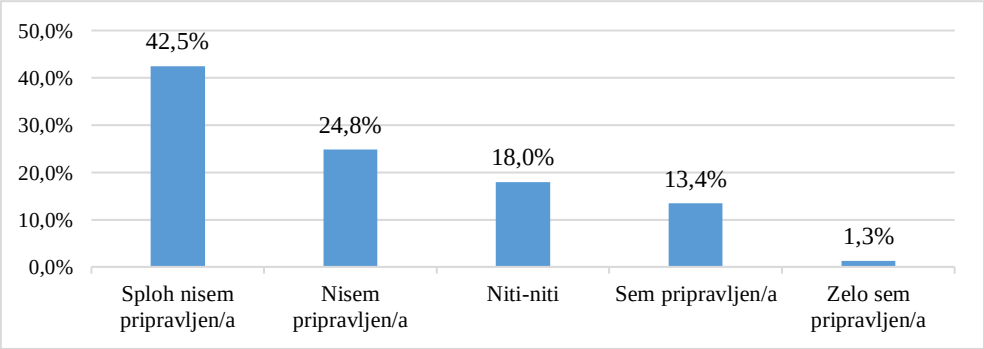
Slika 7: Trditve o koristih spletne personalizacije (n = 306)



Vir: lastno delo.

Naslednji sklop vprašanj se navezuje na pripravljenost anketirancev za deljenje svojih podatkov za namen spletne personalizacije. S pomočjo petega vprašanja sem želela ugotoviti, v kolikšni meri so anketiranci na splošno pripravljeni deliti svoje podatke. Svoj odgovor so lahko podali na lestvici od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a«. Kot je prikazano na sliki 8, največ anketirancev (42,5 %) sploh ni pripravljenih deliti svojih podatkov za namen spletne personalizacije. Skoraj četrtina anketirancev ni pripravljena deliti svojih podatkov. Po drugi strani pa je 13,4 % anketirancev svoje podatke pripravljenih deliti ter zgolj 1,3 % je tistih, ki so zelo pripravljeni deliti svoje podatke. 18,0 % anketirancev je glede svoje pripravljenosti neopredeljenih.

Slika 8: Splošna pripravljenost anketirancev za deljenje svojih podatkov (n = 306)

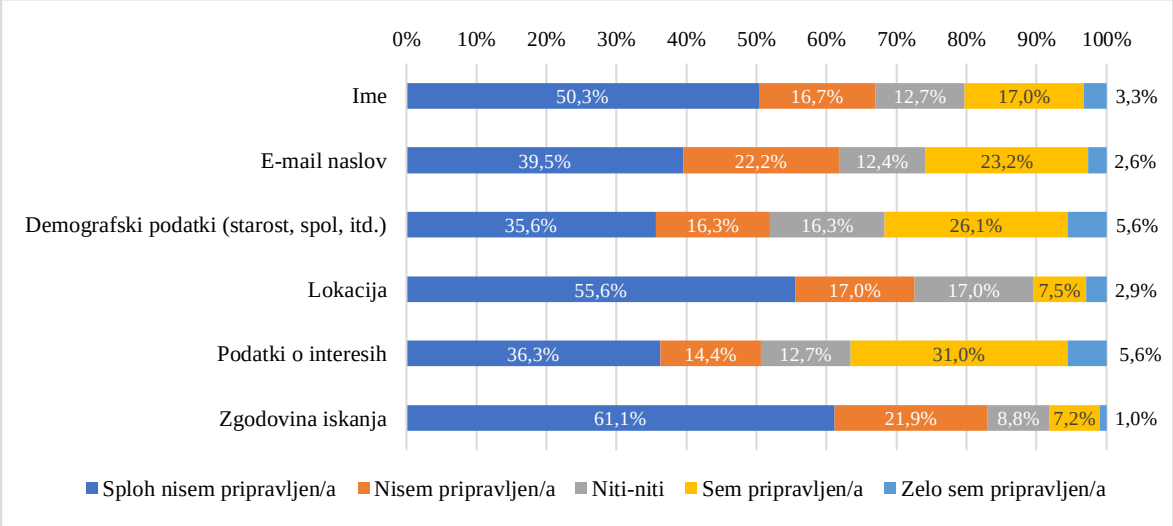


Vir: lastno delo.

Pri šestem vprašanju so anketiranci izrazili svojo pripravljenost za deljenje različnih vrst podatkov, pri čemer so svoje odgovore podali na petstopenjski lestvici (od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a«). S slike 9 je razvidno, da je pri vseh šestih vrstah podatkov, ki jih podjetja uporabljajo za pripravo personaliziranih spletnih vsebin, največ

anketirancev izbralo odgovor »sploh nisem pripravljen/-a«. Največji delež anketirancev (61,1 %) sploh ni pripravljen deliti podatkov o zgodovini iskanja, sledijo podatki o lokaciji (55,6 %) ter podatki o imenu (50,3 %). Za preostale tri vrste osebnih podatkov so deleži anketirancev, ki so izbrali odgovor »sploh nisem pripravljen/-a«, malce nižji, in sicer 39,5 % anketirancev sploh ni pripravljenih deliti svojega e-mail naslova, 36,3 % podatkov o svojih interesih ter 35,6 % svojih demografskih podatkov. Po drugi strani lahko vidimo, da je v vseh šestih primerih le majhen delež anketirancev zelo pripravljenih deliti določen podatek za namen spletne personalizacije. Največji delež anketirancev (5,6 %) je zelo pripravljen deliti podatke o interesih in demografske podatke, najmanjši delež (1,0 %) pa podatke o zgodovini iskanja. Podobno velja tudi za anketirance, ki so izbrali odgovor »sem pripravljen/-a«, pri čemer je največji delež anketirancev (31,0 %) pripravljen deliti podatke o svojih interesih, najmanjši (7,2 %) pa podatke o zgodovini iskanja. Prav tako je s slike 9 razvidno, da za vseh šest vrst podatkov velja, da večina anketirancev ni pripravljena deliti podatka v zameno za personalizirane spletne vsebine. Največja razlika med deležema tistih, ki so določen podatek pripravljeni deliti in tistih, ki ga niso, se pojavi pri podatkih o zgodovini iskanja, saj je tistih, ki tega podatka niso pripravljeni deliti kar 83 %. Po drugi strani pa je razlika med deležema najmanjša pri podatkih o interesih (14,1 %) in demografskih podatkih (20,3 %).

Slika 9: Pripravljenost anketirancev za deljenje različnih vrst podatkov (n = 306)

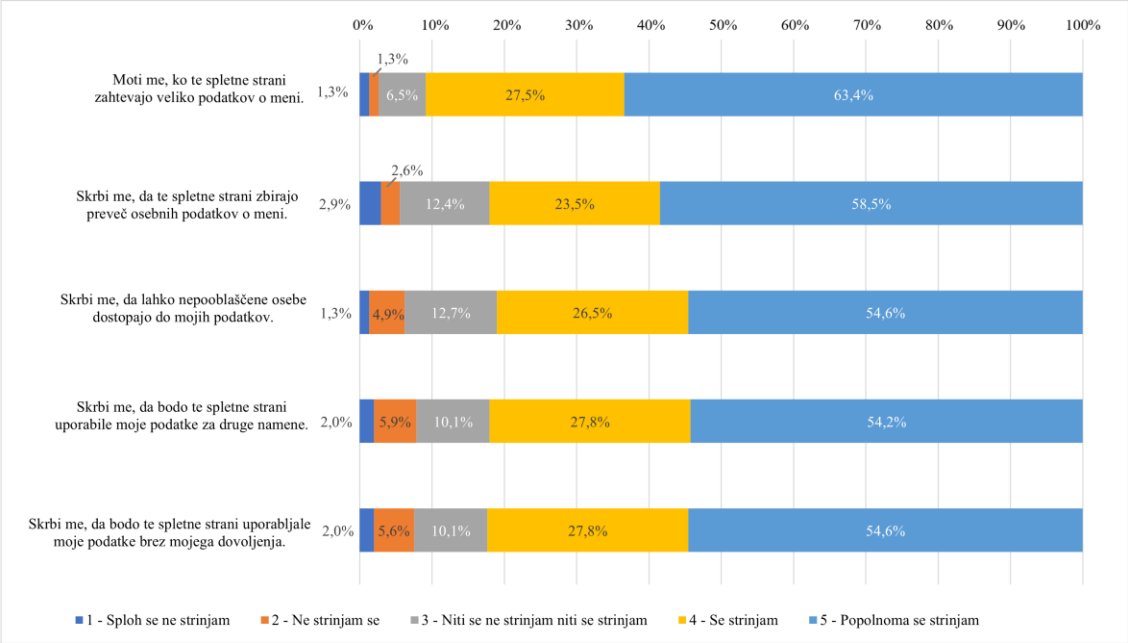


Vir: lastno delo.

Četrti sklop vprašanj se nanaša na zaskrbljenost uporabnikov glede zasebnosti na spletu. Pri sedmem vprašanju so anketiranci izrazili, v kolikšni meri se strinjajo s petimi trditvami glede njihove skrbi za zasebnost v primeru spletnih strani, ki uporabljajo podatke za pripravo personaliziranih vsebin. Stopnjo strinjanja sem merila s petstopenjsko Likertovo lestvico od 1 (sploh se ne strinjam) do 5 (popolnoma se strinjam). Kot je razvidno s slike 10, je pri vseh trditvah večina anketirancev izbrala odgovor »popolnoma se strinjam«. Največji delež anketirancev (63,4 %) se popolnoma strinja s trditvijo, da jih moti, ko spletne strani, ki

uporabljajo podatke za pripravo personaliziranih vsebin, zahtevajo veliko podatkov o njih. 58,5 % anketirancev se popolnoma strinja s trditvijo, da jih skrbi, da te spletne strani zbirajo preveč podatkov o njih. Sledijo preostale tri trditve glede nepooblaščenega dostopa do podatkov, uporabe podatkov brez dovoljenja posameznikov in uporabe podatkov za druge namene, pri katerih je delež tistih, ki so izbrali odgovor »popolnoma se strinjam« okoli 54 %. S slike 10 je prav tako razvidno, da se s posamezno trditvijo popolnoma ne strinja ali ne strinja le majhen delež anketirancev (manj kot 10 %). Na podlagi odgovorov anketirancev sem za vsako trditev izračunala tudi aritmetično sredino in standardni odklon. Rezultati kažejo, da se anketiranci v povprečju strinjajo z vsemi trditvami, saj so bile pri vseh trditvah aritmetične sredine višje od 4. Skupno povprečje vseh trditev znaša 4,33 s standardnim odklonom 0,811, kar kaže, da so anketiranci v povprečju precej zaskrbljeni glede svoje zasebnosti v povezavi s spletno personalizacijo. Povzetek izračunanih aritmetičnih sredin in standardnih odklonov se nahaja v tabeli 2 v Prilogi 2.

Slika 10: Trditve o zaskrbljenosti anketirancev glede zasebnosti (n = 306)

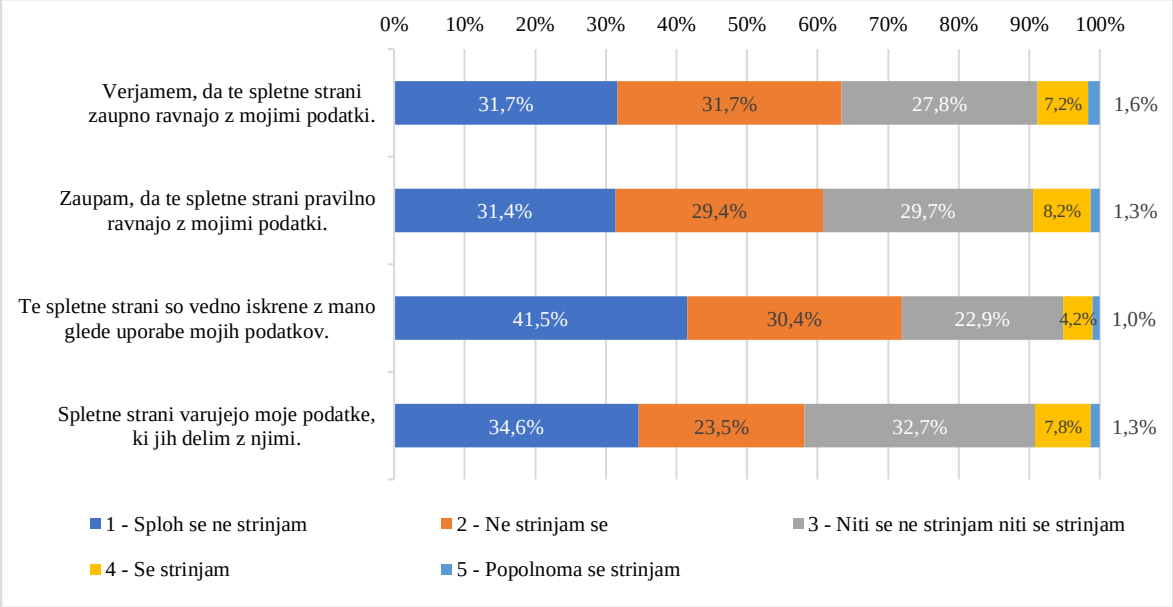


Vir: lastno delo.

Z osmim vprašanjem sem želela preveriti stopnjo strinjanja anketirancev s trditvami glede zaupanja spletnim stranem, ki uporabljajo osebne podatke za pripravo personaliziranih vsebin. Anketiranci so svoje odgovore podali na lestvici od 1 (sploh se ne strinjam) do 5 (popolnoma se strinjam). Kot je razvidno s slike 11, je pri prvi trditvi največ anketirancev (31,7 %) izbralo odgovor »sploh se ne strnjam« oziroma »ne strinjam se«. Pri preostalih trditvah je največ anketirancev izbralo odgovor »sploh se ne strinjam«. Prav tako je s slike 11 razvidno, da je relativno velik delež anketirancev neopredeljen glede posamezne trditve o zaupanju spletnim stranem, ki uporabljajo osebne podatke za pripravo personaliziranih vsebin. Po drugi strani pa se le majhen delež anketirancev strinja s posamezno trditvijo, saj

je delež tistih, ki so izbrali odgovora »strinjam se« ali »popolnoma se strinjam«, pri vseh trditvah manjši od 10 %. Na podlagi odgovorov anketirancev sem za vsako trditev izračunala tudi aritmetično sredino in standardni odklon. Rezultati kažejo, da se anketiranci ne strinjajo z vsemi trditvami, saj so aritmetične sredine pri vseh trditvah nižje od 2,20, kar nakazuje na nizko stopnjo zaupanja spletnim stranem, ki uporabljajo osebne podatke za pripravo personaliziranih vsebin. Anketiranci tako v povprečju ne verjamejo, da te spletne strani zaupno in pravilno ravnajo z njihovimi osebnimi podatki in da so iskrene z njimi glede uporabe teh podatkov ter se ne strinjajo s tem, da spletne strani te podatke varujejo, ko jih delijo z njimi. Anketiranci se v povprečju najmanj strinjajo s trditvijo »Te spletne strani so vedno iskrene z mano glede uporabe mojih podatkov.« (AS = 1,93), prav tako pa so si pri tej trditvi najbolj enotni (SD = 0,949). Povzetek izračunanih aritmetičnih sredin in standardnih odklonov se nahaja v tabeli 3 v Prilogi 2.

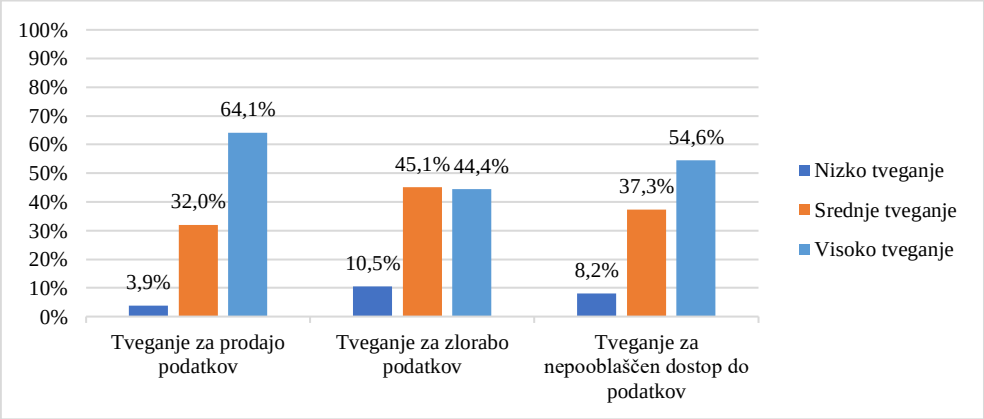
Slika 11: Trditve o zaupanju spletnim stranem (n = 306)



Vir: lastno delo.

Deveto vprašanje se nanaša na tveganja, ki ogrožajo zasebnost uporabnikov v primeru spletne personalizacije, in sicer tveganje za prodajo podatkov tretjim osebam, tveganje za zlorabo podatkov ter tveganje za nepooblaščen dostop do podatkov s strani neznanih oseb. Anketiranci so morali vsako izmed naštetih tveganj oceniti kot nizko, srednje ali visoko tveganje. Kot je prikazano na sliki 12, je največ anketirancev (64,1 %) ocenilo, da v primeru spletnih strani, ki uporabljajo spletno personalizacijo, obstaja visoko tveganje za prodajo podatkov tretjim osebam. Prav tako je največ anketirancev (54,6 %) ocenilo, da se pojavlja visoko tveganje, da bodo njihovi podatki na voljo neznanim deležnikom brez njihovega dovoljenja. Glede tveganja, da bo prišlo pri uporabi teh spletnih strani do zlorabe podatkov, pa je največ anketirancev (45,1 %) ocenilo, da gre za srednje tveganje, prav tako pa je visok delež tudi tistih, ki so označili, da gre v tem primeru za visoko tveganje (44,4 %).

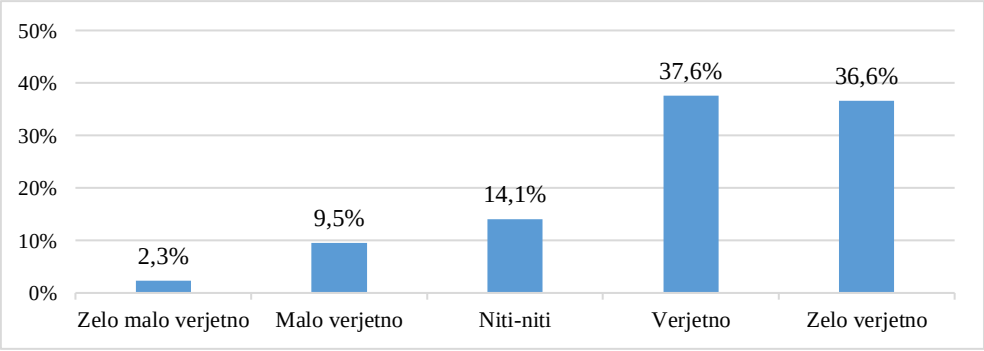
Slika 12: Tveganja za uporabnike spletnih strani, ki omogočajo spletno personalizacijo (n = 306)



Vir: lastno delo.

Peti sklop vprašanj se nanaša na samozaščitno vedenje anketirancev v primeru spletne personalizacije. S pomočjo desetega vprašanja sem želela ugotoviti, kako verjetno se bodo anketiranci v primeru uporabe spletnih strani, ki omogočajo spletno personalizacijo, odločili za zaščito svojih podatkov. Kot je razvidno s slike 13, je največ anketirancev (37,6 %) odgovorilo, da bi se v tem primeru verjetno odločilo za zaščito svojih podatkov. Sledijo tisti, ki bi se za zaščito zelo verjetno odločili (36,6 %). 14,1 % anketirancev je bilo neopredeljenih, 9,5 % anketirancev je odgovorilo, da bi se malo verjetno odločili za zaščito svojih podatkov, najmanj anketirancev (2,3 %) pa je izbralo odgovor »zelo malo verjetno«.

Slika 13: Verjetnost samozaščitnega vedenja anketirancev (n = 306)



Vir: lastno delo.

Z enajstim vprašanjem sem želela preveriti, kako pogosto anketiranci uporabljajo različne tehnike za zaščito zasebnosti na spletu, ki sem jih našla v literaturi. Anketiranci so svoje odgovore podali na lestvici od »nikoli« do »vsak dan«. Za posamezno vrsto tehnike za zaščito zasebnosti so v tabeli 1 prikazani deleži anketirancev, ki so izbrali posamezen odgovor na petstopenjski lestvici. V primeru uporabe razširitev za blokiranje oglasov, največ anketirancev (73,2 %) to počne vsakodnevno. 30,1 % anketirancev nekajkrat na leto briše

piškotke, sledijo tisti, ki to počnejo nekajkrat na mesec (23,5 %). Podobno velja tudi za brisanje zgodovine brskanja, pri čemer 32,4 % anketirancev to počne nekajkrat letno in 21,6 % nekajkrat na mesec. Za nestrinjanje s piškotki se skoraj polovica (48,0 %) odloči na vsakodnevni ravni, sledijo tisti, ki se za to odločijo nekajkrat tedensko (19,6 %). Največji delež anketirancev (33,0 %) se za brskanje v anonimnem načinu odloči nekajkrat na teden. Za uporabo napačnih osebnih podatkov se največ anketirancev (25,2 %) odloči nekajkrat na leto. V primeru uporabe navideznega zasebnega omrežja se 41,5 % nikoli ne odloči za to tehniko zaščite zasebnosti, medtem ko se za to nekajkrat letno odloči 21,2 % anketirancev. Za prenehanje uporabe spletne strani, če od njih zahteva podatke, se največji delež anketirancev (33,0 %) odloči nekajkrat na mesec, sledijo tisti, ki se za to odločijo nekajkrat na leto (24,8 %) ter tisti, ki se za to odločijo nekajkrat na teden (22,5 %).

Tabela 1: Pogostost uporabe tehnik za zaščito zasebnosti (n = 306)

Tehnike za zaščito zasebnosti	**Nikoli**	**Nekajkrat na leto**	**Nekajkrat na mesec**	**Nekajkrat na teden**	**Vsak dan**
Uporaba razširitev za blokiranje oglasov (npr. AdBlock, uBlock)	11,8%	2,9%	4,6%	7,5%	73,2%
Brisanje piškotkov	13,4%	30,1%	23,5%	16,0%	17,0%
Brisanje zgodovine brskanja	16,7%	32,4%	21,6%	14,1%	15,4%
Nestrinjanje s piškotki	10,1%	9,5%	12,7%	19,6%	48,0%
Brskanje v anonimnem načinu	8,5%	10,1%	20,3%	33,0%	28,1%
Uporaba napačnih osebnih podatkov	20,9%	25,2%	17,3%	19,3%	17,3%
Uporaba navideznega zasebnega omrežja (VPN)	41,5%	21,2%	14,1%	12,4%	10,8%
Preneham z uporabo spletne strani, če zahteva podatke od mene	6,9%	24,8%	33,0%	22,5%	12,7%

Vir: lastno delo.

5.4.3 Preverjanje raziskovalnih hipotez

V nadaljevanju so predstavljene analize in rezultati preverjanja predhodno zastavljenih hipotez. Podrobnejši izpisi analiz, ki so bile pripravljene s pomočjo programa SPSS, se nahajajo v prilogah.

Hipoteza 1: Uporabniki so na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije.

Pri preverjanju prve hipoteze sem upoštevala odgovore na vprašanje 7, pri katerem so anketiranci podali svojo stopnjo strinjanja glede petih trditev, ki se navezujejo na

zaskrbljenost glede zasebnosti v primeru spletne personalizacije. Odgovore so podali na petstopenjski lestvici od 1 »Sploh se ne strinjam do 5 »Popolnoma se strinjam«.

S pomočjo koeficienta Cronbach alfa sem najprej preverila zanesljivost nove spremenljivke, ki bi združevala vseh pet trditev. Vrednost koeficienta znaša 0,910, kar pomeni, da lahko oblikujem novo spremenljivko »Zaskrbljenost glede zasebnosti« tako, da izračunam povprečje vseh petih trditev. Skupno povprečje znaša 4,33 s standardnim odklonom 0,811.

S pomočjo t-testa za en vzorec sem preverila, ali je povprečna vrednost nove spremenljivke večja od testne vrednosti. Kot testno vrednost sem vzela 3,5, saj le-ta nakazuje določeno stopnjo strinjanja s trditvami oziroma določeno stopnjo zaskrbljenosti. Rezultat t-testa kaže, da je povprečna stopnja zaskrbljenosti statistično značilno višja od 3,5 ($t = 17{,}885$, $p < 0{,}001$). Podrobnejši SPSS izpis se nahaja v Prilogi 3.

Postopek sem ponovila tudi za vsako posamezno trditev, pri čemer t-test pokazal, da so povprečne vrednosti pri vseh petih trditvah statistično značilno višje od testne vrednosti 3,5 ($p < 0{,}001$). Na podlagi vzorčnih podatkov lahko tako zavrnem ničelno hipotezo pri točni stopnji značilnosti $p < 0{,}001$ in sprejmem sklep, da so uporabniki na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije.

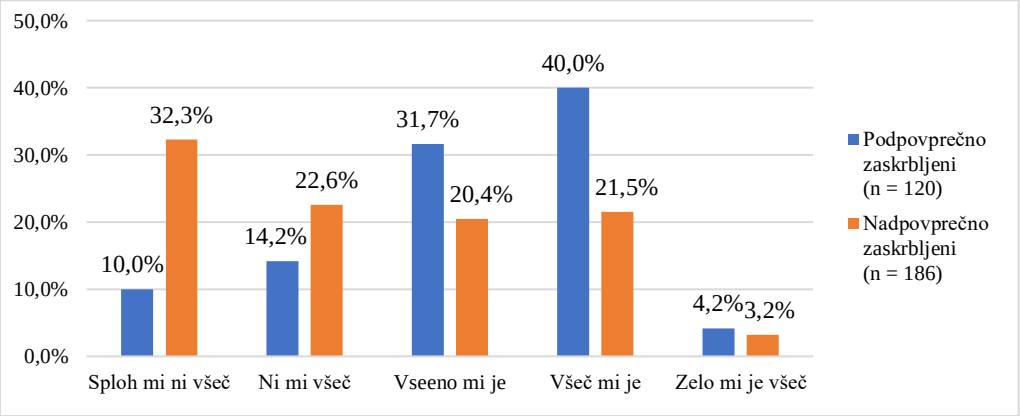
Hipoteza 2: Uporabniki, ki so bolj zaskrbljeni glede zasebnosti, imajo bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni.

Za preverjanje druge hipoteze sem upoštevala odgovore na vprašanje 7, na podlagi katerih sem oblikovala novo spremenljivko »Zaskrbljenost glede zasebnosti« pri preverjanju prve hipoteze, in odgovore na vprašanje 3, ki se nanaša na stališče anketirancev do spletne personalizacije. Pri tem vprašanju so anketiranci podali odgovor na petstopenjski lestvici od »sploh mi ni všeč« do »zelo mi je všeč«.

Za vsakega od anketirancev sem na podlagi odgovorov na vprašanje 7 izračunala stopnjo zaskrbljenosti tako, da sem izračunala povprečno vrednost petih trditev. Anketirance sem nato razdelila v dve skupini glede na to, ali njihova stopnja zaskrbljenosti presega skupno povprečno vrednost 4,33. Nato sem med seboj primerjala njihove odgovore o stališču do spletne personalizacije, kar prikazuje slika 14. Med tistimi s podpovprečno stopnjo zaskrbljenosti glede zasebnosti je največ anketirancev (40 %) odgovorilo, da jim je všeč, če jim spletna stran ponudi vsebine, ki so prilagojene njihovim interesom. S slike 14 je razvidno, da je v tej skupini delež tistih, ki imajo pozitivno stališče (42,2 %), skoraj dvakrat višji od tistih, ki imajo negativno stališče (24,2 %), visok delež anketirancev (31,7 %) pa ima nevtralno stališče. V skupini z nadpovprečno stopnjo zaskrbljenosti glede zasebnosti je največ anketirancev (32,2 %) izbralo odgovor »sploh mi ni všeč«. Odgovora »ni mi všeč« in »všeč mi je« je izbral podoben delež anketirancev (22,6 % in 21,5 %). V tej skupini je delež tistih z negativnim stališčem do spletne personalizacije (54,9 %) malo več kot dvakrat večji od tistih, ki imajo pozitivno stališče (24,7 %). V primerjavi s prvo skupino je v tej skupini manj anketirancev, ki imajo nevtralno stališče. S slike 14 je razvidno, da je pri

odgovorih »sploh mi ni všeč« in »ni mi všeč« delež anketirancev višji v skupini z nadpovprečno stopnjo zaskrbljenosti glede zasebnosti, obratno pa velja pri odgovorih, ki nakazujejo pozitivno stališče, saj je v tem primeru delež anketirancev višji v skupini s podpovprečno stopnjo zaskrbljenosti.

Slika 14: Primerjava odgovorov na 7. vprašanje pri podpovprečno in nadpovprečno zaskrbljenih anketirancih



Vir: lastno delo.

Za preverjanje statistično značilnih razlik v stališču do spletne personalizacije med obema skupinama sem uporabila neparametrični Mann-Whitney U test (Priloga 4). Na podlagi rezultatov, ki so prikazani v tabeli 2, lahko vidimo, da je povprečni rang pri skupini z nadpovprečno stopnjo zaskrbljenosti statistično značilno nižji ($z = -5{,}144$, $p < 0{,}001$), kar pomeni, da imajo glede na range ti anketiranci v povprečju bolj negativno stališče do spletne personalizacije. Na podlagi teh ugotovitev sem naknadno preverila še povezanost spremenljivke »Zaskrbljenost glede zasebnosti« in »Odnos do spletne personalizacije. SPSS izpis se nahaja v Prilogi 4. Spearmanov koeficient korelacije znaša -0,353, kar pomeni, da sta spremenljivki zmerno negativno povezani, povezava pa je statistično značilna ($p < 0{,}001$). Na podlagi vzorčnih podatkov lahko tako zavrnem ničelno hipotezo pri točni stopnji značilnosti $p < 0{,}001$ in sprejmem sklep, da imajo uporabniki, ki so bolj zaskrbljeni glede zasebnosti, bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni.

Tabela 2: Povzetek rezultatov Mann-Whitneyevega U testa

Spremenljivka	**Skupina**	**N**	**Povprečni rang**	**Vsota rangov**	**Mann-Whitneyeva U vrednost**	**Z**	**P vred. (2-stranska)**
Stališče do spletne personalizacije	Podpovprečno zaskrbljeni	120	184,92	22190,00	7390,00	-5,144	<0,001
	Nadpovprečno zaskrbljeni	186	133,23	24781,00			

Vir: lastno delo.

Hipoteza 3: Zaskrbljenost uporabnikov je negativno povezana z njihovo pripravljenostjo za deljenje svojih osebnih podatkov za namen spletne personalizacije.

Za preverjanje tretje hipoteze sem upoštevala odgovore na vprašanje 7 (Zaskrbljenost glede zasebnosti) in vprašanje 5, pri katerem so anketiranci s pomočjo petstopenjske lestvice (od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a«) ocenili svojo splošno pripravljenost za deljenje svojih podatkov v zameno za personalizirane vsebine. Ker gre za dve ordinalni spremenljivki, sem povezanost med njima preverjala s pomočjo Spearmanovega koeficienta korelacije.

Tabela 3: Povezanost med zaskrbljenostjo glede zasebnosti in pripravljenostjo za deljenje podatkov

		Pripravljenost za deljenje podatkov
Zaskrbljenost glede zasebnosti	Spearmanov koeficient korelacije	-0,508
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306

Vir: lastno delo.

Kot je prikazano v tabeli 3, Spearmanov koeficient korelacije znaša -0,508, kar pomeni, da sta spremenljivki zmerno negativno povezani, povezava pa je statistično značilna ($p < 0,001$). Na podlagi vzorčnih podatkov lahko tako zavrnem ničelno hipotezo pri točni stopnji značilnosti $p < 0,001$ in sprejmem sklep, da je zaskrbljenost uporabnikov glede zasebnosti negativno povezana z njihovo pripravljenostjo za deljenje svojih osebnih podatkov za namen spletne personalizacije.

Hipoteza 4: Uporabniki različnih starostnih skupin so različno zaskrbljeni glede zasebnosti v primeru spletne personalizacije.

Za preverjanje četrte hipoteze sem upoštevala odgovore na vprašanje 7 (Zaskrbljenost glede zasebnosti) in vprašanje 13 (starost). V analizo je bilo vključenih 287 enot, saj 19 anketirancev ni želelo podati odgovora o svoji starosti. Podatki v tabeli 4 kažejo, da imajo posamezniki v starostni skupini nad 55 let (AS = 4,533, SD = 0,622) in posamezniki v starostni skupini od 35 do 44 let (AS = 4,530, SD = 0,620) najvišjo stopnjo zaskrbljenosti glede zasebnosti v primeru spletne personalizacije. Najnižjo stopnjo zaskrbljenosti imajo posamezniki v starostni skupini pod 18 let (AS = 3,517, SD = 1,050).

Tabela 4: Aritmetične sredine zaskrbljenosti glede zasebnosti po starostnih skupinah

Starostna skupina	**N**	**AS**	**SD**
pod 18 let	12	3,517	1,050
od 18 do 24 let	91	4,106	0,894
od 25 do 34 let	91	4,415	0,721
od 35 do 44 let	40	4,530	0,620
od 45 do 55 let	38	4,447	0,762
nad 55 let	15	4,533	0,622

Vir: lastno delo.

Za izbiro ustreznega statističnega testa sem najprej preverila normalnost porazdelitve preučevane spremenljivke. Rezultati Kolmogorov-Smirnovega testa (Priloga 6) kažejo, da spremenljivka ni normalno porazdeljena ($p < 0,001$). Normalnost porazdelitve sem preverila tudi preko koeficienta asimetričnost in koeficienta sploščenosti ter grafično s pomočjo histograma in Q-Q grafa, ki potrjujejo, da spremenljivka ni normalno porazdeljena. Na podlagi teh ugotovitev sem za preverjanje četrte hipoteze uporabila neparametrični Kruskal-Wallisov test (Priloga 6). Rezultati testa kažejo, da obstajajo statistično značilne razlike v stopnji zaskrbljenosti glede zasebnosti med starostnimi skupinami ($H = 23,62$, $p < 0,001$). Na podlagi teh ugotovitev lahko tako zavrnem ničelno hipotezo pri točni stopnji značilnosti $p < 0,001$ in sprejmem sklep, da so uporabniki različnih starostnih skupin različno zaskrbljeni glede zasebnosti v primeru spletne personalizacije.

Za podrobnejše razumevanje razlik sem naredila še parno primerjavo med starostnimi skupinami, na podlagi katere sem ugotovila, da prihaja do statistično značilnih razlik med starostno skupino pod 18 let in od 25 do 34 let ($p = 0,012$), starostno skupino pod 18 let in od 35 do 44 let ($p = 0,004$), starostno skupino pod 18 let in od 45 do 55 let ($p = 0,010$) ter starostno skupino pod 18 let in nad 55 let ($p = 0,032$). Med ostalimi pari ne prihaja do statistično značilnih razlik ($p > 0,05$). Podrobnejši SPSS izpis se nahaja v Prilogi 6.

Hipoteza 5: Zaznane koristi so pozitivno povezane s pripravljenostjo uporabnikov za deljenje svojih podatkov za namen spletne personalizacije.

Za preverjanje pete hipoteze sem upoštevala odgovore na vprašanje 4, pri katerem so anketiranci podali svojo stopnjo strinjanja glede treh trditev, ki se navezujejo na koristi spletne personalizacije. Odgovore so podali na petstopenjski lestvici od 1 »Sploh se ne strinjam do 5 »Popolnoma se strinjam«. Prav tako sem upoštevala tudi odgovore na vprašanje 5, pri katerem so anketiranci na petstopenjski lestvici od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a« označili, kako pripravljeni so deliti svoje podatke v zameno za personalizirane vsebine.

Sprva sem preverjala povezanost spremenljivke »Pripravljenost za deljenje podatkov« in posamezne trditve, ki ponazarja eno izmed koristi, ki jo spletna personalizacija omogoča za

uporabnika. Ker gre za primerjavo ordinalnih spremenljivk, sem za preverjanje povezave uporabila Spearmanov koeficient korelacije. Rezultati so prikazani v tabeli 5. Ugotovila sem, da za vse tri trditve velja, da obstaja statistično značilna pozitivna povezava ($p < 0,001$) med trditvijo in spremenljivko »Pripravljenost za deljenje podatkov«. Kot je prikazano v tabeli 5, je spremenljivka »Pripravljenost za deljenje podatkov« najmočneje povezana z dostopom do relevantnih vsebin (korelacijski koeficient znaša 0,609), medtem ko je najšibkeje povezana z olajšanjem sprejemanja odločitev (korelacijski koeficient znaša 0,489).

Tabela 5: Povezanost posameznih trditev glede koristi spletne personalizacije in pripravljenosti za deljenje podatkov

		Pripravljenost za deljenje podatkov
Dostop do relevantnih vsebin	Spearmanov koeficient korelacije	0,609
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306
Dostop do zanimivih vsebin	Spearmanov koeficient korelacije	0,581
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306
Olajšanje sprejemanja odločitev	Spearmanov koeficient korelacije	0,489
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306

Vir: lastno delo.

Nato sem preverjala tudi povezanost spremenljivke »Pripravljenost za deljenje podatkov« in spremenljivke »Koristi spletne personalizacije«, ki združuje vse tri trditve. Vrednost koeficient Cronbach alfa za novo spremenljivko znaša 0,870, kar pomeni, da je nova spremenljivka zanesljiva. Skupno povprečje spremenljivke »Koristi spletne personalizacije« znaša 2,72 s standardnim odklonom 1,079.

Kot je prikazano v tabeli 6, Spearmanov koeficient korelacije znaša 0,619, kar pomeni, da sta spremenljivki zmerno pozitivno povezani, povezava pa je statistično značilna ($p < 0,001$). Na podlagi teh ugotovitev ter ugotovitev povezanosti posameznih trditev lahko tako zavrnem ničelno hipotezo pri točni stopnji značilnosti $p < 0,001$ in sprejmem sklep, da so zaznane koristi pozitivno povezane s pripravljenostjo uporabnikov za deljenje svojih podatkov za namen spletne personalizacije.

Tabela 6: Povezanost zaznanih koristi in pripravljenosti za deljenje podatkov

		Pripravljenost za deljenje podatkov
Zaznane koristi spletne personalizacije	Spearmanov koeficient korelacije	0,619
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306

Vir: lastno delo.

Hipoteza 6: Uporabniki so najbolj pripravljeni deliti podatek o svojem imenu v zameno za personalizirane ponudbe.

Za preverjanje šeste hipoteze sem upoštevala odgovore na vprašanje 6, pri katerem so anketiranci podali odgovore o svoji pripravljenosti za deljenje šestih različnih podatkov v zameno za personalizirane spletne vsebine. Za vsako vrsto podatka so podali odgovor na petstopenjski lestvici od »sploh nisem pripravljen/a« do »zelo sem pripravljen/a«. Pripravljenost za deljenje različnih vrst podatkov sem preverjala z izračunom mediane. Iz tabele 7 je razvidno, da so anketiranci bolj pripravljeni deliti podatke o interesih, demografskih podatkih in e-mail naslovu (Me = 2) kot ostale podatke (Me = 1).

Tabela 7: Opisna statistika pripravljenosti za deljenje posameznega podatka v zameno za personalizirane spletne vsebine

Pripravljenost za deljenje podatka	**Povprečna vrednost**	**Mediana**	**Standardni odklon**
Podatki o interesih	2,552	2,00	1,390
Demografski podatki (starost, spol, itd.)	2,497	2,00	1,351
E-mail naslov	2,271	2,00	1,271
Ime	2,062	1,00	1,267
Lokacija	1,853	1,00	1,128
Zgodovina iskanja	1,650	1,00	0,978

Vir: lastno delo.

Na podlagi teh ugotovitev je razvidno, da ime ni tisti podatek, ki so ga anketiranci najbolj pripravljeni deliti v zameno za personalizirane spletne vsebine. S pomočjo Wilcoxonovega signed rank testa sem preverila, ali je pripravljenost za deljenje imena statistično značilno manjša od pripravljenosti za deljenje podatkov o interesih, demografskih podatkov in e-mail naslovu. Povzetek rezultatov testa je prikazan v tabeli 8, podrobnejši SPSS izpis pa se nahaja v Prilogi 8. Rezultati kažejo, da je pripravljenost za deljenje imena v vseh treh primerih statistično značilno nižja.

Tabela 8: Povzetek rezultatov Wilcoxonovega signed rank testa

	Ime – Podatki o interesih	**Ime – Demografski podatki (starost, spol, itd.)**	**Ime – E-mail naslov**
Z	-5,665[a]	-5,484[a]	-3,059[a]
Stopnja značilnosti (2 - stranska)	< 0,001	< 0,001	0,002

a Temelji na pozitivnih rangih

Vir: lastno delo.

Na osnovi predstavljenih rezultatov ne morem sprejeti šeste hipoteze, saj uporabniki niso najbolj pripravljeni deliti podatka o svojem imenu v zameno za personalizirane ponudbe.

Hipoteza 7: Zaskrbljenost uporabnikov glede zasebnosti je pozitivno povezana z njihovo stopnjo verjetnosti uporabe tehnik za zaščito svoje zasebnosti.

Za preverjanje sedme hipoteze sem upoštevala odgovore na vprašanje 7 (Zaskrbljenost glede zasebnosti) in vprašanje 10, pri katerem so anketiranci s pomočjo petstopenjske lestvice (od »zelo malo verjetno« do »zelo verjetno«) ocenili, kako verjetno se bodo odločili za zaščito svojih podatkov, ko se srečujejo s spletnimi stranmi, ki omogočajo spletno personalizacijo. Ker gre za dve ordinalni spremenljivki, sem povezanost med njima preverjala s pomočjo Spearmanovega koeficienta korelacije.

Tabela 9: Povezanost med zaskrbljenostjo glede zasebnosti in verjetnostjo uporabe tehnik za zaščito zasebnosti

		Verjetnost uporabe tehnik za zaščito zasebnosti
Zaskrbljenost glede zasebnosti	Spearmanov koeficient korelacije	0,465
	Stopnja značilnosti (2 - stranska)	< 0,001
	N	306

Vir: lastno delo.

Kot je prikazano v tabeli 9, Spearmanov koeficient korelacije znaša 0,465, kar pomeni, da sta spremenljivki zmerno pozitivno povezani, povezava pa je statistično značilna ($p < 0,001$). Na podlagi vzorčnih podatkov lahko tako zavrnem ničelno hipotezo pri stopnji značilnosti $p < 0,001$ in sprejmem sklep, da je zaskrbljenost uporabnikov glede zasebnosti pozitivno povezana z njihovo stopnjo verjetnosti zaščite podatkov, kar lahko dosežejo z uporabo različnih tehnik za zaščito svoje zasebnosti.

5.5 Interpretacija ugotovitev

V nadaljevanju bom predstavila ključne ugotovitve kvantitativne raziskave, s katero sem želela preučiti vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije. S pomočjo kvantitativne raziskave sem med drugim želela ugotoviti, kako je zaskrbljenost glede zasebnosti povezana s stališči uporabnikov glede spletne personalizacije, njihovo pripravljenostjo za deljenje podatkov in verjetnostjo uporabe tehnik za zaščito zasebnosti. Povzetek rezultatov preverjanja hipotez je zbran v tabeli 10, v nadaljevanju pa sem te rezultate podrobneje predstavila in jih primerjala z rezultati predhodnih raziskav.

Tabela 10: Rezultati preverjanja hipotez

Hipoteza	**Sklep**
Hipoteza 1: Uporabniki so na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije.	Hipotezo sprejmem.
Hipoteza 2: Uporabniki, ki so bolj zaskrbljeni glede zasebnosti, imajo bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni.	Hipotezo sprejmem.
Hipoteza 3: Zaskrbljenost uporabnikov je negativno povezana z njihovo pripravljenostjo za deljenje svojih osebnih podatkov za namen spletne personalizacije.	Hipotezo sprejmem.
Hipoteza 4: Uporabniki različnih starostnih skupin so različno zaskrbljeni glede zasebnosti v primeru spletne personalizacije.	Hipotezo sprejmem.
Hipoteza 5: Zaznane koristi so pozitivno povezane s pripravljenostjo uporabnikov za deljenje svojih podatkov za namen spletne personalizacije.	Hipotezo sprejmem.
Hipoteza 6: Uporabniki so najbolj pripravljeni deliti podatek o svojem imenu v zameno za personalizirane ponudbe.	Hipoteze ne morem sprejeti.
Hipoteza 7: Zaskrbljenost uporabnikov glede zasebnosti je pozitivno povezana z njihovo stopnjo verjetnosti uporabe tehnik za zaščito svoje zasebnosti.	Hipotezo sprejmem.

Vir: lastno delo.

Zaskrbljenost anketirancev glede zasebnosti sem merila s pomočjo petih trditev glede zahtev in zbiranja podatkov, nepooblaščenega dostopa do podatkov in uporabe teh podatkov za druge namene in brez njihovega dovoljenja. Rezultati kvantitativne raziskave so pokazali, da so anketiranci na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije, saj je pri vseh trditvah več kot 80 % anketirancev izrazilo svojo zaskrbljenost. Te ugotovitve se skladajo z rezultati javnomnenjskih anket, na primer Auxier in drugi (2019), Norton (2023) in Statista (2019), ki so pokazale, da so posamezniki precej zaskrbljeni glede svoje zasebnosti na spletu. Prav tako so rezultati kvantitativne raziskave skladni z ugotovitvami avtorjev Bol in drugi (2018) ter Fernandes in Pereira (2021), ki so ugotovili, da so posamezniki zaskrbljeni glede svoje zasebnosti tudi v primeru spletne personalizacije. Posamezniki lahko na spletu zaznavajo tudi različna tveganja, da bi prišlo

do negativnih posledic zaradi nepravilnega ravnanja podjetij ob zbiranju in obdelavi njihovih podatkov (Featherman in drugi, 2010). Kvantitativna raziskava je pokazala, da več kot polovica anketirancev meni, da se v primeru spletne personalizacije pojavlja visoko tveganje, da se bodo njihovi osebni podatki prodali tretjim osebam in da bodo njihovi podatki na voljo neznanim deležnikom brez njihovega dovoljenja. Prav tako je večina anketirancev ocenila, da v primeru spletne personalizacije obstaja srednje ali visoko tveganje za zlorabo njihovih podatkov.

Raziskovalci so v dosedanjih raziskavah ugotovili, da se zaskrbljenost posameznikov med drugim lahko odraža tudi v njihovih stališčih (Smith in drugi, 2011). Kvantitativna raziskava je pokazala, da je največ anketirancev odgovorilo, da jim je všeč, če jim spletne strani ponudijo personalizirane vsebine. Kljub temu pa ima večji delež anketirancev bolj negativno stališče do spletne personalizacije kot pozitivno. Prav tako sem v okviru kvantitativne raziskave ugotovila, da imajo tisti uporabniki, ki so bolj zaskrbljeni glede zasebnosti, bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni. Poleg tega obstaja tudi statistično značilna negativna povezava med zaskrbljenostjo glede zasebnosti in stališči posameznikov do spletne personalizacije.

Z analizo rezultatov sem ugotovila, da večina anketirancev sploh ni pripravljenih ali ni pripravljenih deliti svojih podatkov za namen spletne personalizacije. Pretekle raziskave so pokazale, da zaskrbljenost posameznikov glede zasebnosti negativno vpliva na njihovo pripravljenost za deljenje podatkov v različnih situacijah, s katerimi se srečujejo na spletu (Baruh in drugi, 2017; Dinev in Hart, 2006; Fernandes in Pereira, 2021; Malhotra in drugi, 2004; Norberg in drugi, 2007; Paine in drugi, 2007; Taylor in drugi, 2009; Wu in drugi, 2012). Podobno je pokazala tudi kvantitativna raziskava, saj sem na podlagi vzorčnih podatkov ugotovila, da je zaskrbljenost posameznikov glede zasebnosti negativno povezana z njihovo pripravljenostjo za deljenje podatkov tudi za namen spletne personalizacije.

V okviru kvantitativne raziskave sem ugotovila, da prihaja do razlik v zaskrbljenosti med posamezniki v različnih starostnih skupinah, kar se sklada z ugotovitvami avtorjev Bergström (2015), Lee in drugi (2019) ter Paine in drugi (2007). Najbolj zaskrbljeni med vsemi anketiranci so posamezniki v starostni skupini nad 55 let, medtem ko so najmanj zaskrbljeni posamezniki v starostni skupini pod 18 let. Čeprav so rezultati pokazali, da prihaja do statistično značilnih razlik v zaskrbljenosti med starostnimi skupinami, so nadaljnje parne primerjave pokazale, da so razlike v zaskrbljenosti statistično značilne le med starostno skupino pod 18 let in starostnimi skupinami nad 25 let. Za boljše razumevanje razlik v zaskrbljenosti glede na starost anketirancev bi bilo potrebno izvesti nadaljnje raziskave, v katere bi vključili bolj skrbno izbrane posameznike v vsaki starostni skupini.

Posamezniki si pri odločitvi za deljenje svojih podatkov pomagajo tako, da med seboj primerjajo pričakovana tveganja in zaznane koristi, ki jih bodo z deljenjem podatkov pridobili (Dinev in Hart, 2006). Pretekle raziskave so pokazale, da personalizacija ponuja različne koristi za posameznike, ki jih lahko pridobijo v zameno za svoje podatke (Bol in

drugi, 2018; Fernandes in Pereira, 2021). V okviru kvantitativne raziskave sem ugotovila, da so anketiranci v povprečju neopredeljeni glede tega, ali jim spletna personalizacija omogoča dostop do relevantnih in zanimivih vsebin. Po drugi strani pa se v povprečju ne strinjajo, da jim spletna personalizacija omogoča lažje sprejemanje odločitev. Pridobljene podatke o zaznanih koristih sem nato primerjala s podatki o pripravljenosti posameznikov za deljenje podatkov, pri čemer sem ugotovila, da med njimi obstaja statistično značilna pozitivna povezava. Te ugotovitve se skladajo z rezultati raziskav avtorjev Bol in drugi (2018) ter Fernandes in Pereira (2021), ki so dokazali, da zaznane koristi pozitivno vplivajo na pripravljenost uporabnikov za deljenje svojih osebnih podatkov.

Pripravljenost posameznikov za deljenje podatkov se razlikuje tudi glede na vrsto podatka, ki ga morajo deliti v zameno za personalizirane ponudbe. V okviru kvantitativne raziskave sem ugotovila, da je največji delež anketirancev pripravljen deliti podatke o interesih, demografske podatke in podatek o e-mail naslovu. Po drugi strani pa več kot polovica anketirancev sploh ni pripravljena deliti podatkov o zgodovini iskanja, lokaciji in svojem imenu. Na podlagi teh rezultatov in statistične analize ne morem sprejeti hipoteze, da so uporabniki najbolj pripravljeni deliti podatke o svojem imenu v zameno za personalizirane ponudbe. Možna razlaga za to je, da ime spada med podatke, preko katerih je možno identificirati uporabnika, s čimer posamezniki izgubijo del zasebnosti in so lahko zato manj pripravljeni te vrste podatkov deliti (Belen Saglam in drugi, 2022; Metzger, 2007). Za globlji uvid bi bilo potrebno ugotovitve kvantitativne raziskave dopolniti s kvalitativno raziskavo, s katero bi pridobili boljši vpogled v razloge za nepripravljenost posameznikov za deljenje določenih vrst osebnih podatkov.

Pretekle raziskave so pokazale, da se lahko posamezniki pred tveganji zaščitijo tudi z uporabo tehnik za zaščito zasebnosti (Baruh in drugi, 2017). V okviru kvantitativne raziskave sem preverila, kako pogosto anketiranci uporabljajo različne vrste tehnik za zaščito zasebnosti. Na podlagi analize podatkov sem ugotovila, da velika večina anketirancev vsakodnevno uporablja razširitve za blokiranje oglasov. Več kot polovica anketirancev vsaj nekajkrat na mesec briše piškotke in preneha z uporabo spletnih mest, če ta zahtevajo njihove podatke. Prav tako več kot polovica anketirancev vsaj nekajkrat letno briše zgodovino brskanja, uporablja napačne osebne podatke in uporablja navidezno zasebno omrežje (VPN). Rezultati kvantitativne raziskave so pokazali, da bi se v primeru uporabe spletnih strani, ki omogočajo spletno personalizacijo, skoraj tri četrtine anketirancev verjetno ali zelo verjetno odločilo za zaščito svojih podatkov. Na podlagi analize rezultatov sem ugotovila, da obstaja statistično značilna pozitivna povezava med zaskrbljenostjo posameznikov in stopnjo verjetnosti, da bodo posamezniki zaščitili svoje podatke. Te ugotovitve se skladajo z ugotovitvami avtorjev Baruh in drugi (2017), ki so dokazali, da imajo bolj zaskrbljeni posamezniki močnejše namere za uporabo ukrepov za zaščito zasebnosti.

5.6 Omejitve raziskave in priporočila za nadaljnje raziskave

Čeprav sem na podlagi rezultatov kvantitativne raziskave prišla do spoznanj, ki omogočajo boljše razumevanje porabnikov in vpogled v vlogo zasebnosti v njihovih stališčih in namerah, moram izpostaviti tudi določene omejitve, ki vplivajo na zanesljivost rezultatov ter ponujajo priložnosti za nadaljnje raziskave.

Eno izmed omejitev predstavlja način vzorčenja, saj sem za namen kvantitativne raziskave uporabila priložnostno vzorčenje, ki ne omogoča reprezentativnega vzorca in posplošitve rezultatov raziskave na celotno populacijo. Prav tako bi bilo potrebno kvantitativno raziskavo izvesti na večjem vzorcu porabnikov, pri čemer bi morali zagotoviti tudi bolj enakomerno razmerje med spolom anketirancev in med starostnimi skupinami. Podobno velja tudi za stopnjo izobrazbe in trenutni status anketirancev, saj v trenutni raziskavi prevladujejo predvsem porabniki s terciarno izobrazbo ter zaposleni in študenti. Dodatno omejitev predstavlja tudi način razpošiljanja anketnega vprašalnika, saj je bil le-ta deljen preko družbenih omrežij in forumov, zato v raziskavo niso bili vključeni tisti porabniki, ki niso redno prisotni na teh kanalih.

V povezavi z anketnim vprašalnikom je potrebno izpostaviti tudi to, da se vsa vprašanja o spletni personalizaciji nanašajo na spletne strani, ki ponujajo personalizirane spletne vsebine. S tem sem poskušala anketirancem omogočiti boljše razumevanje vprašanj, saj so si na konkretnem primeru lažje predstavljali, kaj spletna personalizacija sploh pomeni. Ta poenostavitev vpliva na rezultate kvantitativne raziskave, saj bi anketiranci lahko podali drugačne odgovore, če bi se vprašanja nanašala na priporočilne sisteme ali na kakšno drugo obliko spletne personalizacije. V nadaljnjih raziskavah bi se morali osredotočiti na določeno obliko spletne personalizacije in anketirance povprašati glede njihovih stališč, pripravljenosti in drugih namer v tem konkretnem primeru. Po drugi strani pa bi bilo zanimivo med seboj primerjati različne oblike spletne personalizacije in preveriti, ali med njimi prihaja do razlik v stališčih porabnikov, njihovi pripravljenosti za deljenje podatkov ter verjetnosti za zaščito zasebnosti. Na podoben način bi lahko izvedli tudi primerjavo s personaliziranim oglaševanjem, pri čemer bi ugotavljali, ali tudi v tem primeru prihaja do kakšnih razlik pri ugotovitvah v primerjavi s spletno personalizacijo.

Rezultate kvantitativne raziskave bi bilo smiselno dopolniti še z dodatno kvalitativno raziskavo v obliki intervjujev ali fokusnih skupin, s katero bi pridobili še boljši vpogled v prepričanja porabnikov ter bi jih tako lahko povprašali po razlogih za njihova stališča, namere in odločitve. Poleg tega bi lahko kvantitativno raziskavo izvedli tudi v obliki eksperimenta, pri katerem bi porabnike naključno uvrstili v različne skupine in jim predstavili različne personalizirane vsebine ter na ta način na konkretnem primeru testirali koncepte, ki so bili predstavljeni v magistrskem delu.

Nekatere omejitve kvantitativne raziskave so povezane tudi s številnimi izzivi pri preučevanju zasebnosti, ki so jih avtorji izpostavili že v dosedanjih raziskavah. Po eni strani

sta zaskrbljenost porabnikov glede zasebnosti in s tem povezano vedenje močno odvisna od situacije, v kateri se posameznik v določenem trenutku nahaja (Solove, 2020). Po drugi strani pa so raziskovalci ugotovili, da se namere porabnikov v določenih primerih ne odražajo v njihovem vedenju in da so porabniki kljub poznanim tveganjem pripravljeni žrtvovati del svoje zasebnosti (Norberg in drugi, 2007). Prav tako pa lahko posamezniki v anketah nepravilno poročajo o svojem vedenju, ki ne odraža njihovega odziva v realnih situacijah (Kokolakis, 2017). Obenem pa tudi tehnologija podjetjem omogoča, da lahko brez zavedanja uporabnika zbirajo številne podatke, zaradi česar se v teh primerih ne poskušajo zaščititi ali poskušajo preprečiti zbiranje osebnih podatkov. Vse našteto raziskovalcem otežuje oblikovanje zanesljivih zaključkov in posploševanje ugotovitev, saj bodo odzivi porabnikov v realnih situacijah lahko drugačni od predvidenih.

Tematika zasebnosti v povezavi s spletno personalizacijo ponuja še veliko možnosti za nadaljnje raziskave, predvsem v povezavi s slovenskimi porabniki, saj v Sloveniji na to temo še ni bilo izvedenih veliko raziskav. Koncept zaskrbljenosti porabnikov glede zasebnosti pokriva široko področje tematik, zato bi bilo potrebno v nadaljnjih raziskavah zožiti obseg obravnavanih tematik, s čimer bi se lahko osredotočili na enega izmed konceptov in ga podrobneje preučili. Tako bi lahko na primer merili zaskrbljenost glede zasebnosti z več spremenljivkami, s čimer bi pridobili bolj zanesljive rezultate, ali pa bi se osredotočili samo na pripravljenost za deljenje podatkov in preučevali različne dejavnike, ki vplivajo na to, da se porabniki odločijo, da bodo svoje podatke delili s podjetji.

Prav tako bi bilo zanimivo kvantitativno raziskavo ponoviti čez nekaj let, saj bodo nove tehnologije in napredek na področju umetne inteligence podjetjem omogočale pripravo še bolj personaliziranih izkušenj. Po drugi strani pa bo ta napredek prinesel še več zbiranja podatkov o uporabnikih, zato bi bilo zanimivo raziskati, ali bo prišlo do sprememb v zaskrbljenosti porabnikov ter njihovih stališčih, namerah in vedenju povezanem z varovanjem zasebnosti.

5.7 Implikacije za podjetja

Čeprav je personalizacija zaradi svojih prednosti privlačna za številna podjetja, s seboj prinaša tudi različne izzive, ki se jih morajo tržniki zavedati tako pred kot tudi med samo izvedbo svojih aktivnosti. Enega izmed izzivov, ki so ga izpostavile pretekle raziskave, predstavlja zasebnost uporabnikov in s tem povezana tveganja, ki jih ti zaznavajo. Rezultati kvantitativne raziskave so potrdili, da zaskrbljenost glede zasebnosti igra pomembno vlogo tudi v primeru spletne personalizacije, saj so anketiranci v splošnem precej zaskrbljeni glede zasebnosti prav tako pa jih večina zaznava srednja ali visoka tveganja za izgubo zasebnosti.

Zaskrbljenost glede zasebnosti se v povezavi s spletno personalizacijo nanaša predvsem na zbiranje in obdelavo podatkov, ki predstavljata enega izmed ključnih korakov pri izvedbi spletne personalizacije. Podjetja morajo poiskati ravnovesje med lastnimi koristmi, ki jih lahko pridobijo z zbiranjem in obdelavo podatkov, in poseganjem v zasebnost svojih

uporabnikov. Tako se morajo zavedati, da njihove aktivnosti ne prinašajo le prednosti za uporabnike, ampak lahko prinesejo tudi zaskrbljenost, ki negativno vpliva na stališča uporabnikov glede spletne personalizacije. Pretekle raziskave so pokazale, da imajo različni dejavniki pomembno vlogo pri tem, kako zaskrbljeni so posamezniki glede svoje zasebnosti na spletu. V okviru kvantitativne raziskave sem pokazala, da se posamezniki različnih starostnih skupin razlikujejo v zaskrbljenosti glede zasebnosti. Tako lahko podjetja pri interakcijah s posameznimi starostnimi skupinami uporabijo prilagojene pristope, s katerim se bodo odzvala na njihove skrbi. Glede na rezultate kvantitativne raziskave bi morala podjetja največ pozornosti nameniti starejšim uporabnikom, saj so le-ti najbolj zaskrbljeni.

Podjetja se morajo skozi svoje aktivnosti odzvati na skrbi uporabnikov ter poskusiti blažiti zaznana tveganja, na primer tako, da so pri ravnanju s podatki čim bolj transparentna in svojim uporabnikom jasno predstavijo, kateri osebni podatki in za kakšen namen bodo uporabljeni. Prav tako morajo sprejeti ustrezne ukrepe na področju varovanja zasebnosti uporabnikov, da preprečijo zlorabo, nepooblaščen dostop ali prodajo podatkov tretjim osebam. Zaskrbljenost uporabnikov glede zasebnosti je negativno povezana z njihovo pripravljenostjo za deljenje podatkov, kar še dodatno potrjuje, da se morajo podjetja ustrezno odzvati na skrbi uporabnikov in na ta način poskušati pozitivno vplivati na njihovo pripravljenost. Glede na to, da so posamezniki bolj pripravljeni deliti podatke o interesih, demografskih podatkov in podatkov o e-mail naslovu, lahko podjetja te podatke uporabijo pri oblikovanju prilagojenih ponudb. Nasprotno pa rezultati kvantitativne raziskave kažejo, da so posamezniki manj pripravljeni deliti podatke o svoji lokaciji, zgodovini iskanja in imenu, zato bodo morala podjetja za dostop do teh podatkov uporabnikom ponuditi nekaj v zameno ali pa jih pridobiti na druge načine, na primer brez njihovega zavedanja.

Podjetja lahko pozitivno vplivajo na pripravljenost uporabnikov za deljenje podatkov tako, da izpostavijo koristi, ki jih bodo prejeli v zameno. Rezultati kvantitativne raziskave so pokazali, da so anketiranci razmeroma neodločeni glede zaznanih koristi, ki jih prinaša spletna personalizacija. Tako imajo podjetja na tem področju še veliko priložnosti, da v svoji komunikaciji s porabniki še bolj poudarijo, zakaj je spletna personalizacija zanje koristna, prav tako pa jim lahko predstavijo, kaj vse lahko z deljenjem svojih podatkov pridobijo. Poleg relevantnosti in zanimivosti vsebin ter lažjega sprejemanja odločitev lahko podjetja predstavijo tudi druge koristi, ki so pomembne za njihove uporabnike in bi potencialno odtehtale različna tveganja povezana z izgubo zasebnosti.

Zaskrbljenost glede zasebnosti je pozitivno povezana tudi z verjetnostjo uporabe tehnik, s katerimi posamezniki zaščitijo svojo zasebnost. Kvantitativna raziskava je pokazala, da velik delež anketirancev pogosto uporablja predvsem enostavnejše tehnike za zaščito svoje zasebnosti na spletu. Na ta način lahko v določeni meri podjetjem otežijo zbiranje in obdelavo podatkov, na katerih temeljijo personalizirane ponudbe. Podjetja bodo v določenih primerih težko vplivala na prenehanje uporabe teh tehnik, saj jih posamezniki uporabljajo ob splošni uporabi brskalnika oziroma se jih poslužujejo zaradi obiska drugih spletnih strani. Po drugi strani pa lahko s premišljenim pristopom glede zahtev po osebnih podatkih in

pravilnim ravnanjem s podatki poskušajo omejiti uporabo nekaterih tehnik, ki so bolj povezana s posameznim spletnim mestom, na primer nestrinjanje s piškotki, uporaba napačnih osebnih podatkov in prenehanje z uporabo spletne strani. Prav tako pa se podjetja lahko odločijo tudi za druge načine zbiranja podatkov, kjer uporabniki svoje podatke delijo zavestno in prostovoljno.

Kot sem izpostavila že v prejšnjem poglavju, so raziskovalci že v preteklih raziskavah opozorili, da se uporabniki različno odzivajo na situacije, pri katerih podjetja s svojimi aktivnostmi ogrožajo njihovo zasebnost. Tako se lahko v določenih situacijah vedejo drugače, kot predvidevajo ugotovitve predhodnih raziskav. Podjetja lahko te izzive poskušajo premagati tako, da sama spremljajo vedenje svojih strank na spletnih straneh. Ob tem lahko preko spletne analitike in drugih statistik opazujejo, kako se porabniki odzivajo na njihove aktivnosti, ki zahtevajo osebne podatke. Po drugi strani pa lahko tudi z različnimi orodji s strani porabnikov redno pridobivajo povratne informacije o njihovih stališčih in zadovoljstvu glede ravnanja podjetij v celotnem procesu izvedbe spletne personalizacije.

6 SKLEP

Tržniki imajo danes na voljo številne možnosti, kako lahko digitalna orodja in nove tehnologije vključijo v svoje trženjske strategije in s tem izboljšajo učinkovitost svojih aktivnosti. Med drugim lahko pri interakcijah s porabniki zbirajo in analizirajo različne podatke, na podlagi katerih jim nato ponudijo prilagojene vsebine, spletne strani ali priporočila za izdelke. Na ta način lahko del izkušnje s podjetjem prilagodijo potrebam in željam porabnikom, kar se lahko odraža v njihovi zvestobi in zadovoljstvu. Po drugi strani pa lahko zbiranje in obdelava podatkov za namen spletne personalizacije pri porabnikih vzbudita občutke nelagodja, saj podjetja na ta način dobijo dostop do dela njihove zasebnosti. Številni avtorji so v svojih raziskavah preučevali zaskrbljenost porabnikov glede zasebnosti ter dejavnike za pojav zaskrbljenosti in vedenja, ki jih ta prinaša. Pretekle raziskave so pokazale, da se lahko porabniki zaradi povečanih skrbi glede zasebnosti odločijo, da svojih podatkov ne bodo delili oziroma se odločijo za zaščito svoje zasebnosti z uporabo različnih orodij in drugih tehnik, ki podjetja ovirajo pri zbiranju njihovih osebnih podatkov (Baruh in drugi, 2017; Boerman in drugi, 2021; Dinev in Hart, 2006; Smith in drugi, 2011). Vse to podjetjem otežuje izvajanje spletne personalizacije in drugih trženjskih aktivnosti ter negativno vpliva na njihovo učinkovitost, saj brez dostopa do točnih in podrobnih podatkov ne morejo oblikovati prilagojenih ponudb.

V okviru magistrskega dela sem izvedla kvantitativno raziskavo v obliki spletne ankete, s katero sem preučevala vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije. Rezultati in ugotovitve kvantitativne raziskave se v večji meri skladajo z ugotovitvami tujih avtorjev, ki so svoje raziskave izvedli predvsem v povezavi s splošno zasebnostjo na spletu. Kvantitativna raziskava je pokazala, da so anketiranci na splošno zaskrbljeni glede svoje zasebnosti v primeru spletne personalizacije in v večini zaznavajo srednja ali visoka tveganja

za izgubo zasebnosti. Prav tako sem ugotovila, da imajo uporabniki, ki so bolj zaskrbljeni glede zasebnosti, bolj negativno stališče do spletne personalizacije kot tisti manj zaskrbljeni. V okviru kvantitativne raziskave sem primerjala tudi zaskrbljenost posameznikov glede na različne starostne skupine in ugotovila, da med njimi prihaja do razlik v zaskrbljenosti glede zasebnosti. Prav tako sem na podlagi vzorčnih podatkov dokazala, da je zaskrbljenost uporabnikov glede zasebnosti negativno povezana z njihovo pripravljenostjo za deljenje svojih osebnih podatkov za namen spletne personalizacije in pozitivno povezana z njihovo stopnjo verjetnosti uporabe tehnik za zaščito svoje zasebnosti. Dokazala sem tudi, da obstaja pozitivna povezava med zaznanimi koristmi spletne personalizacije in pripravljenostjo za deljenje podatkov. Edina hipoteza, ki je na podlagi vzorčnih podatkov nisem mogla sprejeti, se nanaša na vrsto podatkov, ki so jih uporabniki najbolj pripravljeni deliti za namen spletne personalizacije. Čeprav sem na podlagi preteklih raziskav pričakovala, da bodo posamezniki najbolj pripravljeni deliti podatek o svojem imenu, se je izkazalo, da so anketiranci bolj pripravljeni deliti podatke o interesih, demografske podatke in podatek o e-mail naslovu. Da bi se bolje prepričali, na kakšen način vrsta podatka vpliva na pripravljenost porabnikov za deljenje podatkov, bi bilo potrebno kvantitativno raziskavo izvesti na večjem vzorcu in vključiti še dodatna vprašanja, s katerimi bi bolj natančno preučili odnos med spremenljivkama. Poleg tega pa bi lahko rezultate kvantitativne raziskave dopolnili še s kvalitativno raziskavo, s katerimi bi dobili vpogled tudi v razloge za odločitve porabnikov.

Tako pregled literature kot tudi empirična raziskava sta pokazala, da problematika zasebnosti porabnikov pokriva širok spekter tematik, kar ponuja številne priložnosti za nadaljnje raziskave. Poleg splošnega razumevanja porabnikov bi bilo smiselno nadaljnje raziskave izvesti na čim konkretnejših primerih, saj sta dojemanje zasebnosti in s tem povezana zaskrbljenost močno odvisni od situacije. Podjetja bodo tako prišla do najbolj zanesljivih zaključkov, če spremljajo svoje uporabnike in njihove odzive v realnih situacijah ter z njihove strani redno pridobivajo povratne informacije o njihovem mnenju tako o personaliziranih ponudbah kot tudi o zbiranju in obdelavi njihovih podatkov. S hitrim in nenehnim napredkom na področju informacijskih tehnologij, ki bo omogočil še bolj učinkovito zbiranje podatkov in pripravo personaliziranih izkušenj, bo ta tematika tudi v prihodnosti ostala relevantna tako za raziskovalce kot za podjetja, ki bodo poskušala poiskati ravnovesje med prednostmi, ki jih spletna personalizacija prinaša, in tveganji zaradi poseganja v zasebnost porabnikov.

LITERATURA IN VIRI

1. Acquisti, A. in Grossklags, J. (2005). Privacy and rationality in individual decision making. *Security & Privacy, IEEE, 3*, 26–33.
2. Acquisti, A. in Grossklags, J. (2007). What Can Behavioral Economics Teach Us about Privacy? V *Digital Privacy: Theory, Technologies, and Practices*. United Kingdom: CRC Press.

3. Adobe. (2021). *Thinking Beyond the Third Party Cookie*. Pridobljeno 22. aprila 2023 s https://business.adobe.com/content/dam/www/us/en/pdfs/Adobe_Thinking_Beyond_the_Third_Party_Cookie.pdf
4. Adomavicius, G., Huang, Z. in Tuzhilin, A. (2008). Personalization and Recommender Systems. V *INFORMS Tutorials in Operations Research. State-of-the-Art Decision-Making Tools in the Information-Intensive* (str. 55–107).
5. Adomavicius, G. in Tuzhilin, A. (2005). Personalization Technologies: A Process-Oriented Perspective. *Commun. ACM*, *48*(10), 83–90.
6. Ahuja, K., Bauer, T., Meder, C. in Gediehn, O. (2022, 6. april). Mckinsey. *As the cookie crumbles, three strategies for advertisers to thrive*. Pridobljeno 2. aprila 2023, s https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/as-the-cookie-crumbles-three-strategies-for-advertisers-to-thrive
7. Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company.
8. Ansari, A. in Mela, C. F. (2003). E-Customization. *Journal of Marketing Research*, *40*(2), 131–145.
9. Arora, N., Dreze, X., Ghose, A., Hess, J. D., Iyengar, R., Jing, B., Joshi, Y., Kumar, V., Lurie, N., Neslin, S., Sajeesh, S., Su, M., Syam, N., Thomas, J. in Zhang, Z. J. (2008). Putting one-to-one marketing to work: Personalization, customization, and choice. *Marketing Letters*, *19*(3), 305–321.
10. Arora, N., Ensslen, D., Liu, W. W., Robinson, K., Stein, E. in Schüler, G. (2021, 12. november). McKinsey. *The value of getting personalization right or wrong is multiplying*. Pridobljeno 13. februarja 2023 s https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying
11. Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. in Turner, E. (2019, 15. november). Pew Research Center. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pridobljeno 20. aprila 2023 s https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
12. Ball, D., Coelho, P. S. in Vilares, M. J. (2006). Service personalization and loyalty. *Journal of Services Marketing*, *20*(6), 391–403.
13. Baruh, L., Secinti, E. in Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. *Journal of Communication*, *67*(1), 26–53.
14. Bekavac, I. in Garbin Praničević, D. (2015). Web analytics tools and web metrics tools: An overview and comparative analysis. *Croatian Operational Research Review*, *6*(2), 373–386.
15. Belanger, F. in Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*, 1017–1041.

16. Belen Saglam, R., Nurse, J. R. C. in Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103-163.
17. Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426.
18. Blank, G., Bolsover, G. in Dubois, E. (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. *SSRN Electronic Journal*.
19. Boerman, S. C., Kruikemeier, S. in Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, *48*(7), 953–977.
20. Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N. in de Vreese, C. H. (2018). Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts†. *Journal of Computer-Mediated Communication*, *23*(6), 370–388.
21. Bujlow, T., Carela-Español, V., Solé-Pareta, J. in Barlet-Ros, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, *105*(8), 1476–1510.
22. Cai, F., Wang, S. in de Rijke, M. (2017). Behavior-based personalization in web search. *Journal of the Association for Information Science and Technology*, *68*(4), 855–868.
23. Cai, H. in Mardani, A. (2023). Research on the impact of consumer privacy and intelligent personalization technology on purchase resistance. *Journal of Business Research*, *161*, 113811.
24. Castañeda, J. A. in Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, *7*(2), 117–141.
25. Chaffey, D. in Ellis-Chadwick, F. (2019). *Digital Marketing: Strategy, implementation and practice* (7. izdaja). Hoboken, New Jersey: Pearson.
26. Chaffey, D. in Patron, M. (2012). From web analytics to digital marketing optimization: Increasing the commercial value of digital analytics. *Journal of Direct, Data and Digital Marketing Practice*, *14*.
27. Chang, H. H. in Chen, S. W. (2008). The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator. *Including the Special Issue: Electronic Games and Personalized eLearning Processes*, *24*(6), 2927–2944.
28. Chellappa, R. K. in Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2/3), 181–202.
29. Chen, X., Sun, J. in Liu, H. (2022). Balancing web personalization and consumer privacy concerns: Mechanisms of consumer trust and reactance. *Journal of Consumer Behaviour*, *21*(3), 572–582.

30. Colas, M., Finck, I., Buvat, J., Nambiar, R. in Singh, R. R. (2014). *Cracking the Data Conundrum: How Successful Companies Make Big Data Operational*. Pridobljeno 15. aprila s https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/big_data_pov_03-02-15.pdf
31. Colnago, J., Cranor, L. in Acquisti, A. (2023). *Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors.*
32. Deloitte. (2020). *Connecting with meaning—Hyper-personalizing the customer experience using data, analytics, and AI*. Pridobljeno 2. aprila 2023, s https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-omnia-ai-marketing-pov-fin-jun24-aoda.pdf
33. Desai, D. (2019). An Empirical Study of Website Personalization Effect on Users Intention to Revisit E-commerce Website Through Cognitive and Hedonic Experience. V V. E. Balas, N. Sharma in A. Chakrabarti (ur.), *Data Management, Analytics and Innovation* (str. 3–19). Singapore: Springer Singapore.
34. Dinev, T. in Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*, 61–80.
35. Duncan, S. (2010). Using web analytics to measure the impact of earned online media on business outcomes: A methodological approach. *Institute for Public Relations*.
36. Edquist, A., Grennan, L., Griffiths, S. in Rowshankish, K. (2022, 23. september). McKinsey. *Data ethics: What it means and what it takes*. Pridobljeno 10. aprila 2023 s https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes
37. Eirinaki, M. in Vazirgiannis, M. (2003). Web Mining for Web Personalization. *ACM Trans. Internet Technol.*, *3*(1), 1–27.
38. Fan, H. in Poole, M. S. (2006). What Is Personalization? Perspectives on the Design and Implementation of Personalization in Information Systems. *Journal of Organizational Computing and Electronic Commerce*, *16*(3), 179–202.
39. Featherman, M. S., Miyazaki, A. D. in Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, *24*(3), 219–229.
40. Fernandes, T. in Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*, 101717.
41. Gao, M., Liu, K. in Wu, Z. (2010). Personalisation in web computing and informatics: Theories, techniques, applications, and future research. *Information Systems Frontiers*, *12*(5), 607–629.
42. Ghasemaghaei, M., Ebrahimi, S. in Hassanein, K. (2018). Data analytics competency for improving firm decision making performance. *The Journal of Strategic Information Systems*, *27*(1), 101–113.
43. Google. (brez datuma a). *[GA4] Engagement rate and bounce rate*. Pridobljeno 15. aprila 2023 s https://support.google.com/analytics/answer/12195621?hl=en

44. Google. (brez datuma b). *The Privacy Sandbox: Technology for a More Private Web*. Pridobljeno 15. april 2023 s https://privacysandbox.com/
45. Google. (brez datuma c). *Topics API: Relevant Ads without Cookies*. Pridobljeno 15. aprila 2023 s https://privacysandbox.com/proposals/topics/
46. Gozman, V. (2022, 14. maj). Council Post: Zero-Party Data Is The New Oil. *Forbes*. Pridobljeno 18. aprila 2023 s https://www.forbes.com/sites/theyec/2022/03/14/zero-party-data-is-the-new-oil/
47. Haden, J. (2012, 5. marec). How to Dig Deeper into Your Web Analytics. *Inc*. Pridobljeno 15. aprila 2023 s https://www.inc.com/jeff-haden/website-analytics-conversion-rate-vs-take-rate.html
48. Hong, W. in Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275–298.
49. Hoofnagle, C., King, J., Li, S. in Turow, J. (2010). How Different Are Young Adults From Older Adults When It Comes to Information Privacy Attitudes & Policies? *SSRN Electronic Journal*.
50. Isinkaye, F. O., Folajimi, Y. O. in Ojokoh, B. A. (2015). Recommendation systems: Principles, methods and evaluation. *Egyptian Informatics Journal*, *16*(3), 261–273.
51. Järvinen, J. in Karjaluoto, H. (2015). The use of Web analytics for digital marketing performance measurement. *Industrial Marketing Management*, *50*, 117–127.
52. Jesus, V. in Mustare, S. (2019). I Did Not Accept That: Demonstrating Consent in Online Collection of Personal Data. V S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa in I. Khalil (ur.), *Trust, Privacy and Security in Digital Business* (str. 33–45). Cham: Springer International Publishing.
53. Kalyanaraman, S. in Sundar, S. S. (2006). The Psychological Appeal of Personalized Content in Web Portals: Does Customization Affect Attitudes and Behavior? *Journal of Communication*, *56*, 110–132.
54. Kaniewska-Sejba, A. in Pilarczyk, B. (2014). Negative effects of personalization in direct marketing. *International Journal of Arts & Sciences*, *7*(2), 89.
55. Kaushik, A. (2009). *Web Analytics 2.0: The Art of Online Accountability and Science of Customer Centricity*. Wiley.
56. Ke, T. T. in Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*, *69*(8), 4389–4412.
57. Kemppainen, T., Frank, L., Makkonen, M. in Kallio, A. (2022, junij). Barriers to Data-Driven Decision-Making Among Online Retailers. V A. Pucihar, M. Kljajić Borštnar, R. Bons, A. Sheombar, G. Ongena, & D. Vidmar (ur.), *35th Bled eConference : Digital Restructuring and Human (Re)action* (str. 327–342). University of Maribor.
58. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.
59. Kotler, P., Armstrong, G. in Harris, L. C. (2019). *Principles of marketing* (8. izdaja). Hoboken, New Jersey: Pearson.
60. Kulyk, O., Gerber, N., Hilt, A. in Volkamer, M. (2021). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, *6*.

61. Kumar, V. in Ogunmola, G. (2019). Web Analytics for Knowledge Creation: A Systematic Review of Tools, Techniques, and Practices. *International Journal of Cyber Behavior, Psychology and Learning*, *10*, 1–14.
62. Lee, E.-J. in Park, J. K. (2009). Online service personalization for apparel shopping. *Journal of Retailing and Consumer Services*, *16*(2), 83–91.
63. Lee, H., Wong, S. F., Oh, J. in Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, *36*(2), 294–303.
64. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354.
65. Liang, T.-P., Lai, H.-J. in Ku, Y.-C. (2006). Personalized Content Recommendation and User Satisfaction: Theoretical Synthesis and Empirical Findings. *Journal of Management Information Systems*, *23*(3), 45–70.
66. Liu, H., Li, K., Chen, Y. in Luo, X. (Robert). (2023). Is personally identifiable information really more valuable? Evidence from consumers' willingness-to-accept valuation of their privacy information. *Decision Support Systems*, 114010.
67. Love, J. (2022, 27. julij). Bloomberg. *Google Delays Phasing Out Ad Cookies on Chrome Until 2024*. Pridobljeno 20. aprila 2023 s https://www.bloomberg.com/news/articles/2022-07-27/google-delays-phasing-out-ad-cookies-on-chrome-until-2024
68. Madden, M. (2014, 12. november). Pew Research Center. *Americans Consider Certain Kinds of Data to be More Sensitive than Others*. Pridobljeno 19. aprila 2023 s https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/
69. Malhotra, N. K. (2013). *Basic Marketing Research* (4. izdaja). Harlow: Pearson Education Canada.
70. Malhotra, N., Kim, S. in Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*, 336–355.
71. Mansur, F., Patel, V. in Patel M. (2017). A review on recommender systems. *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 1–6.
72. Martin, K. D. in Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155.
73. Mehrnezhad, M., Coopamootoo, K. in Toreini, E. (2022). How Can and Would People Protect From Online Tracking? *Proceedings on Privacy Enhancing Technologies*, *2022*, 105–125.
74. Metzger, M. J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361.
75. Milne, G. R., Labrecque, L. I. in Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449–473.

76. Moores, T. (2005). Do Consumers Understand the Role of Privacy Seals in E-commerce? *Commun. ACM*, *48*, 86–91.
77. Mulligan, D. K., Koopman, C. in Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, *374*(2083).
78. Murthi, B. P. S. in Sarkar, S. (2003). The Role of the Management Sciences in Research on Personalization. *Management Science*, *49*(10), 1344–1362.
79. Nissenbaum, H. (2004). Privacy As Contextual Integrity. *Washington Law Review*, *79*.
80. Norberg, P. A., Horne, D. R. in Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 100–126.
81. Norton. (2023, februar). *2023 Norton Cyber Safety Insights Report*. Pridobljeno 27. maja 2023 s https://www.gendigital.com/media/qcymrc1i/2023-ncsir-us-global-report_final.pdf
82. Paine, C., Reips, U.-D., Stieger, S., Joinson, A. in Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, *65*(6), 526–536.
83. Petronio, S. (2002). *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.
84. Phelps, J., Nowak, G. in Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41.
85. Plaza, B. (2009). Monitoring web traffic source effectiveness with Google Analytics. *Aslib Proceedings*, *61*(5), 474–482.
86. Quach, S., Thaichon, P., Martin, K. D., Weaven, S. in Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323.
87. Quint, M. in Rogers, D. (2015). *What Is the Future of Data Sharing?* Columbia Business School. Pridobljeno 18. aprila 2023 s https://business.columbia.edu/sites/default/files-efs/imce-uploads/global_brands/The_Future_of_Data_Sharing_Columbia-Aimia_October_2015.pdf
88. Riemer, K. in Totz, C. (2003). The Many Faces of Personalization. V M. M. Tseng in F. T. Piller (ur.), *The Customer Centric Enterprise: Advances in Mass Customization and Personalization* (str. 35–50). Berlin, Heidelberg: Springer Berlin Heidelberg.
89. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. V J. R. Cacioppo in R. E. Petty (ur.), *Social Psychology: A sourcebook* (str. 153–176). Guilford.
90. Salesforce. (2022). *State of the Connected Customer* (5. izdaja). Pridobljeno 3. aprila 2023 s https://www.salesforce.com/content/dam/web/en_ie/www/PDF/state-of-connected-customer-fifth-ed-comp.pdf

91. Sapateiro, C. in Gomes, J. (2017). Leverage Web Analytics for Real Time Website Browsing Recommendations. V Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis in S. Costanzo (ur.), *Recent Advances in Information Systems and Technologies* (str. 538–548). Cham: Springer International Publishing.
92. Schafer, J. B., Konstan, J. A. in Riedl, J. (2001). E-Commerce Recommendation Applications. *Data Mining and Knowledge Discovery*, *5*(1), 115–153.
93. Smith, Dinev, T. in Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 989–1015.
94. Smith, H. J., Milberg, S. J. in Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. JSTOR.
95. Solove, D. (2020). The Myth of the Privacy Paradox. *GW Law Faculty Publications & Other Works*.
96. Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. JSTOR.
97. Statista. (2019, 21. avgust). *Perceptions and concerns on data privacy among mobile users in the United States as of April 2019, by generation*. Pridobljeno 23. aprila 2023, s https://www.statista.com/statistics/1052516/us-consumer-concerns-on-data-privacy/
98. Strycharz, J., van Noort, G., Smit, E. in Helberger, N. (2019). Consumer View on Personalized Advertising: Overview of Self-Reported Benefits and Concerns. V E. Bigne in S. Rosengren (ur.), *Advances in Advertising Research X: Multiple Touchpoints in Brand Communication* (str. 53–66). Wiesbaden: Springer Fachmedien Wiesbaden.
99. Sundar, S. S., Kim, J., Rosson, M. B. in Molina, M. D. (2020). Online Privacy Heuristics that Predict Information Disclosure. *CHI 2020 - Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery.
100. Sundar, S. S. in Marathe, S. S. (2010). Personalization versus Customization: The Importance of Agency, Privacy, and Power Usage. *Human Communication Research*, *36*(3), 298–322.
101. Swani, K., Milne, G. R. in Slepchuk, A. N. (2021). Revisiting Trust and Privacy Concern in Consumers' Perceptions of Marketing Information Management Practices: Replication and Extension. *Journal of Interactive Marketing*, *56*, 137–158.
102. Tam, K.Y. in Ho, S. Y. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, *30*(4), 865.
103. Tan, E. (2018, 9. februar). Seven out of ten customers would boycott a brand that mishandled their data. Pridobljeno 6. maja 2023 s https://www.campaignlive.co.uk/article/seven-ten-customers-boycott-brand-mishandled-data/1456749
104. Tavani, H. T. in Moor, J. H. (2001). Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *SIGCAS Computers and Society*, *31*(1), 6–11.

105. Taylor, D. G., Davis, D. F. in Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, *9*(3), 203–223.
106. Toch, E., Wang, Y. in Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction*, *22*(1), 203–220.
107. Twilio. (2022). State of Customer Engagement Report 2022. Pridobljeno 3. aprila s https://twilio-cms-prod.s3.amazonaws.com/documents/Twilio_SOCER_2022 _EN.pdf
108. UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. Aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
109. Vafopoulos, M. in Oikonomou, M. (2013). Recommendation Systems: Bridging Technical Aspects with Marketing Implications. V I. E. Anagnostopoulos, M. Bieliková, P. Mylonas in N. Tsapatsoulis (ur.), *Semantic Hyper/Multimedia Adaptation: Schemes and Applications* (str. 155–180). Berlin, Heidelberg: Springer Berlin Heidelberg.
110. W3Techs. (2023). *Usage Statistics and Market Share of Google Analytics for Websites, April 2023*. Pridobljeno 11. aprila 2023 s https://w3techs.com/ technologies/details/ta-googleanalytics
111. Warren, S. D. in Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.
112. Westin, A. F. (1967). *Privacy and freedom* (1. izdaja). New York, NY: Atheneum.
113. Wilson, D. W. in Valacich, J. (2012). Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *International Conference on Information Systems, ICIS 2012*, *5*, 4152–4162.
114. Wu, K.-W., Huang, S. Y., Yen, D. C. in Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897.
115. Xu, H., Dinev, T., Smith, H. in Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. V *ICIS 2008 Proceedings—Twenty Ninth International Conference on Information Systems*.
116. Yoganarasimhan, H. (2020). Search Personalization Using Machine Learning. *Management Science*, *66*(3), 1045–1070.
117. Zanker, M., Rook, L. in Jannach, D. (2019). Measuring the impact of online personalisation: Past, present and future. *50 years of the International Journal of Human-Computer Studies. Reflections on the past, present and future of human-centred technologies*, *131*, 160–168.
118. Zhang, B. in Sundar, S. S. (2019). Proactive vs. Reactive Personalization: Can Customization of Privacy Enhance User Experience? *International Journal of Human-Computer Studies*, *128*, 86–99.

119. Zhang, B., Wang, N. in Jin, H. (2014). Privacy Concerns in Online Recommender Systems: Influences of Control and User Data Input. *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, 159–173. USA: USENIX Association.
120. Zheng, J. in Peltsverger, S. (2015). *Web Analytics Overview*. V M. Khosrow-Pour (ur.), *Encyclopedia of Information Science and Technology* (str. 7674–7683). Hershey: IGI Global.

PRILOGE

Priloga 1: Anketni vprašalnik

Pozdravljeni, sem Tjaša Kokalj, študentka Ekonomske fakultete v Ljubljani, in v sklopu svojega magistrskega dela proučujem vlogo zasebnosti v odnosu uporabnikov do spletne personalizacije. Za potrebe raziskave vas vljudno prosim, da rešite anketni vprašalnik.

Za reševanje ankete boste potrebovali 5-10 minut. Vsi vaši odgovori so anonimni in bodo uporabljeni izključno za namen raziskave magistrskega dela.

Za vaše odgovore in sodelovanje se vam iskreno zahvaljujem.

Q1 - Koliko prostega časa na dan preživite na spletu?

○ 1 uro ali manj
○ več kot 1 uro do vključno 2 uri
○ več kot 2 uri do vključno 3 ure
○ več kot 3 ure do vključno 4 ure
○ več kot 4 ure do vključno 5 ur
○ Več kot 5 ur

Q2 - Kako pogosto se na spletu srečujete z naslednjimi oblikami personalizacije?

	Nikoli	Nekajkrat na leto	Nekajkrat na mesec	Nekajkrat na teden	Vsak dan
Personalizirana priporočila izdelkov ali vsebin					
Personalizirana vsebina spletne strani					
Personalizirani rezultati iskanja					
Personalizirana cena produkta ali storitve					

Naslednja vprašanja se nanašajo na spletno personalizacijo, ki predstavlja proces prilagajanja vsebin na spletu glede na potrebe in interese uporabnika.

Q3 - Kako vam je všeč, če vam spletna stran ponudi vsebine, ki so prilagojene vašim interesom?

○ Sploh mi ni všeč
○ Ni mi všeč
○ Vseeno mi je

○ Všeč mi je

○ Zelo mi je všeč

Q4 - Na lestvici 1 do 5 označite, v kolikšni meri se strinjate z naslednjimi trditvami (1 – sploh se ne strinjam, 5 - popolnoma se strinjam):

	1 - Sploh se ne strinjam	2 - Ne strinjam se	3 - Niti se ne strinjam niti se strinjam	4 - Se strinjam	5 - Popolnoma se strinjam
Spletna personalizacija mi omogoča dostop do relevantnih vsebin.					
Spletna personalizacija mi omogoča dostop do vsebin, ki so mi zanimive.					
Spletna personalizacija mi omogoča lažje sprejemanje odločitev.					

Q5 - V kolikšni meri ste na splošno pripravljeni deliti svoje podatke v zameno za personalizirane spletne vsebine?

○ Sploh nisem pripravljen/a

○ Nisem pripravljen/a

○ Niti-niti

○ Sem pripravljen/a

○ Zelo sem pripravljen/a

Q6 - V kolikšni meri ste pripravljeni deliti naslednje podatke v zameno za personalizirane spletne vsebine?

	Sploh nisem pripravljen/a	Nisem pripravljen/a	Niti - niti	Sem pripravljen/a	Zelo sem pripravljen/a
Ime					
E-mail naslov					
Demografski podatki (starost, spol, itd.)					
Lokacija					
Podatki o interesih					
Zgodovina iskanja					

Q7 - Naslednje trditve se nanašajo na spletne strani, ki uporabljajo vaše podatke za pripravo personaliziranih vsebin. Na lestvici 1 do 5 označite, v kolikšni meri se strinjate z naslednjimi trditvami (1 – sploh se ne strinjam, 5 - popolnoma se strinjam):

	1 - Sploh se ne strinjam	2 - Ne strinjam se	3 - Niti se ne strinjam niti se strinjam	4 - Se strinjam	5 - Popolnoma se strinjam
Moti me, ko te spletne strani zahtevajo veliko podatkov o meni.					
Skrbi me, da te spletne strani zbirajo preveč osebnih podatkov o meni.					
Skrbi me, da lahko nepooblaščene osebe dostopajo do mojih podatkov.					
Skrbi me, da bodo te spletne strani uporabile moje podatke za druge namene.					
Skrbi me, da bodo te spletne strani uporabljale moje podatke brez mojega dovoljenja.					

Q8 – Na lestvici 1 do 5 označite, v kolikšni meri se strinjate z naslednjimi trditvami (1 – sploh se ne strinjam, 5 - popolnoma se strinjam):

	1 - Sploh se ne strinjam	2 - Ne strinjam se	3 - Niti se ne strinjam niti se strinjam	4 - Se strinjam	5 - Popolnoma se strinjam
Verjamem, da te spletne strani zaupno ravnajo z mojimi podatki.					
Zaupam, da te spletne strani pravilno ravnajo z mojimi podatki.					
Te spletne strani so vedno iskrene z mano glede uporabe mojih podatkov.					

Spletne strani varujejo moje podatke, ki jih delim z njimi.					

Q9 - Kakšno je po vašem mnenju tveganje za uporabnike spletnih strani, ki omogočajo spletno personalizacijo, da:

	Nizko tveganje	Srednje tveganje	Visoko tveganje
se bodo njihovi podatki prodali tretjim osebam?			
bo prišlo do zlorabe njihovih podatkov?			
bodo njihovi podatki na voljo neznanim deležnikom brez njihovega dovoljenja?			

Q10 - Kako verjetno se boste odločili za zaščito svojih podatkov, ko se srečujete s spletnimi stranmi, ki omogočajo spletno personalizacijo?

- ○ Zelo malo verjetno
- ○ Malo verjetno
- ○ Niti-niti
- ○ Verjetno
- ○ Zelo verjetno

Q11 - Kako pogosto uporabljate naslednje tehnike za zaščito svoje zasebnosti na spletu?

	Nikoli	Nekajkrat na leto	Nekajkrat mesečno	Nekajkrat na teden	Vsak dan
Uporaba razširitev za blokiranje oglasov (npr. AdBlock, uBlock)					
Brisanje piškotkov					
Brisanje zgodovine brskanja					
Nestrinjanje s piškotki					
Brskanje v anonimnem načinu					
Uporaba napačnih osebnih podatkov					
Uporaba navideznega					

zasebnega omrežja (VPN)					
Preneham z uporabo spletne strani, če zahteva podatke od mene					

Q12 - Prosim označite svoj spol:

- ○ Moški
- ○ Ženski
- ○ Ne želim odgovoriti

Q13 - V katero starostno skupino spadate?

- ○ Pod 18 let
- ○ Od 18 do 24 let
- ○ Od 25 do 34 let
- ○ Od 35 do 44 let
- ○ Od 45 do 55 let
- ○ Nad 55 let
- ○ Ne želim odgovoriti

Q14 - Kakšna je vaša najvišje dosežena formalna izobrazba?

- ○ Dokončana osnovna šola
- ○ Srednješolska izobrazba (poklicna šola, gimnazija)
- ○ Dodiplomska izobrazba (visoka ali višja šola)
- ○ Podiplomska izobrazba (magisterij ali doktorat)
- ○ Ne želim odgovoriti

Q15 - Kakšen je vaš trenutni status?

- ○ Dijak/-inja
- ○ Študent/-ka
- ○ Zaposlen/-a
- ○ Brezposeln/-a
- ○ Upokojenec/-ka
- ○ Ne želim odgovoriti

Priloga 2: Aritmetične sredine in standardni odkloni preučevanih konstruktov

Tabela 1: Aritmetične sredine in standardni odkloni trditev o koristih spletne personalizacije (n =306)

Trditve o koristih spletne personalizacije	**Aritmetična sredina**	**Standardni odklon**
Spletna personalizacija mi omogoča dostop do relevantnih vsebin.	2,87	1,267
Spletna personalizacija mi omogoča dostop do vsebin, ki so mi zanimive.	3,08	1,252
Spletna personalizacija mi omogoča lažje sprejemanje odločitev.	2,22	1,108
Koristi spletne personalizacije	**2,72**	**1,079**

Tabela 2: Aritmetične sredine in standardni odkloni trditev o zaskrbljenosti anketirancev glede zasebnosti (n =306)

Trditve o zaskrbljenosti glede zasebnosti	**Aritmetična sredina**	**Standardni odklon**
Moti me, ko te spletne strani zahtevajo veliko podatkov o meni.	4,50	0,786
Skrbi me, da te spletne strani zbirajo preveč osebnih podatkov o meni.	4,32	0,989
Skrbi me, da lahko nepooblaščene osebe dostopajo do mojih podatkov.	4,28	0,954
Skrbi me, da bodo te spletne strani uporabile moje podatke za druge namene.	4,26	0,994
Skrbi me, da bodo te spletne strani uporabljale moje podatke brez mojega dovoljenja.	4,27	0,987
Zaskrbljenost glede zasebnosti	**4,33**	**0,811**

Tabela 3: Aritmetične sredine in standardni odkloni trditev o zaupanju spletnim stranem (n =306)

Trditve o zaupanju spletnim stranem	**Aritmetična sredina**	**Standardni odklon**
Verjamem, da te spletne strani zaupno ravnajo z mojimi podatki.	2,15	1,005
Zaupam, da te spletne strani pravilno ravnajo z mojimi podatki.	2,19	1,012
Te spletne strani so vedno iskrene z mano glede uporabe mojih podatkov.	1,93	0,949
Spletne strani varujejo moje podatke, ki jih delim z njimi.	2,18	1,038
Zaupanje spletnim stranem	**2,11**	**0,902**

Priloga 3: SPSS izpis za preverjanje 1. hipoteze

Tabela 4: Izračun koeficienta Cronbach alfa za združeno spremenljivko »zaskrbljenost glede zasebnosti«

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,910	,908	5

Tabela 5: Rezultati t-testa za en vzorec za preverjanje 1. hipoteze

	Test value = 3.5						
	t	df	Significance		Mean Difference	95% Confidence Interval of the Difference	
			One-Sided p	Two-Sided p		Lower	Upper
Moti me, ko te spletne strani zahtevajo veliko podatkov o meni.	22,324	305	<,001	<,001	1,003	0,91	1,09
Skrbi me, da te spletne strani zbirajo preveč osebnih podatkov o meni.	14,501	305	<,001	<,001	0,820	0,71	0,93
Skrbi me, da lahko nepooblaščene osebe dostopajo do mojih podatkov.	14,315	305	<,001	<,001	0,781	0,67	0,89
Skrbi me, da bodo te spletne strani uporabile moje podatke za druge namene.	13,453	305	<,001	<,001	0,765	0,65	0,88
Skrbi me, da bodo te spletne strani uporabljale moje podatke brez mojega dovoljenja.	13,731	305	<,001	<,001	0,775	0,66	0,89
Zaskrbljenost glede zasebnosti	**17,885**	**305**	**<,001**	**<,001**	**0,82876**	**0,7376**	**0,9199**

Priloga 4: SPSS izpis za preverjanje 2. hipoteze

Tabela 6: Frekvenčna porazdelitev in deleži odgovorov anketirancev glede stališča do spletne personalizacije

	Podpovprečno zaskrbljeni		Nadpovprečno zaskrbljeni	
Stališče do spletne personalizacije	**Frekvenca**	**Delež**	**Frekvenca**	**Delež**
Sploh mi ni všeč	12	10,0%	60	32,3%
Ni mi všeč	17	14,2%	42	22,6%
Vseeno mi je	38	31,7%	38	20,4%
Všeč mi je	48	40,0%	40	21,5%
Zelo mi je všeč	5	4,2%	6	3,2%
Skupaj	120	100%	186	100%

Tabela 7: Rezultati Mann-Whitneyjevega U testa za preverjanje 2. hipoteze – povprečni rangi in vsote rangov

Ranks				
	zaskrbljenost glede zasebnosti	**N**	**Mean Rank**	**Sum of Ranks**
Stališče do spletne personalizacije	podpovprečno zaskrbljeni	120	184,92	22190,00
	nadpovprečno zaskrbljeni	186	133,23	24781,00
	Total	306		

Tabela 8: Rezultati Mann-Whitneyjevega U testa za preverjanje 2. hipoteze – testne statistike

Test Statistics[a]	
	Stališče do spletne personalizacije
Mann-Whitney U	7390,000
Wilcoxon W	24781,000
Z	-5,144
Asymp. Sig. (2-tailed)	<,001

a. Grouping Variable: zaskrbljenost_skupine

Tabela 9: Povezanost spremenljivk zaskrbljenost glede zasebnosti in stališče do spletne personalizacije

Correlations				
			zaskrbljenost glede zasebnosti	**stališče do spletne personalizacije**
Spearman's rho	**zaskrbljenost glede zasebnosti**	Correlation Coefficient	1,000	-,353**
		Sig. (2-tailed)	.	<,001
		N	306	306
	stališče do spletne personalizacije	Correlation Coefficient	-,353**	1,000
		Sig. (2-tailed)	<,001	.
		N	306	306

**. Correlation is significant at the 0,01 level (2-tailed).

Priloga 5: SPSS izpis za preverjanje 3. hipoteze

Tabela 10: Povezanost spremenljivk zaskrbljenost glede zasebnosti in pripravljenost za deljenje podatkov

Correlations				
			zaskrbljenost glede zasebnosti	**pripravljenost za deljenje podatkov**
Spearman's rho	**zaskrbljenost glede zasebnosti**	Correlation Coefficient	1,000	-,508**
		Sig. (2-tailed)	.	<,001
		N	306	306
	pripravljenost za deljenje podatkov	Correlation Coefficient	-,508**	1,000
		Sig. (2-tailed)	<,001	.
		N	306	306

**. Correlation is significant at the 0,01 level (2-tailed).

Priloga 6: SPSS izpis za preverjanje 4. hipoteze

Tabela 11: Opisna statistika spremenljivke »zaskrbljenost glede zasebnosti«

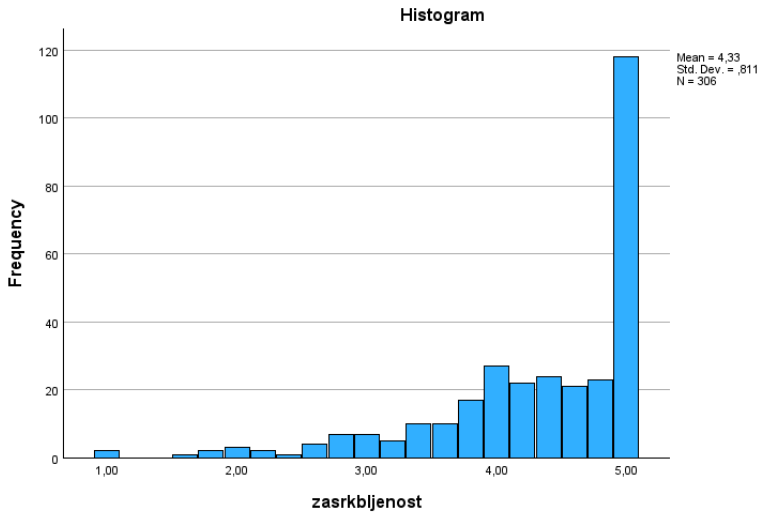
Descriptives				
			Statistic	Std. Error
zaskrbljenost glede zasebnosti	Mean		4,3288	,04634
	95% Confidence Interval for Mean	Lower Bound	4,2376	
		Upper Bound	4,4199	
	5% Trimmed Mean		4,4185	
	Median		4,6000	
	Variance		,657	
	Std. Deviation		,81060	
	Minimum		1,00	
	Maximum		5,00	
	Range		4,00	
	Interquartile Range		1,00	
	Skewness		-1,468	,139
	Kurtosis		2,136	,278

Tabela 12: Rezultati Kolmogorov-Smirnovega in Shapiro-Wilkovega testa

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
zaskrbljenost glede zasebnosti	Statistic	df	Sig.	Statistic	df	Sig.
	0,204	306	<,001	0,810	306	<,001

a. Lilliefors Significance Correction

Slika 1: Histogram porazdelitve spremenljivke »zaskrbljenost glede zasebnosti«



Slika 2: Q-Q graf porazdelitve spremenljivke »zaskrbljenost glede zasebnosti«

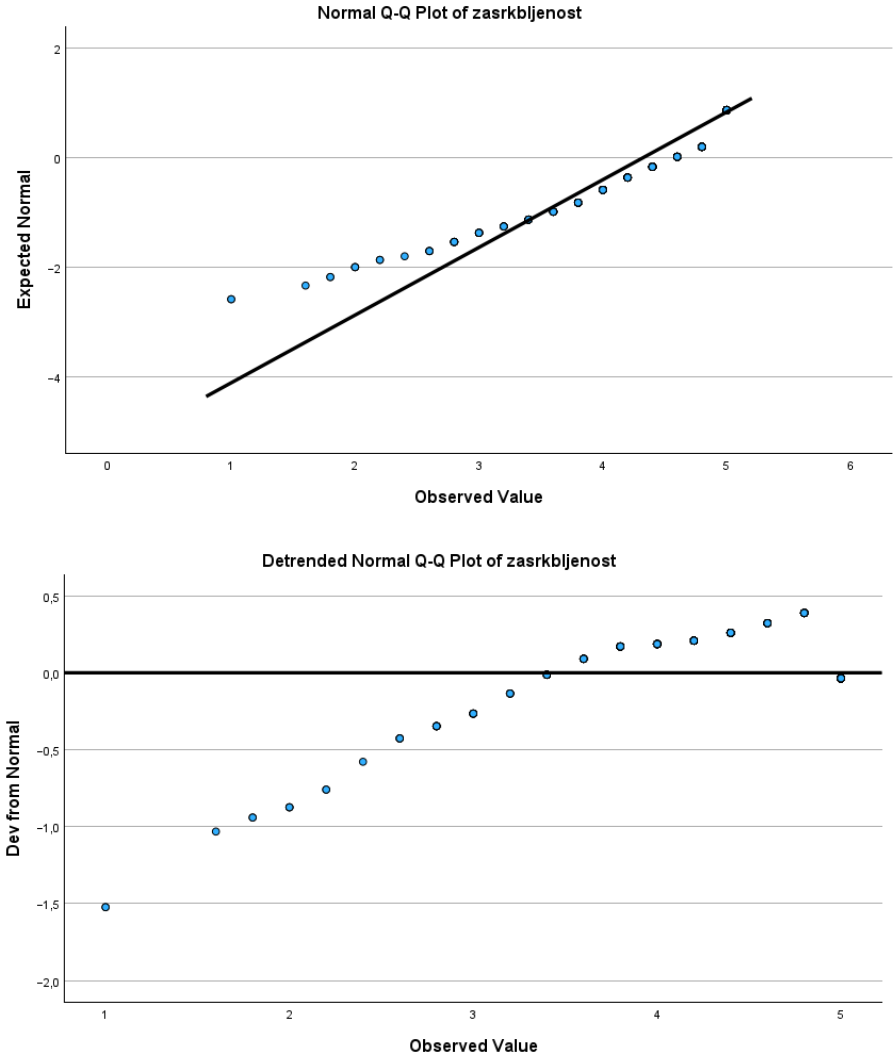


Tabela 13: Povzetek rezultatov Kruskal-Wallisovega testa

Independent-Samples Kruskal-Wallis Test Summary	
Total N	287
Test Statistic	23,620a
Degree Of Freedom	5
Asymptotic Sig.(2-sided test)	<,001

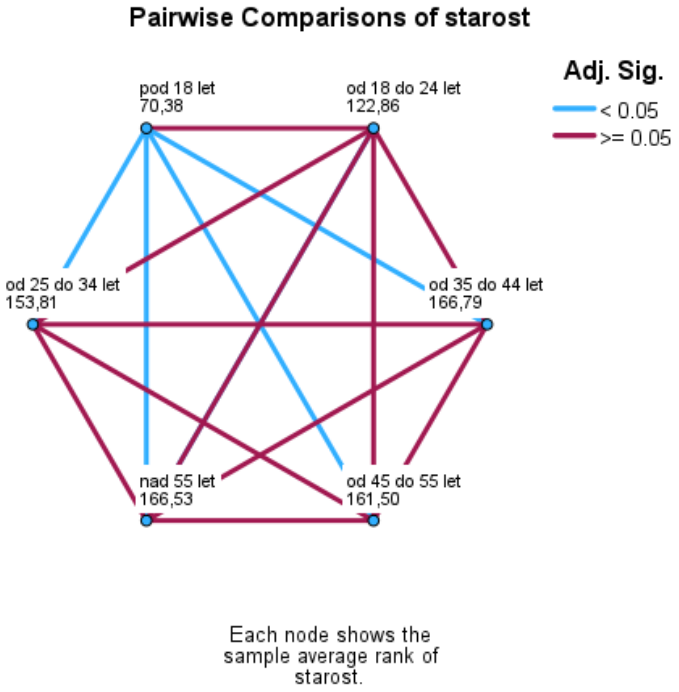
a. The test statistic is adjusted for ties.

Tabela 14: Rezultati Kruskal-Wallisovega testa – parne primerjave med starostnimi skupinami

Pairwise Comparisons of starost					
Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
pod 18 let-od 18 do 24 let	-52,488	24,837	-2,113	,035	,519
pod 18 let-od 25 do 34 let	-83,433	24,837	-3,359	<,001	,012
pod 18 let-od 45 do 55 let	-91,125	26,779	-3,403	<,001	,010
pod 18 let-nad 55 let	-96,158	31,322	-3,070	,002	,032
pod 18 let-od 35 do 44 let	-96,413	26,618	-3,622	<,001	,004
od 18 do 24 let-od 25 do 34 let	-30,945	11,989	-2,581	,010	,148
od 18 do 24 let-od 45 do 55 let	-38,637	15,620	-2,474	,013	,201
od 18 do 24 let-nad 55 let	-43,671	22,536	-1,938	,053	,790
od 18 do 24 let-od 35 do 44 let	-43,925	15,342	-2,863	,004	,063
od 25 do 34 let-od 45 do 55 let	-7,692	15,620	-,492	,622	1,000
od 25 do 34 let-nad 55 let	-12,726	22,536	-,565	,572	1,000
od 25 do 34 let-od 35 do 44 let	-12,980	15,342	-,846	,398	1,000
od 45 do 55 let-nad 55 let	-5,033	24,660	-,204	,838	1,000
od 45 do 55 let-od 35 do 44 let	5,287	18,320	,289	,773	1,000
nad 55 let-od 35 do 44 let	,254	24,485	,010	,992	1,000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2-sided tests) are displayed. The significance level is ,050.
a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Slika 3: Grafični prikaz statistične značilnosti parnih primerjav glede na starostno skupino



Priloga 7: SPSS izpis za preverjanje 5. hipoteze

Tabela 15: Povezanost posameznih trditev glede koristi spletne personalizacije in pripravljenosti za deljenje podatkov

Correlations						
			pripravljenost za deljenje podatkov	**dostop do relevantnih vsebin**	**dostop do zanimivih vsebin**	**olajšanje sprejemanja odločitev**
Spearman's rho	**pripravljenost za deljenje podatkov**	Correlation Coefficient	1,000	,609**	,581**	,489**
		Sig. (2-tailed)	.	<,001	<,001	<,001
		N	306	306	306	306
	dostop do relevantnih vsebin	Correlation Coefficient	,609**	1,000	,753**	,673**
		Sig. (2-tailed)	<,001	.	<,001	<,001
		N	306	306	306	306
	dostop do zanimivih vsebin	Correlation Coefficient	,581**	,753**	1,000	,628**
		Sig. (2-tailed)	<,001	<,001	.	<,001
		N	306	306	306	306
	olajšanje sprejemanja odločitev	Correlation Coefficient	,489**	,673**	,628**	1,000
		Sig. (2-tailed)	<,001	<,001	<,001	.
		N	306	306	306	306

**. Correlation is significant at the 0,01 level (2-tailed).

Tabela 16: Izračun koeficienta Cronbach alfa za združeno spremenljivko »zaznane koristi spletne personalizacije«

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,870	,870	3

Tabela 17: Povezanost zaznanih koristi in pripravljenosti za deljenje podatkov

Correlations				
			koristi spletne personalizacije	**pripravljenost za deljenje podatkov**
Spearman's rho	**koristi spletne personalizacije**	Correlation Coefficient	1,000	,619**
		Sig. (2-tailed)	.	<,001
		N	306	306
	pripravljenost za deljenje podatkov	Correlation Coefficient	,619**	1,000
		Sig. (2-tailed)	<,001	.
		N	306	306

**. Correlation is significant at the 0,01 level (2-tailed).

Priloga 8: SPSS izpis za preverjanje 6. hipoteze

Tabela 18: Rezultati Wilcoxonovega signed rank testa – povprečni rangi in vsote rangov

Ranks				
		N	Mean Rank	Sum of Ranks
Ime - E-mail naslov	Negative Ranks	88[a]	74,24	6533,00
	Positive Ranks	54[b]	67,04	3620,00
	Ties	164[c]		
	Total	306		
Ime - Demografski podatki (starost, spol, itd.)	Negative Ranks	106[d]	81,52	8641,00
	Positive Ranks	45[e]	63,00	2835,00
	Ties	155[f]		
	Total	306		
Ime - Podatki o interesih	Negative Ranks	114[g]	83,30	9496,00
	Positive Ranks	44[h]	69,66	3065,00
	Ties	148[i]		
	Total	306		

a. Ime < E-mail naslov
b. Ime > E-mail naslov
c. Ime = E-mail naslov
d. Ime < Demografski podatki (starost, spol, itd.)
e. Ime > Demografski podatki (starost, spol, itd.)
f. Ime = Demografski podatki (starost, spol, itd.)
g. Ime < Podatki o interesih
h. Ime > Podatki o interesih
i. Ime = Podatki o interesih

Tabela 19: Rezultati Wilcoxonovega signed ranks testa – testne statistike

Test Statistics[a]			
	Ime – Podatki o interesih	Ime – Demografski podatki (starost, spol, itd.)	Ime – E-mail naslov
Z	-5,665[b]	-5,484[b]	-3,059[b]
Stopnja značilnosti (2 - stranska)	< 0,001	< 0,001	0,002

a. Wilcoxon Signed Ranks Test

b. Based on positive ranks.

Priloga 9: SPSS izpis za preverjanje 7. hipoteze

Tabela 20: Povezanost zaskrbljenosti glede zasebnosti in verjetnosti uporabe tehnik za zaščito zasebnosti

Correlations				
			zaskrbljenost glede zasebnosti	**verjetnost uporabe tehnik za zaščito zasebnosti**
Spearman's rho	**zaskrbljenost glede zasebnosti**	Correlation Coefficient	1,000	,465**
		Sig. (2-tailed)	.	<,001
		N	306	306
	verjetnost uporabe tehnik za zaščito zasebnosti	Correlation Coefficient	,465**	1,000
		Sig. (2-tailed)	<,001	.
		N	306	306

**. Correlation is significant at the 0,01 level (2-tailed).