UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ZAZNAVANJE IN VAROVANJE ZASEBNOSTI NA DRUŽBENIH OMREŽJIH

Ljubljana, december 2019 KATJA PEZDIRC

IZJAVA O AVTORSTVU

Podpisana Katja Pezdirc, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Zaznavanje in varovanje zasebnosti na družbenih omrežjih, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Alešem Popovičem

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.

V Ljubljani, dne 20.12.2019 Podpis študentke: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

KAZALO PRILOG

SEZNAM KRATIC

ang. - angleško

EU – (ang. European Union); Evropska unija

GDPR – (ang. General Data Protection Regulation); Splošna uredba o varstvu podatkov

ZDA – (ang. United States of America); Združene države Amerike

UVOD

Ljudje smo družbena bitja – v naravi človeka so odnosi, druženje in medsebojno komuniciranje. Digitalna doba tega ni spremenila, spremenila pa je način komuniciranja, saj je prenesla druženje in komunikacijo ter odnose med ljudmi tudi v virtualni svet (Tayouri, 2015). Danes poznamo več načinov digitalne komunikacije, med njimi tudi družbena omrežja, ki uporabnikom omogočajo, da se predstavijo, si oblikujejo svojo mrežo stikov, vzdržujejo stike z ljudmi, ki jih poznajo, ali pa si ustvarijo nova poznanstva. Uporabniška kultura uporabe družbenih omrežij je močno vpeta v vsakdanje življenje uporabnikov. Uporabniki se povezujejo z drugimi uporabniki in z njimi delijo osebne podatke in informacije. Uporaba teh družbenih platform postaja za uporabnike vse bolj udobna, brez védenja o dolgoročnih posledicah, ki jih prinaša (Trottier, 2012).

V zadnjem desetletju smo priča eksponentnemu razvoju informacijsko-komunikacijskih tehnologij. S pojavom interneta in porastom priljubljenosti družbenih omrežij se danes ustvarja več informacij, kot jih je bilo doslej ustvarjenih v zgodovini naše družbe. Več milijard uporabnikov s participacijo in dejavnostmi na družbenih omrežjih razkriva informacije, zavedno ali nezavedno. S tem proizvaja ogromno količino podatkov, in ti osebni podatki so postali blago, s katerim trgujejo družbena omrežja.

Družbena omrežja so za uporabnike brezplačna, uporabniki sami pa so postali produkt, kajti lastniki teh platform so našli način, kako njihove osebne podatke pretvarjati v denar. Izkoriščanje osebnih podatkov je postalo večmilijardna panoga. Podjetje Forbes (2019) je med najvrednejše svetovne znamke na prva mesta, daleč pred ostalimi, uvrstilo tehnološka podjetja, ki se med drugim ukvarjajo tudi z obdelavo osebnih podatkov, to so Apple, Google, Microsoft, Amazon in Facebook.

Napredna tehnologija ne omogoča le zbiranja podatkov, temveč tudi pretvorbo podatkov v nove podatke in informacije. Vsakdanje navade uporabnikov je mogoče prepoznati z veliko natančnostjo, saj je po nekaterih raziskavah polovica tega, kar ljudje počnejo, le ponavljanje vzorcev prejšnjega dne. Tako imajo tisti, ki pridobijo podatke, ogromno moč, saj lahko vplivajo ne le na nakupovalne navade, temveč celo na razpoloženje, način komunikacije, vedenje, dojemanje, mišljenje in počutje.

S tehnološkim napredkom in hitro rastjo industrije, ki temelji na obdelavi osebnih podatkov, posameznik izgublja nadzor nad svojimi podatki ter vse bolj postaja predmet obdelave in manipuliranja, saj je razumevanje za povprečnega uporabnika nepregledno in nepredstavljivo. V zadnjih letih so številna podjetja začela spremljati posameznike in jim slediti na skoraj vsakem koraku in področju njihovega življenja. Stvari, ki so bile nekoč zasebne, zdaj puščajo sledi podatkov, ki izpostavljajo vedenje, gibanje, družbene odnose, interese, prepričanja, namere, mnogi zasebni trenutki pa se zdaj beležijo, ocenjujejo in analizirajo sproti v realnem času (Christl, 2017).

Nova generacija digitalnih komunikacij uporabnikom zagotavlja veliko vrednost z vidika izbire, dostopa in priložnosti. In čeprav obstajajo tudi pozitivni vplivi te vse bolj izpopolnjene analitike v vedno večjih in vse bolj medsebojno povezanih bazah podatkov v virtualnem prostoru, tako za uporabnike kot tudi podjetja, pa je zaskrbljujoča možnost zlorabe osebnih podatkov – ekonomska in socialna diskriminacija, skriti vpliv in manipulacija, prisila ter cenzura. Skupna raba vse večjih količin osebnih podatkov ne pomeni vedno večjega napredka, učinkovitosti ali enakosti. In propad zasebnosti lahko ogrozi našo avtonomijo (Acquisti, Brandimarte & Loewenstein, 2015).

Živimo v dobi informacij, zasebnost pa je vprašanje našega časa in področje, ki se mu v zadnjem času posveča vse več pozornosti. Z uporabo družbenih omrežij je pojem zasebnosti pogosto predmet različnih opredelitev in polemiziranja, saj informacijsko-komunikacijska tehnologija omogoča številne grožnje in zlorabe zasebnosti. Veliko prahu dvigujejo tudi aktualne afere o zlorabah osebnih podatkov (Cambridge Analytica, Edward Snowden), ozaveščenost ljudi pa se posledično postopoma povečuje. Kljub temu uporabniki še vedno dnevno razkrivajo svojo zasebnost in osebne podatke, ne da bi se dobro zavedali, da kar je bilo enkrat razkrito, ostane razkrito za vedno. Dosegli smo stopnjo, ko se zavedamo nevarnosti, ne vemo pa, kakšne bodo dolgoročne posledice v prihodnosti.

Namen magistrskega dela je predstaviti problem zasebnosti in varovanja osebnih podatkov uporabnikov na družbenih omrežjih ter osvetliti prakse družbenih omrežij, ki predstavljajo grožnjo zasebnosti za uporabnike. Cilj magistrskega dela pa je ugotoviti kako uporabniki zaznavajo zasebnost in varovanje osebnih podatkov, in ali je njihovo vedenje skladno z njihovim zaznavanjem.

V teoretičnem delu je metoda dela pregled in raziskovanje tega področja, predvsem na podlagi obstoječe literature tujih avtorjev. Glavna metoda raziskovanja v empiričnem delu je deskriptivna statična analiza na podlagi podatkov, pridobljenih z anketo. Namen moje raziskave je proučiti odnos uporabnikov do zasebnosti in varovanja osebnih podatkov na družbenih omrežjih. Moj cilj pa je ugotoviti, kako uporabniki zaznavajo zasebnost in varovanje osebnih podatkov in ali je njihovo vedenje v skladu z njihovim zaznavanjem, ter ugotovitve primerjati z nekaterimi že obstoječimi študijami na tem področju.

Magistrsko delo je razdeljeno v štiri poglavja. Uvodu sledi prvo poglavje, v katerem sem najprej opredelila osnovna pojma: osebni podatek in zasebnost, ki sta pomembna za razumevanje celotnega dela. Zasebnost je večdimenzionalni koncept, ki ga težko opredelimo, poleg tega pa se je skozi različna časovna obdobja pogled na zasebnost spreminjal, zato sem opisala razvoj zasebnosti na podlagi starejših opredelitev, kot tudi informacijsko zasebnost, ki je dobila velik pomen z razvojem interneta v dobi informacij. Informacijska zasebnost je tesno povezana z varovanjem osebnih podatkov in zaščito zasebnosti, zato sem opisala »poštene informacijske prakse« na področju zbiranja in

upravljanja z osebnimi podatki na internetu. Pomembno vlogo pri varovanju zasebnosti ima tudi država, zato sem predstavila Splošno uredbo o varstvu podatkov (angl. General Data Protection Regulation – GDPR), v nadaljevanju Splošna uredba, ki v obstoječo zakonodajo na področju varstva osebnih podatkov prinaša veliko novosti in sprememb.

V drugem poglavju sem pozornost namenila družbenim omrežjem. Glede na veliko število uporabnikov in priljubljenost sem želela orisati pomembnost družbenih omrežij za uporabnike in vpliv, ki ga imajo ta omrežja v družbi. To prinaša tudi problematiko družbenih omrežij z vidika zasebnosti, saj se osebni podatki in informacije uporabnikov zbirajo in analizirajo, družbena omrežja pa z njimi trgujejo z namenom dobička. V tem poglavju sem predstavila tudi grožnje in nevarnosti v zvezi z zasebnostjo, ki pretijo uporabnikom družbenih omrežij.

V tretjem poglavju sem proučevala zasebnost na družbenih omrežjih; predvsem me je zanimal pogled z vidika uporabnikov. Pri tem sem si pomagala s pregledom obstoječe literature tujih avtorjev in že opravljenih študij. V tem poglavju me je zanimalo, kakšen odnos imajo uporabniki do lastne zasebnosti na družbenih omrežjih, kako jo sami zaznavajo in kakšno je njihovo vedenje na teh omrežjih. Opisala sem tudi paradoks zasebnosti, ki omenja neskladje med zaskrbljenostjo uporabnikov glede zasebnosti in dejanskim razkrivanjem zasebnosti.

V četrtem poglavju sem naredila raziskavo na podlagi ankete in pridobljene podatke združila v več vsebinskih sklopov, ki so bistveni za obravnavano temo: priljubljenost in uporaba družbenih omrežij, razkrivanje zasebnosti, zaskrbljenost uporabnikov glede zasebnosti ter zaznavanje zasebnosti. Poglavje se zaključi z rezultati analize in primerjavo z rezultati nekaterih drugih tujih študij. Na koncu sem na podlagi proučevanja, raziskovanja in analiziranja podala svoje predloge izboljšav, ki bi lahko pripomogli k boljšemu in zavestnejšemu varovanju zasebnosti na družbenih omrežjih. V sklepu magistrskega dela sem strnila glavna dejstva in ugotovitve.

1 ZASEBNOST IN VARNOST OSEBNIH PODATKOV

1.1 Opredelitev osebnih podatkov in zasebnosti

V šestem členu Zakona o varstvu osebnih podatkov je osebni podatek opredeljen kot kateri koli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Ključna pri tem je določljivost oziroma možnost razlikovanja med posamezniki. Osebni podatki zajemajo vse informacije, ki se nanašajo na določeno ali določljivo fizično osebo. Določljiva fizična oseba je tista, ki jo je mogoče neposredno ali posredno identificirati, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so

značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto (Kotsios, Magnani, Rossi, Shklovski & Vega, 2019).

Po besedah Evropske komisije veljajo za osebne podatke tudi različne posamezne informacije, ki lahko skupaj privedejo do identifikacije določene osebe, kot tudi osebni podatki, ki so bili deidentificirani, šifrirani ali psevdonimizirani, vendar se lahko uporabijo za ponovno identifikacijo osebe.

Osebni podatki zajemajo torej vse informacije, ki se nanašajo na posameznika in s pomočjo katerih je mogoče neposredno ali posredno ugotoviti posameznikovo identiteto. Primeri osebnih podatkov, ki jih navaja Evropska komisija (brez datuma), so med drugim ime in priimek, domači naslov, naslov elektronske pošte (npr. ime.priimek@podjetje.si), številka osebne izkaznice, podatki o lokaciji (npr. funkcija posredovanja podatkov o lokaciji na mobilnem telefonu), naslov IP, oznaka piškotka, identifikator za oglaševalce na mobilnem telefonu ter podatki, ki jih hrani bolnišnica ali zdravnik in na podlagi katerih bi bilo mogoče na edinstven način identificirati osebo.

Poleg tega poznamo tudi podatke, ki veljajo za »občutljive« in za katere so določeni posebni pogoji za obdelavo. Evropska komisija (brez datuma) jih opredeljuje kot podatke, ki razkrivajo rasno ali etično poreklo, politična mnenja, veroizpoved ali filozofska prepričanja, članstvo v sindikatu, genetske podatke, biometrične podatke, ki se obdelujejo samo za namene identifikacije osebe, podatke o zdravstvenem stanju in podatke o spolnem življenju ali spolni usmerjenosti posameznika.

Zasebnost je težko opredeliti, saj zaradi svoje subjektivnosti ni nedvoumno ali jasno opredeljena. Opredelitve zasebnosti se zelo razlikujejo glede na kontekst in okolje, in čeprav univerzalna opredelitev zasebnosti ne obstaja, poznamo več vrst opredelitev zasebnosti, ki jih navajajo številni avtorji.

Že leta 1890 je Brandeis trdil, da je zasebnost najbolj cenjena svoboščina v demokraciji, in jo opredelil kot »pravico, da te pustijo pri miru« (World Legal Information Institute, 2006). Prav tako kot Brandeis je tudi Westin vplival na to, kako razumemo zasebnost. Westinova teorija zasebnosti govori o tem, da se ljudje zaščitijo pred drugimi tako, da drugim začasno omejijo dostop do sebe. Zasebnost opredeljuje kot »pravico posameznikov, skupin ali institucij, da same določijo, kdaj, kako in v kolikšni meri se bodo podatki o njih posredovali drugim« (World Legal Information Institute, 2006).

Bloustein (1964) je zasebnost opredelil kot interes človekove osebnosti, ki varuje nedotakljivost osebnosti, posameznikovo neodvisnost, dostojanstvo in integriteto.

Smith (2004, str. 8) opredeljuje zasebnost kot »željo vsakega od nas po fizičnem prostoru, kjer smo lahko brez prekinitev, vdora, zadrege ali odgovornosti ter poskusa nadzora časa in razkrivanja osebnih podatkov o sebi«.

Clarke (1999) pravi, da »je zasebnost interes, ki ga imajo posamezniki za ohranjanje ‚osebnega prostora', brez vmešavanja drugih ljudi in organizacij«. O zasebnosti govori kot o večdimenzionalnem konceptu, ki vključuje:

- **telesno zasebnost**, ki se ukvarja z integriteto posameznikovega telesa, kar vključuje obvezno cepljenje, transfuzijo krvi brez privolitve, obvezno zagotavljanje vzorcev telesnih tekočin in tkiv ter obvezno sterilizacijo;
- **zasebnost obnašanja**, ki se nanaša na vse vidike vedenja posameznika, zlasti na vedenje z občutljivo konotacijo, kot so spolne preference in navade, politične dejavnosti ter verska prepričanja, tako na zasebnih kot javnih mestih;
- **zasebnost osebnega komuniciranja**, ki se nanaša na interes posameznika, da z drugimi komunicira prek različnih medijev, brez nadzora s strani drugih oseb ali organizacij;
- **zasebnost osebnih podatkov (t. i. informacijska zasebnost)**, ki se nanaša na to, da osebni podatki posameznika ne bi smeli biti samodejno na razpolago drugim posameznikom in organizacijam – v primeru, da ima podatke druga oseba, bi moral imeti posameznik možnost nadzora nad temi podatki in njihovo uporabo.

Ne glede na opredelitve, ki so se oblikovale v preteklosti, moramo v sedanjosti o zasebnosti razmišljati nekoliko drugače. Pojav interneta in uporaba družbenih omrežij v digitalni dobi sta problem zasebnosti prenesla v virtualni prostor, kjer je ogrožena zasebnost uporabnikov spleta in družbenih omrežij. Novejše opredelitve poudarjajo pomen informacijske zasebnosti z vidika razkrivanja, posredovanja osebnih podatkov tretjim osebam in upravljanja z njimi. V nadaljevanju se bom osredotočila na t. i. informacijsko zasebnost.

1.2 Informacijska zasebnost

V današnjem času smo ob napredku in razvoju informacijsko-komunikacijskih tehnologij priča številnim spremembam, ki zaznamujejo moderno družbo. Napredne tehnologije omogočajo zbiranje, analiziranje in posredovanje informacij o vseh vidikih posameznikovega življenja hitreje in v večjem obsegu kot kadar koli prej.

Smith, Milberg in Burke (1996) opredeljujejo štiri dimenzije informacijske zasebnosti: zbiranje, nepooblaščeno uporabo, nepravilen dostop in napake. Sekundarna uporaba podatkov se nanaša na uporabo podatkov za druge namene kot tiste, za katere so bili prvotno zbrani. Večina opredelitev informacijske zasebnosti vključuje neko obliko nadzora posameznikov nad uporabo njihovih osebnih podatkov (Bélanger, Hiller & Smith, 2002;

Stone, Gardner, Gueutal & McClure, 1983), med drugim tudi Clarkova (1999), v kateri informacijsko zasebnost opredeljuje kot »interes posameznika po nadzoru ali vsaj z možnostjo bistvenega vplivanja na obdelavo podatkov o sebi«.

Informacijsko-komunikacijske tehnologije danes omogočajo namensko in naključno zbiranje, procesiranje, klasificiranje in povezovanje podatkov. Poleg množične obdelave in kombiniranja pa omogočajo tudi prenos in povezovanje različnih podatkov. Zbrani podatki lahko na ta način (naključno ali z določenim namenom) postanejo dostopni osebam ali organizacijam, ki za njihovo uporabo niso pooblaščene, ali pa se začnejo uporabljati za druge namene kot tiste, za katere so bili zbrani, pogosto brez zavedanja posameznikov (Kovačič, 2000).

Na podlagi zgoraj opisanega lahko sklepamo, da je informacijska zasebnost pravica posameznika, ki pa je v današnjem svetu ogrožena. Glavno skrb predstavljajo zbiranje, uporaba in posredovanje osebnih podatkov. Napredna informacijsko-komunikacijska tehnologija lahko z zbiranjem in obdelavo osebnih podatkov oblikuje profile posameznikovih navad in vedenja, sledi njegovi lokaciji in ugotavlja, kje se nahaja, ocenjuje tveganja in priložnosti ter oblikuje politike in poslovne načrte. Vsak posameznik bi moral imeti pravico do nadzora nad svojimi osebnimi podatki ter nad tem, kako in kdaj se bodo posredovali drugim. Ta zamisel je povezana z idejo o **»poštenih informacijskih praksah«** (angl. Fair Information Practices), ki je vplivala na razvoj zakonov o varstvu podatkov po svetu in je bila v središču razprav o ustreznem ravnovesju med posameznikovim nadzorom nad osebnimi podatki in interesi tretjih oseb pri obdelavi podatkov (Raab & Gold, 2011).

Informacijska zasebnost govori o varovanju podatkov posameznikov, kjer je nadzor nad lastnimi osebnimi podatki bistvenega pomena, zato jo številni avtorji enačijo z varstvom osebnih podatkov.

1.3 Varstvo osebnih podatkov in varovanje zasebnosti

Varstvo osebnih podatkov je temeljna pravica v Evropski uniji (v nadaljevanju EU). V Listini o temeljnih pravicah EU, ki državljanom EU zagotavlja varstvo osebnih podatkov, je zapisano, da ima »vsakdo pravico do varstva osebnih podatkov, ki se nanj nanašajo«. V Sloveniji varovanje osebnih podatkov določa 38. člen Ustave, ki pravi:

»Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.«

Pojem zasebnosti uporabnikov spleta in družbenih omrežij se največkrat razume kot pravica uporabnika do nadzora nad zbiranjem, obdelovanjem in prikazovanjem podatkov o njem. Razkrivanje podatkov je pravica posameznika, da odloča o tem, katere osebne podatke bo razkril in komu. Zasebnost na spletu se tako največkrat prepleta z varstvom osebnih podatkov, in sicer v smislu upravljanja osebnih podatkov. Varovanje zasebnosti se pogosto obravnava z vidika določanja meje, kako daleč lahko družba posega v posameznikove zadeve.

Pri varovanju zasebnosti gre za postopek iskanja ustreznega ravnotežja med zasebnostjo in različnimi konkurenčnimi interesi. Zaradi nasprotujočih si interesov med različnimi udeleženci je oblikovanje pravil o varstvu zasebnosti izjemno težko. Najbolj konstruktiven pristop je vzpostavitev splošnih načel in uporaba teh načel za vse organizacije, učinkovite sankcije v primeru neskladnosti oziroma kršitev, razvijanje operativnih kodeksov ravnanja, ki so skladni z načeli, vzpostavitev postopka reševanja sporov na ravni posameznih organizacij in industrijskh panog ter okvir, ki povezuje, da bodo načela, kodeksi in sankcije postali izvršljivi z izvensodnimi in sodnimi postopki (Clarke, 1999).

1.3.1 Poštene informacijske prakse

Obstajajo različne informacijske prakse glede zbiranja in upravljanja z osebnimi podatki na internetu. Ameriška Zvezna komisija za trgovino (1998) v poročilu opredeljuje pet temeljnih načel varstva zasebnosti. Gre za ukrepe, ki so potrebni za zagotavljanje »poštenih informacijskih praks«, ki so bile zasnovane za zagotavljanje ravnovesja med željo potrošnikov po zaščiti zasebnosti in željo podjetij po pridobitvi informacij o potrošnikih (Bélanger & Crossler, 2011).

1.3.1.1 Obvestilo/ozaveščenost (angl. notice/awareness)

Vsak uporabnik bi moral biti seznanjen z informacijskimi praksami subjektov, ki upravljajo z osebnimi podatki, še preden se ti podatki zberejo. Brez predhodnega obvestila uporabnik ni informiran in ne more sprejeti informirane odločitve o tem, ali želi razkriti svoje osebne podatke. Pred razkritjem osebnih podatkov bi uporabniki torej morali biti obveščeni o subjektu, ki zbira podatke, o namenu njihove uporabe in morebitnih prejemnikih, o tem, ali je predložitev zahtevanih podatkov prostovoljna ali zahtevana in kakšne so posledice zavrnitve posredovanja zahtevanih podatkov, ter o ukrepih, ki jih je sprejel zbiralec podatkov za zagotovitev njihove zaupnosti, celovitosti in kakovosti. Obvestilo mora biti jasno, nedvoumno in razumljivo ter objavljeno na vidnem mestu, kjer se zbirajo informacije o uporabnikih. Le tako je lahko učinkovito z vidika obveščanja

uporabnikov o tem, kaj se bo z razkritimi osebnimi podatki zgodilo (Zvezna komisija za trgovino, 1998).

1.3.1.2 Izbira/soglasje (angl. choice/consent)

Drugo splošno sprejeto temeljno načelo informacijske prakse je izbira ali soglasje. Izbira pomeni, da se lahko uporabniki odločijo, na kakšen način se lahko zbrani osebni podatki uporabljajo. Nanaša se zlasti na sekundarno uporabo informacij, ki je lahko notranja ali zunanja. Notranja sekundarna uporaba informacij je na primer dajanje potrošnikov na seznam za pošiljanje (mailing lista) podjetja, ki zbira podatke, z namenom trženja dodatnih izdelkov ali promocij. Pri zunanji sekundarni uporabi informacij pa gre za prenos informacij tretjim osebam (Zvezna komisija za trgovino, 1998).

Tradicionalno sta bili obravnavani dve vrsti režima izbire oziroma soglasja: možnost privzete vključitve in privzete zavrnitve (angl. opt-in/opt-out). Pri izbiri privzete vključitve gre za potrditev zbiranja in/ali uporabe informacij, pri izbiri privzete zavrnitve pa gre za zavrnitev le-tega. Subjekti lahko uporabnikom omogočajo tudi, da sami uravnavajo naravo informacij, ki jih razkrijejo, in načine uporabe teh informacij. Za učinkovitost tega sistema je ključno uporabnikom zagotoviti enostaven in lahko dostopen način za uveljavitev izbire. V spletnem okolju se izbira lahko izvede s klikom polja na računalniškem zaslonu, ki označuje uporabnikovo odločitev glede uporabe in razširjanja zbranih informacij. Spletno okolje poleg tega predstavlja nove možnosti za preseganje paradigme privzetih vključitev in zavrnitev. Od uporabnikov se lahko na primer zahteva, da pred obiskom spletnega mesta navedejo svoje nastavitve glede uporabe informacij. Na ta način se učinkovito odpravi kakršna koli potreba po privzetih pravilih (Zvezna komisija za trgovino, 1998).

1.3.1.3 Dostop/sodelovanje (angl. access/participation)

Dostop oziroma sodelovanje je tretje temeljno načelo, ki je bistveno za zagotavljanje točnosti in popolnosti podatkov. Nanaša se na zmožnost uporabnika, da dostopa do svojih podatkov in jih v primeru nepopolnosti ali netočnosti izpodbija oziroma zanika. Za smiselnost tega načela so pomembni pravočasen in cenovno ugoden dostop do podatkov, preprosto sredstvo za izpodbijanje netočnih in nepopolnih podatkov, mehanizem, s katerim lahko zbiralec podatkov preveri informacije, in mehanizem, s katerim se lahko dodajo popravki ali ugovori uporabnikov, ki se nato pošljejo vsem prejemnikom podatkov (Zvezna komisija za trgovino, 1998).

1.3.1.4 Integriteta/varnost (angl. integrity/security)

Četrto splošno sprejeto načelo je točnost in varnost podatkov. Subjekti, ki podatke zbirajo, morajo za celovitost podatkov sprejeti ukrepe, kot so uporaba uglednih virov podatkov,

navzkrižno primerjanje podatkov z več viri, zagotavljanje dostopa do podatkov in uničenje zastarelih podatkov ali pretvorba podatkov v anonimno obliko (Zvezna komisija za trgovino, 1998).

To načelo vključuje tako organizacijske kot tudi tehnične ukrepe za zaščito podatkov pred izgubo, nepooblaščenim dostopom, uničenjem, uporabo ali razkritjem. Ukrepi vključujejo notranje organizacijske ukrepe, ki omejujejo dostop do podatkov in zagotavljajo, da tisti, ki imajo dostop, podatkov ne uporabljajo za nedovoljene namene. Med tehnične varnostne ukrepe, ki preprečujejo nepooblaščen dostop do podatkov, sodijo: šifriranje pri prenosu in shranjevanju podatkov, omejitev dostopa z uporabo gesel in shranjevanje podatkov na varnih strežnikih ali računalnikih, ki niso dostopni prek interneta (Zvezna komisija za trgovino, 1998).

1.3.1.5 Uveljavljanje/odškodnina (angl. enforcement/redress)

Temeljna načela varovanja zasebnosti so učinkovita, če obstaja mehanizem za njihovo uveljavljanje. Brez tega mehanizma je kodeks poštenih informacijskih praks le sugestiven in ne predpisujoč ter posledično ne zagotavlja spoštovanja načel poštene informacijske prakse. Ti postopki so potrebni, da se zagotovi skladnost organizacij z njihovimi politikami, in z vidika obravnave pritožb uporabnikov (Zvezna komisija za trgovino, 1998).

1.3.2 Kritika informacijskih praks

Zvezna komisija za trgovino (1998) je komponento obvestila označila kot temeljno načelo zaščite osebnih podatkov; ostala načela, ki poskušajo potrošnikom nuditi nadzor nad podatki, so namreč smiselna le v primeru, da je uporabnik seznanjen s politiko podjetja in svojimi pravicami v zvezi s tem (Obar & Oeldorf-Hirsch, 2018).

»Okvir za obveščanje in izbiro zasebnosti je bil zasnovan tako, da so posamezniki sami odgovorni za zbiranje in uporabo njihovih osebnih podatkov« (Reidenberg, Russell, Callen, Qasir & Norton, 2014, str. 3). Obstajajo varnostni mehanizmi, ki priporočajo, kako lahko uporabniki preverjajo, popravljajo in odobrijo osebne podatke, s katerimi upravljajo različne organizacije (Obar & Oeldorf-Hirsch, 2018).

Družbena omrežja, ki sodelujejo pri zbiranju in obdelavi podatkov uporabnikov, poskušajo politiko obveščanja spoštovati tako, da uporabnikom zagotovijo obvestila s soglasjem, navadno v obliki politike zasebnosti (angl. Privacy Policy) in pogojev uporabe (angl. Terms of Use). Ti najpogostejši praksi obveščanja se prikažeta na spletnih mestih in v aplikacijah, ko se uporabnik prvič poveže s subjektom, ter ob spremembi teh politik (Obar & Oeldorf-Hirsch, 2018) .

Sprva se je zdelo, da je politika zasebnosti dobra ideja, toda v praksi pogosto ostanejo nerešene težave. Uporabniki v mnogih primerih ne opazijo, ne berejo ali ne razumejo pravilnikov o zasebnosti (Leibowitz, 2007, str. 4). V tem kontekstu Obar in Oeldorf-Hirsch (2018) v svoji študiji frazo »prebral sem in strinjam se s pogoji« označujeta kot največjo laž na internetu, neprebiranje politik zasebnosti in pogojev uporabe pa dojemata kot realnost in obenem kot težavo.

Praksa nespoštovanja zasebnosti je zelo razširjena, kar kaže na to, da politike obveščanja ne delujejo. Eden od razlogov za neučinkovitost tega načina varovanja zasebnosti je ta, da so obvestila oziroma pravilniki o zasebnosti prezapleteni in predolgi. Poleg tega se pogosto spreminjajo, kar pomeni, da bi jih morali uporabniki ob spremembah znova prebrati. McDonald in Cranor (2008) sta v svoji študiji ugotovila naslednje: če bi uporabniki spleta enkrat prebrali pravila o zasebnosti spletnih mest, ki jih obiščejo, bi vsak porabil približno 244 ur na leto, kar znese več kot šest delovnih tednov in je nesmiselno tudi s časovnega vidika. Rezultati študije kažejo na to, da večina uporabnikov komponento obvestila dojema kot nadlogo na svoji poti do konzumiranja digitalnih vsebin, kot so pogovor s prijatelji na družbenih omrežjih, objave statusov, fotografij in podobno.

Kljub kritikam glede neučinkovitosti politik zasebnosti je regulacija s strani države zelo pomembna, saj napredek tehnologije omogoča številne posege v zasebnost uporabnikov. Glavni namen pravnih aktov in načel za varovanje zasebnosti je povečanje nadzora uporabnikov nad njihovimi osebnimi podatki ter večja transparentnost uporabe podatkov. V nadaljevanju bom opisala, kako je varovanje informacijske zasebnosti in osebnih podatkov urejeno v Evropski uniji.

1.4 Pravni vidik zasebnosti in varstva osebnih podatkov

Hiter razvoj informacijsko-komunikacijske tehnologije in digitalizacija na skoraj vseh področjih našega življenja omogočata vse večji obseg zbiranja osebnih podatkov in pretok informacij o posameznikih. Informacijska tehnologija, ki omogoča lažje sledenje, profiliranje in uporabo informacij v različne namene, predstavlja vse večjo grožnjo zasebnosti posameznikov in možnost številnih zlorab, zato je regulacija na področju varovanja osebnih podatkov nujno potrebna.

Razvoj digitalne dobe in posledično okrnjene pravice posameznikov so pripeljale do sprejema novega predpisa, ki v državah članicah Evropske unije zagotavlja poenoteno in usklajeno ukrepanje v zvezi z varstvom osebnih podatkov. Evropski parlament in Svet Evropske unije sta s Splošno uredbo po večletnih pogajanjih dosegla dogovor o novih pravilih Evropske unije glede varstva osebnih podatkov (Informacijski pooblaščenec, 2017.

1.4.1 Splošna uredba

Splošna uredba, ki določa nova pravila glede varstva osebnih podatkov, je začela veljati 24. maja 2016, v državah članicah EU pa se je začela uporabljati 25. maja 2018. Načela, opredeljena v Splošni uredbi, so obvezna za organizacije, ki delujejo v Evropski uniji, in za organizacije po vsem svetu, vključno z družbenimi omrežji, ki zbirajo in obdelujejo osebne podatke uporabnikov iz Evropske unije (Peras, Mekovec & Picek, 2018). Cilj Splošne uredbe je omogočiti prebivalcem več nadzora nad njihovimi osebnimi podatki ter poenotiti in dvigniti raven varstva osebnih podatkov v Evropski uniji (Informacijski pooblaščenec, 2017).

Nove tehnologije in organizacijski modeli so tako v zasebnem kot javnem sektorju olajšali zbiranje, uporabo, združevanje in druge oblike obdelovanja velike količine osebnih podatkov, toda brez ustreznega nadzora. Cilj Splošne uredbe je zaščita temeljnih pravic in svoboščin posameznikov, na katere se osebni podatki nanašajo, in sicer z oblikovanjem ustreznega režima v zvezi z obdelavo osebnih podatkov. Splošna uredba poleg tega podpira oblikovanje enotnega evropskega trga z optimalnimi pogoji za prost pretok osebnih podatkov, vzporedno s prostim pretokom blaga in storitev (Kotsios, Magnani, Rossi, Shklovski & Vega, 2019).

Večina podatkov, ki se pojavljajo na družbenih omrežjih, je povezanih z osebnim življenjem uporabnikov in takorekoč predstavljajo osebne podatke. Uporabniki, ki razkrivajo osebne podatke, se pogosto ne zavedajo njihove potencialne tržne vrednosti. V skladu s Splošno uredbo bi morali biti osebni podatki zbrani z upoštevanjem načel zakonitosti, poštenosti in transparentnosti ter z omejitvami glede namena, zmanjševanja podatkov, točnosti, omejitve shranjevanja, celovitosti, zaupnosti in odgovornosti (Peras, Mekovec & Picek, 2018).

Glede na obstoječo zakonodajo na področju varstva osebnih podatkov prinaša Splošna uredba precej novosti in sprememb. Posameznikom, ki so v kontekstu družbenih omrežij uporabniki teh omrežij, zagotavlja boljše varovanje osebnih podatkov in okrepljene pravice na tem področju, z upoštevanjem naslednjih načel Splošne uredbe (Peras, Mekovec & Picek, 2018):

- Podatki morajo biti obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo. Uporabniki bi morali vedeti, na kakšen način se osebni podatki zbirajo in uporabljajo, kdo jih uporablja, ter poznati namen in trajanje obdelave podatkov.
- Podatki, ki so zbrani za en namen, ne smejo biti obdelani za noben drug namen. Za vsak namen obdelave je treba pridobiti soglasje uporabnikov.
- Podatki morajo biti ustrezni, relevantni in omejeni na namen obdelave. Zbiranje podatkov, ki niso potrebni za namen obdelave, ni dovoljeno.

- Podatki morajo biti točni in posodobljeni, kadar je to potrebno. Uporabnik bi moral imeti možnost izbrisa ali spreminjanja napačnih podatkov.
- Podatki se hranijo le toliko časa, kot je potrebno za namene, za katere se obdelujejo. Določiti je treba roke za izbris in uničenje podatkov.
- Podatke je treba zaščititi pred nepooblaščeno ali nezakonito obdelavo in nenamerno izgubo, poškodbo ali uničenjem.
- Najpomembnejša novost je načelo odgovornosti, kar pomeni, da so družbena omrežja odgovorna za ravnanje z osebnimi podatki, njihovo obdelavo ali uporabo.

Komponenti Splošne uredbe, ki sta v kontekstu družbenih omrežij še posebej pomembni, sta politika zasebnosti in soglasje uporabnikov. Obe komponenti predstavljata temelj, na katerem lahko družbena omrežja uporabljajo osebne podatke. Preden uporabnik soglaša s politiko zasebnosti družbenega omrežja, mora to politiko razumeti. Družbeno omrežje pa mora politiko zasebnosti uporabniku podati v jasni in razumljivi obliki.

1.4.2 Soglasje uporabnikov (zakonitost obdelave osebnih podatkov)

Pri obdelavi podatkov na družbenih omrežjih je poudarek na soglasju uporabnikov, čeprav soglasje ni edina veljavna pravna podlaga za obdelavo osebnih podatkov. Soglasje je ustrezna zakonita podlaga le v primeru, ko sta uporabniku ponujena nadzor in izbira v zvezi s sprejemanjem ali zavračanjem ponujenih pogojev. Obenem pa zavračanje pogojev ne sme imeti škodljivih posledic za uporabnika (Peras, Mekovec & Picek, 2018).

Splošna uredba opredeljuje šest pravnih podlag zakonitosti obdelave osebnih podatkov. Družbena omrežja morajo določiti, katera od teh pravnih podlag je primerna za obdelavo osebnih podatkov uporabnikov glede na namen obdelave, vrsto osebnih podatkov in uporabnika, na katerega se nanašajo, ter namen uporabe podatkov (Peras, Mekovec & Picek, 2018):

Obdelava je zakonita le, kadar je izpolnjen vsaj eden od naslednjih pogojev:

- Posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo svojih osebnih podatkov za enega ali več določenih namenov.
- Obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe.
- Obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca.
- Obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe.
- Obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu.

- Obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika.

Obstajajo štiri vrste dejanj, ki lahko predstavljajo kršitev varnosti osebnih podatkov (Chander, Gelman & Radin, 2008):

- Zbiranje podatkov: zbiranje osebnih podatkov je v nasprotju z željami uporabnika.
- Zloraba podatkov: uporaba osebnih podatkov je v nasprotju z željami uporabnika.
- Souporaba podatkov: prostovoljno razkritje osebnih podatkov tretjim osebam na način, ki je v nasprotju z željami uporabnika.
- Kršitev varnosti: nepooblaščen dostop do osebnih podatkov.

Vsem opisanim kršitvam osebnih podatkov je skupno pomanjkanje soglasja uporabnika. Soglasje je dovoljenje za zbiranje, shranjevanje in obdelavo osebnih podatkov, ki jih uporabniki posredujejo družbenim omrežjem. Obrazec za soglasje mora imeti kratke in berljive izraze, prostori, ki jih je potrebno označiti, pa morajo biti prazni. Vendar če to ni nujno, privolitev uporabnika ne sme biti pogoj za dostop. »Soglasje izraža prostovoljno, specifično, informativno in nedvoumno uporabniško soglasje o obdelavi njegovih osebnih podatkov« (Peras, Mekovec & Picek, 2018).

Če želijo družbena omrežja zbirati osebne podatke, morajo uporabnike obvestiti o namenu obdelave teh podatkov. Družbena omrežja morajo biti sposobna kadarkoli dokazati, da je uporabnik podal soglasje za obdelavo osebnih podatkov za ta namen. Uporabniki lahko kadarkoli zavrnejo pravico do zbiranja, shranjevanja ali obdelave osebnih podatkov. Vendar pa je praksa daleč od teorije. Raziskava je pokazala, da uporabniki družbenih omrežij ne morejo zavrniti pravilnikov o zasebnosti, ki v večini primerov vplivajo na razkritje osebnih podatkov. Poleg tega so politike zasebnosti za običajnega uporabnika prezapletene in zbirajo več podatkov, kot je potrebno (Peras, Mekovec & Picek, 2018).

1.4.3 Politike zasebnosti

Predhodne raziskave kažejo, da večina uporabnikov ne bere pravilnikov o zasebnosti. Le minimalen odstotek uporabnikov spremeni visoko prepustne preference zasebnosti, in na splošno so popolnoma določljive informacije na voljo vsakomur, ki je prisoten na določenem družbenem omrežju in pridobi vsaj en edinstven identifikator (Gross & Acquisti, 2005). Kljub pomislekom glede razkritja osebnih podatkov na družbenih omrežjih v povezavi z varnostjo in zasebnostjo osebnih podatkov se zdi, da koristi, ki jih uporabniki pričakujejo od razkritja, presegajo njihove zaznane stroške, zato jih še naprej razkrivajo (Young & Quan-Haase, 2009). Obenem večina uporabnikov družbenih omrežij same sebe smatra kot številko, zato niso zaskrbljeni glede zasebnosti osebnih podatkov in posledično razkrivanja le-teh (Bechmann, 2014). Da bi Splošna uredba pomagala zaščititi

njihovo zasebnost, bi morala družbena omrežja spoštovati naslednja načela (Peras, Mekovec & Picek, 2018):

- Ne smejo zbrati več podatkov, kot je potrebno.
- Osebnih podatkov uporabnikov ne smejo uporabljati za namene, ki niso navedeni.
- Podatkov ne obdržijo, če niso več potrebni.
- Podatkov ne smejo posredovati tretjim osebam.

Vse zgoraj navedeno velja v primeru, če uporabnik ne poda svojega soglasja.

Za organizacije, ki ne izpolnjujejo pogojev Splošne uredbe, so zagrožene visoke globe, zato morajo družbena omrežja pregledati svoje poslovne procese in obrazce za soglasja ter zagotoviti njihovo skladnost s Splošno uredbo. Določiti morajo vrste podatkov, ki se bodo hranili, vzpostaviti morajo postopke za ravnanje z osebnimi podatki, razviti in izvajati morajo varnostne ukrepe in podobno (Peras, Mekovec & Picek, 2018).

2 OSEBNI PODATKI IN DRUŽBENA OMREŽJA

2.1 Družbena omrežja in njihov vpliv v sodobni družbi

Družbena omrežja so spletne platforme, ki so v zadnjem desetletju postale priljubljene med uporabniki po vsem svetu. Uporabniki doživljajo družbena omrežja kot obliko komunikacije in virtualnega druženja z drugimi uporabniki. Na drugi strani družbena omrežja svojim uporabnikom ponujajo širok nabor različnih aktivnosti in jim s tem omogočajo participacijo. Spodbujajo jih, da s prijatelji, znanci, sledilci ali širšo javnostjo delijo fotografije in videoposnetke, sodelujejo v razpravah, komentirajo objave drugih, všečkajo objave in spletne strani, ohranjajo stike s prijatelji in družino, se združujejo v skupine s podobnimi interesi in podobno. Poleg tega jim omogočajo, da se znova povežejo z ljudmi iz preteklosti, predstavljajo seznam kontaktov, beležnik dogodkov, album fotografij in še bi lahko naštevala. Uporabniki tako pogosto delijo osebne fotografije, intimne misli in mnenja, s čimer razkrivajo svoje osebne podatke (npr. o svojih navadah, interesih ali lokaciji).

Družbena omrežja omogočajo in gostijo spletni prostor za uporabnike, skupine ali organizacije, ki želijo brezplačno ustvariti svojo stran ali profil. Zagotavljajo tudi osnovna podporna orodja za izvajanje različnih dejavnosti in mnogim ponudnikom omogočajo nudenje aplikacij. Družbena omrežja so bila prvotno usmerjena k uporabnikom in so se uporabljala izključno za družbene dejavnosti, danes pa imajo korporacije velik interes s poslovnega vidika, saj se družbena omrežja uporabljajo tudi v komercialne namene (Turban in drugi, 2018).

Vodilna družbena omrežja so običajno na voljo v več jezikih in uporabnikom omogočajo, da se povežejo z ljudmi preko geografskih, političnih ali gospodarskih meja. Zaradi stalne prisotnosti v življenju uporabnikov imajo družbena omrežja izrazito močan družbeni vpliv (Statista GmbH, 2019).

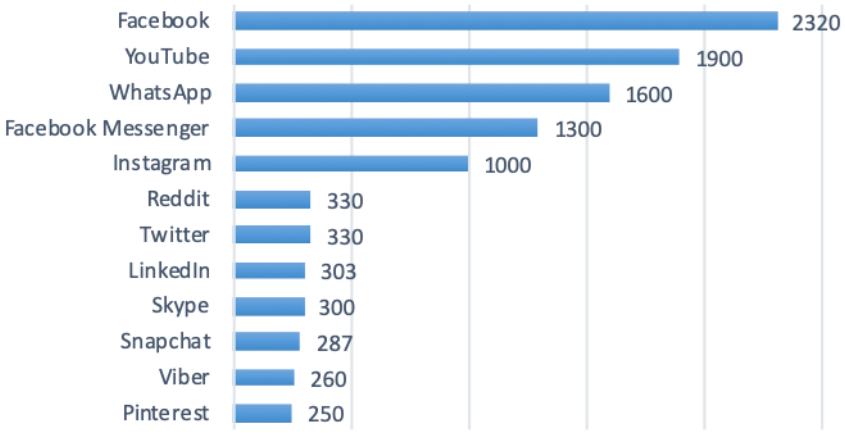
Pomena družbenih omrežij ne moremo zanikati, saj jih velika večina ljudi uporablja vsakodnevno in tam preživijo veliko časa. Čeprav se glede na kontekst družbena omrežja med seboj nekoliko razlikujejo, pa je z vidika zasebnosti vsem skupno to, da uporabniki s participacijo na teh omrežjih težko ohranijo svojo zasebnost resnično zasebno. Postavlja se vprašanje o zasebnosti in varnosti uporabe družbenih omrežjih – tukaj velja tudi rek »kar se zgodi na spletu, ostane na spletu«, česar se veliko uporabnikov še premalo zaveda. Dobro je, da se zavedamo pomena zasebnosti, varnosti in varstva osebnih podatkov na družbenih omrežjih. Osebni podatki na družbenih omrežjih bi morali biti področje, ki mu posvečamo svojo skrb in pozornost.

2.2 Analiza števila uporabnikov družbenih omrežij

Zaradi hitrega razvoja in nižjih stroškov je informacijsko-komunikacijska tehnologija ljudem postala dostopnejša. Posledično se je povečalo tudi število uporabnikov interneta, ki je v aprilu 2019 znašalo 4,44 milijarde, od celotne populacije 7,7 milijarde. Približno 2,46 milijarde uporabnikov interneta uporablja družbena omrežja. Glede na trend se ocenjuje, da bo leta 2021 število uporabnikov teh omrežij doseglo 3,02 milijarde, kar je več kot tretjina trenutne svetovne populacije (Statista GmbH, 2019).

Vodilna družbena omrežja v svetu, ki so med uporabniki najbolj poznana in priljubljena, so Facebook, YouTube, Instagram, Twitter, LinkedIn, SnapChat, Reddit in druga omrežja.

Slika 1: Priljubljenost družbenih omrežij glede na število aktivnih uporabnikov v aprilu 2019 (v mio)



Prirejeno po Statista GmbH (2019).

Opombe:

- WhatsApp, Messenger in Instagram spadajo pod Facebook, ki tako povsem prevladuje med družbenimi omrežji, konkurira mu le Googlova videoplatforma YouTube.
- Izločena so kitajska družbena omrežja WeChat, QQ, Qzone, Douyin/Tik Tok, Sina Weibo, Douban in Baidu Tieba, saj so prisotna predvsem na azijskem trgu.

Aktivnih uporabnikov vseh družbenih omrežij je približno 2,46 milijarde. Slika 1 prikazuje, da je trenutno najbolj priljubljeno družbeno omrežje Facebook, ki ima 2,32 milijarde aktivnih uporabnikov, kar je več, kot je prebivalcev v katerikoli državi na svetu. Sledijo mu YouTube z 1,9 milijarde, WhatsApp z 1,5 milijarde, Facebook Messenger z 1,3 milijarde, Instagram z 1 milijardo, Reddit s 330 milijoni, Twitter s 326 milijoni, LinkedIn s 303 milijoni, Skype s 300 milijoni, SnapChat z 287 milijoni, Viber z 260 milijoni in Pinterest z 250 milijoni aktivnih uporabnikov (Statista GmbH, 2019). Vsi zgoraj navedeni podatki se nanašajo na število aktivnih uporabnikov. Število ustvarjenih računov oziroma profilov na posameznih omrežjih pa je še bistveno večje.

2.3 Oglaševanje na družbenih omrežjih

Družbeni mediji so se iz platforme za zabavo in povezovanje med ljudmi razvili v močno marketinško orodje ter imajo pomembno vlogo pri povezovanju oglaševalskih podjetij in uporabnikov teh platform. Skupaj z bolj tradicionalnimi digitalnimi pristopi, kot sta e-poštno trženje (angl. email marketing) in trženje vsebin, se trženje prek družbenih omrežij šteje za eno najučinkovitejših digitalnih tržnih poti. Večina teh podjetij upošteva to obliko digitalnega trženja pri snovanju svojih trženjskih strategij in ciljev. Tržni potencial se še vedno povečuje, saj se poleg večjega števila uporabnikov povečuje tudi njihovo sodelovanje. Uporabniki interneta v povprečju porabijo približno 135 minut dnevno za brskanje po družabnih omrežjih. To spodbuja svetovne blagovne znamke in njihove oglaševalce, da ta čas in prostor na zaslonu izkoristijo za promocijo izdelkov in storitev (Statista GmbH, 2019).

Najpogostejša prednost uporabe družbenih medijev v tržne namene je večja izpostavljenost, kar glede na velikost potencialnega oglaševanega občinstva na družbenih platformah, ki skupaj znaša približno 2,46 milijarde aktivnih uporabnikov, ne preseneča. Poleg večje izpostavljenosti vplivajo na uspešnejše poslovanje tudi drugi vidiki. Oglaševalska podjetja s trženjem na družbenih platformah povečujejo svoje občinstvo, ozaveščenost o blagovni znamki, preusmerjajo uporabnike na njihove spletne strani, imajo vpogled na trg in trende, generirajo potencialne kupce in povečujejo njihovo zvestobo ter izboljšujejo prodajo (Statista GmbH, 2019).

Najpogosteje uporabljene družbene platforme med globalnimi oglaševalskimi podjetji so Facebook, Instagram in Twitter. Kot vodilno omrežje na svetu je Facebook največkrat uporabljena platforma tudi pri poslovanju oglaševalskih podjetij, kar neposredno vpliva na prihodke podjetja, saj oglaševanje predstavlja glavni vir njegovih prihodkov. Sledijo mu

Instagram s 66 %, Twitter z 62 % in LinkedIn s 56 % oglaševalskih podjetij, ki uporabljajo te platforme za trženje. Podjetja poleg tega nameravajo še povečati uporabo svojih promocijskih strategij. Po ocenah so v letu 2018 stroški oglaševanja na družbenih omrežjih po svetu znašali skoraj 27 milijard ameriških dolarjev, po napovedih pa naj bi se do konca leta 2020 povečali na 37 milijard, kar kaže na močno rast v kratkem časovnem obdobju (Statista GmbH, 2019).

2.4 Vrednost osebnih podatkov

Leta 2009 je takratna evropska komisarka za varstvo potrošnikov, Meglena Kuneva (Evropska komisija, 2009), v svojem govoru povedala: »Osebni podatki so novo olje interneta in nova valuta digitalnega sveta.« S tem je prikazala, kako so osebne informacije uporabnikov postale ključno sredstvo v digitalnem svetu. Po besedah Pirc Musarjeve in Burnikove (2011) »še nikdar v zgodovini ni bilo mogoče zbirati tako velikih količin podatkov, jih shranjevati ter s sofisticiranimi orodji analizirati in obdelovati za najrazličnejše namene – od varnosti in ‚vojne proti terorizmu' pa do oglaševanja«.

Dandanes je z naprednimi tehnologijami mogoče zbirati enormne količine podatkov, izkoriščanje zbranih osebnih podatkov pa je postalo večmilijardna industrija. Številna podjetja zbirajo in obdelujejo ogromne količine podatkov, ki jih pridobijo s priljubljenimi orodji. Glavni namen je monetizacija s prodajo oglaševalskim podjetjem, ki so razvila nove poslovne modele za dosego svojih ciljev in podatke kupujejo predvsem z namenom ciljnega oglaševanja.

Osebni podatki so postali sredstvo, ki se uporablja za ustvarjanje dodane vrednosti za podjetja in potrošnike. Podjetja jih uporabljajo za različne namene, na primer za izvedbo analiz tveganja strank, zmanjšanje stroškov prek personaliziranih in filtriranih ponudb, nižje transakcijske stroške za podjetja in potrošnike ter povečanje donosov z boljšim ciljnim oglaševanjem. Osebni podatki so torej strateški kapital, s katerim podjetja izboljšujejo obstoječe operacije, kar pa lahko vodi v nove ali izboljšane oblike razvoja izdelkov (npr. množično prilagajanje potrebam potrošnikov) in tudi v pojav cenovne diskriminacije. Podjetja lahko na ta način pridobijo konkurenčno prednost ali ustvarijo nove ovire za vstop na trg (Spiekermann, Acquisti, Böhme & Hui, 2015).

V gospodarstvu, ki temelji na podatkih, ki jih podjetja pogosto dobijo tako, da uporabnikom ponudijo »brezplačne« digitalne storitve ali popuste za spletne izdelke in storitve, osebni podatki posameznikov predstavljajo denarno vrednost. Podatki o kupcih in algoritmi za profiliranje se že obravnavajo kot poslovno sredstvo ter so zaščiteni kot poslovna skrivnost (Malgieri & Custers, 2018). Z zavedanjem vrednosti osebnih podatkov pa so se pojavili tudi kompleksni ekosistemi subjektov, ki zbirajo, analizirajo in tržijo osebne podatke.

S porastom digitalizacije in interneta so podjetja v spletnem oglaševanju začela s ciljnim oglaševanjem na podlagi podatkov o individualnih preferencah in interesih uporabnikov. Ta podjetja so iz različnih panog, ki si med seboj delijo in tržijo digitalne profile. Digitalno sledenje in profiliranje se ne uporabljata le za spremljanje, temveč tudi za vplivanje na vedenje ljudi.

V naslednjem poglavju bom opisala, kako številna podjetja spremljajo, analizirajo in vplivajo na življenja ljudi prek digitalnih sledi ter kako spletne platforme, tehnološka podjetja in posredniki podatkov zbirajo osebne podatke ter z njimi trgujejo in jih izkoriščajo za svoj dobiček.

2.5 Uporaba osebnih podatkov

2.5.1 Zbiranje osebnih podatkov

V zadnjih letih se srečujemo z naraščajočim trendom spremljanja in sledenja ljudem na skoraj vseh področjih njihovega življenja, kar omogoča moderna tehnologija. Čeprav obstajajo različna družbena omrežja, je vsem skupno to, da zaradi velikega števila aktivnih uporabnikov in ogromne količine vsebin, ki nastajajo dnevno, razpolagajo z ogromnimi količinami podatkov, ki jih ustvari množica uporabnikov. Z različnimi strategijami zbirajo osebne podatke uporabnikov in jih uporabljajo za različne namene. Poleg tega na podlagi že zbranih podatkov z operacijami profiliranja in segmentiranja generirajo tudi nove podatke, kar predstavlja nov izziv za informacijsko zasebnost (Young & Quan-Hasse, 2013).

Po besedah organizacije Privacy Rights Clearinghouse (2010) uporabniki na družbenih omrežjih pogosto delijo naslednje:

• **Profil:** Večina družbenih omrežij uporabnikom omogoča, da si ustvarijo svoj profil in se na ta način povežejo z drugimi uporabniki. Pri ustvarjanju profila lahko uporabniki vnesejo svoje osebne podatke, kot so ime in priimek, datum rojstva, telefonska številka, naslov in druge informacije, nato pa izberejo nastavitve zasebnosti profila. Uporabniki na svojem profilu najpogosteje delijo informacije o spolu, starosti, interesih, izobrazbi in zaposlitvi.
• **Status:** Uporabnikom je na družbenih omrežjih omogočeno posodabljanje njihovega statusa z namenom hitrega obveščanja in komunikacije z drugimi uporabniki. Čeprav obstajajo nastavitve zasebnosti, s katerimi lahko sami omejijo dostop do teh informacij, so družbena omrežja namenjena predvsem hitremu in javnemu deljenju informacij.
• **Lokacija**: Uporabniki na družbenih omrežjih lahko beležijo svojo lokacijo v realnem času, bodisi kot informacijo o svoji trenutni lokaciji bodisi kot posodobitev, ki je vidna njihovim stikom. To jim omogoča možnost prijave (»check in«) na dogodkih ali preprosto deljenje njihove trenutne lokacije s stiki.

• **Vsebina v skupni rabi:** Družbena omrežja so zasnovana tako, da uporabnike spodbujajo k skupni rabi različnih vsebin, kot so glasba, fotografije, videoposnetki in povezave do drugih spletnih strani.

Uporabniki družbenih omrežij ustvarjajo profile, ki vsebujejo številne bogate osebne podatke, ki jih lahko enolično identificirajo (ime, elektronska pošta, zaposlitev in kraj dela), prepoznavne informacije (domači naslov, izobrazba ali prejšnje delovno mesto in naziv), demografske podatke (starost in spol) ter občutljive informacije, ki so lahko skrite drugim uporabnikom (dohodek, partnerski status, verska in politična prepričanja). Obstaja tudi bogat nabor podatkov, pridobljenih iz interakcij med različnimi uporabniki. Ti podatki lahko vključujejo tudi občutljive informacije, kot so nakupne navade uporabnikov in podobno (He, Cai & Yu, 2018).

Večina stvari, ki jih uporabniki objavijo na družbenih omrežjih, je povezana z njihovim osebnim življenjem, zato predstavljajo osebne podatke. Družbena omrežja o svojih uporabnikih zbirajo predvsem naslednje osebne podatke (Hasan, Habegger, Brunie, Bennani & Damiani, 2013):

- Interesi: poklicni interesi ali interesi uporabnikov glede hobijev, zabave, športa in izdelkov.
- Znanja in veščine: informacije se lahko uporabijo za odkrivanje strokovnjakov na določenem področju.
- Cilji uporabnikov: kaj se uporabniki odločijo doseči v kratkem ali dolgoročnem obdobju.
- Vedenje: uporabniki imajo ponavljajoče se vedenje, ki ga je mogoče spremljati.
- Osebnostne značilnosti: starost, spol, elektronski naslov, demografske značilnosti.
- Kontekst: okoljske, osebne, družbene, prostorske in časovne značilnosti.

Vsak od teh atributov vsebuje osebne podatke uporabnika. Raziskava, ki so jo na podlagi najbolj priljubljenih družbenih omrežij izvedli Peras, Mekovec in Picek (2018), je pokazala, da vsa družbena omrežja zbirajo naslove IP, identifikatorje naprav in informacije o lokaciji svojih uporabnikov, medtem ko jih 90 % zbira uporabniško ime, elektronski naslov, telefonsko številko, fotografije, podatke o starosti in spolu, 80 % datum rojstva in številko kreditne ali debetne kartice, 70 % jih zbira naslov, 60 % ime in priimek, 30 % pa politična prepričanja in versko pripadnost. Iz tabele 1 je razvidno, da Facebook in vse njegove platforme (WhatsApp, Messenger in Instagram) zbirajo največ vrst osebnih podatkov. Platforma Youtube ne zbira političnih prepričanj, verskih pripadnosti in številk kreditnih/debetnih kartic.

Tabela 1: Vrste osebnih podatkov, ki jih zbirajo družbena omrežja

Vrsta osebnega podatka	Facebook	YouTube	WhatsApp	Messenger	Instagram
Ime in priimek	+	+	+	+	+
Uporabniško ime	+	+	-	+	+
E- poštni naslov	+	+	-	+	+
Telefonska številka	+	+	+	+	+
Fotografija	+	+	+	+	+
Datum rojstva	+	+	+	+	-
Naslov	+	+	-	+	-
Starost	+	+	+	+	-
Spol	+	+	-	+	+
Politična prepričanja	+	-	-	+	-
Verska pripadnost	+	-	-	+	-
Lokacija	+	+	+	+	+
Št. kreditne / debetne kartice	+	-	-	+	+
Identifikatorji naprav	+	+	+	+	+
Naslov IP	+	+	+	+	+

Prirejeno po Peras, Mekovec & Picek (2018).

2.5.2 Analiziranje podatkov

Znanstvene študije ugotavljajo, da je mogoče iz precej osnovnih informacij o spletnem vedenju (na podlagi podatkov o spletnih iskanjih, zgodovini brskanja, aktivnostih na družbenih omrežjih, ogledih videoposnetkov in nakupih) sklepati o številnih osebnostnih lastnostih posameznikov, ki se obravnavajo kot zasebne.

O osebnostnih lastnostih posameznika lahko torej sklepamo iz informacij o spletnih straneh, ki jih je obiskal, podatkov o uporabi mobilnih aplikacij, pa tudi iz zapisov telefonskih klicev. Kanadski raziskovalci so z analiziranjem tipkanja po tipkovnici uspešno izračunali čustvena stanja, kot so zaupanje, živčnost, žalost in utrujenost (Christl, 2017).

Študija, ki je bila izvedena na univerzi Cambridge, je pokazala, da je mogoče na podlagi všečkov na Facebooku precej natančno napovedati etnično pripadnost, verska in politična prepričanja, partnerski status, spol in spolno usmerjenost, kot tudi konzumiranje alkohola, cigaret in drog (Kosinski, Stillwell & Graepel, 2013). Metode analiziranja, kot je napovedna analiza, omogočajo analiziranje profilov uporabnikov družbenih omrežij na podlagi zbranih podatkov. Z analiziranjem je mogoče predvideti tudi osebnostne lastnosti, kot so čustvena stabilnost, zadovoljstvo, impulzivnost, depresija in podobno. Čeprav te metode temeljijo na statističnih korelacijah in verjetnostih, so rezultati dovolj dobri za samodejno razvrščanje, ocenjevanje in kategoriziranje ljudi (Christl & Spiekermann, 2016). Montjoye, Quoidbach, Robic in Pentland (v Christl & Spiekermann, 2016) navajajo, da všečki na Facebooku »predstavljajo eno izmed najbolj generičnih vrst digitalnih odtisov« ter da njihovi rezultati predstavljajo »pomembne priložnosti in izzive na področjih psihološke ocene, trženja in zasebnosti«.

Kot primer lahko vzamemo družbeno omrežje Facebook, ki analizira objave, všečke, povezave, fotografije in številna druga vedenja uporabnikov na svoji platformi. Na podlagi tega lahko razvršča in kategorizira uporabnike glede na njihovo politično prepričanje, etnično pripadnost in prihodek z najmanj 52.000 atributi (Christl, 2017). Lastnosti in atributi so predvidljivi iz digitalnih zapisov vedenja uporabnikov. Uporabniki se sicer lahko odločijo, da določenih informacij o svojem življenju (npr. starost ali spolno usmerjenost) ne bodo razkrili, vendar je mogoče z analizami te podatke napovedati iz drugih vidikov njihovega življenja, ki ga razkrivajo (Kosinski, Stillwell & Graepel, 2013).

2.5.3 Trgovanje z osebnimi podatki

Osebni podatki vse bolj postajajo sredstvo, s katerim se lahko trguje. Pojavljajo se trgi za osebne podatke in predlagajo se novi načini vrednotenja podatkov posameznikov. Ob tem še vedno obstajajo pravne obveznosti v zvezi z varstvom osebnih podatkov in pomisleki posameznikov glede njihove zasebnosti (Spiekermann, Acquisti, Böhme & Hui, 2015).

V trgovanje z osebnimi podatki so vključeni različni akterji, in sicer marketinške in oglaševalske agencije, posredniki podatkov, ponudniki upravljanja baz podatkov, spletni in mobilni oglaševalci ter podjetja, ki ponujajo programe zvestobe in se ukvarjajo z direktno pošto, telefonskimi prodajnimi storitvami in podatkovno usmerjenim trgovanjem. Podjetja za tržne podatke se pogosto imenujejo tudi »posredniki podatkov« (angl. data brokers) (Christl, 2017).

Posredniki podatkov so podjetja, ki zbirajo podatke (tudi osebne podatke o potrošnikih) iz različnih virov in svoj primarni dohodek pridobijo s posredništvom podatkov, zbranih iz spletnih in drugih virov. Ogromne količine teh podatkov združujejo v profile o vsakem posamezniku in jih ponujajo kot tržne podatkovne storitve. Te storitve si nato med seboj posredujejo, večinoma brez vednosti potrošnikov. Informacije pridobijo iz komercialnih, vladnih in javnih virov (npr. demografski podatki, poklic, izobrazba, podatki o nakupih, lastništvu nepremičnin, interesih, verski in politični pripadnosti ipd.). Največji posredniki podatkov so podjetja Acxiom, Core Logic, Datalogix, ID Analytics, PeekYou in drugi (Christl, 2017).

Tudi največje družbeno omrežje Facebook od leta 2013 sodeluje s štirimi posredniki podatkov – Acxiom, Epsilon, Datalogix in BlueKai – ki mu pomagajo s sledenjem in profiliranjem uporabnikov ter mu posredujejo podatke, ki jih pridobijo iz drugih virov, zbranih izven njegove platforme (Christl, 2017). Facebook ve, kdo so prijatelji njegovih uporabnikov, v lasti ima njihove fotografije, uporablja prepoznavo obraza, ve, katere naprave uporabljajo in podobno, vendar ob vsem tem od posrednikov kupuje še podatke o življenju uporabnikov (npr. kakšen avto vozijo, kaj kupujejo v trgovini ipd.) za izboljšanje njihovega profila z namenom ciljnega oglaševanja. Sami temu pravijo optimizacija

izkušnje na Facebooku, v bistvu pa gre za monetizacijo vedenja uporabnikov (Angwin, Mattu & Parris Jr., 2016).

2.5.4 Targetiranje in ciljno oglaševanje

Družbena omrežja z različnimi orodji spodbujajo uporabnike k participaciji na svojih platformah. Na ta način uporabniki razkrivajo podatke o sebi in jih delijo s prijatelji ali širšo javnostjo. Z všečkanjem sporočajo, kaj jim je všeč, kje dopustujejo, kakšna so njihova politična prepričanja in podobno. Digitalne tehnologije omogočajo vse več personaliziranih storitev, ki zbirajo različne vrste osebnih podatkov uporabnikov, in z vse manj podatki je mogoče določiti konkretnega posameznika, na katerega se nanašajo. Podatke zbirajo in uporabljajo številna oglaševalska podjetja ter jih s tako imenovanim ciljnim oglaševanjem izkoriščajo brez vedenja uporabnikov.

Oglaševanje na spletu je postalo ena najnaprednejših panog, ki si prizadeva za pridobivanje vrednosti in monetizacijo podatkov. Družbena omrežja so za uporabnike brezplačna, sama pa se financirajo s prihodki od oglaševanja. Oglasi se običajno prilagajajo s sistemi »vedenjskega ciljanja«, ki profilirajo uporabnike na podlagi njihovega vedenja na spletu in družbenih omrežjih.

V spletno oglaševanje so vključena številna podjetja, ki se osredotočajo na nenehno sledenje in profiliranje milijard ljudi. Vsakič, ko se oglas prikaže na spletnem mestu ali v mobilni aplikaciji, je bil digitalni profil uporabnika pravkar prodan najboljšemu ponudniku. V zadnjih letih se obsežne informacije o življenju ljudi združujejo s podatkovnimi bazami uporabnikov, ki jih upravljajo velike platforme, podjetja za spletno oglaševanje in nešteto drugih podjetij v različnih panogah (Christl, 2017).

2.6 Grožnje zasebnosti in zlorabe osebnih podatkov

Razprava o zasebnosti je z vse večjim pomenom interneta in porastom družbenih omrežij dobila nov zagon. Družbena omrežja so ekosistem, v katerem sodelujejo družbena omrežja kot ponudniki storitev, njihovi uporabniki in tretje osebe, in vsi ti udeleženci so potencialni kršitelji zasebnosti (Benson, Saridakis & Tennakoon, 2015). S prisotnostjo na družbenih omrežjih uporabniki hote ali nehote o sebi razkrijejo veliko osebnih podatkov, s čimer so izpostavljeni resnim tveganjem za zlorabo zasebnosti. Družbena omrežja osebne podatke pogosto zbirajo, razkrivajo in uporabljajo brez vednosti in privolitve uporabnikov, kar predstavlja grožnjo zasebnosti, ki se z razvojem družbenih omrežij in njihovo množično uporabo še povečuje.

Z deljenjem in skupno rabo uporabniki razkrivajo podatke o sebi, vključno s kontekstnimi informacijami, ki se jih niti ne zavedajo. Z razkrivanjem teh informacij oglaševalcem ali hekerjem omogočijo, da jim lahko sledijo oziroma izkoristijo njihovo spletno identiteto

(Privacy Rights Clearinghouse, 2010). Uporabnikom so sicer na voljo nastavitve zasebnosti, vendar kljub temu obstajajo številne možnosti za resne napade na zasebnost. Glede na število osebnih podatkov iz fotografij in videoposnetkov ter ostalih zasebnih informacij, ki se izmenjujejo na družbenih omrežjih, so uporabniki izpostavljeni grožnjam zasebnosti, kot so kraja identitete, kibernetsko zalezovanje in drugo (Ghazinour & Ponchak, 2017).

Obstajajo različne oblike tveganj, ki jih lahko razdelimo v dve skupini. V prvi skupini so tveganja, pri katerih »sodelujejo« ponudniki družbenih omrežij, ki jim je zaradi ohlapne zakonodaje in nadzora omogočeno upravljanje z osebnimi podatki uporabnikov. To vključuje uporabo podatkov brez uporabnikovega soglasja in njihovo posredovanje tretjim osebam (ki nato uporabijo te podatke za pošiljanje neželenih oglaševalskih ponudb), izgubo osebnih podatkov in diskriminacijo (v postopku izbire za delovno mesto ali cenovna diskriminacija, ko je zaračunana višja cena). V drugo skupino uvrščamo zlorabe, ki jih prek družbenih omrežij zagrešijo kriminalne entitete (t. i. hekerji), na primer kraja osebnih podatkov, uporaba osebnih podatkov brez vednosti uporabnikov, nadlegovanje, kraja identitete, zvabljanje, zlonamerne povezave in sporočila ter drugo. Hekerji lahko vgradijo zlonamerno programsko opremo in s tem povzročijo, da še več ljudi postane žrtev zlonamerne povezave. Uporabnik lahko zlonamerni spletni aplikaciji dovoli dostop do svojega računa in ta aplikacija lahko nato ogrozi uporabnikov račun ali prenese v njegov računalnik nepooblaščeno programsko opremo. Resno tveganje predstavljajo tudi lažne identitete, saj uporabniki ne morejo z gotovostjo vedeti, kdo stoji za določenim profilom. Napredek tehnologije hekerjem poleg tega omogoča uporabo novih tehnik za ciljanje na uporabnike z namenom povzročitve škode ali okoriščenja (Tayouri, 2015).

Pri družbenih omrežjih se pojavljajo vprašanja o tem, kdo ima pravico do uporabe podatkov uporabnikov in ali se lahko osebne informacije, ki jih uporabniki delijo, uporabljajo v poslovne namene. V nadaljevanju se bom osredotočila na zlorabe zasebnosti z vidika družbenih omrežij, saj so za magistrsko delo relevantnejše.

Grožnje zasebnosti, ki jih omogočata uporaba in deljenje informacij v družbenih omrežjih (Privacy Rights Clearinghouse, 2010):

• **Javno dostopne informacije:** Vsako družbeno omrežje omogoča objavo informacij, ki so popolnoma dostopne javnosti. Te informacije lahko na primer vključujejo uporabniško ime, posamezne objave ali celoten račun uporabnika. T. i. javne objave nimajo nikakršnih omejitev dostopa, kar pomeni, da lahko vsakdo, vključno z neznanci, dostopa do vsega, kar je bilo objavljeno kot »javno«. Hkrati obstajajo tudi nekatere informacije, ki se delijo na manj očiten način, brez zavedanja uporabnikov, in so prav tako javno dostopne. To vključuje naslednje:

- Podatki, ki so lahko privzeto javno vidni – v nekaterih primerih lahko uporabnik spremeni nastavitve zasebnosti in izbere možnost, da te podatke vidijo samo

uporabniki, ki jim to dovoli. V nekaterih primerih pa informacije ostanejo javne, saj uporabnik nima možnosti omejitve dostopa (npr. ime računa uporabnika).

- Družbena omrežja lahko kadarkoli spremenijo politiko zasebnosti brez uporabnikovega dovoljenja. Ob spremembi pravilnika zasebnosti lahko tako vsebina, ki je bila objavljena kot zasebna, postane vidna širši javnosti.
- Osebe na uporabnikovem seznamu stikov (t. i. prijatelji ali sledilci) lahko brez dovoljenja kopirajo ali delijo podatke uporabnikov, vključno z njihovimi osebnimi podatki, fotografijami itd.
- Aplikacijam drugih proizvajalcev na družbenih omrežjih je omogočen dostop do podatkov in informacij, ki jih uporabniki objavijo kot »zasebne«.
- Družbena omrežja sama po sebi ne zagotavljajo varstva informacij, objavljenih na profilih uporabnikov, tudi če so bile objavljene kot zasebne. Čeprav so napake in kršitve zasebnosti običajno hitro odpravljene, še vedno obstaja možnost, da te informacije nekdo izkoristi oziroma zlorabi.

• **Oglaševanje:** Oglaševalci se zelo zanimajo za informacije, ki jih lahko zberejo s spremljanjem uporabnikovih spletnih aktivnosti na družbenih omrežij. Objavljena vsebina uporabnikov niti ni edini način spremljanja oglaševalcev; spremljanje namreč vključuje tudi sledenje spletnih mest, ki si jih je uporabnik ogledal, shranjevanje informacij, povezanih z določenimi spletnimi mesti (npr. izdelki v nakupovalni košarici), in analizo agregiranih podatkov, ki se uporabljajo v tržne namene.

• **Ciljno oglaševanje:** Poleg navadnega oglaševanja se je pojavila tudi praksa prilagajanja oglasov osebnim interesom uporabnikov, t. i. ciljno oglaševanje. Ciljno oglaševanje je učinkovitejše od navadnega, saj je pri tej vrsti oglaševanja nakup pogostejši kot pri navadnem oglaševanju (neciljani oglasi). Iz tega vidika oglaševalci raje uporabljajo ciljne oglase, večji dobiček pa prinašajo tudi družbenim omrežjem, saj jih je mogoče prodati po višji ceni. Družbena omrežja so za uporabnike brezplačna, dobiček jim prinaša oglaševanje na njihovih platformah.

• **Aplikacije drugih proizvajalcev:** Gre za programe, ki delujejo na družbenih omrežjih, čeprav niso del njih (spletne ankete, kvizi, igre, ki jih lahko uporabniki igrajo, ali vmesniki tretjih oseb). Za pravilno delovanje teh aplikacij lahko družbena omrežja na podlagi uporabnikovega dovoljenja razvijalcem omogočijo dostop do javnih in celo zasebnih podatkov. Uporabniki lahko nehote dovolijo dostop do svojih profilov, brez zavedanja o posledicah podeljenih dovoljenj. Morali bi se zavedati, da večina družbenih omrežij ne prevzema odgovornosti za aplikacije drugih proizvajalcev na svojih spletnih platformah, poleg tega pa je lahko tem aplikacijam omogočen dostop do več informacij, kot je potrebno za opravljanje njihovih funkcij, in lahko vsebujejo zlonamerno programsko opremo, ki je namenjena napadu na uporabnikovo napravo. Družbeno omrežje ima nenazadnje lahko z določenimi spletnimi mesti in aplikacijami sklenjene sporazume, ki

tem spletnim mestom in aplikacijam omogočajo dostop do javnih informacij vseh uporabnikov družbenega omrežja.

• **Država (vlada in organi pregona):** Država nadzoruje družbena omrežja z namenom, da bi pridobila dragocene informacije za odkrivanje kriminalnih dejavnosti. Organi pregona se med preiskavo pogosto obrnejo na profile osumljencev na družbenih omrežjih. Čeprav ima vsako družbeno omrežje opredeljene postopke za obravnavo prošenj organov kazenskega pregona, pa ni nujno, da je njihovo sodelovanje v celoti pojasnjeno v politiki zasebnosti.

• **Zaposlovanje:** Delodajalci pri zaposlovanju vse pogosteje preverjajo tudi profile kandidatov za zaposlitev na družbenih omrežjih z namenom pridobiti čimveč informacij, ki bi jim olajšale odločitev o izbiri kandidata, čeprav pri tem obstajajo pravna tveganja, vključno z morebitnimi kršitvami zakonov o diskriminaciji.

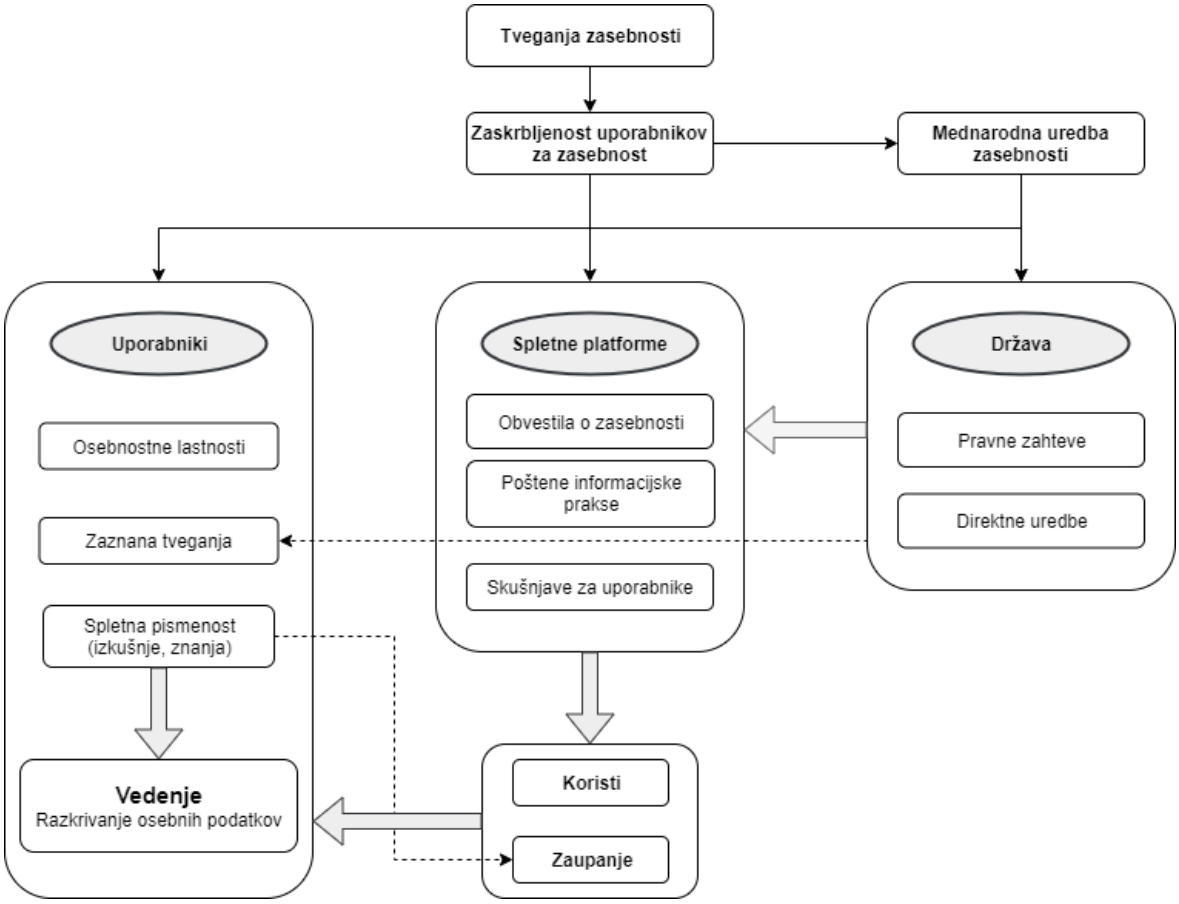
Uporabniki na družbenih omrežjih razkrijejo in si izmenjajo ogromno informacij, kar bi lahko imelo neželene dolgoročne posledice. Družbena omrežja si izmenjujejo informacije z drugimi spletnimi mesti družbenih medijev, dovoljena je skupna raba objavljenih lokacij in ljudje takšne informacije vedno lažje razkrivajo. Če upoštevamo še navdušene uporabnike, ki namerno ali nenamerno razkrivajo preveč osebnih podatkov, in razvijalce, ki lahko dostopajo do osebnih informacij na družbenih omrežjih, predstavlja participacija na teh omrežjih zelo veliko varnostno tveganje z vidika groženj in zlorab zasebnosti (Tayouri, 2015). Škodljive posledice zlorab zasebnosti lahko vplivajo na psihološko in fizično počutje ter ugled uporabnika (Buglass, Binder, Betts & Underwood, 2016).

3 ZAZNAVANJE ZASEBNOSTI IN VEDENJE NA DRUŽBENIH OMREŽJIH

3.1 Vedenje uporabnikov

V nadaljevanju bom na podlagi študije avtorjev Ginosar in Ariel (2017) obravnavala tri skupine deležnikov, ki so v zvezi z razkrivanjem osebnih podatkov pomembni z vidika zasebnosti in vedenja uporabnikov spleta in spletnih platform ter posledično tudi družbenih omrežij. Kot prikazuje slika 2 so to uporabniki (njihove osebnostne lastnosti, njihova zaskrbljenost glede zasebnosti in spletna pismenost), spletne platforme (obvestila in politike spletnih platform) in država (pravna ureditev držav v obliki zakonodaje o zasebnosti in varnosti osebnih podatkov).

Slika 2: Vpliv deležnikov na vedenje uporabnikov



Prirejeno po Ginosar & Ariel (2017).

3.1.1 Uporabniki

Uporabnike spletnih platform v zvezi z zasebnostjo skrbi predvsem naslednje: zbiranje osebnih podatkov brez njihovega soglasja, obseg informacij, ki se posreduje tretjim osebam, in ali se njihovi osebni podatki uporabljajo za nepooblaščene sekundarne namene. Vedenje uporabnikov pri razkrivanju osebnih podatkov je zapleteno. Številne študije kažejo, da so uporabniki resda v skrbeh glede zasebnosti in tveganja za kršitve, vendar kljub temu razkrivajo osebne podatke. Ta fenomen se imenuje »**paradoks zasebnosti**«. To je odvisno od treh spremenljivk, in sicer od majhnih materialnih ali družbenih koristi/ugodnosti, ki jih uporabnik pridobi z razkritjem podatkov, od ravni njegovega zaupanja do specifičnih spletnih strani ali platform oziroma do različnih aktivnosti na internetu ter od ravni uporabnikovega poznavanja tehnoloških značilnosti interneta in njegovih tveganj ter ozaveščenosti v zvezi s tem. To znanje in ozaveščenost lahko opišemo tudi kot spletno pismenost uporabnikov, ki posledično vpliva na stopnjo zaupanja v spletne dejavnosti (Ginosar & Ariel, 2017).

3.1.2 Spletne platforme

Zgoraj opisani vidik se osredotoča na različne dejavnike, ki lahko vplivajo na vedenje uporabnikov na spletu, zlasti z vidika razkrivanja osebnih podatkov. To vedenje vpliva na uspeh spletnih platform, zato se pojavlja vprašanje, ali spletna mesta res poskušajo vplivati na vedenje uporabnikov in na kakšen način to počnejo. Oziroma z drugimi besedami, kako spletne platforme oblikujejo politiko zasebnosti, da bi uporabniki kljub pomislekom razkrivali osebne podatke. Iz tega vidika sta pomembna dva pristopa: prvi pristop je institucionalna teorija, v skladu s katero večina organizacij oblikuje politike zasebnosti kot odziv na zunanje pritiske, in z njimi zagotovi legitimnost. Drugi pristop se nanaša na zavedanje, da so informacije o uporabnikih pomemben vir za doseganje konkurenčne prednosti. Na podlagi tega je politiko zasebnosti treba obravnavati kot sestavni del poslovnega modela spletnih platform. Cilj obeh pristopov je vzpostavitev zaupanja med spletnimi platformami in njihovimi uporabniki ter predstavlja neke vrste »pogodbo«, s katero se vzpostavi ravnotežje med potrebami uporabnika po zasebnosti in potrebami spletnih platform po zbiranju in uporabi osebnih podatkov. To ravnotežje je mogoče doseči, če spletne platforme upoštevajo poštene informacijske prakse kot glavno komponento pri oblikovanju politik zasebnosti (Ginosar & Ariel, 2017).

Pojavlja se pomembno vprašanje: ali objava in izvajanje politik zasebnosti, ki temeljijo na poštenih informacijskih praksah, vplivata na vedenje uporabnikov v zvezi z razkrivanjem osebnih podatkov? Predpogoj je, da jo uporabniki preberejo, kajti le tako lahko predpostavljamo, da politika zasebnosti nanje vpliva (Ginosar & Ariel, 2017).

Nekatere raziskave kažejo, da takrat, ko uporabniki preberejo obvestila o zasebnosti, ta obvestila vplivajo na njihovo vedenje. Študija, ki so jo izvedli Gerlach, Widjaja in Buxmann (2015), razkriva, da obstaja povezava med vsebino politike zasebnosti družbenih omrežij in razkrivanjem osebnih podatkov s strani uporabnikov. Stopnja permisivnosti politike zasebnosti vpliva na uporabnikovo zaznavanje tveganj v zvezi z zasebnostjo, kar posledično vpliva na njegovo vedenje. Do podobnih rezultatov so prišli tudi Oulasvirta, Suomalainen, Lampinen in Karvonen (2014), ki v svoji študiji ugotavljajo, da transparentnost glede identitete, namenov in praks spletnih platform, ki zbirajo podatke, zmanjšuje zaskrbljenost uporabnikov glede zasebnosti oziroma povečuje njihovo zaupanje. V tretjem primeru sta Mollick in Mykytyn (2009) na podlagi spletne potrošniške domene ugotovila, da obstaja povezava med tremi spremenljivkami politike zasebnosti: informirano privolitvijo uporabnikov v zbiranje podatkov, omejevanjem izmenjave podatkov znotraj organizacije in omejevanjem sekundarne uporabe podatkov ter uporabnikovim zaznavanjem poštenosti spletne platforme.

Na podlagi zgoraj opisanega lahko povzamemo, da pregledne in poštene politike in prakse zasebnosti vplivajo na vedenje uporabnikov, da razkrijejo svoje osebne podatke. Vendar pa številne druge študije kažejo na zaupanje kot na intervencijsko spremenljivko med

politikami spletnih platform in praksami na eni strani ter vedenjem uporabnika, da je pripravljen razkriti svoje osebne podatke, na drugi (Ginosar & Ariel, 2017). Joinson, Reips, Buchanan in Schofield (2010) trdijo, da visoka raven zaupanja kompenzira nizko zasebnost, in obratno.

Če povzamemo, so glavne spremenljivke, ki vplivajo na vedenje uporabnikov, da razkrijejo svoje osebne podatke, naslednje (Ginosar & Ariel, 2017):

- vrsta in vsebina obvestila o zasebnosti;
- prakse, ki jih spletne platforme uporabljajo pri ravnanju z osebnimi podatki uporabnikov;
- koristi, ki jih spletne platforme lahko zagotovijo uporabnikom v zameno za njihove osebne podatke.

3.1.3 Država

V svetu obstajajo različne pravne ureditve glede varstva in zasebnosti osebnih podatkov. Pomembno vlogo pri tem ima država, saj z zakonodajo uravnava področje zasebnosti na spletnih platformah. V Evropski uniji je v letu 2018 vstopila v veljavo Splošna uredba, ki je poenotila evropski trg, v podobno smer gredo tudi azijsko-pacifiške države. V Združenih državah Amerike (v nadaljevanju ZDA) je obdelava osebnih podatkov odvisna od zapletenega sklopa tako zveznih kot državnih, sektorskih zakonov in predpisov (Ginosar & Ariel, 2017). Čeprav je Evropa zaenkrat vodilna na področju varovanja zasebnosti, pa se podobna zakonodaja širi tudi drugod po svetu. Kalifornija je na področju varovanja osebnih podatkov sprejela zakon, ki bo začel veljati v začetku leta 2020 (Zomorodi, 2019). Glede na to, da v Kaliforniji delujejo vsa večja tehnološka podjetja, kot sta Google in Apple, ter priljubljena družbena omrežja Facebook, Instagram, Twitter, Pinterest, LinkedIn in druga, lahko predpostavljamo, da se na tem področju obetajo spremembe tudi na območju ZDA.

V obstoječih zakonih o varstvu podatkov je mogoče opredeliti šest načel za obdelavo in uporabo osebnih podatkov, ki so skupna zakonom skoraj po vsem svetu (Millard, 2014):

- Osebni podatki se obdelujejo samo s privolitvijo ali drugo pravno utemeljitvijo.
- Podatki morajo biti obdelani pošteno in zakonito.
- Podatki morajo biti ustrezni, relevantni in omejeni na namen obdelave.
- Podatki so točni in se posodabljajo po potrebi.
- Podatki se hranijo v določljivi obliki le toliko časa, kot je potrebno.
- Podatki so zaščiteni pred nepooblaščeno ali nezakonito obdelavo in nenamerno izgubo ali uničenjem.

O politiki zasebnosti potekajo številne razprave. Na eni strani se omenjajo koristi in pasti državne ureditve, na drugi pa samoupravljanje panoge in špekulacije ter vprašanje, kateri pristop je učinkovitejši pri zmanjševanju zlorab zasebnosti in posledično zmanjševanju zaskrbljenosti uporabnikov glede njihove zasebnosti (Ginosar & Ariel, 2017). Zagovorniki državne regulative trdijo, da je državna ureditev nujno potrebna za zaščito nič hudega slutečih uporabnikov pred vedenjem in interesi spletnih platform. Nasprotno pa zagovorniki samoupravljanja trdijo, da imajo podjetja že sama spodbudo za zaščito uporabnikov, z namenom ohranitve svojih strank (Strauss & Rogerson, 2002). Hirsch (2011) predlaga režim, v katerem si odgovornost za zasebnost uporabnikov delita država in internetna panoga.

Avtorja Ginosar in Ariel (2017) v svojem članku postavita zanimivo vprašanje, na katerega ni jasnega odgovora, in sicer: »Ali zakonodaja glede varstva osebnih podatkov in zasebnosti vpliva na vedenje uporabnikov spletnih platform?« V zvezi s tem sta Miltgen in Smith (2015) v svoji študiji ugotovila, da se uporabniki na spletu vedejo manj previdno, če zaupajo državnemu regulativnemu sistemu zasebnosti. Luzakova (2014) pa je v svoji študiji prišla do zaključka, da čeprav evropska direktiva o zasebnosti in elektronskih komunikacijah zahteva informirano soglasje uporabnikov za zbiranje, shranjevanje in obdelavo njihovih osebnih podatkov, ne moremo govoriti o »informiranem soglasju«, saj uporabniki ne poznajo tehnologije, s katero se zbirajo podatki.

3.2 Zaskrbljenost uporabnikov glede zasebnosti

Da bi lahko uporabniki nadzorovali svoje osebne podatke, morajo sprejemati odločitve, ki so v skladu z njihovimi obstoječimi stališči in preferencami. Poleg tega morajo biti s strani obdelovalcev podatkov seznanjeni z načini upravljanja svojih podatkov. Predpogoj za uporabnikov nadzor nad njegovimi osebnimi podatki je torej obveščanje o obdelavi podatkov (van Ooijen & Vrabec, 2018).

Grožnjo nadzoru nad informacijami predstavlja kognitivno razmišljanje uporabnikov o upravljanju podatkov. Pomembno je omeniti, da te težave niso le posledica možnih kognitivnih pomanjkljivosti uporabnikov, kot je nepismenost, temveč so povezane tudi s sodobnim spletnim okoljem. Uporabniki se vsakodnevno srečujejo z ogromnimi količinami informacij, ki so razpršene prek različnih medijev, naprav in storitev. Obremenjenost z informacijami ogroža njihovo sposobnost in motivacijo za proučitev ključnih podrobnosti, ki so potrebne za sprejemanje odločitev glede zasebnosti. Za racionalno odločanje o tem, kaj razkriti, bi uporabnik moral oceniti prednosti in slabosti, ki so povezane z razkritjem podatkov, ter na podlagi tega pretehtati, ali so le-te v skladu z njegovimi stališči in preferencami. To bi bilo mogoče le, če bi uporabnik najprej upošteval vse informacije, ki so na voljo v politikah zasebnosti (van Ooijen & Vrabec 2018).

Za uporabnikovo razumevanje je pomembno, da je seznanjen z načinom upravljanja svojih podatkov. Zbiralci podatkov lahko uporabniku tovrstne informacije zagotovijo s pomočjo politike uporabe podatkov. V nadaljevanju bom razložila, zakaj takšen način ni učinkovit in uporabniku ne zagotavlja nadzora nad njegovimi podatki.

Zaradi hitrega razvoja tehnologije postajajo mehanizmi za varovanje zasebnosti, kot so politike zasebnosti, vse obširnejši in kompleksnejši (Shore & Steinman, 2015). Posledično je obremenjeno kognitivno delovanje uporabnikov, ki se soočajo z ogromnimi količinami informacij. Politike zasebnosti se poleg tega pogosto spreminjajo, kar pomeni, da bi morali uporabniki ob vsaki spremembi znova prebrati obširne obrazce, da bi bili seznanjeni z novostmi na področju zasebnosti (van Ooijen & Vrabec, 2018). Vse to privede do **informacijske asimetrije**, ki je pogost pojav na družbenih omrežjih.

Največji in najočitnejši vir negotovosti v zvezi z zasebnostjo so torej nepopolne in asimetrične informacije. Napredek v informacijski tehnologiji omogoča zbiranje in uporabo osebnih podatkov, v kar uporabniki pogosto nimajo vpogleda. Zato le malokrat natančno vedo, katere njihove osebne podatke in informacije imajo v lasti družbena omrežja, podjetja ali država ter kako se te informacije uporabljajo in kakšne so lahko posledice. Če uporabniki teh informacij nimajo ali pa se zavedajo svoje nevednosti, bodo najverjetneje negotovi glede količine deljenih informacij (Acquisti, Brandimarte & Loewenstein, 2015).

Dandanes se podatki obdelujejo s prefinjeno umetno inteligenco, kot so algoritmi, ki jih ni mogoče enostavno razložiti, zato je za uporabnike razumevanje tega področja omejeno. Uporabniki pogosto slabše razumejo kratkoročne in dolgoročne posledice, ki jih imajo tehnologije in kompleksni tehnološki procesi na njihovo življenje. Poleg tehnološkega vidika pa je eden od razlogov tudi ta, da se podjetja večinoma niti ne trudijo izboljšati preglednosti ali razumevanja, temveč celo nasprotno – uporabnike obveščajo nepopolno in netočno ter pri tem uporabljajo zavajujoč jezik, ali pa jih sploh ne obveščajo. Ne glede na to, da obstajajo politike zasebnosti in pogoji uporabe oziroma storitve (ki so nejasne oziroma težko razumljive), podjetja pogosto sistematično zavajajo uporabnike v pogodbe (soglasja) o prenosu podatkov. Če se kdo spotakne ob njihove prakse, na primer zagovorniki zasebnosti, organizacije za varstvo pravic potrošnikov, zakonodajalci, znanstveniki in novinarji, ter izrazi svoje pomisleke ali zahteva več informacij, se podjetja izogibajo odgovoru in trdijo, da je njihova praksa podatkov poslovna skrivnost, ki je ne smejo razkriti (Christl, 2017).

Koncepta zasebnosti in samorazkritja sta povezana, zato se domneva, da uporabniki, ki so v skrbeh glede svoje zasebnosti na spletu, ne bodo razkrili nobenih ali le nekaj svojih osebnih podatkov. Predhodne empirične raziskave potrjujejo, da uporabniki družbenega spleta na splošno menijo, da je varovanje njihove zasebnosti pomembno, vendar pa kljub temu le redko dovolijo, da bi težave z zasebnostjo vplivale na njihovo vedenje (Acquisti &

Gross, 2006; Boyd & Hargittai, 2010; Debatin, Lovejoy, Horn & Hughes, 2009; Tufekci, 2008). Zaskrbljenost glede varnosti osebnih podatkov na spletu tako ni nujno v skladu z ustreznim vedenjem, kot je razkrivanje manjše količine informacij ali spreminjanje nastavitev zasebnosti na družbenih omrežjih. Pojasnilo za to je pomanjkanje ozaveščenosti uporabnikov o težavah ali tveganjih, pa tudi nepoznavanje možnosti za zaščito osebnih podatkov (npr. sprememba nastavitev zasebnosti) oziroma neznanje o tem, kaj se z objavljenimi informacijami dogaja, saj uporabniki smernice za varstvo podatkov v obliki politik zasebnosti pogosto sprejmejo, ne da bi jih sploh prebrali (Tadiccken, 2014). Predpostavlja se, da se uporabniki ne morejo racionalno vesti, ko so v skrbeh glede zasebnosti, ker nimajo dejanske moči ali nadzora nad dogajanjem.

3.3 Razkrivanje zasebnosti na družbenih omrežjih

3.3.1 Motivi za razkrivanje zasebnosti

Medtem ko je zasebnost konceptualizirana kot omejevanje dostopa do informacij, pa je narava družbenih omrežij takšna, da spodbuja uporabnike k deljenju informacij. Deljenje informacij je takorekoč bistvena komponenta družbenih omrežij ter ključnega pomena za sodelovanje in participacijo. Uporabniki prispevajo vsebinske objave, fotografije, všečkajo vsebine in komentirajo objave drugih, kar jim omogoča prepoznavnost in sodelovanje z drugimi uporabniki. Poleg tega se z deljenjem prispeva vsebina v široko dostopni ekosistem druženih omrežij. Glede na to, da so lahko vsebine družbenih medijev vidne ogromnemu občinstvu, bi lahko trdili, da je edini način ohranjanja zasebnosti ta, da se informacije sploh ne delijo (Marwick & Boyd, 2014).

Deljenju osebnih podatkov na družbenih omrežjih z drugimi besedami rečemo tudi samorazkritje (angl. self-disclosure), ki sta ga Wheeless in Grotz (1976) opredelila kot »vsako sporočilo o sebi, ki ga oseba sporoči drugemu«. Samorazkritje je običajno rezultat upoštevanja tveganj in koristi. V kontekstu družbenih omrežij pogosto obstaja želja po samorazkritju na eni strani in želja po zaščiti zasebnosti na drugi (Taddicken, 2014).

Želja po razkritju osebnih podatkov in informacij o sebi izvira iz osebnostnih lastnosti posameznika. Nekaterim ljudem je v interesu, da drugi vedo podrobnosti o njihovem življenju, medtem ko se drugi raje držijo bolj zase in z ljudmi delijo manj informacij iz zasebnega življenja. Pripravljenost za samorazkritje lahko štejemo za dispozicijsko osebnostno lastnost in na podlagi tega sklepamo, da je pripravljenost posameznika za samorazkritje eden glavnih motivatorjev za uporabnikovo samorazkritje na družbenih omrežjih (Taddicken, 2014).

Ne glede na to, da je razkrivanje zasebnosti na družbenih omrežjih odvisno od več dejavnikov, med drugim od zgoraj omenjenih osebnostnih lastnosti uporabnikov, pa smo

ljudje družbena bitja in izmenjava informacij je temeljna značilnost medsebojnega povezovanja. Človeški motivi za razkrivanje zasebnosti niso nič manj temeljni od potrebe po zasebnosti. Močna motivacija za razkrivanje zasebnosti z deljenjem informacij je interakcija in socializacija med ljudmi, želja po prepoznavnosti širši javnosti, po razkritju in slavi ter nasprotno, strah pred anonimno nepomembnostjo (Acquisti, Brandimarte & Loewenstein, 2015).

Družbena omrežja nudijo izjemne priložnosti za delovanje in interakcijo med uporabniki. Razkritja uporabnikov prek družbenih omrežij ustvarjajo socialni kapital, večajo samozavest in izpolnjujejo potrebe ega. Podobno kot zasebnost tudi razkrivanje zasebnosti prinaša številne koristi, vključno s psihološkim in fizičnim zdravjem. V seriji funkcionalnih eksperimentov z magnetno resonanco je bilo ugotovljeno, da je razkrivanje v telesu aktiviralo nevronske mehanizme, podobne tistim, ki so povezani z nagrajevanjem. Ugotovili so, da ljudje cenijo možnost izmenjevanja misli in občutkov z drugimi (Acquisti, Brandimarte & Loewenstein, 2015).

3.3.2 Razkrivanje zasebnosti glede na kontekst in občinstvo

Ljudje se poznamo na podlagi sorodstvenih vezi, skupnih življenjskih dogodkov, izkušenj, namenov in podobno. Vsak človek je središče družbenih krogov, ki jih sestavljajo posamezniki z različnih področij njegovega življenja. Z različnimi krogi ljudi imamo pogosto različne odnose. V vsakem krogu so lahko močne ali šibke vezi; lahko gre za prijatelje, ki jih poznamo že desetletja, ali pa za nova poznanstva. Različni krogi ljudi običajno niso medsebojno izpostavljeni, lahko pa se prekrivajo in nekateri ljudje so lahko del več krogov. Različni krogi imajo različne norme v zvezi s tem, kaj je sprejemljivo oziroma nesprejemljivo, in tudi različne norme glede pričakovanj o tem, kaj naj ostane zasebno in kaj se lahko razkrije. Informacije, ki so dobro poznane in dostopne v krogu družine, so lahko v drugem krogu sramotne ali celo škodljive (občutljive informacije o zdravju, nosečnosti, incidenti na počitnicah in podobno se na primer lahko delijo s prijatelji ali družino, v pogovorih s sodelavci ali delodajalci pa to ni najbolj sprejemljivo). Gre za osebni oziroma medosebni vidik zasebnosti. Poleg tega obstaja še vidik zasebnosti iz perspektive države. Država je še en krog z normami, ki jih določajo zakoni. Moč in sredstva, ki jih ima država v lasti, jo uvrščajo v drugačno kategorijo kot druge kroge. Vprašanja glede zasebnosti države se razlikujejo od vprašanj glede zasebnosti v drugih krogih – to so predvsem pravno formalna vprašanja, ki so drugačna od družbenih norm v osebnejših družbenih krogih. Na družbenih platformah je dojemanje (zaznavanje) zasebnosti uporabnikov kombinacija njihovih pogledov v vseh družbenih krogih, od državnih, podjetniških do osebnih družbenih krogov (Blank, Bolsover & Dubois, 2014).

Zasebnost izhaja iz temeljnih značilnosti družbenega življenja. Družbena struktura je tista, ki ustvarja kontekst. Zasebnost je deloma negotova (nedorečena), ker imajo različni družbeni krogi različne norme (Blank, Bolsover & Dubois, 2014).

Samorazkritje uporabnikov na družbenih omrežjih se pogosto prikaže heterogenemu občinstvu z različnimi družbenimi odnosi (npr. družina, prijatelji, kolegi). Ta pojav se imenuje **»kolaps konteksta«** (Marwick & Boyd, 2014). Zaradi prostorske in časovne ločitve je pogosto nejasno, katere osebe in v kolikšnem številu so vključene v t. i. občinstvo. Občinstvo, ki mu uporabnik namerava razkriti osebne podatke in informacije, se lahko razlikuje od občinstva, ki je dejansko doseženo. S tem pa se lahko pojavijo neželene posledice za uporabnike. Pride lahko do nepooblaščene uporabe, ko tretje osebe posredujejo osebne podatke uporabnikov in jih prenesejo v druge kontekste (npr. družbena omrežja), ki nato uporabijo osebne podatke uporabnikov v oglaševalske namene, ter ko drugi uporabniki kopirajo in distribuirajo vsebino v druge namene (Taddicken, 2014).

Zasebnost je odvisna od kroga ljudi oziroma občinstva ter od družbenega konteksta takšnega kroga in njegovih normativnih pričakovanj. Tega, kaj je zasebno in kaj bi moralo ostati zasebno, torej ni mogoče presojati na podlagi enega samega standarda, temveč je potrebno upoštevati družbeni kontekst; družbena omrežja pa bi morala uporabnikom omogočiti upravljanje z njihovo zasebnostjo na način, ki ustreza tem kompleksnim potrebam.

Poznamo več konceptov razumevanja zasebnosti, saj gre dejansko za to, kako zasebnost zaznavajo različni akterji na družbenih omrežjih. Študije so pokazale, da uporabniki zaznavajo zasebnost predvsem v odnosu do drugih uporabnikov družbenih omrežij (npr. prijateljev na Facebooku, sledilcev na Instagramu in Twitterju ipd.). Ko uporabniki na družbenem omrežju objavijo svojo fotografijo, trenutno lokacijo in podobno, največkrat ne razmišljajo o tem, da delijo svojo zasebnost neposredno z družbenim omrežjem, ki njihove podatke nato uporabi v druge namene (npr. prediktivne analize), temveč razumejo to delitev kot interakcijo s svojimi krogi na družbenih omrežjih (Hull, 2015).

Zasebnost je močna družbena norma, vendar pogosto ni v interesu ponudnikov družbenih omrežij, ki imajo korist od uporabe osebnih podatkov uporabnikov. Družbena omrežja so že tako vpletena v naša življenja, da mora uporabnik, če želi ohraniti družabno življenje na družbenih omrežjih, razkriti osebne informacije kljub dejstvu, da obstaja veliko tveganje za kršitve zasebnosti in da družbena omrežja uporabnikom ne zagotavljajo ustreznega nadzora nad zasebnostjo (Blank, Bolsover & Dubois, 2014).

3.3.3 Razkrivanje osebnih podatkov na podlagi zaznanega nadzora

Psihološke raziskave so pokazale, da zaznave vplivajo na čustva in vedenje ljudi (Averill 1973; Skinner 1996). Na podlagi zaznanega nadzora posameznikov nad okoljem se oblikuje želeni rezultat, kot je sprejemanje informacijskih sistemov s strani uporabnikov (Baronas & Louis, 1988). Nasprotno pa posameznikovo psihološko dojemanje nadzora prispeva k njegovi želji po dejanskem vedenju (Hajli & Lin, 2014).

Razumevanje in zaznavanje nadzora uporabnikov neposredno vpliva na vedenje oziroma razkrivanje osebnih podatkov na družbenih omrežjih. Pri sprejemanju odločitev o tem, koliko podatkov o sebi bodo uporabniki razkrili, je pomembno, kakšen nadzor imajo nad temi podatki. Glede na to, da informacijska tehnologija družbenih omrežij vključuje zapletene algoritme in mehanizme, katerih načina delovanja večina uporabnikov ne razume, govorimo torej o njihovem zaznanem nadzoru nad podatki. Zaznani nadzor nad podatki je odvisen od zavedanja uporabnikov, v kolikšni meri sami nadzorujejo uporabo informacij prek nastavitev zasebnosti, in ima na njihovo vedenje precej večji vpliv kot dejanski nadzor (Hajli & Lin, 2014).

Hajli in Lin (2014) sta v študiji ugotavljala razumevanje uporabnikov z vidika zaznanega nadzora nad njihovimi podatki, v povezavi z njihovim vedenjem oziroma deljenjem informacij. Ugotovila sta, da je zaznani nadzor negativno povezan z zaznanim tveganjem v zvezi z zasebnostjo in odnosom do izmenjave informacij, kar posledično vpliva na vedenje uporabnikov pri izmenjavi informacij. Višje zaznavanje informacijskega nadzora ustvarja pozitivnejši odnos, saj so uporabniki, ko svoje osebne podatke posredujejo družbenim omrežjem, manj v skrbeh glede zbiranja teh podatkov. Podobno višje zaznavanje informacijskega nadzora vpliva na namere uporabnikov, da delijo svoje osebne podatke na družbenih omrežjih. Uporabniki običajno delijo svoje osebne podatke, kadar imajo večji nadzor nad informacijami, kar pomeni, da je nadzor uporabnikov nad informacijami ključnega pomena pri sprejemanju odločitev o razkrivanju informacij na družbenih omrežjih, kot sta Facebook in Twitter. Z večjim naborom možnosti za nadzor zasebnosti na družbenih omrežjih imajo uporabniki večje zaupanje v ta omrežja – uporabnik namreč misli, da lahko ponujene možnosti kadarkoli uporabi in družbenemu omrežju odvzame pravice za uporabo zbranih osebnih podatkov, kar pa se skoraj nikoli ne zgodi.

Uporabniki družbenih omrežij si močno želijo nadzorovati uporabo objavljenih informacij. Zmožnost nadzora nad tem, katere informacije o nas lahko ljudje pridobijo in v kolikšnem obsegu, je za uporabnike pomembna, saj s tem ocenjujejo varnost družbenih omrežij. Nobenega dvoma ni, da uporabniki družbenih omrežij potrebujejo nadzor nad svojimi osebnimi podatki, da bi lahko zaščitili svojo zasebnost. Številni delijo svoje osebne podatke in informacije z mislijo, da jih bodo videli le njihovi prijatelji, družina in drugi ljudje, ki jih bodo sami izbrali. Toda do osebnih podatkov in informacij posameznikov imajo dostop tudi drugi, na primer družbena omrežja, ki na ta način zlorabljajo njihovo zasebnost. Na podlagi tega bi bilo treba uravnotežiti zaznani in dejanski nadzor uporabnikov, kar bi lahko dosegli z bolj funkcionalnimi nastavitvami zasebnosti (Hajli & Lin, 2014).

3.3.4 Razkrivanje na podlagi zaznanega tveganja

Družbena omrežja beležijo interakcije med uporabniki z namenom podatkovnega rudarjenja in izkoriščanja podatkov v komercialne ali druge namene, večinoma brez

vedenja uporabnikov. Zbiranje in posredovanje lahko posledično privedeta do nezakonitega razkritja in uporabe osebnih podatkov. Zaznano tveganje zlorab zasebnosti v okviru družbenih omrežij je pomemben dejavnik, ki vpliva na psihološko zaznavanje uporabnikov in njihove namene pri uporabi informacijske tehnologije, kar posledično vpliva na vedenje uporabnikov na družbenih omrežjih (Hajli & Lin, 2014).

Pomisleki glede zasebnosti informacij negativno vplivajo na odnos uporabnikov do razkrivanja osebnih podatkov na družbenih omrežjih. Ob zaznavanju visokega tveganja v zvezi z zasebnostjo se zmanjša njihova pripravljenost za izmenjavo osebnih podatkov na družbenih omrežjih. Zato bodo uporabniki, ki zaznavajo večje tveganje v zvezi z zasebnostjo, na družbenih omrežjih razkrili manj informacij, saj so glede svoje zasebnosti bolj zaskrbljeni. Uporabnikovo visoko dojemanje nadzora nad informacijami bo verjetno omililo njegovo zaskrbljenost glede zasebnosti in izboljšalo varnost uporabe družbenih omrežij, ki jo zaznava. Večji kot je nadzor uporabnikov družbenih omrežij nad informacijami, manjše tveganje zaznavajo (Hajli & Lin, 2014).

Uporaba družbenih omrežij lahko privede tudi do slabih izkušenj oziroma zlorab zasebnosti, na podlagi česar se lahko zmanjša zaupanje v uporabo tehnologije in posledično ustvarjanje vsebin na teh omrežjih. Debatin, Lovejoy, Horn in Hughes (2009) so v svoji raziskavi ugotovili, da obstaja pri uporabnikih, ki so doživeli vdor v zasebnost (npr. krajo ali zlorabo osebnih podatkov, nadlegovanje, zalezovanje, neprimerne govorice ipd.), večja verjetnost, da bodo spremenili svoje nastavitve zasebnosti, kot to velja za ostale uporabnike. Na podlagi tega lahko sklepamo, da so ti uporabniki bolj zaskrbljeni glede svoje zasebnosti ter želijo večji nadzor nad podatki in manjše tveganje za pojav zlorab.

3.4 Paradoks zasebnosti

V zadnjem času je veliko člankov, v katerih se govori o paradoksu zasebnosti, kar v splošnem pomeni, da uporabnike družbenih omrežij skrbi njihova zasebnost, njihovo vedenje na družbenih omrežjih pa kaže na to, da s tem, ko objavljajo fotografije in videoposnetke, komentirajo različne objave, všečkajo vsebine, objavijo svojo trenutno lokacijo in podobno, razkrivajo ogromno količino osebnih podatkov in informacij o sebi. Paradoks zasebnosti lahko opišemo tudi kot neskladje med zaskrbljenostjo uporabnikov glede njihove zasebnosti in razkrivanjem zasebnosti na družbenih omrežjih (Barth & de Jong, 2017; Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Tufekci, 2008).

Neskladnost glede preferenc pri pojmu zasebnosti pride do izraza z merjenjem razlik med posamezniki in skupinami. To področje je raziskoval tudi Westin, ki je v svoji raziskavi želel posameznike združiti v različne segmente – fundamentaliste zasebnosti, pragmatike in nezaskrbljene glede zasebnosti – ter pri tem uporabil široka, kontekstualno nespecifična vprašanja. Pri neposrednem vprašanju »Ali ste v skrbeh glede svoje zasebnosti?« je veliko

posameznikov padlo v prvi segment fundamentalistov, ki so zelo zaskrbljeni glede zasebnosti – skrbi jih izguba nadzora nad lastnimi osebnimi podatki in nepooblaščen dostop do teh podatkov (Acquisti, Brandimarte & Loewenstein, 2015). Vedenje uporabnikov tako pogosto ne odraža njihovega stališča glede zaskrbljenosti v zvezi z zasebnostjo. Vzvodi za takšno ravnanje, ko uporabniki pravijo, da jih skrbi zasebnost, hkrati pa na družbenih omrežjih razkrivajo osebne podatke in informacije o sebi, so lahko posledica pomanjkljivega razumevanja tveganja, pomanjkanja znanja o mehanizmih, ki varujejo zasebnost, ali prednosti, ki jih uporabnikom prinaša razkritje informacij na družbenih omrežjih (Hargittai & Marwick, 2016).

Hull (2015) ugotavlja, da ljudje sicer pravijo, da cenijo svojo zasebnost; ko pa se pojavi priložnost, da izpostavijo (prodajo) svoje osebne podatke in informacije za takojšnje, četudi majhne koristi (npr. dostop do spletne strani), pa običajno to brez težav storijo. S tem pogosto dokažejo, da svoje zasebnosti v bistvu ne cenijo v tolikšni meri, kot bi si želeli.

Avtorji študij so pri raziskovanju paradoksa zasebnosti prišli do več razlogov za neskladje med domnevno zaskrbljenostjo uporabnikov glede zasebnosti in njihovim vedenjem (Norberg, Horne & Horne, 2007; Acquisti & Gross, 2006). Ena od možnosti, ki pa ni povsem zadovoljiva, je ta, da je paradoks iluzoren (navidezen) in da ne moremo sklepati, da so odnos do zasebnosti ter nameni in vedenje tesno povezani. V tem primeru bi lahko uporabnike skrbela zasebnost v širšem smislu, vendar bi v določenih situacijah glede na stroške in koristi iskali (ali pa ne) zaščito zasebnosti. Ta razlaga paradoksa zasebnosti ni povsem zadovoljiva iz dveh razlogov. Prvi razlog je ta, da razlaga ne upošteva situacij, v katerih se dihotomije odnosa in vedenja pojavljajo pod visoko ujemajočo se izraženo zaskrbljenostjo in vedenjskimi dejanji. V študiji, v kateri so primerjali odgovore iz anketnih vprašalnikov z dejanskim vedenjem posameznikov, je bilo ugotovljeno naslednje: med anketiranci, ki so izrazili najvišjo stopnjo zaskrbljenosti nad neznanci, jih je 48 % na spletu dejansko javno razkrilo svojo spolno usmerjenost, 47 % jih je razkrilo svoja politična prepričanja, 21 % pa jih je razkrilo ime svojega trenutnega partnerja. Drugi razlog je ta, da je sprejemanje odločitev glede zasebnosti le delno posledica razumnega tehtanja stroškov in koristi. Na to vplivajo tudi napačna dojemanja teh stroškov in koristi, pa tudi družbene norme, čustva in hevristika. Vsak od teh dejavnikov lahko vpliva na vedenje drugače, kar je odvisno od tega, kakšen je vpliv teh dejavnikov na vedenje. Zaradi pristranskosti v sedanjosti se lahko uporabnik na primer odloči za tvegano razkritje informacij, če je takojšnje zadovoljstvo ob tem večje od poznejših možnih posledic (Acquisti, Brandimarte & Loewenstein, 2015).

Paradoks zasebnosti vse do danes ni povsem jasno razložen. Glavna razloga za to naj bi bila pomanjkanje ozaveščenosti o težavah ali tveganjih in nezadostno zavedanje uporabnikov o možnostih varovanja zasebnosti (Acquisti & Gross, 2006; Boyd & Hargittai, 2010; Debatin, Lovejoy, Horn & Hughes, 2009; Tufekci, 2008). Domneva se

tudi, da uporabniki pri razkrivanju osebnih podatkov običajno podcenjujejo potencialne nevarnosti v zvezi z zasebnostjo (Taddicken, 2014).

4 RAZISKAVA ZASEBNOSTI NA DRUŽBENIH OMREŽJIH

4.1 Raziskovalno vprašanje in namen raziskave

Z raziskavo sem želela dobiti vpogled v odnos uporabnikov do njihove zasebnosti in do varovanja osebnih podatkov na družbenih omrežjih. Zanimalo me je, v kolikšni meri se zavedajo uporabe svojih osebnih podatkov v druge namene ter ali jih to moti oziroma se poslužujejo metod za zaščito zasebnosti. Namen moje raziskave je proučiti, kako uporabniki zaznavajo zasebnost in varnost osebnih podatkov na družbenih omrežjih in ali je njihovo vedenje v skladu z njihovim zaznavanjem.

Izhajala bom iz teorije in drugih raziskav, ki so že bile izvedene na to temo, nato pa bom podatke raziskave primerjala z že obstoječo teorijo. Podatki, ki jih želim pridobiti od sodelujočih v anketi, se nanašajo predvsem na zaznavanje zasebnosti in njihovo vedenje na družbenih omrežjih.

4.2 Metodologija

4.2.1 Sestava anketnega vprašalnika

Anketni vprašalnik sem zastavila široko, da bi pridobila čimveč različnih podatkov za celostno razumevanje teme, ki jo raziskujem. Po pregledu in analizi pridobljenih podatkov sem vključila le relevantne podatke, kar je bil tudi cilj mojega dela.

Anketni vprašalnik je obsegal 20 vprašanj za uporabnike družbenih omrežij. Večina vprašanj je bila zaprtega tipa, pri enem vprašanju pa sem pustila možnost odprtega odgovora, in sicer pri opisu nenavadne ali slabe izkušnje v zvezi z zasebnostjo na družbenih omrežjih. Anketni vprašalnik sem poskusila sestaviti tako, da bi bil anketirancem razumljiv in jasen. S pomočjo testne skupine šestih ljudi sem želela preveriti, ali so vprašanja razumljiva ali pa so morda potrebni popravki. Na podlagi predlogov testne skupine sem določena vprašanja preoblikovala tako, da bi bila kar se da jasna in nedvoumna.

Anketni vprašalnik sem zasnovala po naslednjih sklopih:

- Vprašanja glede uporabe družbenih omrežij.

- Vprašanja glede zasebnosti (zaznavanje zasebnosti, zaskrbljenost v zvezi z zasebnostjo).
- Vprašanja glede razkrivanja zasebnosti.
- Demografska vprašanja.

4.2.2 Metoda zbiranja in obdelave podatkov

V empiričnem delu magistrskega dela sem izvedla anketo prek spletne ankete 1KA. Podatki za raziskavo so bili zbrani v obdobju od 17. februarja 2019 do 8. aprila 2019. V anketi so sodelovali študenti dodiplomskega študija na Ekonomski fakulteti, ki spadajo v starostno skupino od 18 do 25 let, posredovala pa sem jo tudi prek družbenega omrežja, kjer je bila dostopna širšemu krogu vseh starostnih skupin, predvsem posameznikom, starim od 26 do 40 let. Manjše število ljudi je povabilo in povezavo do ankete prejelo prek elektronske pošte. Za analizo podatkov, pridobljenih z anketo, sem uporabila deskriptivno statistično metodo. Pridobljene podatke sem statistično analizirala s programom SPSS in za njihovo lažjo predstavitev uporabila grafe v programu Microsoft Excel.

4.2.3 Opis vzorca

Za vzorčni okvir raziskovanja sem uporabila posameznike, ki so v anketnem vprašalniku odgovorili, da uporabljajo družbena omrežja – skupaj 259 anketirancev, ki jih bom v nadaljevanju imenovala uporabniki. Tiste, ki so na vprašanje o uporabi družbenih omrežij odgovorili, da jih ne uporabljajo, sem izločila iz nadaljne analize – teh je bilo 10. V anketnem vprašalniku nisem opredelila starostnega razreda, saj me je zanimalo, kakšno je dojemanje zasebnosti vseh starostnih skupin. Glede na starost sem uporabnike razvrstila v pet starostnih skupin, in sicer do 18 let, od 18 do 25 let, od 26 do 40 let, od 40 do 61 let in 61 let ali več. Na podlagi različnih starostnih skupin sem ugotavljala morebitne razlike, ki se pojavljajo glede na starost uporabnikov, in uporabnike v tem primeru združila v dve starostni skupini. Največ uporabnikov družbenih omrežij je tako starih od 18 do 25 let in od 25 do 40 let.

4.3 Analiza in predstavitev pridobljenih podatkov

Čeprav je bil anketni vprašalnik zastavljen široko, z željo dobiti celovit vpogled v zaznavanje in varovanje zasebnosti na družbenih omrežjih, sem se pri analizi osredotočila predvsem na bistvene podatke. Za lažjo predstavitev sem pridobljene podatke združila v naslednje sklope:

- Demografske značilnosti.
- Priljubljenost družbenih omrežij.
- Razkrivanje zasebnosti na družbenih omrežjih.

- Zaskrbljenost uporabnikov glede zasebnosti.
- Zaznavanje zasebnosti z vidika uporabe osebnih podatkov v tržne namene.

4.3.1 Demografske značilnosti

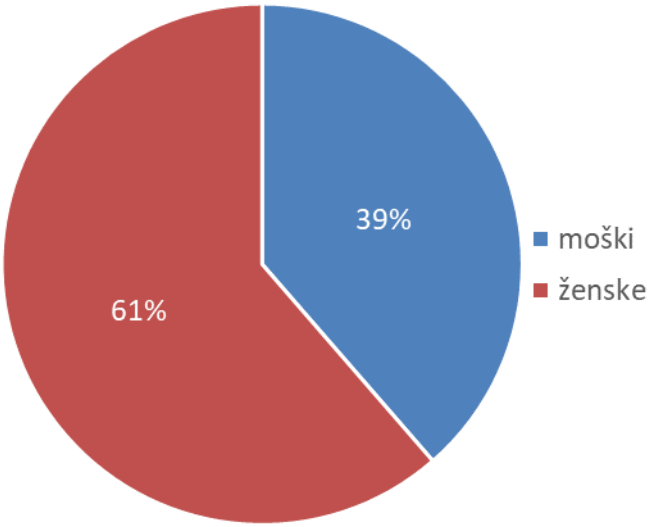
Slika 3 prikazuje strukturo po spolu uporabnikov, iz katere je razvidno, da je od vseh anketiranih uporabnikov 100 (39 %) moških in 159 (61 %) žensk.

Glede na starostno strukturo uporabnikov družbenih omrežij sem vzorec razdelila v pet skupin, kot je prikazano v sliki 4. Po številu uporabnikov jih največ spada v starostno skupino od 18 do 25 let, in sicer 157 (61 %), sledi starostna skupina od 26 do 40 let z 91 (35 %) uporabniki. Le nekaj jih je v preostalih starostnih skupinah, ki si po številu uporabnikov sledijo s 6 (2 %) uporabniki v starostni skupini od 41 do 60 let, 3 (1 %) uporabniki v starostni skupini 61 let ali več ter 2 (1 %) uporabnikoma v starostni skupini do 18 let.

4.3.2 Priljubljenost družbenih omrežij

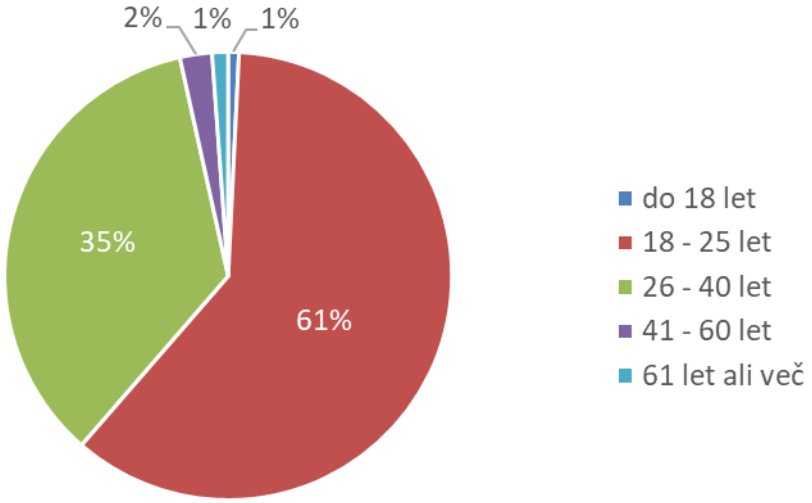
Slika 5 kaže, da je med uporabniki najbolj priljubljeno družbeno omrežje Facebook, ki ga uporablja 249 (96 %) uporabnikov. Sledijo mu Instagram z 202 (78 %) uporabnikoma, Snapchat s 147 (67 %) uporabniki, Pinterest s 111 (43 %) uporabniki in LinkedIn s 65 (25 %) uporabniki. Od ponujenih družbenih omrežij najmanj uporabnikov uporablja Twitter, teh je 59 (23 %). Druga družbena omrežja uporablja 38 (15 %) uporabnikov, med njimi so navedli Youtube, WhatsApp, Tumblr, Reddit in druge.

Slika 3: Struktura uporabnikov glede na spol (n=259)



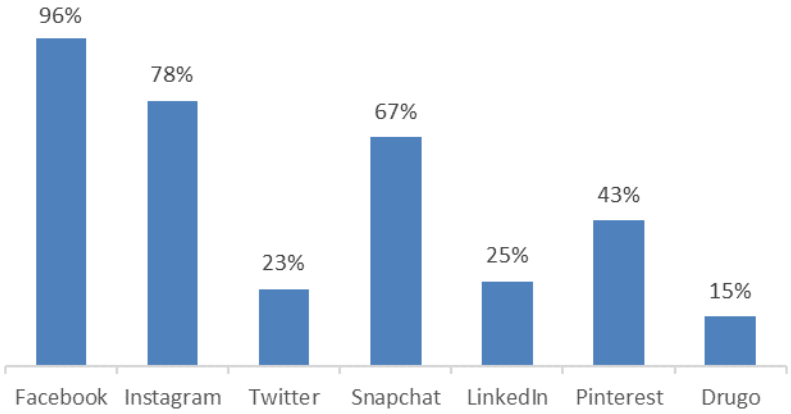
Vir: lastno delo.

Slika 4: Struktura uporabnikov glede na starost (n=259)



Vir: lastno delo.

Slika 5: Priljubljenost družbenih omrežij (n=259)

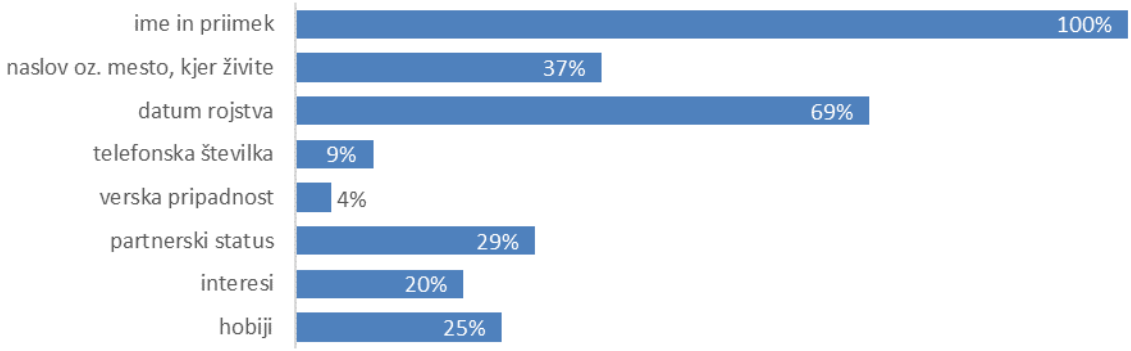


Vir: lastno delo.

4.3.3 Razkrivanje zasebnosti na družbenih omrežjih

Ob ustvarjanju profila in po tem družbena omrežja ponujajo možnost objave različnih osebnih podatkov, kot so ime in priimek, naslov, datum rojstva, telefonska številka, verska pripadnost, partnerski status in drugo. Zanimalo me je, katere osebne podatke razkrivajo uporabniki družbenih omrežij. Iz slike 6 je razvidno, da se vseh 259 (100 %) anketiranih uporabnikov na družbenih omrežjih predstavlja z imenom in priimkom, datum rojstva jih je objavilo 178 (69 %), mesto, v katerem živijo, je navedlo 95 (37 %) uporabnikov, partnerski status 74 (29 %) uporabnikov, hobije 64 (25 %) uporabnikov, interese 52 (20 %) uporabnikov, telefonsko številko 24 (9 %) uporabnikov in versko pripadnost 11 (4 %) uporabnikov.

Slika 6: Objava osebnih podatkov uporabnikov (n=259)



Vir: lastno delo.

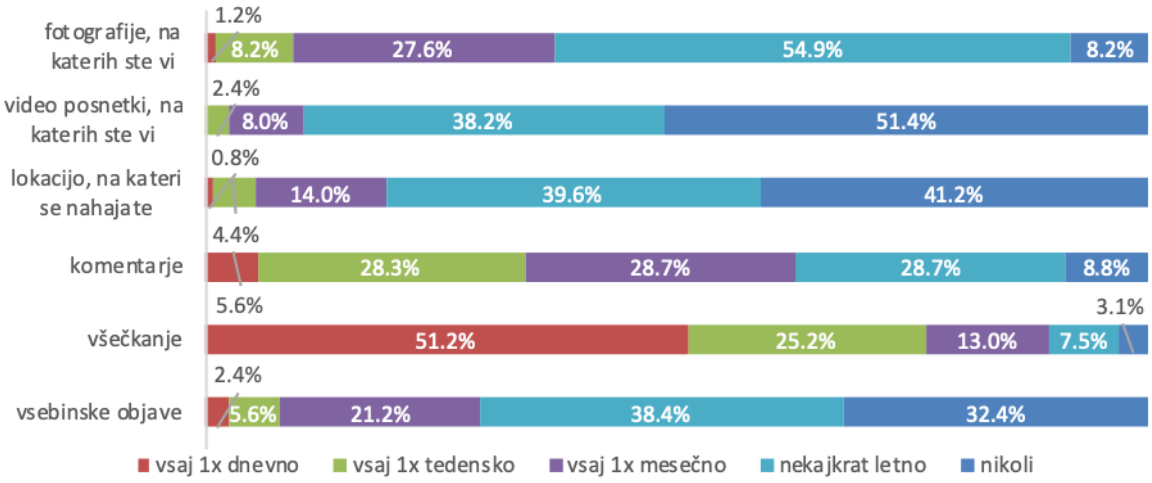
V zvezi z razkrivanjem uporabnikov na družbenih omrežjih me je v nadaljevanju zanimalo tudi, kaj uporabniki objavljajo in kako pogosto to počnejo. Anketiranci so lahko izbirali med različnimi vrstami objav, ki so na družbenih omrežjih najpogostejše: objava fotografij in videoposnetkov, trenutna lokacija, komentarji in všečki ter vsebinske objave. Slika 7 prikazuje, da všečkanje izvaja 246 (97 %) od 254 uporabnikov, ki so se opredelili glede všečkanja. Svoje fotografije objavlja 236 (91 %) od 257 uporabnikov, ki so se opredelili glede objavljanja fotografij. Komentira 229 (91 %) od skupno 251 uporabnikov, ki so se opredelili glede komentiranja. Vsebine objavlja 169 (68 %) od 250 uporabnikov, ki so se opredelili glede objavljanja vsebin. Sledijo tisti, ki objavljajo svojo trenutno lokacijo – to počne 147 (59 %) od skupno 250 uporabnikov, ki so se opredelili glede objavljanja lokacije. Najmanj jih objavlja svoje videoposnetke – le 121 (49 %) od skupno 249 uporabnikov, ki so se opredelili glede objavljanja videoposnetkov. Iz slike 7 je razvidna tudi pogostost navedenih dejavnosti.

4.3.4 Zaskrbljenost uporabnikov glede zasebnosti

S sklopom vprašanj o zasebnosti na družbenih omrežjih sem želela raziskati odnos uporabnikov do njihove zasebnosti in osebnih podatkov. Na vprašanje o tem, ali se jim zasebnost zdi pomembna, jih je 116 (45 %) odgovorilo, da jim je zelo pomembna, 98 (38 %) uporabnikov je odgovorilo, da jim je pomembna, 8 (3 %) uporabnikom ni niti pomembna niti nepomembna, 4 (1 %) uporabniki so zasebnost opredelili kot nepomembno, 33 (13 %) uporabnikom pa je zasebnost zelo nepomembna. Rezultati so prikazani v sliki 8.

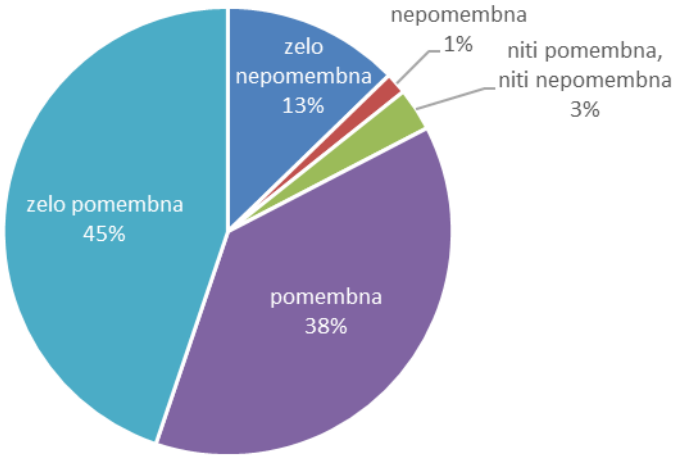
Od 214 (83 %) uporabnikov, ki jim je zasebnost pomembna (pomembna oz. zelo pomembna), jih 206 (96 %) uporablja všečke, 196 (92 %) uporabnikov objavlja fotografije, 192 (90 %) jih komentira, 142 (66 %) uporabnikov objavlja vsebine, 132 (57 %) jih objavlja svojo trenutno lokacijo, najmanj uporabnikov, to je 195 (49 %), pa objavlja videoposnetke. Rezultati so prikazani v sliki 9.

Slika 7: Vrste in pogostost objav na družbenih omrežjih



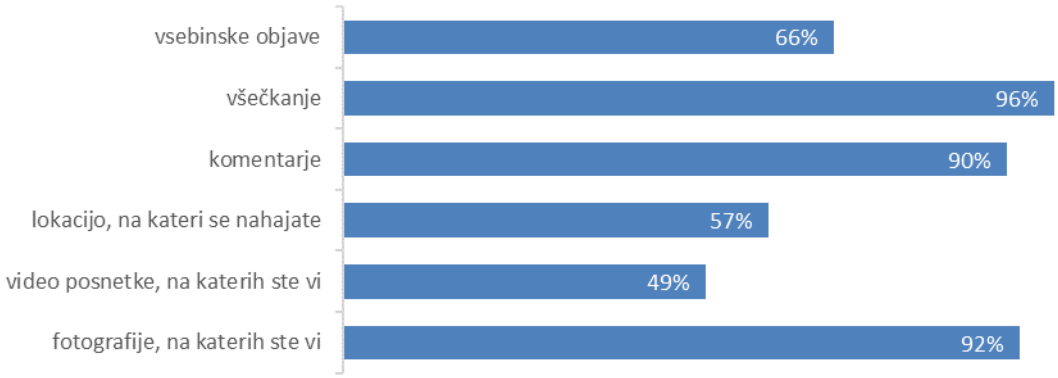
Vir: lastno delo.

Slika 8: Pomen zasebnosti (n=259)



Vir: lastno delo.

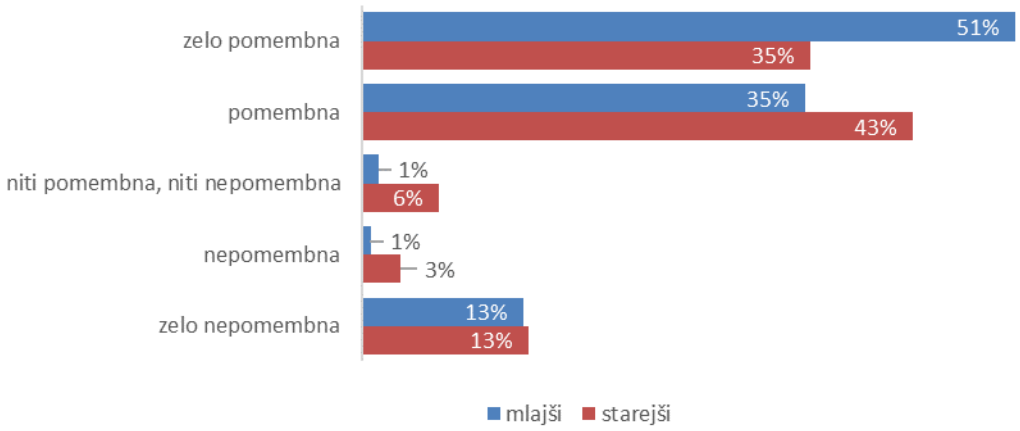
Slika 9: Objava podatkov uporabnikov, ki jim je zasebnost pomembna (n=214)



Vir: lastno delo.

V nadaljevanju me je zanimalo, kakšne so razlike v odnosu do zasebnosti mlajših in starejših uporabnikov, zato sem starostne razrede razdelila v dve skupini: mlajše uporabnike (do 25 let) in starejše uporabnike (26 let ali več). Mlajših uporabnikov je bilo skupno 159, starejših pa 100. V sliki 10 so prikazani rezultati, ki kažejo na to, da je 81 (51 %) mlajšim uporabnikom zasebnost na družbenih omrežjih zelo pomembna, medtem ko je enakega mnenja 35 (35 %) starejših uporabnikov. Zasebnost je pomembna 55 (35 %) mlajšim uporabnikom in 43 (43 %) starejšim uporabnikom. Sledijo tisti, ki jim je zasebnost zelo nepomembna – delež le-teh je pri mlajših in starejših uporabnikih enak, in sicer 13 %, kar pomeni, da je zasebnost zelo nepomembna 20 mlajšim in 13 starejšim uporabnikom. Glede pomena zasebnosti se nista opredelila 2 (1 %) mlajša uporabnika in 6 (6 %) starejših uporabnikov. Podoben rezultat je bil tudi pri odgovoru, da jim je zasebnost nepomembna – tako menijo 1 (1 %) mlajši uporabnik in 3 (3 %) starejši uporabniki.

Slika 10: Pomen zasebnosti glede na starost uporabnikov (n=259)

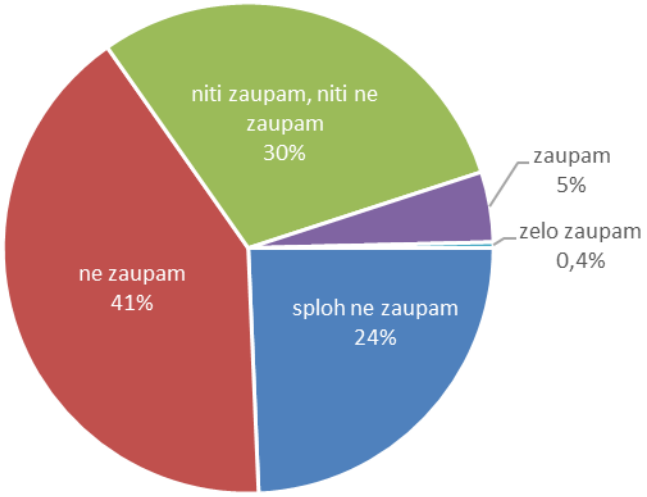


Vir: lastno delo.

Na vprašanje o tem, koliko zaupajo družbenim omrežjem, da le-ta ne posredujejo njihovih osebnih podatkov v obdelavo tretjim osebam (npr. oglaševalcem), rezultati kažejo, da jim večina uporabnikov ne zaupa. Največ jih je odgovorilo z »ne zaupam«, to je 106 (41 %) uporabnikov, sledijo jim tisti, ki družbenim omrežjem sploh ne zaupajo, teh je 63 (24 %). Neopredeljenih je 77 uporabnikov, kar predstavlja 30 %. Zaupa jim 12 (5 %) uporabnikov, le 1 uporabnik pa je na to vprašanje odgovoril, da jim zelo zaupa, kar predstavlja 0,4 % vseh anketiranih uporabnikov. Rezultati so prikazani v sliki 11.

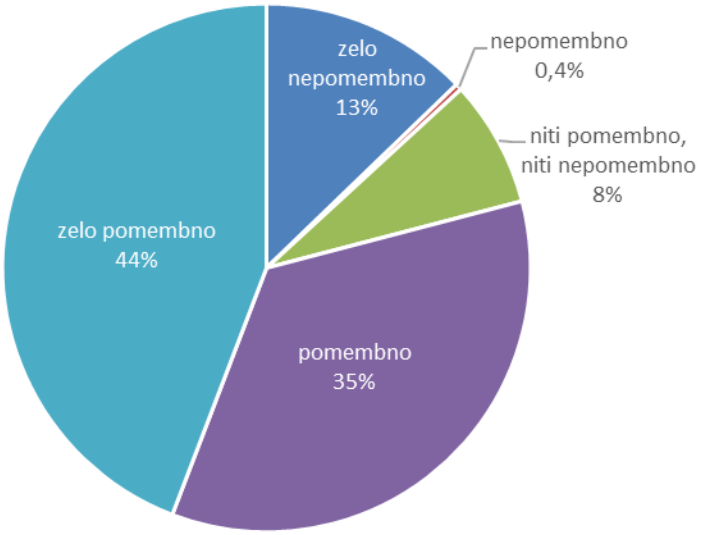
V tem sklopu sem želela ugotoviti tudi, kako pomembno se zdi uporabnikom, da država z zakonodajo uravnava področje zasebnosti na družbenih omrežjih. Iz slike 12 je razvidno, da je to zelo pomembno 114 (44 %) uporabnikom. Sledijo jim uporabniki, ki jim je to pomembno, teh je 90 (35 %). To se zdi zelo nepomembno 33 (13 %) uporabnikom. Neopredeljenih je 20 (8 %) uporabnikov, le 1 uporabnik pa je na to vprašanje odgovoril z »nepomembno«, kar predstavlja 0,4 % vseh uporabnikov.

Slika 11: Zaupanje uporabnikov v družbena omrežja (n=259)



Vir: lastno delo.

Slika 12: Pomen državne regulative zasebnosti na družbenih omrežjih (n=259)



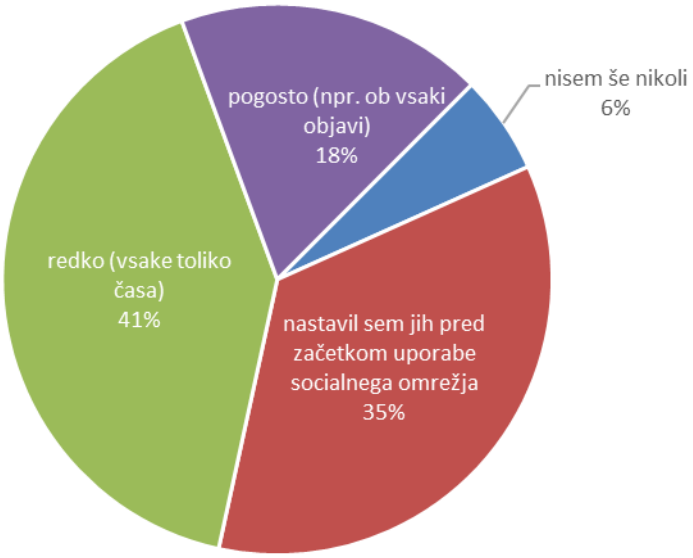
Vir: lastno delo.

Odgovori uporabnikov na vprašanje o tem, kako pogosto uporabljajo nastavitve zasebnosti, so bili naslednji. Največ jih nastavitve zasebnosti uporablja redko oziroma vsake toliko časa, takšnih je 106 (41 %). Sledijo jim tisti, ki so nastavitve nastavili na začetku uporabe družbenega omrežja, takšnih uporabnikov je 91 (35 %). Uporabnikov, ki so odgovorili, da nastavitve zasebnosti uporabljajo pogosto, je 47 (18 %), še nikoli pa jih ni uporabljalo 15 (6 %) uporabnikov. Rezultati so prikazani v sliki 13.

Pri tem vprašanju me je zanimalo tudi, kakšne so razlike pri uporabi nastavitev med starejšimi in mlajšimi uporabniki. Iz slike 14 je razvidno, da 43 (43 %) starejših uporabnikov uporablja nastavitve redko oziroma vsake toliko časa, medtem ko je takšnih

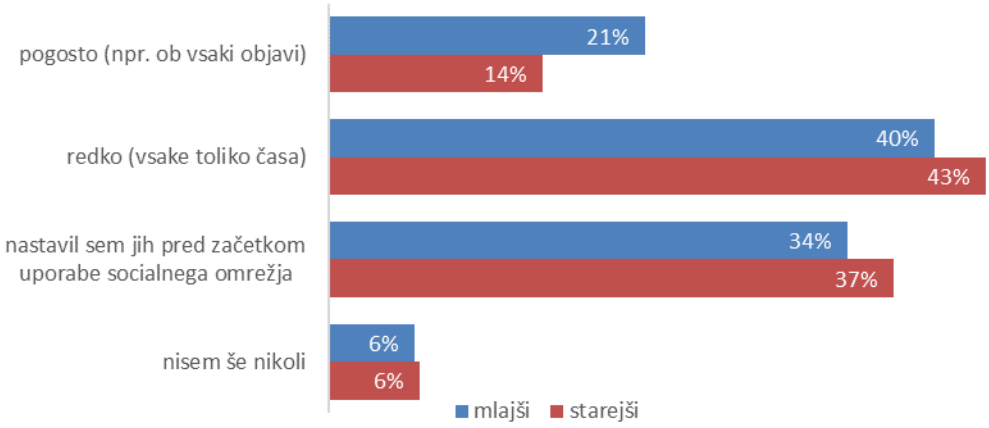
mlajših uporabnikov 63 (40 %). Pred začetkom uporabe družbenega omrežja je nastavitve zasebnosti uporabilo 37 (37 %) starejših in 54 (34 %) mlajših uporabnikov. Pogosto jih uporablja 14 (14 %) starejših in 33 (21 %) mlajših uporabnikov, nikoli pa jih ne uporablja 6 starejših in 9 mlajših uporabnikov, kar v obeh primerih predstavlja 6 %.

Slika 13: Uporaba nastavitev zasebnosti (n=259)



Vir: lastno delo.

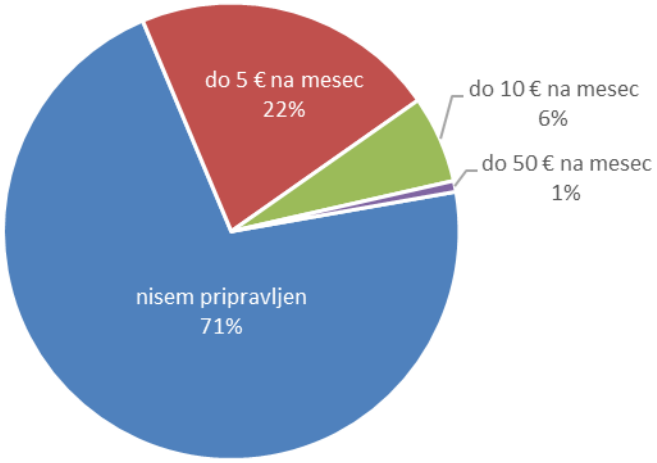
Slika 14: Uporaba nastavitev zasebnosti glede na starost (n=259)



Vir: lastno delo.

V nadaljevanju sem želela ugotoviti, ali so uporabniki pripravljeni plačati za to, da družbena omrežja ne bi uporabljala njihovih osebnih podatkov v tržne namene, ter na ta način zavarovati svojo zasebnost. Rezultati v sliki 15 kažejo na to, da večina uporabnikov za to ni pripravljena plačati, to je 185 (71 %) uporabnikov. Do 5 € na mesec je pripravljenih plačati 56 (22 %) uporabnikov. Uporabnikov, ki so pripravljeni plačati do 10 € na mesec, je 16 (6 %). Najmanj uporabnikov je pripravljenih plačati do 50 € na mesec – to sta 2 uporabnika, kar predstavlja le 1 % vseh uporabnikov

Slika 15: Pripravljenost uporabnikov na plačilo v zameno za zasebnost (n=259)

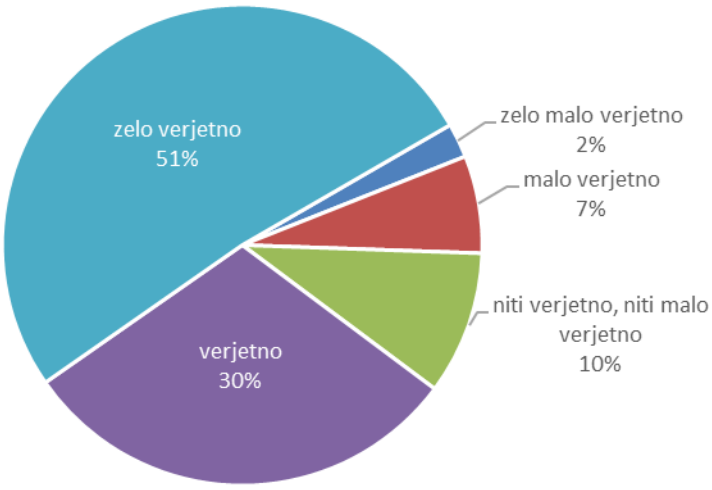


Vir: lastno delo.

4.3.5 Zaznavanje zasebnosti z vidika uporabe podatkov v tržne namene

Pri vprašanju o tem, koliko se uporabnikom zdi verjetno, da oglaševalci uporabljajo njihove osebne podatke v tržne namene, me je zanimalo, kakšno je zavedanje uporabnikov o uporabi njihovih osebnih podatkov v druge namene. Rezultati v sliki 16 kažejo, da se to zdi zelo verjetno 133 (51 %) uporabnikom, medtem ko 78 (30 %) uporabnikov meni, da se to verjetno dogaja. Sledi jim 25 (10 %) uporabnikov, ki pravijo, da to niti ni verjetno niti malo verjetno. 25 (7 %) uporabnikov je mnenja, da je to malo verjetno. Najmanj pa jih meni, da je to zelo malo verjetno – skupaj 6 uporabnikov, kar predstavlja le 2 % vseh uporabnikov.

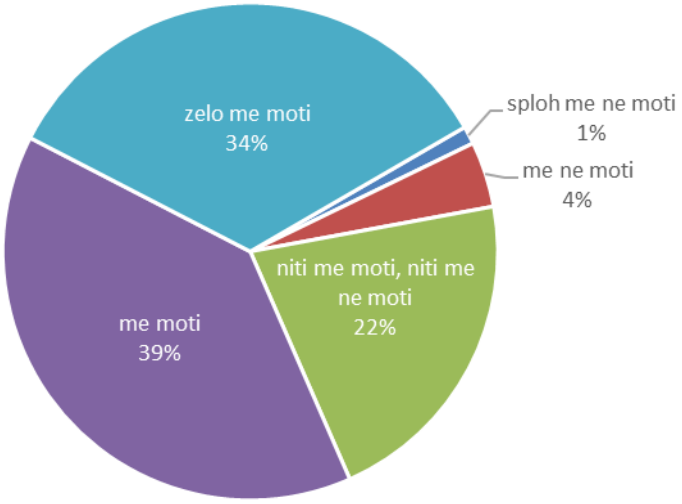
Slika 16: Verjetnost uporabe osebnih podatkov v tržne namene (n=259)



Vir: lastno delo.

Ker oglaševalci dejansko uporabljajo osebne podatke uporabnikov za svoj dobiček, sem v povezavi s prejšnjim vprašanjem želela ugotoviti, ali uporabnike to vedenje moti. Iz rezultatov v sliki 17 je razvidno, da se večina uporabnikov z vedenjem oglaševalcev ne strinja oziroma jih to moti. 101 uporabnika takšno vedenje zelo moti, kar predstavlja največji delež vseh anketiranih uporabnikov, to je 39 %. Uporabnikov, ki jih to moti, je 88 (34 %). Sledi jim 55 uporabnikov, ki so neopredeljeni oziroma jih to niti ne moti niti moti, kar predstavlja 21 %. 11 (4 %) uporabnikov uporaba osebnih podatkov v tržne namene ne moti. Najmanj je tistih uporabnikov, ki jih to sploh ne moti, skupno 3 (1 %) od vseh anketiranih uporabnikov.

Slika 17: Uporaba osebnih podatkov s strani oglaševalcev za njihov dobiček (n=259)



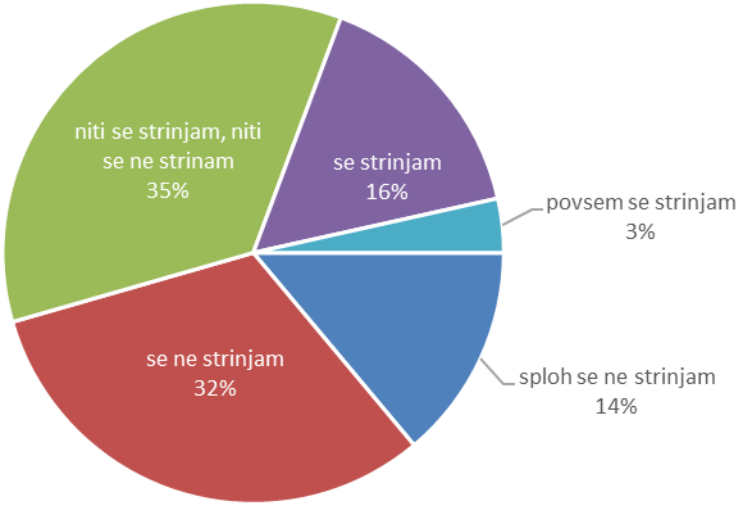
Vir: lastno delo.

Odgovore uporabnikov na vprašanje o tem, ali se strinjajo, da imajo nadzor nad zasebnostjo na družbenih omrežjih, prikazuje slika 18. Glede na prejšnje odgovore so bili tukaj odgovori zelo razpršeni. Največ uporabnikov, to je 91 (35 %), je neopredeljenih, saj so odgovorili, da se niti strinjajo niti ne strinjajo. Sledijo jim tisti, ki se ne strinjajo, da imajo nadzor nad zasebnostjo, takšnih je 82 (32 %). 41 uporabnikov oziroma 16 % se z nadzorom strinja. 36 uporabnikov, kar predstavlja 14 %, se s tem sploh ne strinja. Najmanj se jih z navedeno trditvijo povsem strinja, to je 9 uporabnikov oziroma 4 % vseh anketiranih uporabnikov.

Naslednje vprašanje se je nanašalo na zlorabe zasebnosti, in sicer me je zanimalo, koliko se uporabnikom zdi verjetno, da bodo njihovi osebni podatki postali javni. Iz rezultatov v sliki 19 je razvidno, da jih je na to vprašanje največ odgovorilo z »verjetno«, to je 96 uporabnikov oziroma 37 %. Sledijo jim uporabniki, ki se jim to zdi malo verjetno – teh je 72, kar predstavlja 28 %. Neopredeljenih je 67 uporabnikov, to je v deležu 26 % uporabnikov. 17 uporabnikom oziroma 7 % se to zdi zelo verjetno, najmanj pa jih je

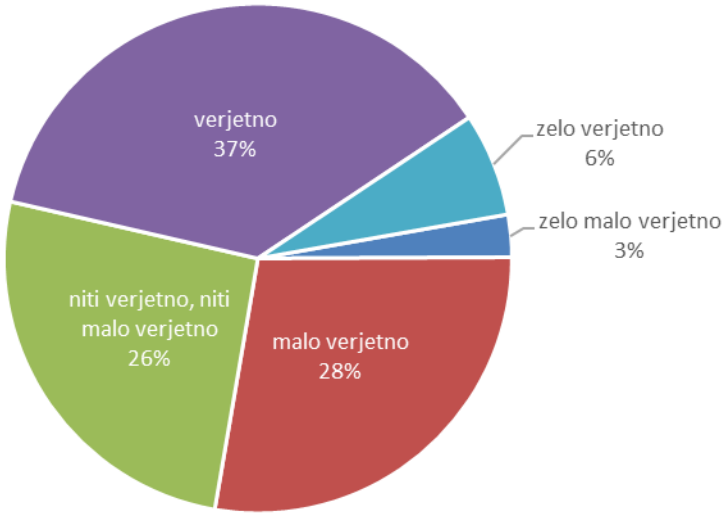
odgovorilo z »zelo malo verjetno«, to je 7 uporabnikov, kar predstavlja 3 % vseh anketiranih uporabnikov.

Slika 18: Strinjanje glede nadzora nad zasebnostjo na družbenih omrežjih (n=259)



Vir: lastno delo.

Slika 19: Verjetnost, da osebni podatki na družbenih omrežjih postanejo javni (n=259)

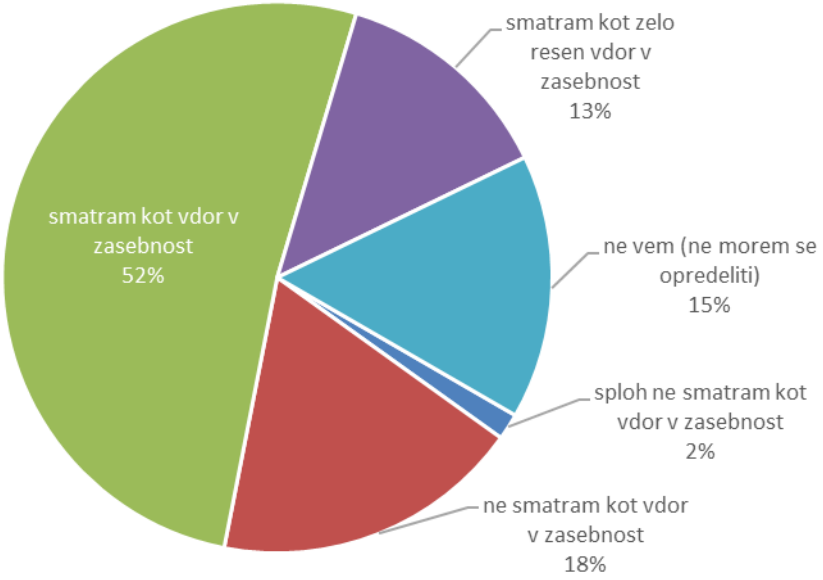


Vir: lastno delo.

V sklopu zaznavanja zasebnosti na družbenih omrežjih sem želela ugotoviti, ali uporabniki personalizirane oglase (tj. oglase, ki so prirejeni njim), ki se jim prikazujejo na teh omrežjih, smatrajo kot vdor v svojo zasebnost. Rezultati v sliki 20 kažejo na to, da personalizirane oglase kot vdor v zasebnost smatra večina uporabnikov – tako je odgovorilo 133 uporabnikov, kar predstavlja 52 %. 47 (18 %) uporabnikov prikazanih personaliziranih oglasov ne smatra kot vdor v zasebnost. 40 (15 %) uporabnikov ne ve oziroma se ne more opredeliti. Sledi jim 34 (13 %) uporabnikov, ki menijo, da je to zelo

resen vdor v zasebnost. Najmanj, to so 4 uporabniki oziroma 2 %, jih je odgovorilo, da personaliziranih oglasov ne smatrajo kot vdor v zasebnost.

Slika 20: Personalizirani oglasi kot vdor v zasebnost uporabnikov (n=259)



Vir: lastno delo.

Z zadnjim vprašanjem sem želela ugotoviti, ali so imeli anketiranci kot uporabniki na družbenih omrežjih doslej že kakšno neprijetno izkušnjo v zvezi z zasebnostjo. 242 (93 %) od 259 uporabnikov je odgovorilo, da te izkušnje niso imeli, preostalih 17 (7 %) pa je zlorabo osebnih podatkov že doživelo. Vprašanje je bilo odprtega tipa; najpogostejši med prejetimi odgovori so bili vdori v osebni profil na družbenih omrežjih Facebook in SnapChat. Uporabniki so opisali še naslednje slabe izkušnje: kraja fotografij, nedovoljena objava fotografij, grožnje ter prenos podatkov in fotografij v drugo družbeno omrežje brez njihovega soglasja.

4.4 Ugotovitve raziskave in diskusija

Družbena omrežja so priljubljena in zelo vpeta v življenje ljudi, kar je potrdila tudi raziskava, saj jih uporablja kar 96 % vseh anketirancev. Najbolj priljubljen je Facebook, ki ga uporablja 96 % uporabnikov, sledita mu Instagram (78 %) in SnapChat (67 %). Manj priljubljena omrežja med uporabniki so Pinterest (43 %), LinkedIn (25 %) in Twitter (23 %), ki jih uporablja le manjši delež uporabnikov.

Družbena omrežja predstavljajo velik izziv za ohranjanje osebnih podatkov, saj spodbujajo uporabnike k deljenju informacij o njihovem osebnem življenju. Na podlagi rezultatov raziskave sem ugotovila, da so družbena omrežja del vsakdanjika večine uporabnikov. S tem je potencialna ogroženost zasebnosti uporabnikov še večja. Iz raziskave lahko sklepam, da je zasebnost pomembna, saj je kar 83 % anketirancev odgovorilo, da jim je

zasebnost pomembna oziroma zelo pomembna. Po drugi strani pa je zaupanje uporabnikov v družbena omrežja v povezavi z zasebnostjo relativno nizko, saj jim večina uporabnikov z vidika uporabe in obdelave svojih osebnih podatkov ne zaupa. Na podlagi pridobljenih podatkov družbenim omrežjem sploh ne zaupa oziroma ne zaupa 63 % uporabnikov. Menim, da je možen razlog za to večja ozaveščenost uporabnikov o zlorabah osebnih podatkov, tudi zaradi visoke medijske pokritosti odmevnih afer v zadnjih letih.

Glede na predhodne študije, s katerimi sem primerjala ugotovitve svoje raziskave, sem želela ugotoviti, kako vpliva uporabnikova starost na njegov odnos do zasebnosti. Na tem področju so avtorji v svojih študijah prišli do zelo različnih ugotovitev. Barnesova (2006) je v svojem članku trdila, da so starejši bolj zaskrbljeni glede svoje zasebnosti, medtem ko mlajši prosto delijo svoje zasebno življenje in jih zasebnost ne skrbi. Navedla je, da je razlog v tem, da se mlajši pogosto ne zavedajo narave in razsežnosti interneta. Nekateri so v študijah ugotovili, da starost in zaskrbljenost glede zasebnosti nista povezani ter da starost ne vpliva na odnos uporabnikov do zasebnosti (Taddicken, 2014; Hoofnagle, King, Li & Turow, 2010). Blank, Bolsover in Dubois (2014) v svoji raziskavi omenjenim študijam nasprotujejo – ugotovili so namreč, da so mlajši bolj zaskrbljeni glede zasebnosti in si v primerjavi s starejšimi bolj prizadevajo, da bi jo ohranili, saj pogosteje upravljajo z nastavitvami zasebnosti. V svoji raziskavi sem ugotovila, da je mlajšim uporabnikom zasebnost pomembnejša kot starejšim uporabnikom: 86 % mlajših uporabnikov je zasebnost pomembna (pomembna ali zelo pomembna), medtem ko je zasebnost pomembna ali zelo pomembna 78 % starejših uporabnikov. Podoben rezultat sem dobila, ko sem raziskovala, ali se mlajši pogosteje poslužujejo načinov za zaščito zasebnosti, kot so nastavitve zasebnosti. Čeprav razlika pri slednjem ni tako velika, sem ugotovila, da mlajši uporabniki (21 %) pogosteje upravljajo z nastavitvami zasebnosti kot starejši (14 %). Na podlagi raziskave sklepam, da težava ni v tem, da se mlajši uporabniki ne zavedajo nevarnosti zlorab zasebnosti na družbenih omrežjih ali da jih to ne skrbi. Družbeno življenje predvsem mlajše generacije se dandanes namreč v veliki meri odvija tudi na družbenih omrežjih, le-ta pa jim ne zagotavljajo učinkovitih orodij za ustrezno upravljanje njihove zasebnosti.

Zaznano tveganje zlorab zasebnosti je pomemben dejavnik, ki vpliva na psihološko zaznavanje uporabnikov in posledično na njihovo vedenje. Z raziskavo sem ugotovila, da je zaznano tveganje možnosti zlorab zasebnosti z vidika uporabe podatkov v tržne namene visoko, saj 81 % uporabnikov meni, da je zelo verjetno oziroma verjetno, da oglaševalci uporabljajo njihove osebne podatke, 73 % uporabnikov to vedenje moti, 65 % uporabnikov pa smatra personalizirane oglase kot vdor v svojo zasebnost. Manj kot polovica (43 %) uporabnikov meni, da bodo njihovi osebni podatki postali javni, kar kaže na bistveno manjšo dejansko zaskrbljenost uporabnikov v primerjavi z njihovim zavedanjem o možnosti zlorab zasebnosti. Čeprav se uporabniki zavedajo, da je njihova zasebnost ogrožena, jih večina za varovanje zasebnosti ni pripravljena plačati (71 %). Na podlagi analize lahko sklepam, da v veliki večini niso pripravljeni plačati ali pa so pripravljeni

plačati le manjši znesek. Do podobnih ugotovitev so prišle tudi Spiekermann, Korunovska in Bauer (2012), ki so v svoji raziskavi ocenjevale pripravljenost uporabnikov družbenega omrežja Facebook, da plačajo za varstvo osebnih podatkov, in ugotovile, da jih približno polovica tega ni pripravljena storiti.

Uporabniki imajo o lastnem nadzoru nad zasebnostjo na družbenih omrežjih zelo različno mnenje: največ je neopredeljenih (35 %), 32 % jih meni, da nimajo nadzora nad zasebnostjo, 16 % pa jih meni, da nadzor imajo. Iz tega lahko sklepam, da uporabniki menijo, da imajo premajhen nadzor nad zasebnostjo, in da je njihova ozaveščenost – z vidika zavedanja, da je posameznik v primerjavi z velikimi korporacijami, ki zbirajo in uporabljajo osebne podatke, premajhen – visoka, zato je nujno potrebno, da vmes posega država in z zakonodajo vpliva na varstvo osebnih podatkov. S tem se strinja tudi večina uporabnikov, saj jih 79 % meni, da je pomembno oziroma zelo pomembno, da država z zakoni uravnava področje zasebnosti na družbenih omrežjih.

Za zagotovitev zasebnosti lahko uporabniki z ozaveščenostjo o zlorabah največ storijo sami, in sicer tako, da ne razkrivajo preveč podatkov. Na podlagi raziskave lahko povzamem, da je stopnja razkrivanja osebnih podatkov velika, kljub zavedanju, da družbena omrežja ne varujejo uporabnikove zasebnosti, saj zbirajo in posredujejo podatke v tržne namene. Vendar uporabnikov to ne odvrača od objavljanja (razkrivanja) zasebnosti. Vsi (100 %) uporabniki, ki so sodelovali v raziskavi, navajajo, da imajo na družbenih omrežjih profil, ki vsebuje ime in priimek, večina (96 %) jih ima na družbenih omrežjih tudi datum rojstva. Poleg tega je iz rezultatov vidno, da se veliko uporabnikov poslužuje dejavnosti, pri katerih razkrivajo svojo zasebnost z objavo fotografij (91 %) in videoposnetkov (49 %), z objavo trenutne lokacije (59 %), s komentiranjem (91%), všečkanjem (97 %) in vsebinskimi objavami (68 %), čeprav so rezultati glede pogostosti teh objav zelo različni. Ugotovila sem, da tudi tisti, ki sicer dajejo zasebnosti velik pomen, o sebi še vedno razkrivajo veliko, saj jih 96 % všečka, 92 % jih objavlja svoje fotografije, 90 % jih komentira, 66 % objavlja vsebino, 57 % jih objavlja svojo trenutno lokacijo, najmanj pa jih objavlja svoje videoposnetke (49 %).

Nenazadnje sem skušala iz raziskave ugotoviti, ali paradoks zasebnosti drži ali ne. Na podlagi vseh ugotovitev lahko povzamem, da danes izjemno veliko ljudi uporablja družbena omrežja, zasebnost jim je pomembna, prav tako se zavedajo potencialnih zlorab zasebnosti in pomena državne regulative na tem področju. Večina uporabnikov pa z vedenjem na družbenih omrežjih še vedno razkriva veliko osebnih podatkov. Tukaj pride do neskladja, kar pomeni, da je prisoten fenomen paradoksa zasebnosti. Zaskrbljenost glede zasebnosti na družbenih omrežjih se ne odraža v ustreznem vedenju, kot je razkrivanje manj informacij na teh omrežjih.

4.5 Predlogi za izboljšave zasebnosti na družbenih omrežjih

Zasebnost in varovanje osebnih podatkov na internetu ter posledično na družbenih omrežjih je v današnjem času pogosto obravnavana tema, ki je zaradi različnih dejavnikov in nasprotujočih si interesov zelo kompleksna. V smeri varovanja zasebnosti se dogajajo premiki tako na področju zakonodaje kot tudi na področju ozaveščanja uporabnikov. Na podlagi raziskave predlagam naslednje ukrepe, ki bi lahko pripomogli k še učinkovitejšemu zaznavanju in varovanju zasebnosti uporabnikov na družbenih omrežjih.

4.5.1 Predlogi za zakonodajalca

Država mora z zakonodajo zagotoviti interes prostega pretoka podatkov in informacij na eni strani ter zasebnost uporabnikov na drugi strani. V ta namen je stopila v veljavo Splošna uredba, ki si z zagroženimi visokimi globami prizadeva za izpolnjevanje pogojev te uredbe. Glede na to, da so upravljavci družbenih omrežij velike korporacije z ogromnim dobičkom, menim, da ta politika ni zadostna, saj si večina teh podjetij plačilo glob lahko brez težav privošči. Država bi morala vključiti tudi zakonsko odgovornost, in sicer zagrožene zaporne kazni za odgovorne osebe v primeru kršitev zasebnosti uporabnikov na družbenih omrežjih, saj bi to skupaj z zagroženimi visokimi globami imelo še večji učinek zastraševanja in bi tako lahko vplivalo na zmanjšanje zlorab osebnih podatkov.

Zelo pomembno se mi zdi tudi ozaveščanje uporabnikov, saj sta prav zavedanje in znanje tisto, kar vpliva na preudarnost in kritičnost pri uporabi družbenih omrežij. Za ozaveščanje bi si morala prizadevati predvsem država, ki bi z ustreznimi programi lahko že v šolah mlade uporabnike ozaveščala o značilnostih interneta in tveganjih, ki jih prinašata uporaba in razkrivanje osebnih podatkov. Na ta način bi se povečala spletna pismenost mladih generacij. Ozaveščanje bi se lahko izvajalo tudi z oglaševanjem v širših medijih (npr. na televiziji, radiu in internetu), kar bi potencialno doseglo širše občinstvo.

4.5.2 Predlogi za uporabnike

Uporabniki bi morali biti zelo kritični do družbenih omrežij in do načinov, kako ta omrežja zbirajo njihove osebne podatke, informacije o zbiranju in uporabi pa pred njimi skrivajo. Ugotoviti bi morali, v katerih okoliščinah bi lahko sami določili, kaj se jim bo prikazovalo na zaslonih. V zvezi s tem bi uporabnikom predlagala, da začnejo v večjem obsegu uporabljati določena orodja, ki omogočajo večji nadzor nad zasebnostjo. V zadnjem času se ogromno sredstev vlaga v orodja za preprečevanje prikazovanja oglasov (AdBlocker-ji). Takšno orodje učinkovito preprečuje sledenje uporabnikov in posledično povečuje zasebnost na družbenih platformah.

Z uporabo orodja, ki omogoča enostaven in hiter vpogled v politike zasebnosti in pogoje uporabe, uporabnikom določenega spletnega mesta teh dokumentov ne bi bilo treba v

celoti prebrati, temveč bi lahko na hitro preleteli posamezne sporne segmente. Na tem področju sta se oblikovali dve iniciativi, ki pripravljata strnjene povzetke politik zasebnosti in pogojev uporabe; na eni strani so tako poskusi uporabe umetne inteligence (https://futurism.com/ai-reads-your-privacy-policies, https://pribot.org/), na drugi pa so se oblikovale skupnosti (https://tosdr.org/), ki ocenjujejo vsebino teh dokumentov. Uporabnikom so te ocene na voljo tam, kjer jih potrebujejo – na spletnem mestu, ki ga obiščejo.

SKLEP

Z globalizacijo in hitrim razvojem informacijsko-komunikacijskih tehnologij zasebnost in varovanje osebnih podatkov pridobivata na pomenu. Osebni podatki uporabnikov predstavljajo za družbena omrežja veliko vrednost, zato se grožnje zasebnosti z razvojem družbenih omrežij in njihovo množično uporabo povečujejo. Problem oz. izziv torej predstavljajo prakse družbenih omrežij, ki zbirajo, analizirajo, razkrivajo in uporabljajo osebne podatke uporabnikov ter jih posredujejo tretjim osebam, pogosto brez njihove vednosti in privolitve. Uporabniki se tako soočajo z novimi izzivi na področju zasebnosti, saj morajo uravnotežiti kompromis med razkritjem in zadrževanjem osebnih podatkov. Najboljša zaščita je ozaveščenost uporabnikov in njihova lastna, kritična presoja glede razkrivanja osebnih podatkov. Pomembna pa je tudi vključenost države, ki lahko zakonodajno regulira področje varovanja osebnih podatkov in tako do določene stopnje zavaruje uporabnike pred posegom v njihovo zasebnost. Kljub vsemu pa sedanja ureditev še zdaleč ni dovolj učinkovita.

V magistrskem delu sem proučevala odnos uporabnikov do zasebnosti in varovanja osebnih podatkov na družbenih omrežjih ter ugotavljala, kako uporabniki zaznavajo zasebnost in ali je njihovo vedenje skladno z zaznavanjem. Svoje ugotovitve sem nato primerjala z nekaterimi že obstoječimi študijami. Na podlagi proučevanja tematike in lastne raziskave sem ugotovila, da se uporabniki sicer zavedajo pomena zasebnosti in morebitnih zlorab njihovih osebnih podatkov, ki so lahko posledica uporabe družbenih omrežij, vendar obenem želijo tudi večjo vključenost državnih oblasti, ki lahko z zakoni regulirajo področje zasebnosti – posameznik kot fizični subjekt ima namreč v primerjavi s pravnimi subjekti, ki imajo v lasti družbena omrežja in jih upravljajo, premajhen vpliv, da bi lahko sam zaščitil svojo zasebnost. Kljub zavedanju, kaj se z njihovimi osebnimi podatki dogaja, in dejstvu, da večina uporabnikov družbenim omrežjem ne zaupa, pa večinoma za zaščito zasebnosti niso pripravljeni plačati. Z raziskavo sem potrdila, da paradoks zasebnosti drži: vedenje uporabnikov na družbenih omrežjih ne potrjuje njihove zaskrbljenosti glede zasebnosti, saj večina uporabnikov še vedno razkriva ogromno osebnih podatkov.

Družbena omrežja so sodoben način digitalne komunikacije in dinamično okolje, ki se hitro razvija in spreminja. Številne zlorabe v zadnjem času kažejo, da je na področju

zasebnosti potreben boljši nadzor in pravočasno ukrepanje vseh udeležencev. Razvoj družbenih omrežij ter način in obseg varovanja zasebnosti bo nedvomno aktualno področje, ki ga bo zanimivo spremljati tudi v prihodnje.

LITERATURA IN VIRI

1. Acquisti, A. & Gross, R. (2006). Imagined Communities: Awareness, information sharing, and privacy on the Facebook. V G. Danezis & P. Golle, *Privacy Enhancing Technologies* (str. 36–58). Cambridge, UK.
2. Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. *American Association for the Advancement of Science, 347*(6221), 509–514.
3. Angwin, J., Mattu, S. & Parris Jr., T. (2016, 28. september*). Breaking the black box: What Facebook Knows About You.* Pridobljeno 5. avgusta 2019 iz https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you
4. Averill, J. R. (1973). Personal control over aversive stimuli and its relationship to stress. *Psychological Bulletin, 80*(4), 286–303.
5. Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).
6. Baronas, A.-M. K. & Louis, M. R. (1988). Restoring a Sense of Control during Implementation: How User Involvement Leads to System Acceptance. *MIS Quarterly, 12*(1), 111–124.
7. Barth, S. & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058.
8. Bechmann, A. (2014). Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies, 11*(1), 21–38.
9. Bélanger, F. & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017–1041.
10. Bélanger, F., Hiller, J. & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems, 11*(3-4), 245–270.
11. Benson, V., Saridakis, G. & Tennakoon, H. (2015). "Information disclosure of social media users: Does control over personal information, user awareness and security notices matter?". *Information Technology & People, 28*(3), 426–441.
12. Blank, G., Bolsover, G. & Dubois, E. (2014, 15. avgust). *A New Privacy Paradox: Young people and privacy on social network sites.* Pridobljeno 20. januara 2019 iz http://dx.doi.org/10.2139/ssrn.2479938
13. Bloustein, E. (1964). *Privacy as an aspect of human dignity: an answer to Dean Prosser.* New York: New York University, School of Law.

14. Boyd, D. & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8).
15. Buglass, S. L., Binder, J. F., Betts, L. R. & Underwood, J. D. M. (2016). When »friends« collide: Social heterogeneity and user vulnerability on social network sites. *Computers in Human Behavior, 54*, 62–72.
16. Chander, A., Gelman, L. & Radin, M. J. (2008). *Securing Privacy in the Internet Age.* Stanford: Stanford Univerity Press.
17. Christl, W. & Spiekermann, S. (2016). *Networks of Control. A report on Corporate Surveillance, Digital Tracking, Big Data &Privacy*. Dunaj: Facultas.
18. Christl, W. (2017). *Corporate surveillance in everyday life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions.* Dunaj: Cracked Lab – Institute for Critical Digital Culture. A Report by Cracked Labs.
19. Clarke, R. (1999). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.* Pridobljeno 23. marca 2019 iz http://www.rogerclarke.com/DV/Intro.html
20. Debatin, B., Lovejoy, J. P., Horn, A.-K. & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108.
21. Evropska komisija. (2009, 31. marec). *Meglena Kuneva - European Consumer Commissioner - Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling.* Pridobljeno 10. junija 2019 iz https://europa.eu/rapid/press-release_SPEECH-09-156_en.htm
22. Evropska komisija. (brez datuma). Kaj so osebni podatki? Pridobljeno 23. marca 2019 iz https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_sl
23. Forbes Media LLC. (2019). *The World's Most Valuable Brands*. Pridobljeno 9. avgusta 2019 iz https://www.forbes.com/powerful-brands/list/#tab:rank
24. Gerlach, J., Widjaja, T. & Buxmann, P. (2015). Handle with care: how online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems, 24*(1), 33–43.
25. Ghazinour, K. & Ponchak, J. (2017). Hidden privacy risks in sharing picture on social media. *Procedia Computer Science, 113*, 267–272.
26. Ginosar, A. & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management, 54*(7), 948–957.
27. Gross, R. & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). V *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (str. 71–80). Alexandria, VA, USA: ACM.
28. Hajli, N. & Lin, X. (2014). Exploring the security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics, 133*(1), 111–123.
29. Hargittai, E. & Marwick, A. (2016). »What can I really do?«: Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication, 10*(21), 3737–3757.

30. Hasan, O., Habegger, B., Brunie, L., Bennani N. & Damiani, E. (2013). A discusion of privacy challenges in user profiling with big data techniques: The EEXCESS use case. *2013 IEEE International Congress on Big Data*, (str. 25–30). Santa Clara, CA: IEEE.
31. He, Z., Cai, Z & Yu, J. (2018). Latent-Data Privacy Preserving With Customized Data Utility for Social Network Data. *IEEE Transactions on Vehicular Technology, 67*(1), 665–673
32. Hirsch, D. (2011). The law and policy of online privacy: regulation, self-regulation or co-regulation? *Seattle University Law Review, 34*(2), 439–480.
33. Hoofnagle, C. J., King, J., Li, S. & Turow, J. (2010, 14. april). *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes & Policies?* Pridobljeno iz http://repository.upenn.edu/asc_papers/399
34. Hull, G. (2015). Successful failure: What Foucalt can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology, 17*(2), 89–101.
35. Informacijski pooblaščenec (2017, 25. maj). *Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov?* Pridobljeno 24. maja 2019 iz https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/uporabna-gradiva/
36. Joinson, A. N., Reips, U.-D., Buchanan, T. & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction, 25*(1), 1–24.
37. Kosinski, M., Stillwell, D. & Graepel, T. (2013). Private traits and attributes are predictable from digital record of human behavior. *National Academy of Sciences, 110*(15), 5802–5805.
38. Kotsios, A., Magnani, M., Rossi L., Shklovski, I. & Vega, D. (2019, 7. marec). *An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research*. Pridobljeno iz https://www.researchgate.net/publication/331645097
39. Kovačič, M. (2000). Zasebnost v informacijski družbi (izvirni znanstveni članek). *Teorija in praksa, 37*(6), 1019–1034.
40. Leibowitz, J. (2007, 1. november). *So private, so public: Individuals, the internet & the paradox of behavioral marketing.* Pridobljeno iz https://www.ftc.gov/public-statements/2007/11/so-private-so-public-individuals-internet-paradox-behavioral-marketing
41. Luzak, J. A. (2014). Privacy Notice for Dummies? Towards European Guidelines on How to Give »Clear and Comprehensive Information« on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy. *Journal of Consumer Policy, 37*(4), 547–559.
42. Malgieri, G. & Custers, B. (2018). Pricing privacy - The Right to Know the Value of Your Personal Data. *Computer Law & Security Review, 34*(2), 289–303.
43. Marwick, A. E. & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New media & society 2014, 16*(7), 1051–1067.

44. McDonald, A. M. & Cranor, L. F. (2008). The cost of reading privacy policies. *A Journal of Law and Policy for the Information Society, 4*(3), 540–565.
45. Millard, C. (2014). Data Privacy in the Cloud. V Graham, M. & Dutton, W. H. (2014). *Society and the Internet: How Networks of Information and Communication are Changing Our Lives* (str. 333–347). Oxford Scholarship Online.
46. Miltgen, C. L. & Smith, H. J. (2015*).* Exploring information privacy regulation, risks, trust and behavior. *Information & Management, 52*(6), 741–759.
47. Mollick, J. S. & Mykytyn, P.P. (2009). An Empirical Investigation on the Effects of Privacy Policies on Perceived Fairness of Online Vendor. *Journal of Internet Commerce, 8*(1-2), 88–112.
48. Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The journal of consumer affairs, 41*(1), 100-126.
49. Obar, J. A. & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 2018.* Pridobljeno iz https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465
50. Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A. & Karvonen, K. (2014). Transparency of intentions decreases privacy concerns in ubiquitous surveillance. *CyberPsychology, Behavior, and Social Networking, 17*(10), 633–638.
51. Peras, D., Mekovec, R. & Picek, R. (2018). Influence of GDPR on social networks used by omnichannel contact center. *41st International Convention on Information and Communication Technology, Electronics and Microelectronics,* (str.1132–1137). Opatija: MIPRO.
52. Pirc Musar, N. & Burnik, J. (2011, 29. januar). *Nevarnosti elektronskih sledi: Ko pride do zlorabe, bo že prepozno.* Pridobljeno iz https://www.dnevnik.si/1042420653
53. Privacy Rights Clearinghouse. (2010). *Social Networking Privacy: How to be Safe, Secure and Social.* Pridobljeno 9. avgusta 2019 iz https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social
54. Raab, C. & Goold, B. (2011). *Protecting information privacy*. Equality and Human Rights Commission Research report 69. Manchester: Univerity of Edinburgh and University of British Columbia.
55. Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S. & Norton, T. B. (2014). *Privacy Harms and the Effectiveness of the Notice and Choice Framework.* 2014 TPRC Conference Paper; Fordham Law Legal Studies Research Paper No. 2418247. Pridobljeno iz http://dx.doi.org/10.2139/ssrn.2418247
56. Shore J. & Steinman J. (2015, 11. avgust). *Did You Really Agree to That? The Evolution of Facebook's Privacy Policy*. Pridobljeno iz http://techscience.org/a/2015081102
57. Skinner, E. A. (1996). A guide to constructs of control. *Journal of Personality and Social Psychology, 71*(3), 549–570.

58. Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20*(2), 167–196.
59. Smith, R. E. (2004). *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet.* Providence RI USA: Privacy Journal.
60. Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161–167.
61. Spiekermann, S., Korunovska, J. & Bauer, C. (2012). *Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy.* Pridobljeno iz http://dx.doi.org/10.2139/ssrn.2148886
62. Statista GmbH. (2019). *Most popular social networks worldwide as of October 2019, ranked by number of active users (in millions).* Pridobljeno 20. maja 2019 iz https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
63. Stone, E.F., Gardner, D. G., Gueutal, H.G. & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology, 68*(3), 459–468.
64. Strauss, J. & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics, 19*(2), 173–192.
65. Taddicken, M. (2014). The »Privacy Paradox« in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248–273.
66. Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Tecnology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing, 3*, 1096–1100.
67. Trottier, D. (2012). *Social Media as Surveillance: Rethinking Visibility in a Converging World.* New York, USA: Routledge.
68. Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36.
69. Turban, E., Outland, J., King, D., Lee, J. K., Liang T. P, Turban, D. C. (2018). *Electronic Commerce 2018: A Managerial and Social Networks Perspective*. 8th edition. Springer Texts in Business and Economics.
70. van Ooijen, I. & Vrabec, H. U. (2018*).* Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy, Springer US, 42*(1), 91–107.
71. Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338–346.
72. World Legal Information Institute. (2006). *Privacy and Human Rights Report*. Pridobljeno 13. marca 2019 iz http://www.worldlii.org/int/journals/EPICPrivHR/2006/
73. Young, A. L. & Quan-Hasse, A. (2009). *Information revelation and internet privacy concerns on social network sites: A case study of Facebook. C&T '09 Proceedings of the fourth international conference on Communities and technologies*, str. 265–274.

74. Zomorodi, M. (2019, 26. avgust). IRL - Online Life Is Real Life. Pridobljeno iz https://irlpodcast.org/season5/episode6/
75. Zvezna komisija za trgovino (Federal Trade Commission). (1998). *Privacy Online: A report to Congress. Pridobljeno iz* https://www.ftc.gov/reports/privacy-online-report-congress

PRILOGE

Priloga 1: Anketni vprašalnik

1. Ali uporabljate družbena omrežja?

◌ da
◌ ne

2. Katera družbena omrežja uporabljate in kako pogosto?

	nikoli oz. ne uporabljam	vsaj 1x dnevno	vsaj 1x tedensko	vsaj 1x mesečno	nekajkrat letno
Facebook	◌	◌	◌	◌	◌
Instagram	◌	◌	◌	◌	◌
Twitter	◌	◌	◌	◌	◌
SnapChat	◌	◌	◌	◌	◌
LinkedIn	◌	◌	◌	◌	◌
Pinterest	◌	◌	◌	◌	◌
Drugo:	◌	◌	◌	◌	◌

3. Katere od spodaj navedenih podatkov imate objavljene na družbenih omrežjih?
Možnih je več odgovorov

☐ ime in priimek
☐ naslov oz. mesto kjer živite
☐ datum rojstva
☐ telefonska številka
☐ verska pripadnost
☐ partnerski status
☐ interesi
☐ hobiji
☐ nič od zgoraj naštetega

4. Kaj od spodaj naštetega smatrate za osebni podatek?
Možnih je več odgovorov

☐ vaša barva las
☐ vaši všečki na socialnem omrežju
☐ naslov IP računalnika v kavarni
☐ vaša mobilna telefonska številka
☐ vaši podatki o nakupih, preferencah
☐ naslov IP vaše mobilne naprave
☐ vaša trenutna lokacija

5. Kako pomembna se vam zdi zasebnost na družbenih omrežjih?

◌ zelo nepomembna
◌ nepomembna
◌ niti pomembna, niti nepomembna
◌ pomembna
◌ zelo pomembna

6. Kako močno se strinjate z izjavo: »Zasebnost na spletu me ne skrbi, saj nimam kaj skrivati?«

- ◯ sploh se ne strinjam
- ◯ se ne strinjam
- ◯ niti se strinjam, niti se ne strinjam
- ◯ se strinjam
- ◯ povsem se strinjam

7. Kaj in kako pogosto objavljate na družbenih omrežjih?

	nikoli	vsaj 1x dnevno	vsaj 1x tedensko	vsaj 1x mesečno	nekajkrat letno
fotografije, na katerih ste vi	◯	◯	◯	◯	◯
video posnetke, na katerih ste vi	◯	◯	◯	◯	◯
lokacijo, na kateri se nahajate	◯	◯	◯	◯	◯
komentarje	◯	◯	◯	◯	◯
všečkanje	◯	◯	◯	◯	◯
vsebinske objave	◯	◯	◯	◯	◯

8. Katere osebe sprejmete za prijatelje na družbenih omrežjih?
Možnih je več odgovorov

- ☐ osebe, ki jih dobro poznam
- ☐ osebe, ki jih poznam samo »na videz«
- ☐ prijatelje od mojih prijateljev
- ☐ osebe, ki jih sploh ne poznam

9. Kako pogosto uporabljate nastavitve zasebnosti na družbenih omrežjih?

- ◯ nisem še nikoli
- ◯ nastavil sem jih pred začetkom uporabe družbenega omrežja
- ◯ redko (vsake toliko časa)
- ◯ pogosto (npr. ob vsaki objavi)

10. Kako pomembno se vam zdi, da zakoni uravnavajo področje zasebnosti na družbenih omrežjih?

- ◯ zelo nepomembno
- ◯ nepomembno
- ◯ niti pomembno, niti nepomembno
- ◯ pomembno
- ◯ zelo pomembno

11. Koliko se vam zdi verjetno, da oglaševalci uporabljajo vaše osebne podatke v tržne namene?

- ◯ zelo malo verjetno
- ◯ malo verjetno
- ◯ niti verjetno, niti malo verjetno

◌ verjetno
◌ zelo verjetno

12. Koliko vas moti, da oglaševalci uporabljajo vašo zasebnost za svoj dobiček?

◌ sploh me ne moti
◌ me ne moti
◌ niti me moti, niti me ne moti
◌ me moti
◌ zelo me moti

13. Koliko bi bili pripravljeni plačati, da družbena omrežja ne bi uporabljala vaših osebnih podatkov v tržne namene (prikaz personaliziranih oglasov)?

◌ nisem pripravljen
◌ do 5 € na mesec
◌ do 10 € na mesec
◌ do 50 € na mesec
◌ do 100 € na mesec

14. Koliko zaupate družbenim omrežjem, da ne dajejo v obdelavo vaših osebnih podatkov tretjim osebam npr. oglaševalcem?

◌ sploh ne zaupam
◌ ne zaupam
◌ niti zaupam, niti ne zaupam
◌ zaupam
◌ zelo zaupam

15. Ali se strinjate, da imate nadzor nad zasebnostjo na družbenih omrežjih?

◌ sploh se ne strinjam
◌ se ne strinjam
◌ niti se strinjam, niti se ne strinam
◌ se strinjam
◌ povsem se strinjam

16. Koliko se vam zdi verjetno, da bodo vaši osebni podatki na družbenih omrežjih postali javni (npr. zaradi t.i. data breach oz. hekerjev)?

◌ zelo malo verjetno
◌ malo verjetno
◌ niti verjetno, niti malo verjetno
◌ verjetno
◌ zelo verjetno

17. Ali smatrate, da so personalizirani oglasi (oglasi, ki so prirejeni vam), ki se vam prikazujejo na družbenih omrežjih, vdor v vašo zasebnost?

◌ sploh ne smatram kot vdor v zasebnost

◌ ne smatram kot vdor v zasebnost
◌ smatram kot vdor v zasebnost
◌ smatram kot zelo resen vdor v zasebnost
◌ ne vem (ne morem se opredeliti)

18. Ali ste imeli kakšno nenavadno (neprijetno) izkušnjo glede zasebnosti na družbenih omrežjih?

◌ ne
◌ da; prosim opišite:

19. Spol:

◌ moški
◌ ženski

20. V katero starostno skupino spadate?

◌ do 18 let
◌ 18 - 25 let
◌ 26 - 40 let
◌ 41 - 60 let
◌ 61 let ali več

21. Vpisna številka:
(izpolnijo študenti 1. letnika dodiplomskega študija EF)