

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
AKADEMIJA ZA UMJETNOST I KULTURU
ODSJEK ZA KULTURU, MEDIJE I MENADŽMENT
SVEUČILIŠNI PREDDIPLOMSKI STUDIJ KULTURA, MEDIJI I
MENADŽMENT

IVAN MARTINOVIĆ

**ZLOUPORABA PODATAKA KORISNIKA
DRUŠTVENIH MREŽA U POLITIČKE SVRHE**

ZAVRŠNI RAD

MENTOR: izv. prof. dr. sc. Nives Tomašević
SUMENTOR: Tomislav Levak, predavač

Osijek, 2022

SAŽETAK

Ovaj se rad bavi sve prisutnijim i raširenijim problemima kršenja privatnosti i zlouporabe osobnih podataka korisnika društvenih mreža, s fokusom na njihovu pojavu na području politike. U radu se proučavaju načini korištenja osobnih podataka korisnika društvenih mreža te ukratko iznosi tko sve ima pristup tim podacima. U tu svrhu objašnjeni su i pojmovi zaštite privatnosti, odnosno zaštite osobnih podataka u državama članicama Europske unije i u Sjedinjenim Američkim Državama. U radu se također razmatra zašto je potrebno kritički analizirati praktički sve informacije koje dosežu do brojnih korisnika društvenih mreža, zašto dezinformacije i lažne vijesti ponajviše kolaju upravo društvenim mrežama i kako mogu biti upotrijebljene kao opasno političko oružje.

Kao središnji primjer za istraživanje tematike ovoga rada obrađen je poznati slučaj Cambridge Analytica, odnosno umiješanost te britanske analitičke tvrtke u dvama globalno važnim političkim događajima 2016. godine: predsjedničkim izborima u SAD-u i referendumu za izlazak Velike Britanije iz Europske unije, tzv. Brexit. Objasnjeno je da je spomenuta tvrtka, kršeći Facebookove uvjete pružanja usluga, prikupila osobne podatke mnogih korisnika Facebooka te da su ciljanom komunikacijom i posebnom oglasnom metodom manipulirani birači u navedenim zemljama. Kroz ovaj slučaj prikazano je ujedno i kako se takvim i sličnim potezima može utjecati na ishode određenih političkih događaja i ugroziti demokratske sustave pojedinih država.

Ključne riječi: Cambridge Analytica, društvene mreže, korisnici, osobni podatci, politika, zaštita privatnosti, zlouporaba

ABSTRACT

This paper deals with the increasingly present and widespread problems of privacy violations and misuse of personal data of social network users, with a focus on their appearance in the field of politics. The paper studies the ways of using personal data of social network users and briefly explains who has access to this data. For this purpose, the concepts of privacy protection, i.e. protection of personal data in the member states of the European Union and in the United States of America are also explained. The paper also examines why it is necessary to critically analyze practically all information that reaches numerous users of social networks, why disinformation and fake news mostly circulate on social networks and how they can be used as a dangerous political weapon.

The well-known Cambridge Analytica case, i.e. the involvement of that British analytical company in two globally important political events in 2016: the presidential elections in the USA and the referendum for Great Britain's exit from the European Union, or "Brexit", was used as the main case study for this work's research. It is explained how the mentioned company, in violation of Facebook's terms of service, collected the personal data of many Facebook users and how voters in the mentioned countries were manipulated with targeted communication and a special advertising method. Through this case, it is also shown how such and similar moves can influence the outcomes of certain political events and threaten the democratic systems of individual countries.

Keywords: Cambridge Analytica, misuse, personal data, politics, privacy protection, social networks, users

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

AKADEMIJA ZA UMJETNOST I KULTURU U OSIJEKU

IZJAVA O AKADEMSKOJ ČESTITOSTI

kojom ja, Ivan Martinović potvrđujem da je moj završni rad pod naslovom *Zlouporaba podataka korisnika društvenih mreža u političke svrhe* te mentorstvom izv. prof. dr. sc. Nives Tomašević i sumentorstvom Tomislava Levaka, predavača, rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima i oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio diplomskog rada nije napisan na nedopušten način, odnosno da nije prepisan iz necitiranog rada, pa tako ne krši ničija autorska prava. Također izjavljujem da nijedan dio ovoga završnog/diplomskog rada nije iskorišten za bilo koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanove.

U Osijeku, 19. rujna 2022. godine

Potpis _____

SADRŽAJ

1. UVOD	1
2. OSOBNI PODATCI	3
2.1. Osobni podatci na društvenim mrežama	4
2.2. Zaštita privatnosti	6
2.2.1. Zaštita privatnosti u Europskoj uniji	6
2.2.2. Zaštita privatnosti u Sjedinjenim Američkim Državama	8
3. ŠIRENJE INFORMACIJA POSREDSTVOM DRUŠTVENIH MREŽA	9
3.1. Lažne vijesti	10
3.1.1. Lažne vijesti kao političko oružje	12
4. SLUČAJ CAMBRIDGE ANALYTICA	14
4.1. Britanska analitička tvrtka Cambridge Analytica	16
4.2. Američki predsjednički izbori 2016. godine	21
4.3. Referendum za izlazak Velike Britanije iz Europske unije - Brexit	23
5. ZAKLJUČAK	25
6. LITERATURA	27
7. PRILOZI	33

1. UVOD

„Ako izgovorite dovoljno veliku laž i stalno je ponavljate, ljudi će na kraju povjerovati u nju“, citat je koji je pokretačka misao u ovome radu. Citat je to koji se pripisuje ministru propagande njemačkog Trećeg Reicha, Josephu Goebbelsu, čovjeku koji je zajedno s Hitlerom stvorio jedan od najefikasnijih, ali i najokrutnijih propagandnih sustava 20. stoljeća. Neupitno je da su djela ovog dvojca nehumana i zločinačka te ih je potrebno najstrože osuditi, ali je zanimljivo proučavati tehnike pomno osmišljene propagande kojom su uspjeli stvoriti režim koji je okupio i ujedinio milijune ljudi. Uspjeli su to uvelike zahvaljujući medijima, prijenosnicima tih izmišljenih, senzacionalističkih ili lažnih informacija. Mediji poput radija, TV-a, novina i najmoćnijeg medija toga vremena, filma, uspjeli su dočarati ljudima lažnu iluziju. Okupili su i ujedinili ljude koji su povjerovali lažnoj superiornosti, iskrivljenim činjenicama i izvrtanju istine. Pokazalo se da će čovjek prije povjerovati i prihvatiti spektakularnu laž, nego jednostavnu istinu. Iako ovaj uvod navodi na razmišljanje o nacističkoj propagandi, ovaj se rad ne bavi izravno tom temom. Ovaj se rad bavi mnogo novijom temom, koja, zabrinjavajuće, ima slične odlike Goebbelsovoj propagandi. Citat s početka uvoda govori da neka laž izrečena dovoljno puta, postaje istina, a povezujući citat i tematiku ovoga rada, naglasak se ne stavlja primarno na „laž“ ili „istinu“ neke informacije, nego na „dovoljno puta“. Koliko je važno neku informaciju, bila ona istinita ili lažna, izreći dovoljno puta, pravim metodama, putem kojih medija te na koji način?

Društvene se mreže razvijaju svakoga dana i korisnicima je prilično teško popratiti svaku izmjenu koju neka mreža uvede. Od nekadašnjih platformi na kojima su korisnici provodili slobodno vrijeme radi zabave ili međusobnog umrežavanja, društvene su mreže dobrim dijelom postale „tržnica s prodajom informacija“. U trenutku kada su društvene mreže razvile mogućnosti tzv. targetiranog oglašavanja, brojne neprovjerene informacije, odnosno dezinformacije, postale su jako prisutne u svakodnevnom životu. Tako su društvene mreže, osim prostora za zabavu i međusobno povezivanje korisnika, postale i opasno mjesto za političko manipuliranje javnim mnijenjem, na što upozorava i izvješće s Oxford Internet Institute (The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, 2019).

Prema Howard i Bradshaw (2019), izvješće s Oxford Internet Institute pokazalo je da je tijekom 2018. i 2019. godine 70 zemalja koristilo računalnu propagandu za manipulaciju

svojih građana. Prema navedenom izvješću, u 45 demokratskih zemalja, političari i političke stranke koristile su računalne propagandne alate skupljajući lažne sljedbenike ili šireći izmanipulirane medijske poruke da bi pridobili podršku birača, a u 26 autoritarnih država vladini subjekti koristili su se računalnom propagandom kao alatom za kontrolu informacija za suzbijanje javnog mnijenja i slobode tiska, diskreditiranje kritike i oporbenih glasova te gušenje političkog neslaganja.

Ovaj se rad bavi prikazom zlorabe osobnih podataka korisnika interneta i društvenih mreža, a glavni je cilj prikazati kako se to čini, u prvom redu, u političke svrhe. Koristeći primarno primjer poznatoga slučaja Cambridge Analytica, odnosno umiješanosti te britanske analitičke tvrtke u dvama globalno važnim političkim događajima 2016. godine (predsjedničke izbore u SAD-u i referendum za izlazak Velike Britanije iz Europske unije, tzv. Brexit), prikazuje se kako se zlorabljaju osobni podaci korisnika društvenih mreža te kako se na taj način može utjecati na ishode određenih političkih događaja i ugroziti demokratske sustave pojedinih zemalja.

Pri izradi ovoga rada upotrebljavani su ponajprije sekundarni izvori podataka i rezultati prethodnih istraživanja. S obzirom da se radi o još uvijek relativno novoj i aktualnoj temi, većinu literature čine inozemni znanstveni i stručni članci te izvori u stranim medijima koji obuhvaćaju potrebne informacije vezane uz osobne podatke, zaštitu privatnosti, društvene mreže, dezinformacije i lažne vijesti, Cambridge Analytica, predsjedničke izbore u SAD-u i Brexit.

2. OSOBNI PODATCI

Osobni podatci dio su čovjekova identiteta. To su informacije koje opisuju lik osobe u društvu. Prema Europskoj komisiji (2018), osobni su podatci svaka informacija koja se odnosi na identificiranu ili prepoznatljivu živuću osobu, a primjeri osobnih podataka mogu biti: ime i prezime, kućna adresa, adresa e-pošte formata ime.prezime@tvrtka.com, broj osobne iskaznice, podatci o lokaciji (na primjer funkcija podataka o lokaciji na mobilnom telefonu), IP (internetski protokol) adresa, ID kolačića (*cookie*), oglasni identifikator na mobilnom uređaju, podatci koje imaju bolnice ili liječnici, a koji bi mogli jedinstveno identificirati osobu. Iz ovoga popisa koji objašnjava što su sve osobni podatci, vidljivo je da osobni podatci mogu biti izravno povezani s osobom, kao na primjer; ime i prezime ili adresa u kojoj osoba prebiva. Može se reći da je čovjek naučen da takve informacije o sebi ne otkriva pred nepoznatim ljudima te uvijek bude oprezan tijekom iznošenja tih istih podataka u javnosti jer postoji mogućnost krađe identiteta. No, postoje i oni osobni podatci na koje osoba ne može utjecati u zadržavanju anonimnosti ili ne obraća pozornost na njih jer su s osobom povezani na neizravan način, a Rodgers (2020) objašnjava da se takvi podatci i dalje smatraju osobnim podacima, čak i ako su šifrirani ili maskirani na takav način da nisu izravno povezani s korisnikom, ali se ipak mogu koristiti za ponovnu identifikaciju osobe te navodi da to mogu biti „ID oznake za praćenje u pregledniku, korisnikova IP adresa ili podatci o ponašanju korisnika na web-mjestu, uključujući korisnikov popis postova koje je označio sa „sviđa mi se“ ili korisnikov popis prijatelja“ (Rodgers, 2020: 2).

Problem je što osobe nisu svjesne da iako fizički nisu ostavile trag o sebi ili se izravno predstavile u javnosti, njihovi su osobni podatci vidljivi i zabilježeni svakim njihovim klikom na internetu. Čak i u slučaju da osoba nije korisnik društvenih mreža, svaka aplikacija na njihovom računalnom i mobilnom uređaju koja zahtijeva korištenje interneta, pamti trag koji je korisnik ostavio iza sebe te koristi njihove osobne podatke. Dakle, anonimnost je gotovo nemoguća s obzirom na to da je internet postao dijelom čovjekova svakodnevnog života te je nemoguće zamisliti život bez njegova korištenja. Rodgers navodi da se „podatci više ne smatraju osobnima nakon što su postali anonimni na takav način da ih je nemoguće povezati s osobom“ (Rodgers, 2020: 2).

Upravo zato što korisnici internet usluga nesvjesno iznose svoje podatke, a tvrtke, vlasnici aplikacija i društvenih mreža pohranjuju te iste podatke, postavljaju se pitanja, kako i u koje

svrhe netko koristi osobne podatke korisnika društvenih mreža te postoji li zakonska regulativa i zaštita po tome pitanju?

2.1. Osobni podatci na društvenim mrežama

Prema Boyd i Ellison (2008), društvene su mreže definirane kao web stranice koje omogućuju stvaranje profila i vidljivost odnosa među korisnicima web-bazirane aplikacije, a koje prema Kietzmann et al. (2011) pružaju mogućnost razgovora, dijeljenja informacija, stvaranje odnosa i grupa. Kapoor et al. (2017) navode da su društvene mreže skup informacijskih tehnologija koje olakšavaju interakcije i umrežavanje. Društvene mreže, poput Facebooka, Twittera i LinkedIna, pružaju ljudima snažnu mrežnu povezanost (Asur i Huberman, 2010).

Prethodno je objašnjeno da neizravni osobni podatci koji su šifrirani su podatci koje osoba gradi putem interneta, najčešće na društvenim mrežama. Podatci su to na koje prosječan korisnik internet usluga ne obraća pozornost i ne razmišlja o tome da su takvi podatci također dio njegova identiteta. Rodgers (2020: 3) upozorava da tijekom korištenja društvenih mreža ono identificira interakcije koje korisnik ima tijekom korištenja usluge, kao što je vrsta sadržaja koji smatra zanimljivim, vrsta sadržaja koji korisnik dijeli, drugi korisnici s kojima korisnik komunicira i reklame na koje korisnik odgovara i stupa u interakciju. Slučaj Cambridge Analytica primjer je kako se može zlouporabiti mogućnost da računalo pamti svaku interakciju na društvenoj mreži, od klika na oznaku „sviđa mi se“, komentiranja, praćenja drugih korisnika i njihovih profila do dijeljenja sadržaja te od korisnika čini idealnu osobu kojoj će kasnije ponuditi one informacije za koje računalo, odnosno algoritam, zna da će kao korisnik konzumirati te biti najviše zainteresiran. Rodgers (2020: 3) dalje objašnjava da na temelju kombinacije podataka koje korisnik daje, kao i korisnikove interakcije (na društvenoj mreži), tvrtka koja posjeduje web stranicu, može izgraditi (čuvati) informacije koje ima o korisniku da bi ih mogla bolje razumjeti. To se obično radi upotrebom strojnog učenja i vlasništva algoritama.

Dakle, društvene su mreže platforme na kojima korisnici ostavljaju svoje osobne podatke na temelju svojih interakcija, gdje se uz pomoć algoritama, pamti svaka interakcija korisnika gdje kasnije, Rodgers (2020: 3) objašnjava da na temelju interakcija korisnika, stranica može razviti prijedloge drugih objava koje korisnika mogu zanimati među velikim brojem drugih objava na stranici. Ovim algoritmom preporuke upravlja algoritam strojnog učenja, koji

prikuplja informacije o objavama s kojima korisnik komunicira, predlaže nove objave (važno je napomenuti i oglase) i na temelju toga kako korisnik reagira, može prilagoditi svoje preporuke. Tako se korisniku, po već dobivenom iskustvu, predlažu sadržaji koji će zainteresirati korisnika, web mjesto će dobiti više pregleda jer je veći angažman korisnika, a time i oglasi na istim stranicama dobivaju veću zapaženost. Dakle, iz ovoga dijela bitno je zapamtiti kako tvrtke uz pomoć društvenih mreža na temelju algoritama mogu kontrolirati koji će se sadržaj predstavljati korisnicima i to na temelju njihovih preferencija koje je računalo zapamtilo od prijašnje interakcije kojom su korisnici ostavili svoje osobne podatke.

Sve su današnje popularne društvene mreže besplatne za svoje korisnike, ali tvrtke vlasnici tih mreža vrijedne su više milijardi dolara. Rodgers (2020: 3) objašnjava na primjeru Facebooka i Googlea da je razlog tomu jer velik dio svojih prihoda ostvaruju putem korištenja i prodaje oglasnog prostora drugim tvrtkama. Budući da su takve stranice društvenih mreža često dizajnirane za držanje pozornosti korisnika pokušavaju što je dulje moguće vratiti korisnika na aplikaciju, više puta dan. To omogućuje stranicama da prikažu više oglasa svojim korisnicima i tako ostvare više prihoda.

Zastrašujuća je pomisao da računalo uz pomoć algoritama poznaje čovjekove preferencije možda bolje i od samoga čovjeka, ali gledajući iz pozicije marketinga, društvene su mreže odličan alat za promociju proizvoda. No, kada tvrtke kao što su Instagram, Facebook ili Google pretraživač oglašavaju svoje proizvode na društvenim mrežama, iste te tvrtke dobivaju puno veći pristup od samog oglasnog prostora na web stranici. Smith i Anderson (2018) objašnjavaju da tvrtke (Facebook, Google) oglašivačima daju alate kojima imaju dopuštenje da svoje oglase ciljaju na određene vrste gledatelja prema općoj demografiji korisnika.

Prema informacijama koje je moguće vidjeti na Facebookovoj službenoj stranici, Facebook, odnosno trenutna Meta tvrtka, na svojim društvenim mrežama nudi opcije kojima oglašivači mogu ciljati svoje oglase korisnicima između ostalih značajki na temelju dobi, spola, lokacije, jezika i interesa. Ovakav način oglašavanja omogućuje oglasima da učinkovitije prenesu svoju poruku korisnicima, kao i oglašivačima ciljanje željene publike. Ovakav sustav oglašavanja, uz pomoć korištenja algoritama, postao je uobičajen, ali s obzirom da su algoritmi prepoznali korisnike društvenih mreža po dobi, spolu, lokaciji, jeziku i interesima, bilo je slučajeva u kojima je isti taj sustav oglašavanja zloupotrijebljen. Tako su oglasi korišteni za širenje dezinformacija i sisanje nesuglasica oko političkih kandidata, što je

dovelo do toga da je Kongres Sjedinjenih Država zatražio od društvenih mreža da provjere činjenice ili ograniče političko oglašavanje na svojim stranicama. Twitter je odgovorio uklanjanjem svih političkih reklama, Google je ograničio političke reklame na svojem oglasnom prostoru, dok Facebook nije napravio takve ustupke. Isaac i Kang pišu za New York Times (2020) da je Facebookov direktor za upravljanje proizvodima Rob Leathern izjavio da su se u Facebooku temeljili na načelu da ljudi trebaju moći čuti one koji ih žele voditi te da ono što govore treba pomno ispitati i raspravljati u javnosti.

2.2. Zaštita privatnosti

Prethodno je ukratko objašnjeno kako se koriste osobni podatci korisnika društvenih mreža. Na takvo obrađivanje osobnih podataka, korisnici sami pristaju tijekom izrade računa za društvenu mrežu i to onoga trenutka kada korisnik prihvati uvjete pružanja usluga društvene mreže. Uvjeti pružanja usluga Googlea (2022) pravno su obvezujući dokument koji navodi pravne smjernice za korištenje usluge, ograničenja obveza i pravila o privatnosti koja detaljno opisuju korištenje osobnih podataka i još mnogo toga. Međutim ti su dokumenti često dugi i koriste pravni jezik koji prosječni korisnik možda neće razumjeti i iz toga razloga korisnici prihvaćaju sve što se od njih zahtjeva. Korisnici često nisu svjesni mogućih rizika povezanih s potpunim korištenjem njihovih osobnih podataka, posebno kada nisu obaviješteni o namjeni obrade. Iz tih razloga, lako dolazi do zlouporabe osobnih podataka.

2.2.1. Zaštita privatnosti u Europskoj uniji

Nažalost, zaštita osobnih podataka na internetu ozbiljnije se shvaća tek kada se dogodi veliki propust u narušavanju privatnosti, krađi identiteta i zlouporabi osobnih podataka. Republika Hrvatska svojim Ustavom i Zakonom o zaštiti osobnih podataka (2012) navodi da je „pravo na zaštitu osobnih podataka jedno od temeljnih prava svakog čovjeka. Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.“ Sasvim je jasno da se osobni podatci moraju obrađivati zakonito, pošteno i transparentno. Europska unija, čija je članica i Hrvatska, uvela je posebne Uredbe za zaštitu privatnosti i osobnih podataka. Uvedena je Opća uredba o zaštiti podataka

(na engleskom: *General Data Protection Regulation*, skraćeno GDPR), koja se primjenjuje u svim državama članicama Europske unije. Cilj uvođenja GDPR-a bio je korisnicima interneta dati više nadzora nad načinom na koji se njihovi podatci (zlo)upotrebljavaju.

Prema GDPR-u (2018), podatci se smatraju osobnima ako se iz njih s velikom vjerojatnošću može otkriti identitet pojedinca, a sam opseg podataka koje GDPR pokriva nije se značajno promijenio, osim dodavanja mrežnih identifikatora koji se smatraju osobnim podacima. Ukupno gledano, GDPR (2018) pokriva sljedeće kategorije podataka: osnovni podatci (ime i prezime, broj osobne iskaznice, lokacijski podatci), podatci s kreditnih kartica, zdravstveni karton, biometrijski podatci (sken rožnice, otisci prsta i tako dalje), genetski podatci (DNA i slično), vjerska i filozofska uvjerenja, etnička pripadnost, ekonomsko stanje, članstvo u sindikatu, seksualna orijentacija, IP adresa, e-pošta, kolačići u pregledniku i pseudonimizirani podatci.

Prema GDPR-u (2018), građani imaju više prava nad svojim osobnim podacima, kao što su pravo na trajno brisanje svojih podataka, pravo na informiranost o prikupljanju, korištenju i prodaji svojih podataka, pravo na ispravak svojih podataka, pravo na ograničenje obrade svojih osobnih podataka informacije te pravo na prigovor na prikupljanje osobnih podataka. Prema Službenom listu Europske unije (2016) GDPR tvrtke koje prikupljaju osobne podatke drži odgovornima za pravilnu obradu, pohranu te sigurnost i pristup osobnih podataka te isto tako nalaže da te tvrtke koje prikupljaju osobne podatke, dobivaju informirani pristanak od korisnika za prikupljanje osobnih podataka.

Za sve tvrtke koje se ne budu pridržavale ovih propisa, nadzorna tijela imaju izbor od nekoliko mjera kojima mogu sankcionirati tvrtke koje se ne pridržavaju novih propisa. GDPR Informer (2018) navodi da su to: upozorenja, opomene, zabrane obrade podataka i novčane kazne koje mogu iznositi za niži stupanj kazne, najviše 10 milijuna eura ili 2% ukupnog godišnjeg prometa za prethodnu godinu, ili za teška kršenja načela obrade, zaštite podataka i prava pojedinaca, kazne od 20 milijuna eura ili 4 % ukupnog godišnjeg prometa za prethodnu godinu.

2.2.2. Zaštita privatnosti u Sjedinjenim Američkim Državama

U SAD-u je stanje po pitanju zaštite osobnih podataka bitno drugačije, ali se pokušava jednako tako zaštititi korisnike društvenih mreža. Zanimljivo, ali u SAD-u ne postoji niti jedan sveobuhvatan savezni zakon koji regulira privatnost podataka. Zato postoji složena kombinacija zakona specifičnih za razne sektore i medije, uključujući zakone i propise koji se odnose na telekomunikacije, zdravstvene informacije, kreditne informacije, financijske institucije i marketing.

Važna agencija za provedbu zakona u SAD-u je Savezna trgovinska komisija SAD-a (na engleskom *Federal Trade Commission*, skraćeno FTC). Ovlasti ove agencije, za reguliranje zaštite potrošača, proizlaze iz Zakona o saveznoj trgovinskoj komisiji (na engleskom *FTC Act*), a koji ima široku nadležnost za sprječavanje nepoštenih ili „obmanjujuće trgovačke prakse“ nad trgovačkim subjektima.

FTC ne regulira izričito koje bi informacije trebale biti uključene u pravila o privatnosti web-mjesta, ali koristi svoje ovlasti za izdavanje propisa, provođenje zakona o privatnosti i poduzimanje izvršnih radnji za zaštitu potrošača. Osano (2022) navodi da FTC poduzima mjere protiv organizacija koje:

- ne provode razumne mjere sigurnosti podataka,
- ne pridržavaju se važećih samoregulatornih načela industrije organizacije,
- ne pridržavaju se objavljenih pravila o privatnosti,
- provode prijenos osobnih podataka na način koji nije naveden u politici privatnosti,
- iznose netočne izjave o privatnosti i sigurnosti o potrošačima i pravilima o privatnosti,
- ne osiguravaju dovoljnu sigurnost osobnih podataka,
- krše prava na privatnost podataka potrošača prikupljanjem, obradom ili dijeljenjem podataka o potrošačima,
- sudjeluju u zavaravajućoj praksi oglašavanja.

Ostali savezni zakoni koji reguliraju prikupljanje podataka na internetu uključuju:

- Zakon o zaštiti privatnosti djece na internetu (1998) (na engleskom: *Children's Online Privacy Protection Rule*, skraćeno COPPA), koji regulira prikupljanje osobnih podataka na internetu za djecu mlađu od 13 godina te nameće određene zahtjeve

operaterima web stranica ili internetskih usluga usmjerenih na djecu mlađu od 13 godina.

- Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja (2021) (na engleskom: *Health Insurance Portability and Accountability Act*, skraćeno HIPAA), zahtijeva odgovarajuće zaštitne mjere za zaštitu privatnosti zdravstvenih informacija i postavlja ograničenja i uvjete za korištenje i otkrivanje takvih informacija bez odobrenja pojedinca.
- Zakon *Gramm Leach Bliley Act* (2022) (skraćeno GLBA), regulira osobne podatke koje prikupljaju banke i financijske institucije, tvrtke koje potrošačima nude financijske proizvode ili usluge poput zajmova, financijskih ili investicijskih savjeta ili osiguranja.
- Zakon o poštenom kreditnom izvještavanju (2018) (na engleskom: *Fair Credit Reporting Act*, skraćeno FCRA) koji regulira prikupljanje i korištenje kreditnih podataka.

Iz ovih pravilnika i zakona vidljivo je da su osobni podatci građana Europske unije zakonski na internetu više zaštićeniji od građana SAD-a, s obzirom na to da u SAD-u ne postoje zakoni u smislu regulacije na saveznoj razini koji bi detaljno opisali kako je tvrtkama dopušteno prikupljati, pohranjivati, dijeliti i prodavati osobne podatke.

3. ŠIRENJE INFORMACIJA POSREDSTVOM DRUŠTVENIH MREŽA

U zadnjih nekoliko godina pojam „lažne vijesti“, ili na engleskom „*fake news*“, redovito je prisutan u javnosti. Iako se u raznoj literaturi i javnosti mogu sresti i drugi izrazi i pojmovi, autor u radu pretežno koristi pojam „lažne vijesti“, odnosno „*fake news*“ jer je općeprihvaćen za označavanje (ne)namjerne produkcije i širenja neistinitih ili nepouzdanih informacija. Danas su lažne vijesti, govor mržnje, senzacionalističke informacije i slične pojave, nažalost, uobičajena pojava na društvenim mrežama. S obzirom na to da se sve više građana oslanja upravo na društvene mreže kao glavni i jedini izvor informacija, takvi sadržaji utječu na njih jer mnogi ljudi nisu u stanju razlikovati istinu od lažnih vijesti.

Upravo je zato potrebno zaštititi korisnike od različitih oblika lažnih informacija koje su dostupne na društvenim mrežama, no takav način zaštite često podrazumijeva ukidanje potpune slobode govora u javnome prostoru koji čine društvene mreže. Carnahan (2020) navodi da je jedno stajalište stručnjaka da je javni interes najbolje zadovoljen kada je sav sadržaj vidljiv na društvenim mrežama, bez obzira koliko netočan, pun mržnje ili zao. Iako ljudi mogu prosuđivati sadržaj i pozivati govornike na odgovornost, loše ideje bit će prikazane onakvima kakve jesu, zanemarene kroz raspravu, a rezultat će biti produktivniji razgovori.

Međutim postavlja se pitanje gdje su granice i kakve su sve posljedice postojanja takvog sadržaja ispunjenoga lažnim informacijama u javnom prostoru, pa tako i na društvenim mrežama? Carnahan (2020) objašnjava da postoji i drugo stajalište stručnjaka koje tvrdi da dopuštanje takvog sadržaja na društvenim mrežama šteti javnom interesu, tvrdeći da „tržište slobodnih ideja“ možda ne funkcionira na društvenim medijima tako dobro kao što se misli. Dezinformacije mogu ometati javni diskurs i donošenje odluka, što čini ljudima teško pronaći zajednički jezik i čak predstavlja prijetnju javnom zdravlju. Nadalje, rubne skupine koriste sadržaj pun mržnje da bi ojačale svoje redove i povećale svoju organizaciju, što je vidljivo iz ponovnog pojavljivanja rasista i drugih radikalnih pokreta.

I jedno i drugo stajalište imaju prednosti i nedostataka, oko kojih se posljednjih godina vode velike rasprave, posebice vezano uz pitanja ograničavanja slobode govora, javnog izražavanja vlastitog mišljenja i stavova te nesmetanog dijeljenja i širenja informacija posredstvom društvenih mreža.

3.1. Lažne vijesti

U današnje se vrijeme lažne vijesti pojavljuju sve češće, a velikom se brzinom šire zahvaljujući društvenim mrežama. Pickard (2016) objašnjava da društvene mreže igraju važnu ulogu kao platforme za širenje lažnih vijesti. Njihova uloga „čuvara vijesti“ uzrokuje trenutno širenje lažnih vijesti veći problem nego ikad prije. Downey i Fenton (2003) navode da se lažne vijesti šire puno brže zbog društvenih mreža i drugih internetskih platformi koje javnosti olakšavaju proizvesti vlastiti medijski sadržaj. Osim toga, ovo znači da društvene mreže pružaju platformu alternativnim medijima za širenje svog sadržaja. Kao rezultat toga, vijesti na alternativnim medijima i njihov utjecaj rastu posljednjih desetljeća.

Prema Campbell i Crain, izraz „lažne vijesti“ počeo se svakodnevno koristiti u javnosti nakon američkih predsjedničkih izbora 2016. godine, iako je njihova pojava postojala i prije. Koncept, poznat kao „dezinformacija“, za vrijeme svjetskih ratova i kao „nakazno novinarstvo“ ili „žuto novinarstvo“ tijekom Španjolskog rata, može se pratiti unazad do 1896. (Campbell, 2001; Crain, 2017). Razlika koju čine lažne vijesti prije i danas je „informativno okruženje u kojem se trenutno živi, gdje su društveni mediji ključni za širenje informacija i informacije se više ne primaju isključivo uz pomoć tradicionalnih gatekeepera. U današnje vrijeme, nije potrebno biti novinar i raditi publikaciju za stvaranje i širenje sadržaja na internetu. Laici pišu, kuriraju i šire informacije putem internetskih medija“ (Molina et al., 2019: 183). Bode i Vraga (2015) smatraju da je ovo posebno problematično, s obzirom na to da pojedinci smatraju vjerodostojnijima i pouzdanijima informacije koje se slažu s prethodnim uvjerenjima stvarajući okruženje koje pogoršava dezinformacije jer se vjerodostojne informacije pojavljuju uz osobna mišljenja.

Uvodni dio ovoga poglavlja ukratko predočava razloge zašto društvene mreže mogu biti pogodne za razvijanje lažnih vijesti. No, postoji više razloga za to. Za prvi razlog Allcott i Gentzkow (2017: 221) navode da su na društvenim mrežama fiksni troškovi ulaska na tržište i proizvodnje sadržaja nevjerovatno mali. To povećava relativnu profitabilnost malih, kratkoročnih strategija koje često prihvaćaju proizvođači lažnih vijesti i smanjuje relativnu važnost izgradnje dugoročne reputacije kvalitete. Za drugi razlog navode sam format društvenih mreža, a to su tanki dijelovi informacija koji se gledaju na telefonima ili samo kratki sažetak vijesti, što može otežati procjenu istinitosti članka. Za treći razlog uzimaju istraživanje koje su proveli Bakshy, Messing i Adamic (2015), a istraživanje pokazuje da su mreže prijatelja na Facebooku ideološki razdvojene. Odnosno, među tim prijateljstvima ljudi koji na svojim profilima navode ideološku pripadnost, prosječni udio prijatelja suprotne ideologije je samo 20% za liberalne i 18% za konzervativce. Dakle, jasno je da će ljudi znatno vjerojatnije čitati i dijeliti novinske članke koji su usklađeni s njihovim ideološkim pozicijama. Ovo sugerira da je manje vjerojatno da će ljudi koji dobivaju vijesti s Facebooka (ili drugih društvenih mreža) dobiti dokaze o pravom stanju u svijetu koji bi se suprotstavili ideološki usklađenim stajalištima, već više lažne vijesti koje će odgovarati njihovim ideološkim stajalištima. Problem kod takvih lažnih vijesti je moguća manipulacija birača koji svoj glas mogu temeljiti na dezinformaciji, što može utjecati na izborne rezultate.

Potrebno je objasniti što se u ovom radu podrazumijeva pod terminom „lažne vijesti“, s obzirom na to da kod njegove definicije postoje neslaganja među teoretičarima. Tako

primjerice Balmas (2014) tvrdi da lažne vijesti postoje samo kao pandan pravim vijestima. Lažne vijesti uvijek se temelje na istinitim vijestima koje se modificiraju, ismijavaju ili tumače na drugačiji način. Štoviše, utjecaj lažnih vijesti ovisi o izloženosti potrošača pravim vijestima. Pojedinaac koji ne prati često aktualne vijesti, češće će percipirati lažne vijesti kao istinite nego pojedinac koji intenzivno prati vijesti.

Kulturalni teoretičar i sociolog Stuart Hall tvrdi da se vijesti ne mogu promatrati kao istinite ili lažne, već kao „prikazi stvarnosti kodirano u poruke i značenja” (Hall, 1989: 276). Da bi utvrdio predstavljaju li vijesti stvarne događaje, Hall (1989) govori o konsenzusu o pozadinskom znanju i okviru odnosa između novinara i publike. Sve dok postoji konsenzus, postoji objektivnost. To znači da vijesti o kontroverznim temama trebaju predstavljati širok raspon okvira referenca ili „ravnoteža mišljenja”.

Postoje znatna neslaganja kada se radi o određivanju koji sadržaj treba smatrati lažnim vijestima, a koji treba isključiti. To posebno vrijedi jer je pojam „lažne vijesti” postao izrazito političan i često se koristi kao poštapalica koja se ne koristi samo za opisivanje izmišljenih informacija, već i za potkopavanje vjerodostojnosti novinskih organizacija ili protiv komentara koji se ne slažu s našim mišljenjem. Štoviše, klasificiranje dijela sadržaja kao lažnog, zahtjeva utemeljenje univerzalne istine, što može biti težak pothvat koji zahtijeva kolektivni konsenzus (Southwell et al., 2017).

S obzirom da je složeno odrediti što jest, a što nije lažna vijest, u ovome se radu autor koristi definicijom iz Cambridge rječnika (2018) jer sama taksonomija odgovara svrsi ovoga rada. U njoj se tvrdi da su lažne vijesti „lažne priče koje izgledaju kao vijesti, šire se internetom ili korištenjem drugih medija, obično stvorene da utječu na politička stajališta ili kao šala”.

3.1.1. Lažne vijesti kao političko oružje

Lažne su vijesti postale sve češće pitanje u političkom kontekstu. Allcott i Gentzkow (2017) navode da su pogotovo tijekom predsjedničkih izbora 2016. godine u SAD-u na društvenim mrežama kružile velike količine lažnih vijesti. Stoga, američki građani su izbor svog glasa možda temeljili na pogrešno dostupnim informacijama. Uostalom, pogrešne informacije mogu dovesti do neopravdane promjene političkih stavova, a potom i do promjena glasačkog

ponašanja. Upravo ovo stvaranje lažnih vijesti stvara potencijalnu prijetnju demokraciji, a izaziva sve veću zabrinutost građana diljem svijeta.

Chrysalis Wright, izvanredna je predavačica psihologije na Sveučilištu Centralna Florida (*University of Central Florida*, skraćeno UCF), stručnjakinja je za lažne vijesti i online dezinformacije te osnivačka direktorica UCF-ovog Laboratorija za medije i migracije gdje identificira i razvija metode za borbu protiv lažnih vijesti. U intervjuu pod naslovom „Kako lažne vijesti utječu na izbore u SAD-u“, koji je s njom vodila J. M. Leeza na UCF-ovoj službenoj web stranici, Wright je rekla da su ljudi skloni misliti da su njihova mišljenja, stavovi i uvjerenja naša vlastita, ali to nije 100 posto točno jer su pod utjecajem onoga što vide. Tvrdi da lažne vijesti apsolutno utječu na stavove i uvjerenja, a to može utjecati na čovjekovo stvarno ponašanje.

Prema Lee (2020), Wright je za tvrdnje da su lažne vijesti i dezinformacije utjecale na izbore u SAD-u 2016. godine, izjavila da su saznali da je Rusija bila umiješana u nešto od ovoga, ali postoje i druge zemlje koje su također vjerojatno imale ulogu na način da bi stvarali lažne vijesti i dijelili ih na platformama društvenih mreža. Odabirali su vruće teme o kojima je nacija podijeljena, poput prava na oružje, rasnih odnosa, imigracijskih pitanja i to koristili kao slabost. Svrha je podijeliti naciju i natjerati da se međusobno bori iznutra, jer, objašnjava Wright, ako ih mogu natjerati da se međusobno bore iznutra, ne moraju ništa više učiniti, već pobjeđuju. Zaključuje da su lažne vijesti bile vrlo uspješne, ako se pogledaju društveni nemiri koji su vladali na ulicama.

Prema Lee (2020), na pitanje koliko su lažne vijesti popularne i raširene, Wright je iznijela podatke da su neposredno prije izbora 2016. godine, prvih 20 lažnih vijesti koje su kružile društvenim medijima dobile više angažmana (lajkanje, dijeljenje, komentiranje) od prvih 20 činjeničnih vijesti koje su bile na društvenim medijima.

Rat u Ukrajini primjer je kako društvena mreža TikTok može dezinformirati milijune svojih korisnika i to vrlo jednostavnom metodom. Prema Sardarizadeh (2022), TikTok se pojavio kao jedna od vodećih mreža za lažne videozapise o ratu u Ukrajini koji velikom brzinom dosežu milijune pregleda. S korisničkom bazom od više od jedne milijarde ljudi, pretežno mladih ljudi do 30 godina, TikTok je mreža na kojoj dobivaju novosti o sukobu i to kroz lažne prijenose uživo, video igre i stare videozapise. Pojedinci iskoriste dramatične snimke starih sukoba ili neke vojne vježbe, presnime lažni zvuk velike eksplozije ili intenzivne pucnjave i pokrenu prijenos uživo, a nakon što se znatna publika uključi, traže donacije za svoj kanal ili

korisnici mogu reagirati na prijenose uživo slanjem bodova na račune koji se mogu pretvoriti u gotovinu. Dakle, ovaj primjer prikazuje kako je lako izmanipulirati mladim ljudima i kako se TikTok mreža može koristiti kao političko oružje, ali i kako pojedinci mogu vrlo jednostavno zaraditi manipuliranjem javnosti.

4. SLUČAJ CAMBRIDGE ANALYTICA

Sve većim brojem korisnika interneta, na globalnoj razini zabilježen je velik broj slučajeva ili sumnji na zlouporabu osobnih podataka korisnika interneta, pa tako i društvenih mreža. Velike se društvene mreže kontinuirano prozivaju za „curenje“ ili omogućavanje korištenja osobnih podataka svojih korisnika trećim stranama bez suglasnosti i znanja korisnika. Primjerice, prema George (2022), Twitter je 2019. godine priznao da je oglašivačima bilo omogućeno dobiti pristup adresama e-pošte i telefonskim brojevima korisnika društvene mreže bez dopuštenja korisnika. Prema Brook (2020), Državno povjerenstvo za informatiku i slobode (CNIL) je 2020. godine kaznilo Google s 57 milijuna dolara jer tvrtka jer nije potvrdila da se podaci korisnika obrađuju. Fokus ovoga poglavlja je pak na zlouporabi osobnih podataka korisnika društvenih mreža u političke svrhe koja se prikazuje kroz jedan od globalno najpoznatijih primjera, slučaj Cambridge Analytice.

Cambridge Analytica bila je tvrtka za analizu podataka, osnovana 2013. godine, a osnovala ju je britanska kompanija Strategic Communication Laboratories Group, s ciljem organizacijskog djelovanja i na američkom tržištu. Prema Rathi (2019), Cambridge Analytica kombinira prediktivnu analitiku podataka, bihevioralne znanosti i inovativnu tehnologiju oglašavanja u jedan nagrađivani pristup. Cadwalladr (2017) navodi da je Cambridge Analytica najpoznatija u radu digitalne kampanje temeljene na tehnikama mikrotargetiranja za američke republikanske političare među kojima su Donald Trump i Ted Cruz, kao i u uključenosti u organizaciji Leave.EU na čelu s britanskim političarom Nigelom Farageom za vrijeme referenduma oko izlaska Velike Britanije iz Europske unije.

U ovome se dijelu rada prikazuje na konkretnim primjerima kako je tvrtka Cambridge Analytica targetirala i uvjeravala korisnike društvenih mreža da glasaju na određeni način prikazivanjem različitih oglasa o „vrućim“ pitanjima. Uvjeravanje je provedeno prikupljanjem informacija o Facebook korisnicima i korištenjem tih podataka za izradu modela koji

predviđaju osobnost. Prema Rathi (2019), utvrđeno je da je tvrtka koja je prikupila osobne podatke za Cambridge Analyticu, Global Science Research, na čelu s Aleksandrom Koganom, prekršila Facebookove uvjete pružanja usluga pa je Facebook 2015. godine zatražio od svih tvrtki kojima je Kogan dao podatke, uključujući Cambridge Analyticu, da izbrišu sve prikupljene podatke s Facebooka. U ožujku 2018., Cambridge Analytica podnijela je zahtjev za stečaj, a prestala raditi 1. svibnja 2018. godine.

Novinari Quartz portala Sarah Todd i Dave Gershgorn(2018) navode da je osnivanje tvrtke Cambridge Analytica inicirao bivši strateg Bijele kuće Steve Bannon. Steve Bannon je, objašnjava istraživačka novinarka Carole Cadwalladr (2017), bio glavni strateg političke kampanje Donalda Trumpa, potpredsjednik tvrtke Cambridge Analytica u periodu referendumske kampanje za izlazak Velike Britanije iz Europske unije te bliski prijatelj britanskog političara Nigela Faragea.

S obzirom da je slučaj Cambridge Analytica povezan s brojnim utjecajnim osobama iz svijeta politike i poduzetništva, potrebno je prvo navesti njihova imena i objasniti njihove funkcije u cijelom slučaju te zatim objasniti tijek događaja koji su se odvijali za vrijeme predsjedničkih izbora 2016. godine i Brexita. Važno ime je Robert Mercer, republikanski megadonator, Cadwalladr (2017) koji navodi da je posjedovao 90 % vlasništva Cambridge Analytice, dok je u Strategic Communication Laboratories Grupi (SCL) imao 10 % vlasništva kompanije. Ostala imena utjecajnih ljudi koje je potrebno spomenuti u ovome slučaju su Alexander Nix, Aleksandr Kogan, Christopher Wylie, Brittany Kaiser i Mark Zuckerberg. Istraživačke novinarko Cadwalladr i Graham-Harrison (2018) za The Observer pišu da je Alexander Nix bio izvršni direktor Cambridge Analytice, od 2007. godine preuzeo je odjel za izbore u SCL tvrtki gdje je radio na 260 kampanja širom svijeta. Aleksander Kogan je znanstvenik-istraživač sa Sveučilišta Cambridge koji je osnovao tvrtku Global Science Research uz pomoć koje je prikupljao podatke iz aplikacije koju je razvio, prije nego što se pridružio Cambridgeu kao predavač psihologije i stručnjak za psihometriju društvenih medija. Christopher Wylie bio je bivši vodeći analitičar u Cambridge Analytici te prvi zviždač koji je progovorio u medijima o slučaju Cambridge Analytice. Druga ključna zviždačica bila je Brittany Kaiser, radila je kao direktorica poslovnog razvoja u Cambridge Analytici. Mark Zuckerberg izvršni je direktor Facebooka. S obzirom da je Facebook društvena platforma koja je korištena za prikupljanje podataka i ciljano političko oglašavanje i on se bitan sudionik u ovome cijelom slučaju.

4.1. Britanska analitička tvrtka Cambridge Analytica

Važno je razumjeti kako je tvrtka Cambridge Analytica uspjela zlouporabiti osobne podatke korisnika društvenih mreža, odnosno kojim se metodama koristila, kako je došla do tih podataka te što su radili s tim podacima. Prema Meredith (2018), prvi korak koji se dogodio bilo je prikupljanje podataka Facebook korisnika uz pomoć aplikacije „*thisisyourdigitallife*“, koju je kreirala tvrtka Global Science Research na čelu s Aleksandrom Koganom 2014. godine. Detrow (2018) objašnjava da je aplikacija poticala korisnike da odgovore na 120 pitanja za utvrđivanje psihološkog profila, odnosno pitanja kojima se „nastojalo ispitati osobnost“.

Cadwalladr i Emma Graham-Harrison (2018) pišu da je tvrtka Global Science Research u suradnji s Cambridge Analytica poticala stotine tisuća Facebook korisnika da pristupe testiranju osobnosti, gdje su korisnici pristali da se njihovi podatci prikupljaju za akademsku upotrebu, uvjereni da su njihovi podatci sigurni te će ostati anonimni. Detrow (2018) navodi da je gotovo 300.000 korisnika bilo plaćeno da pristupe psihološkom testu, a aplikacija je zatim prikupljala njihove osobne podatke, kao što su lokacija, sadržaj koji su korisnici označili sa „svida mi se“, ali i podatke korisnikovih prijatelja. Prema Detrow (2018) i Meredith (2018), također su prikupljeni podatci i od njihovih Facebook prijatelja, što je navodno rezultiralo time da je Kogan od samo 300 000 Facebook korisnika kojih je riješilo kviz, imao pristup podacima više od 50 milijuna Facebook profila.

Utvrđeno je da je tvrtka Global Science Research na čelu s Aleksandrom Koganom, koja je prikupila podatke o ličnosti za Cambridge Analyticu, prekršila Facebookove uvjete pružanja usluge pa je Facebook zatražio od svih tvrtki kojima je Kogan dao podatke, uključujući Cambridge Analyticu, da izbrišu sve podatke koje posjeduju. Prema Todd i Gershgorn (2018), Facebook je 2014. godine prilagodio svoja pravila da bi ograničio programerima pristup osobnim korisničkim podacima. Detrow (2018) navodi da je ova promjena napravljena da bi se osiguralo da treća strana ne može pristupiti podacima o korisnikovim prijateljima bez prethodnog dobivanja dopuštenja. Međutim, prema Meredith (2018), promjene pravila nisu retroaktivno nametnute i Kogan nije izbrisao podatke za koje se smatralo da su nepropisno prikupljeni. Todd i Gershgorn (2018) navode da je Aleksandr Kogan kršeći pravila Facebookovih uvjeta, prosljedio podatke koje je posjedovao Cambridge Analytici.

Cambridge Analytica u tome je trenutku imala podatke s kojima su mogli doći do velikog broja korisnika Facebooka, ali da bi te podatke iskoristili u korist političke kampanje, bila je potrebna strategija koja je uz analitiku podataka uključivala i biheviorističku znanost te inovativnu oglasnu tehnologiju. Rathi (2019) objašnjava da bihevioristička znanost proučava odnose u ponašanju i djelovanju ljudi ili životinja. Krajnji cilj Cambridge Analytice, pri vođenju političkih kampanja, bio je uvjeriti korisnike Facebooka da glasaju za svog klijenta, što je, objašnjava Rathi (2019), uključivalo prikazivanje oglasa koji bi najvjerojatnije rezultirali promjenom ponašanja kod korisnika. Rathi (2019) je naveo i primjer koji je preuzeo iz prezentacije Alexandra Nixa na Concordia summitu 2016. godine. Primjer na slici br. 1 ilustrira biheviorističku komunikaciju, odnosno važnost vođenja znanosti o ponašanju na um čovjeka prilikom prenošenja poruka. Nix (2016) objašnjava da kada bi čovjek šetajući plažom vidio dva znaka kao na slici 1., znak s lijeve strane bi možda potaknuo čovjeka da se okrene, dok bi znak s desne strane imao daleko jači utjecaj da to učinimo.



Slika 1. Primjer prenošenja poruke biheviorističkom komunikacijom

Izvor: preuzeto u cijelosti (Rathi, 2019)

Prema ovom primjeru, sve ili većina osoba imale bi jak poriv napustiti plažu nakon što vide poruku s desne strane. Međutim, objašnjava Nix (2016) u političkom području, ovisno o već postojećim uvjerenjima i vrijednostima, različite ljude bilo bi bolje uvjeriti različitim porukama podrške o istom kandidatu ili problemu. Cambridge Analytica stoga je pretpostavila da bi, kad bi imali mjerenje nečije osobnosti, mogli pripremiti reklamu koja bi im bila najuvjerljivija. Stoga bi pomoću personaliziranih, ciljanih oglasa mogli uvjeriti mnogo

različitih ljudi, s različitim osobnostima da imaju isto mišljenje o određenom pitanju ili kandidatu. Da bi uvjerali potencijalne birače glasati na određeni način uz pomoć bihevioralne znanosti, potrebne su informacije o tome tko je cilj oglasa.

Da bi pronašli taj cilj kojem će prikazati oglas, Cambridge Analytica je morala pronaći način kako dobiti podatke o milijunima korisnika društvenih mreža da bi te podatke mogli upotrijebiti za predviđanje osobnosti korisnika. Rathi (2019) objašnjava da na ovome dijelu priče dolazi analitika podataka, znanost o izvlačenju informacija o korisnicima iz sirovih podataka. Već je ukratko objašnjeno kako je Cambridge Analytica u suradnji s Aleksandrom Koganom, osnivačem tvrtke Global Science Research (GSR), prikupila podatke korisnika Facebooka preko aplikacije „*thisisyourdigitallife*“. Rathi (2019) navodi da je Christopher Wylie, tada zaposlenik Cambridge Analytice, upravljao tim odnosima s Koganom. Kogan je potom izradio anketu koja je ispitanike pitala o njihovoj osobnosti, pri čemu je koristio Qualtrics, dobavljača online anketa koji regrutira sudionike plaćajući svakome po nekoliko dolara dabi pridobio sudionike. U anketi se od ispitanika tražio pristanak za pristup njihovim Facebook podacima, uključujući stranice koje su lajkali. Ključno je da je Kogan također dobio pristup lajkovima stranice prijatelja ispitanika te tako prikupio i podatke o korisnikovim prijateljima. Cambridge Analytica je zatim koristila Facebook podatke svakog korisnika da bi predvidjela njegovu ili njezinu osobnost. Cilj im je bio kvantificirati osobnost ocjenjivanjem pojedinačnih korisnika na pet ključnih osobina korisnika društvenih mreža: otvorenost, savjesnost, ekstraverzija, susretljivost, neuroticizam, što se odnosi na Velikih 5 ili model osobnosti OCEAN.

Slika 2. jasno pokazuje kako se proučavaju osobine korisnika, pa tako na osobinu otvorenosti, proučavaju na koji način korisnici uživaju u novome iskustvu, na osobini savjesnosti, proučavaju opredjeljuju li se korisnici na planove i red; ekstraverzija im govori vole li provoditi vrijeme s drugim ljudima, susretljivost im daje na znanje stavljaju li potrebe drugih ljudi ispred svojih potreba te neuroticizam govori brinu li se previše. Rezultat svake osobe, za svaki atribut određen je ispitivanjem lajkova na Facebook stranici svakog korisnika i stvaranjem prediktivnih modela osobnosti na temelju lajkova stranice.



Slika 2. Prikaz modela osobnosti OCEAN

Izvor: preuzeto u cijelosti (Rathi, 2019)

Konačna strategija, bila je inovativna oglasna tehnologija. Ona se odnosi na individualiziranije načine kojima je tvrtka namjeravala doprijeti do korisnika, uključujući Facebook oglase. Nix je ovu tehniku opisao kao suprotnost općem oglašavanju koje podrazumijeva prikazivanje iste poruke milijunima korisnika. Objasnio je kako danas komunikacija postaje sve više ciljana te je individualizirana za svaku pojedinu osobu. Dakle, inovativna oglasna tehnologija, ili kako ju je Nix nazvao, „adresabilna oglasna tehnologija“, oslanjala se na uzimanje rezultata dobivenih nakon korištenja bihevioralne znanosti i analitike podataka i njihovo prikazivanje gledateljima, kroz visoko individualizirane kanale, od kojih su bile i reklame na Facebooku (Nix, 2016).

David Sumpter, profesor primijenjene matematike na Sveučilištu Uppsala u Švedskoj, analizirao je točnost modela Cambridge Analytica u svojoj knjizi „*Outnumbered*“. Sumpter navodi da je Cambridge Analytica koristila regresijski model za predviđanje osobnosti. On opisuje regresijski model kao „model koji uzima podatke koje već imamo o nekoj osobi i koristi ih za predviđanje nečega što o njemu ili njoj ne znamo“ (Sumpter, 2018: 45). Ovisno o osobnosti korisnika, različiti oglasi prikazani su na istu temu u nadi da će različite korisnike uvjeriti u istu poruku. Jedan takav primjer, preuzet iz prezentacije Alexandera Nixa na Concordia summitu (2016), prikazan je u nastavku na slici 3.



High Neuroticism and Conscientious



Closed and Agreeable

Slika 3. Primjer različitih oglasa s istom porukom

Izvor: preuzeto u cijelosti (Nix, 2016)

Motiv oba oglasa je uvjeriti gledatelje da imaju stav u korist drugog amandmana koji ljudima omogućuje pravo na držanje i nošenje oružja. Ljudi s visokim postotkom neokritičnosti i savjesnosti skloni su punoj brizi i preferiraju red, pa bi poruka s lijeve strane imala veći odjek. Zatvoreni i ugodni ljudi stavljaju tuđe potrebe ispred svojih, ali ne uživaju u novim iskustvima, pa bi poruka s desne strane imala veći odjek (Nix, 2016).

Prema McCausland i Schecter (2018), Christopher Wylie, bivši vodeći analitičar u Cambridge Analytici, vjerovao je da to prelazi granicu i da više nije riječ o uvjeravanju, već o manipulaciji. Tvrdio je da je tvrtka radila u „sivoj etičkoj zoni“ i pokušavala manipulirati biračima, zakačivši se za njihove „ranjivosti“. Međutim, Berghel (2018) objašnjava kako korištenje lukavih metoda za potkopavanje izbornih preferencija javnosti nije ništa novo, u Sjedinjenim Državama to je „stalni pratilac izbora“ pa se ne treba iznenaditi korištenjem navodne manipulativne taktike. Koliki je doista bio utjecaj Cambridge Analytice na američke predsjedničke izbore 2016. godine može se razmotriti tijekom uključenosti same tvrtke u kampanje predsjedničkih kandidata.

4.2. Američki predsjednički izbori 2016. godine

Američki izbori za predsjednika 2016. godine odvijali su se između dva glavna protukandidata: Hillary Clinton kao kandidatkinje Demokratske stranke i Donalda Trumpa kao kandidata Republikanske stranke. Prema Mascaro i Lauter (2015), teksaški senator Ted Cruz među prvima je objavio svoju kandidaturu za predsjedničku nominaciju Republikanske stranke. Gambino i Madhvi (2016) navode da je Clinton svoju kandidaturu objavila 12. travnja 2015. godine, dok je Trump to učinio dva mjeseca kasnije te tako ušao u borbu s Cruzom za predsjedničku nominaciju Republikanske stranke.

Dok se Cambridge Analytica danas najviše povezuje s izbornom kampanjom Donalda Trumpa za predsjedničke izbore 2016. godine, Ted Cruz bio je taj koji je prvi koristio usluge tvrtke. Harry Davies (2015) za The Guardian izvijestio je da Cambridge Analytica pomaže u predsjedničkoj kampanji Teda Cruza. Izvješće je sugeriralo da je republikanski kandidat koristio psihološke podatke temeljene na istraživanju koje je obuhvatilo desetke milijuna korisnika Facebooka u pokušaju da dobije prednost nad svojim političkim suparnicima, uključujući Donalda Trumpa.

Prema Meredith (2018), kao odgovor na priču, iz Facebooka su rekli da su, saznajući za curenje podataka, pokušali zabraniti Koganovu aplikaciju i izvršili pravni pritisak na Kogana i Cambridge Analyticu da uklone sve podatke koje su nepropisno pribavili, nakon čega je Facebook tvrdio da su i Kogan i Cambridge Analytica potvrdili da su podatci izbrisani.

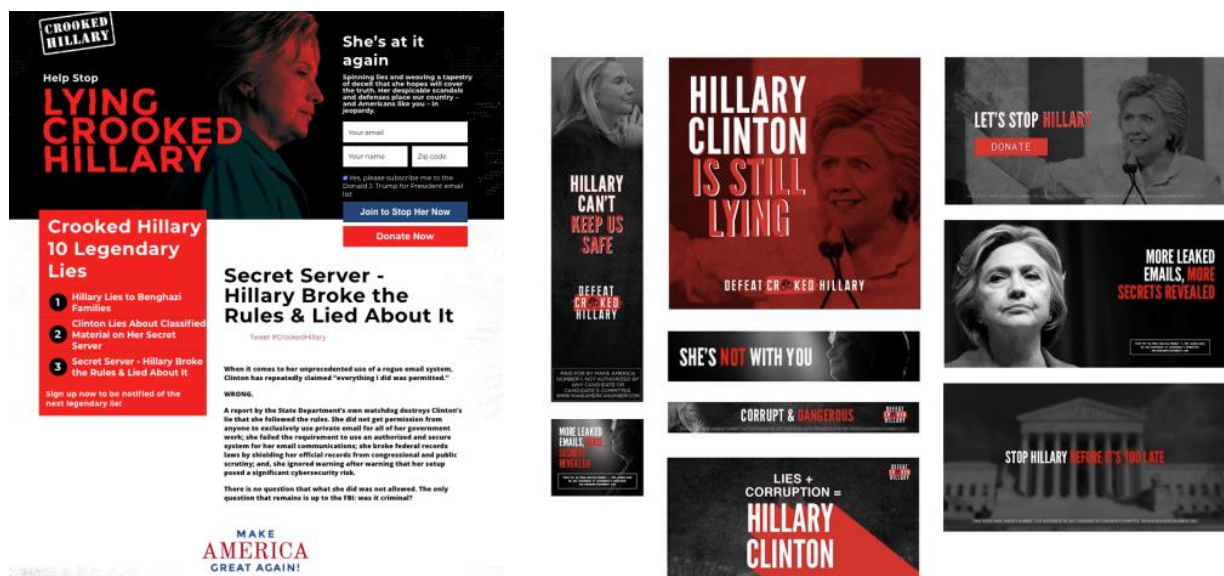
Detrow (2018) navodi da je kampanja Cruza uložila sve u biheviorističku komunikaciju i pristupe velikim podacima u kampanji te je birače podijelila u šest različitih psiholoških profila tijekom ranih predizbora. Kampanja je doprla do birača koje je grupirala kao „plašljive tradicionaliste“ drukčijim porukama nego što je to činila za „temperamentne birače, čak i ako su pozivi, e-mailovi i letci bili o istim Cruzovim stavovima o istim temama.

Napredovanjem kampanje, Cruz je postao skeptičan prema pristupu. Naposljetku je postupno obustavio pokušaje psihološkog profiliranja nakon predizbora u Južnoj Karolini, iako je osoblje Cambridge Analytice ostalo privrženo Cruzovoj kampanji. Prema Detrow (2018), glasnogovornica Cruza Catherine Frazier, u izjavi poslanoj e-poštom, navodi da je Cambridge Analytica sve podatke koje je dobila, koristila u skladu sa zakonom te da će obavljati svoje

operacije u skladu sa svim primjenjivim zakonima i propisima i da imaju sve potrebne dozvole, licence i suglasnosti za vođenje svoje operacije.

Cruz je završio kampanju za predsjednika nakon predizbora u Indiani. S Cruzom koji je ispao iz utrke i Trumpom na putu da predvodi Republikansku listu, Cambridge Analytica počela je raditi za njega kao kandidata Republikanske stranke.

Prema Meredith (2018), uoči predsjedničkih izbora u SAD-u, Trumpov predizborni tim počeo je intenzivno ulagati u Facebook oglase. Ovaj je potez uključivao pomoć Cambridge Analytica, što potvrđuje izvršni direktor tvrtke, Mark Turnbull, koji je rekao za britanski Channel 4 News da je upravo tvrtka odgovorna za video kampanju *Defeat Crooked Hilary* (slika 4.) na Facebooku.



Slika 4. Primjer oglasa protiv Hillary Clinton u kampanji *Defeat Crooked Hillary*

Izvor: preuzeto u cijelosti (Donald J. Trump for President, LyingCrookedHillary.com)

Gershorn i Todd (2018) prenose da je Christopher Wylie u srpnju 2014. godine napustio tvrtku Cambridge Analytica, nakon čega je 2015. osnovao vlastitu tvrtku Eunoia Technologies. Christopher Wylie je za The Guardian i The New York Times otkrio navodnu praksu da je 50 milijuna Facebook profila pokupljeno za Cambridge Analytica, dok je ta brojka kasnije povećana na čak 87 milijuna Facebook profila. Wylie je tvrdio da su podatci prodani Cambridge Analytici korišteni za razvoj „psihografskih“ profila ljudi i isporuku pro-Trump materijala na internetu, što su 2018. godine The Guardian i The New York Times izvijestili, nakon čega su završili dani Cambridge Analytici (Meredith, 2018). Prema Salinas

(2018), Cambridge Analytica je od tada zaniijekala da su Koganovi podatci korišteni u Trumpovoj kampanji.

Prema Meredith (2018), Savezna trgovinska komisija SAD-a (FTC) otvorila je istragu o tome je li Facebook prekršio nagodbu postignutu s agencijom američke vlade 2011. godine o zaštiti privatnosti korisnika. U međuvremenu, američki zakonodavci pozvali su Zuckerberga da svjedoči pred Kongresom.

Dana 21. ožujka 2018., Zuckerberg prekida šutnju te u objavi na Facebooku piše: „Imamo odgovornost zaštititi vaše podatke, a ako to ne možemo, ne zaslužujemo vam služiti. Radim na tome da shvatim što se točno dogodilo i kako se pobrinuti da se to više ne dogodi” (Zuckerberg, 2018). Prema Meredith (2018), Zuckerberg je također najavio da div društvenih medija više neće dopuštati programerima aplikacija pristup podacima svojih korisnika te da će smanjiti količinu informacija koje ljudi moraju predati trećim stranama te je najavio da će Facebook izvršiti reviziju svih aplikacija koje imaju pristup podacima od prije 2014. godine.

Prema Meredith (2018), dva tjedna nakon što su izvještaji objavljeni, Zuckerberg je objavio oglase preko cijele stranice u brojnim britanskim i američkim novinama da bi se ispričao za povredu povjerenja. „Žao mi je što u to vrijeme nismo učinili više. Sada poduzimamo korake kako bismo osigurali da se ovo više ne dogodi,” istaknuo je u oglasima koji se pojavljuju u The New York Timesu, The Washington Postu i The Wall Street Journalu u SAD-u, kao i u britanskom The Observer, The Sunday Times, The Mail on Sunday, Sunday Mirror, Sunday Express i The Sunday Telegraph.

4.3. Referendum za izlazak Velike Britanije iz Europske unije - Brexit

Po pitanju Brexita, odnosno tada potencijalnog izlaska Velike Britanije iz Europske unije, 23. lipnja 2016. godine održan je referendum prema kojemu je većina izašlih birača izabrala da je za izlazak iz Europske unije (Walker, 2021). U javnosti su se pojavile brojne optužbe da je Cambridge Analytica obrađivala podatke građana Velike Britanije te je utjecala na ovaj ishod. Ono što je sigurno, Cambridge Analytica imala je pristup nekim podacima s obzirom na to da ju je trebala angažirati Leave.EU, organizaciju koja je osnovana za političku kampanju usmjerenu na izlazak Velike Britanije iz Europske unije.

Prema Hernu (2019), Brittany Kaiser, bivša direktorica poslovnog razvoja tvrtke Cambridge Analytica, napisala je pismo Damianu Collinsu, tadašnjem predsjedniku Odjela za digitalno, kulturu, medije i sport, u kojemu navodi suradnju Cambridge Analytice s UKIP-om (Stranka nezavisnosti UK, na engleskom UK Independence Party; skraćeno UKIP) i Leave.EU. U pismu navodi da su prikupljeni analizirani podatci koje je obradila Cambridge Analytica, kasnije korišteni u kampanji Leave. EU, bez daljnje pomoći Cambridge Analytice, objašnjava da Cambridge Analytica nikada nije plaćena za posao koji je obavila.

Hern (2019), u članku za The Guardian navodi da je glasnogovornik UKIP-a izjavio da su odbili uslugu Cambridge Analytice jer je bila preskupa i nisu se htjeli baviti onim što je tvrtka radila. Povezanost Cambridge Analytice i Leave.EU ipak postoji, s obzirom na to da je Cambridge Analytica provela analizu u svrhu predlaganja trajnijeg aranžmana. Hern (2019) dalje u članku navodi da je Richard Tice, suosnivač Leave.EU, rekao 2018. godine da Cambridge Analytica nije primila podatke niti je poduzela bilo kakvo modeliranje za Leave.EU. Banks, osnivač Leave.EU, također je potvrdio da Leave.EU nije primio nikakve podatke ili radove od Cambridge Analytice, ali je UKIP Cambridge Analytici dao neke od svojih podataka, a Cambridge Analytica je to analizirala no to nije korišteno u kampanji za Brexit. Banks objašnjava da ga je Cambridge Analytica pokušala natjerati da plati taj posao, ali ga je odbio jer to nije imalo nikakve veze s njima.

Prema Hernu (2019), Collins je odgovorio da postoje važna pitanja koja treba pratiti, posebice jesu li skupovi podataka koje je izradila Cambridge Analytica korišteni u referendumu ili drugim kampanjama i ako jesu, je li to ili nije kršenje zakona o zaštiti podataka za UKIP-ove podatke o biračima.

Iako iz organizacije Leave.EU i UKIP stranke tvrde da Cambridge Analytica nije bila uključena u proces Brexita, tvrtka je sigurno obrađivala podatke koje je prosljedila stranka. Ova su dva događaja, izbori 2016. u SAD-u i Brexit u Velikoj Britaniji, osvijestili korisnike društvenih mreža o zluporabi privatnosti i samom utjecaju društvenih mreža na politiku.

Nakon ovih događaja, pokrenuti su brojni pokreti protiv Facebooka, kao na primjer pokret *#DeleteFacebook*, ali i kampanje kojima su ljudi htjeli osvijestiti korisnike društvenih mreža na sigurnost, kao na primjer kampanja *#OwnYourData*. Kampanju je osmislila Brittany Kaiser, koja je nakon odlaska iz Cambridge Analytice pokrenula peticiju da Facebook promijeni svoja pravila i da svojim korisnicima osigura veću moć i kontrolu nad svojim podacima koje ona naziva imovinom i vlasništvom korisnika. Uz hashtag, Kaiser je također

otvorila i Own Your Data Foundation za promicanje povećanja obrazovanja o digitalnoj inteligenciji (Own Your Data Foundation, 2020).

Prema McAuley (2019), Povjerenik za informiranje u Ujedinjenom Kraljevstvu kaznio je tvrtku Facebook s maksimalnom kaznom od 500.000 funti, upozorio da je „demokracija pod prijetnjom“ te pozvao na „etičku pauzu“ u političkim oglasnim kampanjama mikrociljanja. Prema Ma i Gilbert (2019), Savezna trgovinska komisija SAD-a, osim što je naredila Facebooku da mora platiti kaznu od 5 milijardi dolara zbog tvrdnji da je tvrtka pogrešno postupala s korisničkim podacima, nametnula je i brojna ograničenja tvrtki.

Prema McAuley (2019), Cambridge Analytica je 2018. godine pokrenula stečajni postupak i ugasila svoje poslovanje. Razlozi su, navode Solon i Laughland (2018), negativna slika u medijima o tvrtki koja je u konačnici ostala bez klijenata i kupaca. Iako Cambridge Analytica više ne postoji, Solon i Laughland dalje navode da je tim koji stoji iza tvrtke osnovao novu tvrtku pod nazivom Emerdata, a čiji su direktori Alexander Nix zajedno s drugim rukovoditeljima iz SCL grupe, ali i kćeri milijardera Roberta Mercera.

5. ZAKLJUČAK

Glavna tema ovoga rada bila je zlouporaba osobnih podataka korisnika društvenih mreža i cilj je bio prikazati kako se to čini u političke svrhe na primjeru poznatoga „Slučaja Cambridge Analytica“. Umiješanost te britanske analitičke tvrtke u dvama važnim političkim događajima 2016. godine; predsjedničkim izborima u SAD-u i referendumu za izlazak Velike Britanije iz Europske unije (Brexit), jasno pokazuje da se zluporabljuju osobni podaci korisnika društvenih mreža te kako se na taj način može utjecati na ishode određenih političkih događaja i ugroziti demokratske sustave pojedinih država.

Društvene mreže uveliko prikupljaju podatke o svojim korisnicima, koje u konačnici prodaju trećim stranama, odnosno oglašivačima. Zato je u Europskoj uniji uvedena Opća uredba o zaštiti podataka ili GDPR, dok u SAD-u ne postoji niti jedan sveobuhvatan savezni zakon koji regulira privatnost podataka. Lažne su vijesti sveprisutne jer su društveni mediji ključni za širenje neprovjerenih informacija, a koje pojedinci smatraju vjerodostojnima i pouzdanima jer se slažu s njihovim prethodnim uvjerenjima. Ključni problem kod lažnih vijesti je moguća manipulacija birača koji svoj glas mogu temeljiti na dezinformaciji, što može utjecati na izborne rezultate.

Tvrtka Cambridge Analytica koristila je osobne podatke Facebook korisnika kršeći Facebookove uvjete pružanja usluga. Tvrtka je pomoću personaliziranih, ciljanih oglasa uvjeravala mnogo različitih ljudi s različitim osobnostima da imaju isto mišljenje o određenom pitanju ili kandidatu. Kampanja Donalda Trumpa veže uz tvrtku Cambridge Analytica te je neupitno da je tvrtka imala utjecaj na njegovu pobjedu na izborima. Iako se za Brexit slučaj ne može sa sigurnošću potvrditi da je Cambridge Analytica imala utjecaj s obzirom na to da se nigdje službeno ne navodi suradnja tvrtke, Cambridge Analytica je obrađivala određene podatke i UKIP stranka je imala uvid u te podatke.

Iz svega navedenog, povezujući Goebbelsov citat s početka uvoda i sve zaključke ovoga rada, jasno je vidljivo da će i danas neka informacija, istinita ili lažna, prezentirana pravim metodama, točno ciljanim korisnicima, postati opasno političko oružje. Kako je objasnio Nix objasnio, danas komunikacija postaje sve više ciljana i individualizira se za svaku pojedinu osobu. Takva ciljana komunikacija traži osobne podatke o svimaponasob, a najbolji izvor osobnih podataka upravo su društvene mreže. Osim što se podatci na društvenim mrežama mogu vrlo jednostavno zlouporabiti, društvene su mreže postale platforme za širenje lažnih vijesti i dezinformacija. Ovo se informacijsko razdoblje razvija velikom brzinom i paralelno s tim, događaju se ovakvi problemi. Upravo zbog nemogućnosti praćenja i predviđanja svih problema koje novo razdoblje donosi, ljudima je potrebno medijsko i informacijsko opismenjavanje. Iako je internet postao sastavnim dijelom čovjekova života, ono nije sigurno područje i potrebno je biti oprezan tijekom korištenja, a osobito tijekom ostavljanja osobnih podataka. Ako su nastankom novina ljudi počeli masovno učiti čitati, tako i razvitkom interneta ljudi moraju naučiti koristiti sve što ono nudi, ali na pravilan i koristan način koji neće štetiti drugima. Nažalost, kako je prikazano i u ovom radu, ima mnogo suprotnih slučajeva, posebice na području politike. Berghel (2018) je objasnio da korištenje lukavih metoda za potkopavanje izbornih preferencija javnosti nije ništa novo te da se ne treba iznenaditi korištenjem manipulativnih taktika u politici. Ako je već politika takva da će manipulacijom dolaziti do svojih ciljeva, onda je građane potrebno zaštititi od toga. To se dugoročno može učiniti razvojem i povećanjem razine medijske i informacijske pismenosti kod građana. Time bi oni osvijestili opasnosti koje mediji nose, ali i naučili kritički analizirati svaki medijski sadržaj, proučavati informacije iz više različitih izvora, biti svjesni tko sve i u koje svrhe koristi njihove osobne podatke te naučili zaštititi svoje osobne podatke od zlouporabe.

6. LITERATURA

Knjige, članci i zbornici radova:

1. Allcott, H., i Gentzkow, M. (2017) *Social Media and Fake News in the 2016 Election*. Journal of Economic Perspectives. Volume 31, Broj 2. Stranice: 211–236. URL: <https://web.stanford.edu/~gentzkow/research/fakenews.pdf> [pristupljeno 16.07.2022.]
2. Asur, S. i Huberman, B.A. (2010) *Predicting the Future with Social Media*. International Conference on Web Intelligence and Intelligent Agent Technology, Toronto, 492-499. URL: <https://doi.org/10.1109/WI-IAT.2010.63> [pristupljeno 10.09.2022.]
3. Bakshy, E., Messing, S., i Adamic, L. A. (2015) *Exposure to ideologically diverse news and opinion on Facebook*. Political science. Science 348(6239): 1130–32. URL: https://www.researchgate.net/publication/276067921_Political_science_Exposure_to_ideologically_diverse_news_and_opinion_on_Facebook [pristupljeno 16.07.2022.]
4. Balmas, M. (2014) *When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism*. Communication Research, 41(3), 430-454. URL: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.842.111&rep=rep1&type=pdf> [pristupljeno 17.07.2022.]
5. Berghel, H. (2018) *Malice Domestic: The Cambridge Analytica Dystopia*. Computer: vol. 51, no. 5. University of Nevada, Las Vegas. URL: http://www.berghel.net/col-edit/out-of-band/may-18/oob_5-18.pdf [pristupljeno 22.07.2022.]
6. Bode, L., i Vraga, E. K. (2015) *In related news, that was wrong: The correction of misinformation through related stories functionality in social media*. Journal of Communication, 65, 619-638. URL: <https://doi.org/10.1111/jcom.12166> [pristupljeno 16.07.2022.]
7. Boyd, D. M., i Ellison, N. B. (2008) *Social Network Sites: Definition, History, and Scholarship*. Journal of Computer-Mediated Communication, 13, 210-230. URL: <https://academic.oup.com/jcmc/article/13/1/210/4583062> [pristupljeno 10.09.2022.]
8. Campbell, W. J. (2001) *Yellow journalism: Puncturing the myths, defining the legacies*. Westport, CT: Praeger.

9. Downey, J., i Fenton, N. (2003) *New media, counter publicity and the public sphere*. *New Media & Society*, 5(2), 185-202. URL: <https://journals.sagepub.com/doi/10.1177/1461444803005002003> [pristupljeno 15.07.2022.]
10. Hall, S. (1989) *The Structured Communication of Events*. In D. Potter (Ed.), *Society and the Social Sciences: An Introduction*. Stranice: 269-289. London: Routledge
11. Howard, P. i Bradshaw, S. (2019) *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. URL: <https://www.oii.ox.ac.uk/news-events/news/use-of-social-media-to-manipulate-public-opinion-now-a-global-problem-says-new-report/> [pristupljeno 10.09.2022.]
12. Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., i Nerur, S. (2017) *Advances in Social Media Research: Past, Present and Future*. *Information Systems Frontiers*, 1-28. URL: <https://link.springer.com/article/10.1007/s10796-017-9810-y> [pristupljeno 10.09.2022.]
13. Molina, M. D., Sundar, S. S., Le, T., i Lee, D. (2019) „Fake News” Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content. Penn State University, University Park, PA, USA. *American Behavioral Scientist* 2021, Vol. 65(2) 180–212
14. Pickard, V. (2016) *Media Failures in the Age of Trump*. *The Political Economy of Communication*, 4(2), 118-122. University of Pennsylvania. URL: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1778&context=asc_papers [pristupljeno 15.07.2022.]
15. Rodgers, N. S. (2020) *Understanding Personal Data in the World of Social Media*. Završni projekt dodiplomskog studija. Utah State University. URL: <https://digitalcommons.usu.edu/honors/476> [pristupljeno: 30.06.2022.]
16. Southwell, B. G., Thorson, E. A., i Sheble, L. (2017) *The persistence and peril of misinformation: Defining what truth means and deciphering how human brains verify information are some of the challenges to battling widespread falsehoods*. *American Scientist*, 105(6). Stranice: 372-375. URL: <https://doi.org/10.1511/2017.105.6.372> [pristupljeno 18.07.2022.]
17. Sumpter, D. J. T. (2018) *Outnumbered: from Facebook and Google to Fake News and Filter-Bubbles — the Algorithms That Control Our Lives*. Bloomsbury Sigma.

Internetski izvori:

1. Brook, C. (2020) *Google Fined \$57M by Data Protection Watchdog Over GDPR Violations*. DATA INSIDER: Digital Guardian's Blog. URL: <https://digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations> [10.09.2022.]
2. Cadwalladr, C. (2017) *The great British Brexit robbery: how our democracy was hijacked*. The Guardian: The Observer. URL: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy> [pristupljeno 19.07.2022.]
3. Cadwalladr, C. i Graham-Harrison, E. (2018) *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian: The Observer URL: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [pristupljeno 20.07.2022.]
4. Carnahan D. (2020) *Caroline Brooks: The truth behind fake news and politics on social media*. URL: <https://msutoday.msu.edu/news/2020/the-truth-behind-fake-news-and-politics-on-social-media> [posjećeno 15.07.2022.]
5. Crain, R. (2017) *Fake news could make advertising more believable*. Advertising Age. URL: <https://adage.com/article/rance-crain/fake-news-make-advertising-believable/307836> [pristupljeno 15.07.2022.]
6. Davies, H. (2015) *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. The Guardian. URL: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> [pristupljeno: 23.07.2022.]
7. Detrow, S. (2018) *What Did Cambridge Analytica Do During The 2016 Election?* NPR (National Public Radio). URL: <https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election> [pristupljeno 20.07.2022.]
8. e-Građani. *Što je pravo na zaštitu osobnih podataka i zašto je važno?* URL: <https://gov.hr/hr/sto-je-pravo-na-zastitu-osobnih-podataka-i-zasto-je-vazno/1866> [pristupljeno 11.07.2022.]

9. Europska Komisija (2018) *What is personal data?* URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [pristupljeno 30.06.2022.]
10. Federal Trade Commission (1998) *Children's Online Privacy Protection Rule ("COPPA")*. URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> [pristupljeno 14.07.2022.]
11. Federal Trade Commission (2018) *Fair Credit Reporting Act*. URL: <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act> [pristupljeno 14.07.2022.]
12. Federal Trade Commission. *O FTC-u (eng. About the FTC)*. URL: <https://www.ftc.gov/about-ftc> [pristupljeno 13.07.2022.]
13. Federal Trade Commission (2022) *Gramm-Leach-Bliley Act*. URL: <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act> [pristupljeno 14.07.2022.]
14. Gambino, L. i Madhvi, P. (2016) How we got here: a complete timeline of 2016's historic US election. The Guardian. URL: <https://www.theguardian.com/us-news/2016/nov/07/us-election-2016-complete-timeline-clinton-trump-president> [pristupljeno 10.09.2022.]
15. GDPR Informer (2018) *Vodič kroz GDPR za početnike*. URL: <https://gdprinformer.com/hr/vodic-kroz-gdpr> [pristupljeno 13.07.2022.]
16. General Data Protection Regulation (GDPR) (2018) URL: <https://gdpr-info.eu/> [pristupljeno 13.07.2022.]
17. George, A. (2022) *Twitter apologizes for personal data misuse with timeline alert*. Digital Trends. URL: <https://www.digitaltrends.com/social-media/twitter-alerts-users-of-use-of-personal-data-for-tailored-ads/> [pristupljeno 10.09.2022.]
18. Google (2022) *Googleovi uvjeti pružanja usluge*. URL: <https://policies.google.com/terms?hl=hr> [pristupljeno 11.07.2022.]
19. Health Information Privacy (2021) *The HIPAA Privacy Rule*. URL: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> [pristupljeno 14.07.2022.]
20. Hern, A. (2019) *Cambridge Analytica did work for Leave.EU, emails confirm*. The Guardian. URL: <https://www.theguardian.com/uk-news/2019/jul/30/cambridge-analytica-did-work-for-leave-eu-emails-confirm> [pristupljeno 02.08.2022.]

21. Isaac, M., Kang, C. (2020) *Facebook Says it Won't Back Down from Allowing Lies in Political ads*. URL:<https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html> [pristupljeno 11.07.2022.]
22. Cambridge Online Dictionary (2018) *Fake news*. URL:<https://dictionary.cambridge.org/us/dictionary/english/fake-news> [pristupljeno 18.07.2022.]
23. Ma, A. i Gilbert, B. (2019) *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now*. Insider. URL:<https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3> [pristupljeno 10.09.2022.]
24. Mascaro, L. i Lauter, D. (2015) *Texas Republican Sen. Ted Cruz is running for president*. Los Angeles Times. URL:<https://www.latimes.com/nation/politics/politicsnow/la-na-pn-ted-cruz-presidential-bid-20150322-story.html> [pristupljeno 10.09.2022.]
25. McAuley E. (2019) *WHAT HAPPENED WITH CAMBRIDGE ANALYTICA? The scandal that changed the global data landscape*. Rightly, Champions of Data. URL:<https://right.ly/our-views-and-opinions/cambridge-analytica-explained/> [pristupljeno 10.09.2022.]
26. McCausland, P., i Schecter, A. (2018) *Cambridge Analytica harvested data from millions of unsuspecting Facebook*. NBCUniversal News. URL: www.nbcnews.com/news/us-news/cambridge-analytica-harvested-data-millions-unsuspecting-facebook-users-n857591 [pristupljeno 22.07.2022.]
27. Meta tvrtka (2022) *Facebook oglasavanje*. URL: <https://www.facebook.com/business/ads> [pristupljeno 07.07.2022.]
28. Meredith, S. (2018) *Facebook – Cambridge Analytica: a timeline of the data hijacking scandal*. The CNBC. URL:<https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> [pristupljeno 20.07.2022.]
29. Narodne novine (2012) *Zakon o zaštiti osobnih podataka*. Zagreb: Narodne novine d.d., 106/2012. URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html [pristupljeno: 10.09.2022.]
30. Nix, A. (2016) *The Power of Big Data and Psychographics*. Concordia Annual Summit. Youtube. URL: <https://www.youtube.com/watch?v=n8Dd5aVXLCc> [pristupljeno 21.07.2022.]

31. Službeni list Europske unije (eng. *Official Journal of the European Union*) (2016) *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. URL:<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [pristupljeno 13.07.2022.]
32. Osano (2022) *Data privacy laws: What you need to know in 2022*. URL:<https://www.osano.com/articles/data-privacy-laws> [pristupljeno 13.07.2022.]
33. Own Your Data Foundation (2020) Own Your Data Foundation - About the foundation. URL: <https://ownyourdata.foundation/> [pristupljeno 05.08.2022.]
34. Rathi, R. (2019) *Effect of Cambridge Analytica's Facebook Ads on the 2016 US Presidential Election. Towards Data Science*. URL: <https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d>. [pristupljeno 19.07.2022.]
35. Salinas, S. (2018) *Cambridge Analytica says Wylie is 'misrepresenting himself and the company' in Facebook data scandal*. CNBC. URL: <https://www.cnbc.com/2018/03/19/facebook-data-scandal-cambridge-analytica-denies-whistleblowing-claim.html> [pristupljeno: 02.08.2022.]
36. Sardarizadeh, S. (2022) *Ukraine war: False TikTok videos draw millions of views*. BBC News. URL: <https://www.bbc.com/news/60867414> [pristupljeno 11.09.2022.]
37. Smith, A. i Anderson, M. (2018) *A majority of Americans use Facebook and YouTube, but young adults are especially heavy users of Snapchat and Instagram*. Pew Research Centermarch. URL:<https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/> [pristupljeno: 10.09.2022.]
38. Solon, O. i Laughland, O. (2018) *Cambridge Analytica closing after Facebook data harvesting scandal*. The Guardian. URL: <https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say> [pristupljeno 10.09.2022.]
39. Todd, S. i Gershgorn, D.(2018) *The Cambridge Analytica scandal is wildly confusing. This timeline will help*. Quartz. URL: <https://qz.com/1240039/the-cambridge-analytica-scandal-is-confusing-this-timeline-will-help/> [pristupljeno 19.07.2022.]
40. Walker, N. (2021) *Brexit timeline: events leading to the UK's exit from the European Union*. UK Parliament, House of Commons Library. URL:

<https://commonslibrary.parliament.uk/research-briefings/cbp-7960/>[pristupljeno 02.08.2022.]

41. Lee, J. M. (2020) *How Fake News Affects U.S. Elections?* Sveučilište Centralna Florida (University of Central Florida) URL: <https://www.ucf.edu/news/how-fake-news-affects-u-s-elections/> [pristupljeno 18.07.2022.]
42. Zuckerberg, M. (2018) Objava na Facebook profilu, 21. 3. 2018. URL: [facebook.com/zuck/posts/10104712037900071](https://www.facebook.com/zuck/posts/10104712037900071) [pristupljeno: 02.08.2022.]

7. PRILOZI

Slika 1. Primjer prenošenja poruke biheviorističkom komunikacijom	17
Slika 2. Prikaz modela osobnosti OCEAN	19
Slika 3. Primjer različitih oglasa s istom porukom	20
Slika 4. Primjer oglasa protiv Hillary Clinton u kampanji <i>DefeatCrookedHillary</i>	22