Zloupotreba osobnih e-podataka: studija slučaja na primjeru Cambridge Analytica

Rašić, Josip

Master's thesis / Diplomski rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:928283

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-11-23**

Repository / Repozitorij:

University North Digital Repository

SVEUČILIŠTE SJEVER
SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 164/OJ/2020

ZLOUPOTREBA OSOBNIH E-PODATAKA: STUDIJA SLUČAJA NA PRIMJERU CAMBRIDGE ANALYTICA

Josip Rašić

Varaždin, ožujak 2020.

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij Odnosi s javnostima

DIPLOMSKI RAD br. 164/OJ/2020

ZLOUPOTREBA OSOBNIH E-PODATAKA: STUDIJA SLUČAJA NA PRIMJERU CAMBRIDGE ANALYTICA

Student:
Josip Rašić, 0739/336D

Mentor:
izv. prof. dr. sc. Ljerka Luić

Varaždin, ožujak 2020.

PRIJAVA I ZADATAK DIPLOMSKOG RADA

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

UNIVERSITY NORTH

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL Odjel za odnose s javnostima

STUDIJ diplomski sveučilišni studij Odnosi s javnostima

PRISTUPNIK Josip Rašić | MATIČNI BROJ 0739/336D

DATUM 10. 2. 2020. | KOLEGIJ OJ i Internet

NASLOV RADA Zloupotreba osobnih e-podataka: studija slučaja na primjeru Cambridge Analytica

NASLOV RADA NA ENGL. JEZIKU Misuse of personal e-data: a case study on the example of Cambridge Analytica

MENTOR dr. sc. Ljerka Luić | ZVANJE izvanredni profesor

ČLANOVI POVJERENSTVA

1. prof. dr. sc. Majda Tafra Vlahović - predsjednica
2. doc. dr. sc. Ana Globočnik Žunac - članica
3. izv. prof. dr. sc. Ljerka Luić - mentorica
4. doc. dr. sc. Gordana Lesinger - zamjenska članica
5.

Zadatak diplomskog rada

BROJ 164/OJ/2020

OPIS

U uvodnom dijelu rada potrebno je elaborirati teorijski okvir problematike kojom se rad bavi, obrazložiti cilj i predmet istraživanja, izvore podataka i metodologiju istraživanja, iznijeti prikaz strukture rada kroz kratki opis sadržaja rada te navesti istraživačko pitanje.

U poglavljima koja slijede treba iznijeti (1) teorijske aspekte upravljanja informacijama (2) opisati bitna obilježja zaštite osobnih podataka sagledanih s aspekta (3) zlouporabe. Razradu teme treba fokusirati na istraživačko pitanje "Kako detektirati potencijalne oblike zlouporabe osobnih e-podataka?" cilj kojeg je (4) analizom sadržaja objava na digitalnim platformama na primjeru Cambridge Analytica-a kreirati informacijske konstrukte značajne za detekciju zlouporaba osobnih e-podataka. U drugom dijelu rada potrebno je (5) opisati metodologiju istraživanja, (6) iznijeti hipoteze te (7) analizirati i opisati dobivene rezultate.

Glavne spoznaje do kojih se došlo proučavanjem literature i provedbom istraživanja potrebno je iznijeti u kratkom zaključku na kraju rada, kvaliteti kojeg će doprinijeti prijedlog daljnjih srodnih istraživanja.

ZADATAK URUČEN 18. 02. 2020. | POTPIS MENTORA

SVEUČILIŠTE SJEVER

SAŽETAK

Sukladno razvoju informacijsko-komunikacijske tehnologije, u suvremeno doba život bez internet platforme je nezamisliv. Paralelno s povećanjem korisnika interneta i razvojem društvenih mreža, rasla je i količina korisnika istih. Zabrinjavajuća je činjenica da svaka društvena mreža potražuje određene osobne podatke korisnika kako bi se mogli njome koristiti, ali je upravo zaštita osobnih podataka i način na koji se upotrebljavaju odnosno zloupotrebljavaju upitna. Korisnici koji se smatraju vlasnicima svojih osobnih podataka često nisu svjesni, niti upozoreni, kako će se i koji njihovi podaci koristiti. Upravo radi toga predstavljaju osjetljivu skupinu nad kojima se mogu vršiti ilegalni postupci. Zato u današnje vrijeme zaštita podataka u digitalnom svijetu predstavlja prioritet. Ovaj rad se osim teorijskog razmatranja bavi slučajem tvrtke Cambridge Analytica i političkim kampanjama koje su zloupotrebom podataka korisnika društvene mreže *Facebook* manipulirale rezultatima kampanja.

Ključne riječi: Internet, osobni e-podaci, zloupotreba, upravljanje informacijama

SUMMARY

In the modern world, along with the information and communications technologies, life without Internet is unimaginable. With the growth of Internet users and development on social media networks, the number of social media users is also rising. Social media is collecting sensitive personal data about it's users and the biggest concern arises from the privacy and security issues of that data. Users that think of themselves as owners of their personal information, are often not aware, or warned about which of their personal data is being used and how, which makes them sensitive target group for ilegal actions with them as victims. That is the reason why data privacy protection is priority in today's digital world. This paper's theme, besides theoretical approach, is Cambridge Analytica's case of illegal harvesting personal data through *Facebook* in order to manipulate the results of political campaigns.

Key words: Internet, personal e-data, misuse, information management

SADRŽAJ:

1. UVOD 1
2. TEORIJSKI OKVIR 5
2.1. Informacije i podaci 5
2.2. Društvene mreže kao glavni izvori podataka u digitalnom svijetu 8
2.3. Zaštita privatnosti u digitalnom svijetu 13
3. ZLOUPOTREBA OSOBNIH PODATAKA 15
3.1. Zakonodavni okviri zlouporabe osobnih podataka 15
3.2. Slučajevi narušavanja sigurnosti osobnih podataka u svijetu 19
4. SLUČAJ CAMBRIDGE ANALYTICA 21
4.1. Općenito o poduzeću Cambridge Analytica 21
4.2. Političke kampanje povezane s poduzećem Cambridge Analytica 24
5. MATERIJAL I METODE 27
5.1. Istraživački materijal 27
5.2. Metode istraživanja 27
5.3. Postupak provedbe istraživanja 27
5.4. Metode obrade podataka 27
6. REZULTATI 28
6.1. Cilj i predmet istraživanja 28
6.2. Istraživačko pitanje 28
6.3. Opis rezultata istraživanja 28
6.4. Sažetak rezultata istraživanja 35
7. DISKUSIJA 36
7.1. Elaboracija hipoteza 36
7.2. Interpretacija rezultata istraživanja 37
7.3. Kritički osvrt, primjena rezultata, preporuke 38
8. ZAKLJUČAK 39
9. LITERATURA 40
POPIS ILUSTRACIJA 45
IZJAVA O AUTORSTVU I SUGLASNOST ZA JAVNU OBJAVU ... **Error! Bookmark not defined.**

1. UVOD

Živimo u svijetu u kojem su informacije postale glavni kapital, a ljudi najvrjedniji resurs. Međutim, s razvojem tehnologije i pojavom digitalnog svijeta informacije su postale glavno oružje i instrument za manipulaciju ljudi. Sve veći broj ljudi svih demografskih skupina i obilježja aktivno je na internetu i služi se barem jednom od dostupnih društvenih mreža, koje su danas postale uobičajen dio života ljudi. Društvene mreže podrazumijevaju internet platformu s ciljem povezivanja ljudi na bilo kojoj zajedničkoj osnovi uz učestalo dijeljenje osobnih podataka korisnika. Od pojave društvenih mreža u ranim 2000. godinama, platforme društvenih mreža na internetu bilježe eksponencijalan rast, od kojih se najviše ističu *Facebook*, *Instagram*, *Twitter* i *SnapChat*. Zbog ogromne količine osobnih podataka koja se generira putem društvenih mreža, postavlja se pitanje o sposobnosti spomenutih platformi da sigurno pohranjuju i upravljaju osobnim podacima njihovih korisnika. Do koje razine administratori društvenih mreža mogu imati uvid u te osobne podatke novo je etičko pitanje u današnjem društvu, a legalnost i granice kršenja privatnosti su brige koje za sobom nosi tehnološko i digitalno doba.

Društvena mreža je socijalna struktura koja se sastoji od socijalnih aktera (osoba ili organizacija), skupova dijadskih veza i drugih socijalnih interakcija. Potencijalna narušavanja privatnosti unutar takve socijalne strukture su korištenje osobnih podataka u treće svrhe, prodavanje osobnih podataka trećim stranama ili prezentiranje osobnih podataka javno na internetu. Problemi vezani uz sigurnost i privatnost osobnih podataka na društvenim mrežama proizlaze iz abnormalne količine informacija koje te platforme procesuiraju svaki dan. Značajke koje društvene mreže pružaju svojim korisnicima poput slanja poruka i pozivnica, objavljivanja slika ili korištenja aplikacija najčešće su upravo i izvor iz kojega se mogu crpiti osobne informacije korisnika.

Često sama tehnologija koja stoji iza procesuiranja tih informacija bude i uzrok narušavanja privatnosti kao što je bio slučaj s društvenom mrežom *Facebook*. Naime, u sučelju za programiranje aplikacije *Facebook* bila je otkrivena velika rupa vezana uz sigurnost osobnih podataka prikupljenih putem te platforme. Istraživači koji su radili na tom slučaju, došli su do zaključka kako treća strana ima puno veći uvid u osobne informacije nego što je potrebno za njen rad u kreiranju aplikacijskog sučelja za *Facebook* (Gross i Acquisti, 2005: 71-80).

Zlouporaba podataka i računalna sigurnost dvije su teme koje stoje rame uz rame kada se govori o zaštiti osobnih podataka u digitalnom svijetu. Kada se govori o zlouporabi podataka, treba razlučiti dvije vrste prikupljenih osobnih podataka – prva vrsta su podaci koji su stečeni na legalan način, ali su kasnije zloupotrebljavani, te druga skupina u koju spadaju svi osobni podaci stečeni na ilegalan način, bilo da je riječ o prikupljanju podataka bez pristanka pojedinaca ili o direktnoj krađi osobnih podataka hakiranjem. Krađa podataka podrazumijeva prikupljanje podataka bilo kojom vrstom računalnog napada, što znači da pojedinci nisu svjesni da se njihovi podaci prikupljaju ili modificiraju te je takav tip zločina pokriven Zakonom o informacijskoj sigurnosti. U slučajevima kada se radi o prikupljanju osobnih podataka s pristankom pojedinaca i kada su pojedinci svjesni u koju svrhu će se ti podaci koristiti, a ti podaci zatim budu zlouporabljeni i korišteni na načine koji nisu dozvoljeni, tada na snagu stupaju međunarodni zakoni *Data Protection Act (DPA)* i *General Data Protection Regulation (GDPR)* (Heshmaty, 2019*).*

Izraz „zlouporaba podataka“ obično se upotrebljava za spomenuti scenarij u kojem su osobni podaci prvenstveno dani s pristankom pojedinaca u određenu svrhu, ali su ti podaci ipak korišteni u druge svrhe, odnosno bili zloupotrebljavani direktno od tvrtke koja je primarno pokupila te podatke ili od treće strane. Takva vrsta zlouporabe podataka ujedno je i tema ovog diplomskog rada i istraživanja (Heshmaty, 2019).

Do danas je izbilo mnogo sudskih tužbi protiv velikih poduzeća i organizacija na osnovi narušavanja sigurnosti i zloupotrebe osobnih podataka stanovništva. Jedan od takvih slučajeva je i afera najpoznatije društvene mreže *Facebook* i poduzeća koje se bavi prikupljanjem i obradom podataka Cambridge Analytica. Afera je nastupila 2018. godine kada su u javnost procurile informacije o zlouporabi osobnih podataka korisnika *Facebooka* od strane poduzeća Cambridge Analytica s ciljem manipuliranja javnosti u društveno-političkim događajima kao što su predsjednički izbori u SAD-u i referendum Velike Britanije o izlasku iz EU, što je i glavna tema diplomskog rada.

Cambridge Analytica bivša je britanska politička konzultantska tvrtka koja se koristila pronevjerom digitalne imovine, prikupljanjem i posredovanjem osobnih podataka te analizom osobnih podataka kako bi sudjelovala u kreiranju strategijske komunikacije u političkim izborima. Sve je započelo 2013. godine s nekoliko sestrinskih poduzeća, dok se na kraju nije otvorilo poduzeće Cambridge Analytica s direktorom Alexanderom Nixom. Cambridge Analytica je pod njegovim vodstvom sudjelovala u 44 političke utrke u SAD-u 2014. godine. U 2015. godini tvrtka je bila zadužena za obradu podataka za potrebe predsjedničke kampanje Teda Cruza, a u 2016. godini Cambridge Analytica radila je za Donalda Trumpa i njegovu predsjedničku kampanju te za organizaciju Leave EU koja je zagovarala izlaz Velike Britanije iz Europske Unije na referendumu te godine. Uloga Cambridge Analytica u svim tim kampanjama kontroverzna je sama po sebi te je bila predmetom sudske tužbe u SAD-u i Ujedinjenom Kraljevstvu na kojem su politički znanstvenici preispitivali tvrdnje i metode rada Cambridge Analytice (Scott, 2018).

U 2018. godini podigla se medijska prašina oko poslovanja Cambridge Analytice kada se na sudu utvrdilo da je tvrtka prikupljala i iskorištavala osobne podatke 87 milijuna korisnika *Facebooka* na ilegalan način (Salinas, 2018). Slučaj je privukao veću pozornost uslijed izdavanja knjige i svjedočenja bivšeg zaposlenika Cambridge Analytice o kršenju zaštite osobnih podataka.

Prema njegovom svjedočenju, za tvrtku je podatke prikupljao Amerikanac ruskoga podrijetla Aleksandr Kogan koji je radio na Sveučilištu u Cambridge-u. Kogan je izradio *Facebook* aplikaciju koja ja bila neka vrsta kviza. Aplikacija, osim što je prikupljala podatke o ljudima koji su koristili kviz, već je i prikupljala podatke o svim prijateljima tih korisnika na društvenoj mreži *Facebook*. Rezultat tužbe je zatvaranje tvrtke i kazna *Facebooku* od 5 milijardi dolara za osudu da je obmanjivao korisnike o privatnosti njihovih podataka. To je ujedno bila i najveća kazna za takvu vrstu prekršaja u SAD-u (Rehman, 2019: 1-11).

Problem nastaje kada se krene dublje tražiti odgovor na pitanje radi li se o pogreškama u izradi i implementaciji aplikacije i programa, ili se radi o namjernom kreiranju takve aplikacije. Nadalje, postavlja se pitanje tko je odgovoran za nedostatak zaštite privatnosti, a uvid u mogući odgovor na to pitanje je možda činjenica da postoje marketinška poduzeća koja su izgrađena na temelju ideje da treće strane mogu dobiti pristup podacima i informacijama o korisnicima na *Facebooku*.

2. TEORIJSKI OKVIR

Osobni podaci mogu se usporediti s naftom – oni pokreću najprofitabilnije korporacije danas, baš kao što su to nekad činila fosilna goriva. Međutim, vlasnici tih osobnih podataka često znaju veoma malo o tome kako se njihovi podaci koriste, tko ih prikuplja, tko im može pristupiti i koliko oni vrijede. Svaki dan stotine poduzeća prikupljaju činjenice o internet korisnicima, neke intimnije, neke ne, bez da oni to znaju. Ti podaci tada odlaze u akademska istraživanja, hakerima, vladama, ali i raznim poduzećima u razne svrhe (Matsakis, 2019).

2.1. Informacije i podaci

Osobnim podacima smatraju se sve informacije vezane uz identificirano ljudsko biće. Različiti dijelovi informacija koji zajedno mogu voditi do identifikacije određene osobe, također se smatraju osobnim podacima. Osobni podaci koji su neidentificirani, enkriptirani ili pseudonimizirani, ali se mogu iskoristiti za reidentifikaciju osobe, također se smatraju osobnim podacima. Međutim, osobni podaci koji su anonimni, odnosno ne mogu se upotrijebiti za identifikaciju određene osobe, ne smatraju se osobnim podacima. Kako bi se neki podaci smatrali anonimnima, anonimizacija mora biti ireverzibilna.[1] Primjeri tipičnih osobnih podataka su (European Comission: *What is personal data?*):

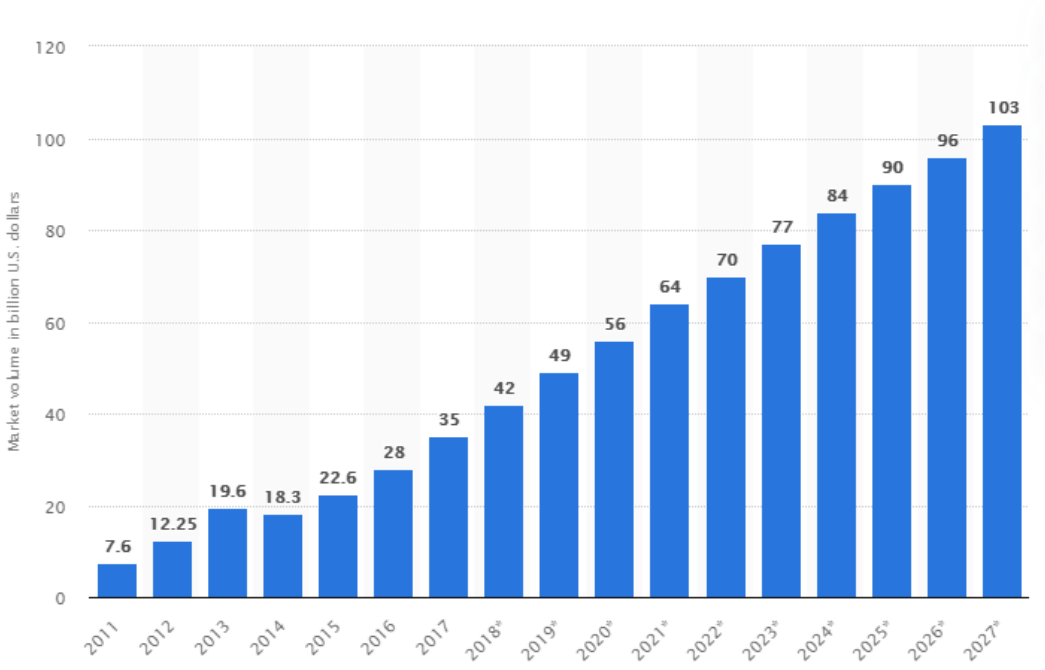
- ime i prezime,
- kućna adresa,
- e-mail adresa formata ime.prezime@tvrtka.com,
- broj osobne iskaznice,
- podaci o lokacijama mobilnog uređaja,
- Internet protokol (IP) adresa,
- podaci koje imaju bolnice ili liječnici, a koji bi mogli jedinstveno identificirati osobu.

[1] European Comission. *What is personal data?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (pristupljeno 26.02.2020.)

U ovom modernom dobu informacijske ekonomije, redukcija troška spremanja informacija omogućila je prikupljanje, spremanje i analizu nikad veće količine informacija o pojedincima. Tvrtke registriraju detalje svake korisničke transakcije. Internet stranice bilježe svako ponašanje osoba koje im pristupaju. Skupljači podataka povezuju informacije s različitih internetskih izvora kako bi stvorili potpune profile pojedinih osoba. Sa sve većim prihvaćanjem digitalnih tehnologija od strane organizacija i pojedinaca, procesuiranje osobnih podataka je sve jeftinije i brže, a s time raste i briga vezana uz privatnost tih podataka. Velik broj svakodnevnih aktivnosti ljudi danas se mogu pratiti pomoću informacijske tehnologije. Mali dijelovi osobnih informacija ulaze u bazu podataka gdje, zajedno s ostalim dijelovima osobnih informacija tog pojedinca, stvaraju kompletnu sliku o privatnom životu tog internet korisnika. Taj proces odvija se najčešće bez pristanka ljudi, ali i bez njihova znanja o tome općenito. Osim toga, stotine milijuna korisnika interneta diljem svijeta sada koristi tehnologiju Web 2.0 (npr. blogovi i društvene mreže), putem koje svoje iznimno privatne informacije svjesno dijele među prijateljima, ali i strancima. (Acquisti, 2010).

S pojavom osobnih podataka i društvenih mreža, pojavio se i pojam velikih podataka za čiji interes raste eksponencijalno u posljednjih desetak godina. Veliki podaci privukli su veliku pozornost javnosti i medija te je došlo do pojave mnoštva definicija ovog pojma. Veliki podaci povezuju se s dvije temeljne ideje: pohranom podataka i analizom podataka. Iako je pojam velikih podataka nov, ove dvije ideje daleko su od novoga i nepoznatoga te se stoga postavlja pitanje kako se zapravo veliki podaci o kojima se danas govori razlikuje od konvencionalnih podataka i procesa obrade tih podataka (Ward i Barker, 2013). Prema definiciji veliki podaci podrazumijevaju volumen, brzinu i raznolikost podataka, odnosno rastuću veličinu baze podataka, rastuću brzinu kojom podaci nastaju te rastući spektar novih formata podataka unutar baze (Laney, 2001). Prema Intelovoj definiciji, veliki podaci mogu se pripisati svakoj organizaciji koja tjedno u prosjeku generira 300 terabajta podataka (Intel, 2012).

Društvene mreže postale su sinonim za velike podatke zahvaljujući širokoj dostupnosti i pozicioniranju kao glavno sredstvo komunikacije diljem svijeta. Masivna veličina, brzina ažuriranja stranica i širok raspon modaliteta sadržaja smatraju se odrednicama koje kreiraju velike podatke u današnjem svijetu (Leetaru, 2019).



Slika 1. Predviđanje tržišta velikih podataka na temelju ukupnih godišnjih prihoda za period 2011.-2027.g.

Izvor: Statista. Forecast of Big Data market size, based on revenue, from 2011 to 2027. https://www.statista.com/statistics/254266/global-big-data-market-forecast/ (pristupljeno 27.02.2020.)

2.2. Društvene mreže kao glavni izvori podataka u digitalnom svijetu

Pojam društvenih mreža odnosi se na internetsku mrežu socijalnih veza koja okružuje internetske korisnike. Strukturalne odrednice društvenih mreža su (Heaney i Israel, 2008: 189-210):

- recipročnost (do koje mjere se podrška i sadržaji izmjenjuju između dvije strane),
- intenzitet (razina emocionalne bliskosti ostvarene putem društvene mreže),
- kompleksnost (broj funkcija koje društvena mreža izvršava),
- formalnost (ima li društvena mreža organizacijsku ili institucionalnu ulogu),
- gustoća (razina međusobnih interakcija korisnika),
- homogenost (skupine korisnika sličnih demografskih karakteristika),
- geografska disperzija (geografska raspršenost korisnika društvenih mreža),
- usmjerenost (razina do koje korisnici dijele zajedničku moć i utjecaj).

Glavne karakteristike internetskih društvenih mreža su zajedničke svakoj od više od 300 stranica društvenih mreža koje postoje danas. Temeljna karakteristika društvenih mreža je sposobnost kreiranja i dijeljenja osobnih profila. Stranica osobnog profila na društvenim mrežama obično uključuje sliku profila osobe, neke osnovne osobne informacije (ime, dob, spol, lokacija stanovanja) te prostor za objavu omiljenih bendova, knjiga, TV emisija, filmova i hobija tog korisnika. Većina društvenih mreža na internetu također korisnicima omogućava dijeljenje slika, glazbe, video sadržaja i blogova putem njihovih osobnih stranica profila. Najvažnija karakteristika i glavna svrha internetskih društvenih mreža je mogućnost pronalaženja novih prijatelja i uspostavljanja odnosa s njima.

Nakon uspostavljanja internetskog prijateljstva, na profilu jedne osobe pojavljuje se poveznica koja vodi na profil druge osobe, što omogućuje posjetiteljima tih profila da istražuju internetsku mrežu poznanstava drugih ljudi. Svaka društvena mreža ima različita pravila i metode pronalaska i kontaktiranja potencijalnih prijatelja, te obzirom na ta pravila, postoje otvorenije i zatvorenije društvene mreže. *Facebook*, koji je u početku bio društvena mreža za osobe koje pripadaju isključivo jednom fakultetu za kojeg je osnovan, i danas je jedna od ekskluzivnijih društvenih mreža, te je u velikoj mjeri orijentirana na grupe unutar te društvene mreže. Na *Facebooku*, pojedinac može pretraživati druge korisnike samo određenih mrežnih socijalnih krugova. Ti krugovi mogu uključivati zaposlenike istog poduzeća, polaznike istog sveučilišta ili srednje škole. Korisnik se također može pridružiti i postati članom manjih mrežnih grupa i zajednica na toj mreži koje su kreirane od strane korisnika *Facebooka*, na temelju stvarnih organizacija koje postoje u fizičkom svijetu ili pak samo na temelju ideja osnivača grupa. (Roos, 2007).

Prikupljene podatke *Facebook* koristi u svrhu personalizacije i poboljšanja njegovih proizvoda, mjerenja i analitike poslovnih usluga, promicanja sigurnosti, integriteta i zaštite komunikacije s korisnicima te istraživanja i inovacija za društveno dobro. Prema Pravilu o upotrebi podataka društvene mreže *Facebook*, ovo su podaci koje ta stranica prikuplja za svakog korisnika:[2]

- Sadržaj, komunikaciju i druge podatke koje korisnici unose prilikom korištenja *Facebooka*, uključujući one koje unesu kada se registriraju za korisnički račun, kreiraju ili dijele sadržaj te kada šalju poruke ili komuniciraju s drugima. To može uključivati informacije u sadržaju koji pružaju ili su povezane s njim (poput metapodataka), kao što je lokacija fotografije ili datum izrade dokumenta. Također može uključivati ono što je vidljivo putem značajki koje *Facebook* i njegovi proizvodi pružaju (poput npr. kamere).

[2] Facebook. *Pravila o upotrebi podataka.* https://www.facebook.com/policy.php (pristupljeno 26.02.2020.)

- Podatke o osobama, stranicama, korisničkim računima, znakovima # i grupama s kojima su korisnici povezani te o načinima interakcije s njima unutar *Facebookovih* proizvoda.
- Podatke o tome kako korisnici upotrebljavaju *Facebookove* proizvode kao na primjer podaci o tipu sadržaja koje korisnici pregledavaju i na koje reagiraju, značajkama koje upotrebljavaju, aktivnostima korisnika, ljudima ili korisničkim profilima s kojima korisnici stupaju u interakciju, ali i podatke o vremenu, učestalosti i trajanju aktivnosti korisnika. Tako na primjer, *Facebook* bilježi kada korisnici koriste i kada su posljednji put prije toga koristili njegove proizvode te koje objave, video i druge sadržaje korisnici pregledavaju putem *Facebookovih* proizvoda te podatke o načinu na koji korisnici upotrebljavaju *Facebookove* značajke, kao što je na primjer kamera.
- Podatke o transakcijama koje su obavljene putem *Facebookovih* proizvoda, ukoliko se ti proizvodi koriste za kupnju ili bilo koje druge financijske transakcije. To uključuje podatke o plaćanju: broj kreditne ili debitne kartice te ostale podatke o kartici, ostale podatke o računu i provjeri autentičnosti, podatke za slanje računa i pošiljke i podatke za kontakt.
- Podatke o aktivnostima drugih osoba i podatke koje te aktivnosti pružaju o drugim korisnicima. U to spadaju podaci o korisnicima kada drugi korisnici podijele ili komentiraju njihove sadržaje, pošalju im poruku ili prenesu njihove podatke za kontakt.
- Podatke s računala, telefonskih uređaja, povezanih televizora i drugih uređaja s internetskom vezom koje korisnici koriste i koji se povezuju s *Facebookovim* proizvodima. Takvi podaci uključuju svojstva uređaja, radnje na uređaju, identifikatore, signale uređaja, podatke iz postavke uređaja, mreže i veze te podatke iz kolačića.

- Podatke koje skupljaju oglašivači, razvojni programeri aplikacija i izdavači koji upotrebljavaju *Facebookove* poslovne alate. Te treće strane *Facebooku* pružaju podatke o aktivnostima korisnika izvan *Facebooka*, bez obzira je li korisnik prijavljen na *Facebook* ili uopće ima korisnički račun na *Facebooku*. Tako *Facebook* prikuplja primjerice podatke o radnjama i kupnjama korisnika na internetu i izvan njega.

Poduzeća danas preživljavaju na temelju razumijevanja i poznavanja svojih potrošača i korisnika do što veće mjere. Praćenje ponašanja potrošača putem interneta je tako postao važan dio uspjeha tih poduzeća. Organizacije ulažu velike količine resursa u prikupljanje takvih analitika na temelju velikih podataka kao ključnih komponenti praćenja aktivnosti na društvenim mrežama. Analitika društvenih mreža obuhvaća ponašanja korisnika interneta. Dostupnost podataka o pretraživanjima po internetu od strane korisnika, njihovim internetskim kupovinama i objavljenih recenzija te marketinška istraživanja na društvenim mrežama omogućavaju organizacijama uvid u aktualne i opširne uvide u osobnost korisnika interneta, odnosno potrošača. Na temelju prikupljenih podataka, organizacije tako mogu usmjeriti svoju tržišnu strategiju na različite načine kao što su oglašavanje određenih proizvoda, publicitet i brand menadžment, pružanje personaliziranih usluga, praćenje tržišnih trendova i konkurencije, minimiziranje rizika, smanjenje troškova i proširenje poslovanja. Fenomen velikih podataka vezan uz društvene mreže pokrenuo je novo rastuće područje istraživanja poznato pod nazivom „analiza osjećaja.“ Cilj analize osjećaja je biti svjestan ili poznavati ono što ljudi govore i dijele u njihovom svakodnevnom životu. Poduzeća prikupljaju takvu vrstu informacija kako bi bolje razumjeli svoje potrošače i sukladno tome unaprijedili svoje poslovne procese. Obrazovne institucije također imaju interesa u „slušanju“ svojih polaznika kako bi imali bolji uvid u njihove percepcije.

Pomoću aktivnosti đaka i studenata na društvenim mrežama, analiza osjećaja pruža informacije i podatke o njihovom ponašanju na internetu, uključujući njihova mišljenja na različite aspekte obrazovnog sustava, kao što su proces prijave na sveučilišta, kvalifikacije za određene studije, provjere znanja i njihove aspiracije i ciljevi. Organizacije takve informacije mogu iskoristiti za razvijanje njihovih marketinških strategija, nadziranje procesa provjera znanja na temelju rasprava u internetskim forumima, razumijevanje značenja branda organizacije u očima studenata i učenika, prikupljanju povratnih informacija o određenim proizvodima i uslugama i sl. (Dhawan i Zanini, 2014: 36-41).

Platforme društvenih mreža većinu svojih prihoda ostvaruju prodavanjem iznimno dobro pozicioniranih i ciljanih oglasnih mjesta određenih na temelju algoritama koji prikupljaju, prate i analiziraju svaku sekundu života korisnika tih društvenih mreža. Naime, danas postoje velike tvrtke koje se bave isključivo prikupljanjem svih vrsta informacija – imena, adresa, veličine prihoda, internet stranice koje ljudi pretražuju te osobe s kojima komuniciraju preko interneta. Te tvrtke tada prikupljene podatke prodaju drugim poduzećima. Ljudi koje rade u takvim poduzećima te se time bave nazivaju se informacijskim brokerima i oni su na tržištu prisutni već dulje vrijeme. O korisnicima interneta mogu reći mnogo stvari, kao što su na primjer podaci voli li osoba više pse ili mačke, vozi li Ford ili Subaru i u kakvoj se financijskoj situaciji nalazi. Najveća količina osobnih podataka koje informacijski brokeri prikupljaju potječe iz društvenih mreža koje su prepune osobnim podacima koje ljudi dobrovoljno javno dijele. Nakon što se osobni podaci prikupe, informacijski brokeri imaju zadaću da te podatke grupiraju i zapakiraju te prodaju – ponekad drugim brokerima, a ponekad raznim poduzećima, a koja tada uglavnom te informacije koriste kako bi usmjerili svoje oglase prema pravoj tržišnoj niši (Naylor, 2016). Jedno od najvećih poduzeća u industriji trgovanja informacijama, Acxiom, u 2018. godini imalo je prihode od 917 mil. dolara (Acxiom 2018 Annual Report).

Mišljenje šire javnosti danas je kako, ne samo da je veoma malo poznato o tome kako velika poduzeća prikupljaju i koriste osobne podatke ljudi, već ta poduzeća prikupljaju toliku količinu podataka na dnevnoj razini da i ona sama ne znaju sve načine prikupljanja i praćenja tih podataka. Poduzeća iza platformi društvenih mreža notorno su tiha kada se radi o detaljima o načinima na koje kontroliraju ono što korisnici vide i dijele putem tih mreža. Društvene mreže imaju velik utjecaj na društvo u cjelini, međutim, nikada ne snose odgovornost za svoja djela i utjecaj. Najproblematičniji aspekt modernog nadziranja članova društva na ovaj način je nedostatak prava i mogućnosti ljudi da saznaju ustvari do koje razine su oni nadgledani i kontrolirani. Poduzeća se pravdaju izjavama za javnost u kojima mogu priopćiti što god žele kako bi stvorila sliku o svom poslovanju koja im odgovara, dok razotkrivanje aktivnosti koje narušavaju privatnost internetskih korisnika često ovisi samo o nezavisnim istražiteljima i njihovom radu da se takve aktivnosti razotkriju (Leetaru, 2018.).

2.3. Zaštita privatnosti u digitalnom svijetu

Suvremen način života temelji se na korištenju elektroničkih uređaja kao što su mobiteli i osobna računala. Koriste se za bankarske transakcije, kupnju, komunikaciju, istraživanje itd. Elektronički uređaji izvor su nikad većeg broja prilika za narušavanje privatnosti i sigurnosti njihovih korisnika. Međutim, korisnici rijetko razmišljaju o narušavanju njihove privatnosti u takvom digitalnom svijetu te o tome što mogu učiniti po tome pitanju (Stafford, 2012: 4).

U svrhu zaštite privatnosti korisnika u digitalnom kontekstu, potrebno je razmotriti sljedeće (Cherry, 2013: 19):

- količinu informacija koje korisnik pohranjuje na internetu,
- načine odabira korisničkih imena i lozinki te ostalih načina autentifikacije i zaštite,
- sigurnost fizičkih komponenti internetske mreže u korisnikovu domu,

- sigurnosne odrednice elektroničkih uređaja koji se koriste,
- mogućnosti ograničavanja podataka koje korisnik dijeli putem interneta,
- načine na koje vlada i ostale organizacije mogu pristupiti korisnikovim podacima,
- zakone i pravilnike vezane uz zaštitu privatnosti na internetu.

Društvene mreže predstavljaju mjesto internetske komunikacije, rasprave korisnika te koncept za dijeljenje sadržaja raznih vrsta između ljudi. S obzirom na to da je opće poznato kako sadržaj i podaci dijeljeni putem društvenih mreža postaju javni, potrebno je posvetiti više pozornosti prilikom objavljivanja istih kako bi se izbjegli potencijalni rizici vezani uz korisnikovu sigurnost. Pružatelj internetske stranice dužan je osigurati informacije koje korisnici na toj stranici dijele te ne dozvoljavati korištenje istih informacija u svrhe koje nisu prethodno dogovorene.

Većina stranica pruža korisnicima izbor između privatnog i javnog dijeljenja njihovih objava te se preporučuje korištenje privatnog modela kako bi bili sigurniji. Postoje neki temeljni savjeti za očuvanje sigurnosti na internetu – korisnici društvenih mreža trebali bi izbjegavati dijeljenje osobnih podataka kao što su adresa stanovanja i broj telefona, korištenje lozinki koje bi se mogle olako identificirati i zloupotrijebiti te korištenje različitih adresa elektroničke pošte za privatne i poslovne svrhe.[3]

[3] The National Supervisory Authority For Personal Data Processing, Romania. *The protection of personal data and the social network websites*. https://www.dataprotection.ro/index.jsp?page=The_protection_of_personal_data_and_the_social_network_websites&lang=en (pristupljeno 27.02.2020.)

3. ZLOUPOTREBA OSOBNIH PODATAKA

3.1. Zakonodavni okviri zlouporabe osobnih podataka

Europska unija jamči sigurnost osobnih podataka internetskih korisnika prilikom svakog prikupljanja podataka, primjerice za vrijeme internetske kupnje, prijavljivanja na natječaj za posao ili podnošenje raznih zahtjeva putem interneta. Pravila Europske unije vezana uz zaštitu osobnih podataka primjenjuju se na sva javna i privatna poduzeća i organizacije unutar Europske unije, ali i na sva javna i privatna poduzeća čija su središta van granica EU, ali obavljaju svoju djelatnost u EU (npr. *Facebook*). Prema pravilima EU o zaštiti podataka, ako se korištenjem podataka može na izravan ili neizravan način identificirati određena osoba, takvi podaci smatraju se osobnima i sukladno tome moraju se poštivati ljudska prava na zaštitu podataka.[4]

Iako je obrada podataka područje koje je strogo ograničeno, postoje određene situacije kada je poduzećima i organizacijama dozvoljeno prikupljati i upotrebljavati osobne podatke korisnike, a to su:[5]

- prilikom sklapanja ugovora s korisnikom,
- prilikom ispunjavanja pravne obveze, odnosno kada je obrada osobnih podataka uvjetovana zakonom,
- ukoliko obrada podataka može biti odlučujući faktor između života i smrti tog korisnika,
- prilikom ispunjavanja zadaća od javnog interesa,
- kada se radi o legitimnim interesima (npr. banka koristi osobne podatke korisnika kako bi utvrdila ima li korisnik pravo na neku željenu uslugu).

[4] Europska unija. *Zaštita podataka i privatnost na internetu*. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm#shortcut-1 (pristupljeno 27.02.2020.)
[5] Isto.

Osim ako se ne radi o prethodno navedenim scenarijima, poduzeća i organizacije dužni su dobiti pristanak od korisnika za bilo kakvu obradu i korištenje njihovih osobnih podataka. Pristanak ili privola smatra se danom na valjani način ukoliko je dana jasnom afirmativnom radnjom kao što je na primjer potpisivanje jasno definiranog obrasca za privolu. Kako bi korisnikova sigurnost podataka bila što veća, prilikom davanja privole trebao bi znati osnovne informacije o tome za što daje privolu, a te informacije trebale bi biti iznesene na jasan i razumljiv način. Korisnik mora imati podatke o poduzeću ili organizaciji koja će obraditi njegove podatke, svrhu obrade podataka, vremenski period zadržavanja i korištenja osobnih podataka, podatke o trećim stranama koje će također time dobiti uvid u njegove osobne podatke te informacije o pravima na zaštitu podataka (pristup, ispravaka, brisanje, pritužba, povlačenje privole).[6] Na razini Europske unije određeni su zajednički pravilnici kako bi se osigurao visok standard zaštite sigurnosti i podataka putem interneta.

Trenutno postoje dva glavna dokumenta donesena od strane EU koja uređuju zakonodavne okvire sigurnosti i zlouporabe osobnih podataka, a to su Opća uredba o zaštiti podataka (poznatija kao GDPR – General Data Protection Regulation) i Direktiva EU o privatnosti i elektroničkim komunikacijama. Opća uredba o zaštiti podataka, GDPR, zadužena je za osiguravanje strogih uvjeta prikupljanja osobnih podataka i njihovo korištenje samo za zakonski opravdane svrhe. Prema GDPR-u, organizacije koje prikupljaju i upravljaju osobnim podacima korisnika također su dužne zaštiti te iste podatke od zloupotrebe. Direktiva EU o privatnosti i elektroničkim komunikacijama osigurava da se svaka komunikacija putem javnih telekomunikacijskih mreža odvija na način koji ne krši osnovna ljudska prava na privatnost, odnosno osigurava visoku razinu zaštite podataka i privatnosti, neovisno o vrsti tehnologije koja se koristi.[7]

---

[6] Europska unija. *Zaštita podataka i privatnost na internetu*. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm#shortcut-1 (pristupljeno 27.02.2020.)
[7] European Commission. *Digital Privacy*. https://ec.europa.eu/digital-single-market/en/online-privacy (pristupljeno 27.02.2020.)

Osnovna načela zaštite osobnih podataka su:[8]

1. Točnost, potpunost, ažurnost, obrada podataka na pošten način. Ukoliko se osobni podaci ne tretiraju sukladno ovom načelu, može doći do zabune i krive identifikacije neke osobe.
2. Povjerljivost. Osobni podaci se čuvaju u formatu koji omogućuje identifikaciju određene osobe isključivo onoliko koliko je potrebno za obavljanje svrhe prikupljanja podataka.
3. Zakonitost. Prikupljanje i obrada podataka može se obavljati isključivo u skladu sa zakonom.
4. Svrhovitost. Svrha prikupljanja i obrade podataka unaprijed je određena i poznata te prihvaćena od strane pojedinca. Bilo kakva upotreba podataka van dogovorenih okvira nije dopuštena.
5. Opseg. Količina i opseg prikupljenih podataka mora biti svedena na minimalnu potrebnu razinu te nije dozvoljeno prikupljanje podataka van tih granica, odnosno u količini većoj nego što je nužno za postizanje svrhe.

Na razini Republike Hrvatske, pravo na zaštitu osobnih podataka propisano je Ustavom: „*Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.*“ (Ustav RH, Članak 37) Na temelju te ustavne odredbe donesena je i Opća uredba o zaštiti podataka te Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine, 42/18) te se ta uredba i zakon smatraju osnovnim aktima koji u Republici Hrvatskoj uređuju okvire prikupljanja, obrade, korištenja i zaštite osobnih podataka. Doneseni akti u RH u skladu je sa standardima i načelima Europske unije.

[8] Agencija za zaštitu osobnih podataka. *Zaštita osobnih podataka u RH*. https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (pristupljeno 27.02.2020.)

Osim navedene uredbe i zakona, na snazi je i Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (Narodne novine, br. 139/04).

Temeljna prava građana/osoba čiji se podaci obrađuju su:[9]

- pravo na informiranost o prikupljanju i obradi osobnih podataka,
- pravo na povlačenje privole za obradu i pravo na zahtjev za prestanak obrade osobnih podataka,
- pravo na uvid u osobne podatke koji se prikupljaju i obrađuju,
- pravo na ispravljanje osobnih podataka koji su prikupljeni i koji se obrađuju u slučaju nepotpunosti i neispravnosti istih,
- pravo na protivljenje prema obradi podataka u marketinške svrhe,
- pravo na naknadu štete u slučaju zloupotrebe osobnih podataka.

Opća uredba o zaštiti podataka (GDPR) propisala je dva razreda za novčane kazne u slučaju kršenja propisa donesenih ovom uredbom. Manje ozbiljna i teška kršenja propisa spadaju u niži kazneni razred i mogu rezultirati novčanom kaznom do 10 milijuna eura ili u iznosu od 2% ukupnog godišnjeg prihoda poduzeća ili organizacije u prethodnoj fiskalnoj godini, ovisno o tome koji iznos je viši. Ozbiljnija i teža kršenja propisa uredbe, koja se smatraju i kršenjem temeljnih načela ljudskih prava na privatnost te kršenjem temeljnih odrednica i načela ove odredbe, mogu rezultirati većim novčanim kaznama – do 20 milijuna eura ili u iznosu od 4% ukupnog godišnjeg prihoda poduzeća ili organizacije u prethodnoj fiskalnoj godini, ovisno o tome koji je iznos viši.[10]

[9] Agencija za zaštitu osobnih podataka. *Zaštita osobnih podataka u RH*. https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (pristupljeno 27.02.2020.)
[10] GDPR. *What are the GDPR Fines?*. https://gdpr.eu/fines/ (pristupljeno 27.02.2020.)

3.2. Slučajevi narušavanja sigurnosti osobnih podataka u svijetu

Namjerno ili slučajno kršenje sigurnosti i privatnosti osobnih podataka sve je češći problem novog modernog digitalnog vremena. U nastavku će se navesti i ukratko objasniti nekoliko najvećih propusta kada se radi o sigurnosti osobnih podataka.

Yahoo je američka tvrtka koja od 1995. godine pruža usluge pretraživanja interneta, elektroničke pošte i druge web usluge. Od 2013. godine nadalje, Yahoo je bio žrtva nekoliko hakerskih napada, od koji su neki bili među najgorima u povijesti kada se gleda količina podataka koja je ukradena. Raznim metodama u nekoliko navrata, hakirano je više od 3 milijarde Yahoo korisničkih računa, a ukradeni su podaci o imenu, adresi, brojevima telefona, lozinke, datumi rođenja i, u nekim slučajevima, sigurnosna pitanja i odgovori korisnika. Nekoliko hakera je optuženo za napad uslijed FBI-eve istrage, a Yahoo je oštećenim korisnicima isplatio naknadu za nastalu štetu (Perlorth, 2017).

First American, američki div koji se bavi nekretninama i osiguranjem, također je doživio propust po pitanju sigurnog čuvanja osobnih podataka svojih korisnika. Propust se dogodio 2019. godine, a uzrok je loša sigurnost od strane poduzeća. Naime, osobni podaci 885 milijuna ljudi bili su pohranjeni na serverima poduzeća bez ikakve zaštite. Pristup podacima zapravo je bio moguć bez izvođenja ikakvih hakerskih radnji. Podaci koji su procurili u javnost sadržavali su brojeve socijalnog osiguranja, slike vozačkih dozvola, brojeve bankovnih računa i bankovne izvatke, dokumente o porezima i hipotekama korisnika i potvrde o financijskim transakcijama (Dellinger, 2019).

Marriott International je međunarodna hotelska grupacija koja je 2018. godine također bila žrtva hakerskog napada prilikom kojeg je ukradeno 500 milijuna osobnih podataka. Potencijalni negativni efekti ovog napada su bili veliki, obzirom da su većina podataka bili slike putovnica i brojevi kreditnih kartica. Međutim, do takvih katastrofalnih scenarija i krađa identiteta nije došlo,

što je zapravo bilo čudno u takvoj situaciji. Postoje neke spekulacije kako je hakerski napad izvršen od strane kineske vlade s ciljem prikupljanja što više osobnih podataka o zaposlenicima američkih državnih institucija. Razlog zašto je napad izvršen na hotelsku grupaciju Marriott je taj što su upravo Marriott hoteli najčešći odabir državnih službenika na putovanjima (Fruhlinger, 2020).

Friend Finder Networks američka je društvena mreža, osnovana 1996. godine. 2016. godine pretrpjela je hakerski napad prilikom kojeg je ukradeno 412,2 milijuna osobnih podataka, međutim, poduzeće je u ovom slučaju također odgovorno za lošu sigurnosnu zaštitu tih podataka. To je već bio drugi takav napad izvršen na poduzeću Friend Finder Networks, a podaci koji su ukradeni obuhvaćali su korisnička imena, e-mail adrese i lozinke korisnika (Ragan, 2016).

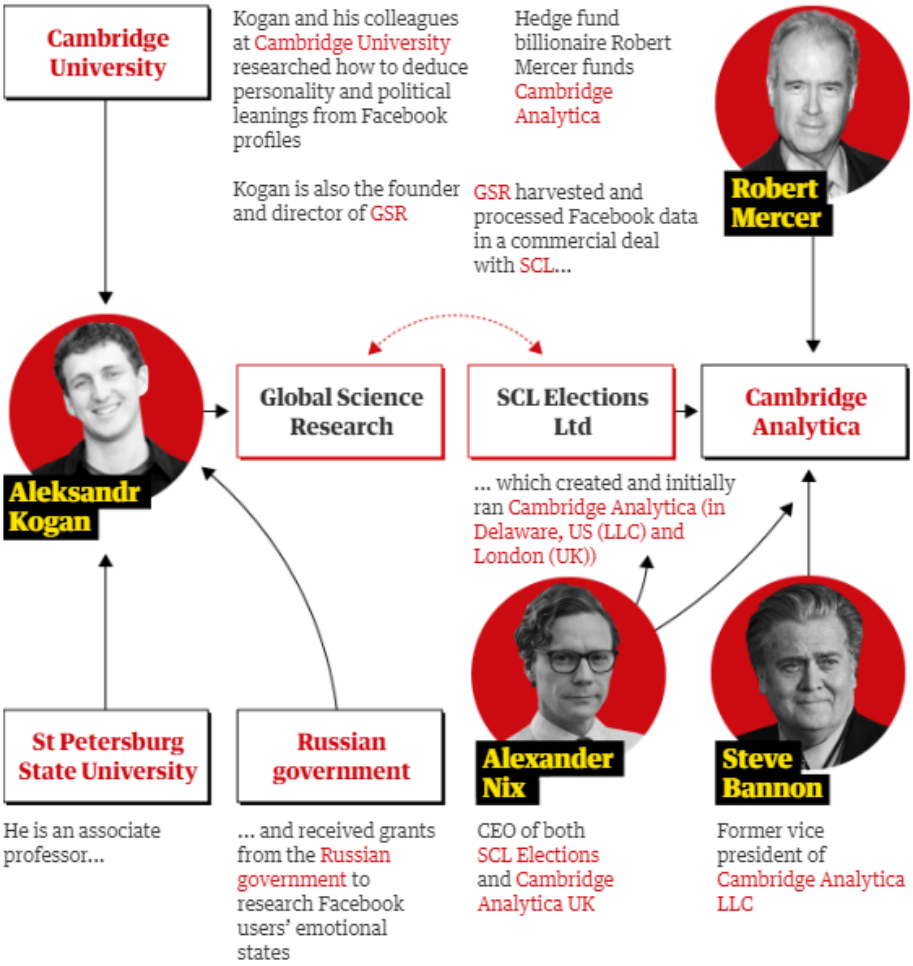
4. SLUČAJ CAMBRIDGE ANALYTICA

Cambridge Analytica bila je britanska tvrtka koja se bavila obradom podataka u svrhe trećih strana. Trenutno je zatvorena radi velikog skandala proizašlog nakon suradnje s tvrtkom *Facebook* i uplitanja u nekoliko političkih kampanja. Poduzeće je bilo poznato kao jedan od glavnih aktera u nekoliko velikih političkih izbora i glasačkih procesa, a zbog zloupotrebe podataka u istima, danas je zatvoreno. U nastavku ovog poglavlja slijedi detaljniji pregled općenitih informacija o spomenutom poduzeću te pregled političkih kampanja s kojima se poduzeće povezivalo u prošlosti. Sve to bit će uvod u detaljnije istraživanje slučaja Cambridge Analytica i *Facebooka* koji je rezultirao najvećom novčanom kaznom ikada u povijesti za kršenje pravila sigurnosti i privatnosti osobnih podataka.

4.1. Općenito o poduzeću Cambridge Analytica

Cambridge Analytica (CA) je poduzeće koje je bilo osnovano 2013. godine i bavilo se pružanjem usluga poduzećima i političkim strankama koje su htjele promijeniti i utjecati na ponašanje svoje publike ili potrošača. Sjedište CA bilo je u Londonu, a tvrtka je bila dio SCL grupacije, koja je slične usluge nudila diljem svijeta. Osnivač Cambridge Analytice, Alexander Nix, glavni je igrač u slučajevima koji povezuju CA i političke kampanje na kojima su radili te je zaslužan za razvoj principa poslovanja poduzeća. Glavni operativni direktor poduzeća je Mark Turnbull, koji imao 18 godina iskustva u komunikacijama prije rada u SCL grupi. CA je tvrdila da može analizirati ogromnu količinu korisničkih podataka i u kombinaciji s primjenom znanja bihevioralne znanosti identificirati ljude koje određena organizacija želi ciljati u sklopu svog marketinškog plana. Poduzeće je te podatke prikupljalo iz različitih izvora, uključujući i platforme društvenih mreža kao što je *Facebook*. (Osborne, 2018).

Cambridge Analytica je na svojoj stranici oglašavala kako ima pristup 5000 jedinica osobnih podataka za preko 220 milijuna Amerikanaca.[11]



Slika 2. Povezanost ključnih osoba Cambridge Analytice

Izvor: The Guardian. https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach (pristupljeno 27.02.2020.)

[11] Cambridge Analytica. Web arhiva. https://web.archive.org/web/20160624121051/https://cambridgeanalytica.org/about (pristupljeno 27.02.2020.)

Cambridge Analytica 2014. godine našla se u centru kontroverzi u SAD-u i Velikoj Britaniji nakon članaka dvojice novinara u kojem se navodi kako je poduzeće prikupljalo i koristilo podatke o korisnicima *Facebooka* na nedozvoljen način. Tvrtka je osnovana 2013. godine prvenstveno s ciljem rada na izborima u SAD-u te s početnim kapitalom u iznosu od 15 milijuna dolara koje je uložio američki republikanski milijarder, Robert Mercer, koji je kasnije surađivao s Trumpovim savjetnikom Bijele kuće, Steve Bannonom. Za CA radili su većinom britanski zaposlenici te je prva politička kampanja za koju je bila angažirana, bila ona Ted Cruza. CA oglašavala se kao tvrtka koja pruža usluge istraživanja potrošača, nišnog oglašavanja te druge usluge povezane s obradom podataka, za potrebe političkih, ali i korporativnih klijenata. Međutim, tvrtka na svojoj internet stranici nije navodila imena korporativnih klijenata s kojima je surađivala, već ih je opisivala kao *dnevne novine koje žele znati više o svojim pretplatnicima, ženski brend odjeće koji želi istražiti svoje kupce* i *američki osiguravatelj automobila zainteresiran za oglašavanje.* Također na svojoj internet stranici, tvrtka je navela kako ima urede na 5 lokacija diljem svijeta – u New Yorku, Washingtonu, Londonu, Brazilu i Maleziji. Nakon pobjede Trumpa 2016. godine, glavni izvršni direktor Cambridge Analytice, Alexander Nix, otišao je drugim potencijalnim klijentima i prezentirao im svoje usluge. CA je naglašavala kako može razviti psihološke profile potrošača i glasača te da je upravo to *tajna* uspješnosti veće od one koja se može postići tradicionalnim oglašavanjem i marketingom. Tvrtka je optužena za prikupljanje osobnih podataka 50 milijuna korisnika *Facebooka* na način koji je zavarao i korisnike, ali i poduzeće *Facebook*. U javnost je proizašlo kako je CA te podatke prikupljala pomoću aplikacije razvijene od britanskog akademika, Aleksandra Kogana. Uslijedio je veliki sudski spor protiv *Facebooka*, Cambridge Analytice, SCL grupacije te njenih odgovornih zaposlenika koji je završio zatvaranjem poduzeća Cambridge Analytica i SCL grupe te najvećom kaznom u povijesti novčanih kazni vezanih uz kršenje zaštite osobnih podataka koju je *Facebook* morao platiti (Ingram, 2018).

Detaljniji pregled istraživanja spomenutog slučaja te vremenski tijek svih relevantnih događaja vezanih uz skandal Cambridge Analytice izložen je u nastavku ovog diplomskog rada u poglavlju 6. Rezultati.

4.2. Političke kampanje povezane s poduzećem Cambridge Analytica

U nastavku slijedi pregled nekih najvažnijih političkih kampanja koje se dovode u vezu s Cambridge Analyticom i SCL grupacijom.

KENIJA: Cambridge Analytica vodila je kampanje političkih izbora u Keniji 2013. i 2017. godine. U 2018. godini zaposlenik CA izjavio je kako je njegov prethodnik pronađen mrtav u hotelskoj sobi u Keniji za vrijeme dok je radio za kampanju Uhuru Kenyatta 2013. godine (Lang'at, 2018). CA na svojoj je stranici izjavila kako je provela istraživanje 47 000 Kenijaca tijekom izbora 2013. godine s ciljem *razumijevanja ključnih nacionalnih i lokalnih političkih pitanja, razine povjerenja ključnim političarima, glasačkih navika i namjera te preferiranih informativnih medijskih kanala.* Cambridge Analytica radila je kenijskom tvrtkom 360 Media, čiji je zadatak bio razvijanje internetske kampanje za izbore u Keniji 2017. godine na način da prezentira Raila Odinga kao *individualca žednog krvi koji simpatizira Al-Shabaab i nema nikakav plan za razvitak*, dok je u isto vrijeme prezentirala sadašnjeg predsjednika Kenyattu kao *netolerantnog prema terorizmu i dobrog za ekonomiju* (Matende, 2018). Nakon otkrivanja incidenata, pokrenuta je istraga poduzeća CA (BBC, 2018).

MEKSIKO: Meksička agencija za transparentnost i zaštitu podataka (INAI) najavila je početak istrage poduzeća Cambridge Analytica te drugih poduzeća koja su s njim surađivala kako bi se otkrilo jesu li spomenute tvrtke odgovorne za kršenje zakona o zaštiti podataka. Točnije, agencija istražuje poduzeća povezana s aplikacijom Pig.gi čija je osnivačka tvrtka izjavila kako je rezultate anketa o predsjedničkim izborima i stavovima glasača podijelila s Cambridge Analyticom i njenim partnerima (Grothaus, 2018).

UJEDINJENO KRALJEVSTVO: Na temelju objavljenih *mailova* kao dokaz, ustanovljeno je kako je Cambridge Analytica radila za kampanju Leave.eu i Nezavisnu stranku Ujedinjenog Kraljevstva prethodno referendumu o izlasku UK-a iz Europske unije (Brexit). Brittany Kaiser, bivša direktorica poslovnog razvoja CA, izjavila je kako je 2016. godine Leave.eu koristila kreirane podatke od strane CA kako bi ciljane grupe glasača obasipala političkim porukama putem interneta u svrhu mijenjanja političkog stava te grupe glasača. Kaiser je javnosti također predočila razne dokumente i prijepise poruka koje potvrđuju njenu izjavu. Leave.eu i Nezavisna stranka UK (UKIP) nekoliko su puta zanijekali suradnju s CA, usprkos javnoj izjavi Arrona Banksa, suosnivača Leave.eu kampanje, kako je njegova organizacija angažirala Cambridge Analyticu (Scott, 2019).

INDIJA: Prema zviždaču Christopheru Wylie-u, bivšem voditelju istraživanja Cambridge Analytice, tvrtka je surađivala s političkim strankama u Indiji na nekoliko izbora. Osobni podaci su prikupljeni također preko aplikacije povezane s *Facebook* računima, a 355 korisnika *Facebooka* u Indiji koji su aplikaciju instalirali, razotkrili su osobne podatke od 562455 korisnika. Glavna stranka za koju je Cambridge Analytica radila bila je Indijski nacionalni kongres (INC). SCL grupa imala je urede u 10 indijskih gradova (Ahmedabad, Bengaluru, Cuttack, Ghaziabad, Guwahati, Hyderabad, Indore, Kolkata, Patna i Pune) te je od 2003. godine nadalje radila na barem osam projekata u Indiji (Punit, 2018).

When	Where	What
2012	Uttar Pradesh (UP)	A caste census in on behalf of a national party
2011	UP	Statewide (200 million people) research campaign to identify voter caste by household.
2010	Bihar elections	Electoral research and strategy for the Janata Dal (United)
2009	National elections	Managed campaigns of a number of Lok Sabha candidates
2007	UP	Full political survey on behalf of a major party
2007	Kerala, West Bengal, Assam, Bihar, Jharkhand and UP	Research communication campaign to counter the recruitment into, and support for, "violent Jihadism" in six states
2003	Madhya Pradesh elections	Psephological study and opinion polling for a national party to identify swing voters
2003	Rajasthan elections	Assessed a major state party's organisational strength, and nature of the voting population and the attitudes and behaviours of politically active individuals within the state

Slika 3. Projekti SCL grupacije u Indiji

Izvor: Quartz. Cambridge Analytica's parent firm proposed a massive political machine for India's 2014 elections. https://qz.com/1239561/cambridge-analyticas-parent-firm-proposed-a-massive-political-machine-for-indias-2014-elections/ (pristupljeno 28.02.2020.)

Osim navedenih slučajeva suradnje političkih organizacija i poduzeća Cambridge Analytice, najveće kršenje sigurnosti osobnih podataka dogodilo se u SAD-u tijekom rada CA u kampanji Donalda Trumpa za izbor predsjednika SAD-a, o čemu će se više reći u istraživačkom dijelu ovog diplomskog rada.

5. MATERIJAL I METODE

5.1. Istraživački materijal

Potencijalni predmet za provedbu istraživanja bili su svi informativni internetski portali u svijetu, društvene mreže svjedoka u sudskom postupku protiv poduzeća Cambridge Analytice, internet stranice javnih institucija uključenih u sudske postupke u promatranom slučaju te dokumentarac „*The Great Hack*“. Za rad je kao uzorak uzet spomenuti dokumentarni film „*The Great Hack*“, a za analizu tekstualnog sadržaja članci vezani uz temu na portalima*The Guardian* i *The Texas Tribune.*

5.2. Metode istraživanja

Za istraživanje je korištena metoda analize sadržaja dokumentarnog filma „*The Great Hack“* produciranog i režiranog od strane Jehane Noujaim i Karim Amer i tekstova članka objavljenih na odabranim digitalnim platformama.

5.3. Postupak provedbe istraživanja

Iz odabranog uzorka analiziran je slijed događaja i radnji od poduzeća *Facebook* i Cambridge Analytice te istražen cijeli sporni proces zloupotrebe osobnih podataka. Istraživanje je obuhvatilo gledanje filma, čitanje članaka i javnih priopćenja, pisanje bilješki i slaganje kronološkog slijeda akcija izvršenih od strane poduzeća koje su rezultirale ilegalnom zlouporabom podataka.

5.4. Metode obrade podataka

Rad je koncipiran kao analitičko-deskriptivni rad u kojem se prilikom izrade koristila metoda analize sadržaja filma i članaka vezanih uz zloupotrebu osobnih podataka u slučaju Cambridge Analytice. Osim metode analize sadržaja, koristila se deskriptivna metoda obrade podataka kojom su opisivani dobiveni rezultati istraživanja i analize te na temelju koje su postavljene hipoteze rada elaborirane.

6. REZULTATI

6.1. Cilj i predmet istraživanja

Cilj ovog rada je utvrditi načine na koji se podacima upravlja u digitalnom svijetu te kroz primjer afere Cambridge Analytica prikazati kako se osobni e-podaci iz digitalnog svijeta zloupotrebljavaju u svrhu manipuliranja javnostima. Predmet ovog diplomskog rada su informacije i podaci u digitalnom svijetu, s naglaskom na osobne e-podatke korisnika društvenih mreža te zaštita privatnosti istih. Proučavali su se zakonodavni okviri zloupotrebe osobnih e-podataka te je pružen pregled primjera zloupotrebe osobnih e-podataka. U radu je fokus na primjeru zloupotrebe podataka od strane *Facebooka* i Cambridge Analytica kroz koji je objašnjen problem upravljanja osobnim e-podacima u digitalnom svijetu.

6.2. Istraživačko pitanje

U svrhu ispunjenja glavnog cilja ovog diplomskog rada, definirano je istraživačko pitanje koje glasi: „Kako detektirati potencijalne oblike zlouporabe osobnih e-podataka i koje su moguće posljedice?“

6.3. Opis rezultata istraživanja

Odabrani dokumentarni film započinje ispitivanjem Brittany Kaiser na sudu, a zatim se prelazi na predavanje profesora Davida Carolla o predviđanju ponašanja internetskih korisnika putem interneta i društvenih mreža i govoru kako se osobni podaci (online interakcije, plaćanja kreditnim karticama, povijest pretraživanja internetskih preglednika, lokacije, reakcije na društvenim mrežama itd.) prikupljaju i iskorištavaju u modernom svijetu. Caroll govori kako se svi ti podaci prikupljaju iz različitih izvora i razvrstavaju sukladno pojedincima na koje se ti podaci odnose kako bi se kreirali individualni profili tih osoba.

Na temelju svakog od tih kreiranih profila, radi se zasebna prosudba svakog karaktera i ponašanja pojedinca te se prema tome kreiraju sadržaji, oglasi i materijali koji će biti vidljivi samo tom određenom korisniku kada pristupi internetu, i to vrijedi za svakog zasebnog internet korisnika. Takvi podaci pomažu određivanju određenih karakteristika tih pojedinaca koje su svojstvene isključivo njima, kao na primjer: čega se boje, što vole, što im privlači pozornost, koje su im granice i što je potrebno kako bi prešli te granice.

Tablica 1. Glavni likovi dokumentarnog filma (po redoslijedu prikazivanja)
Izvor: Izrada autora prema: Amer, Karim; Noujaim, Jehane. 2019. The Great Hack. Dokumentarni film. Netflix.

Brittany Kaiser	- bivša stažistica u kampanji Baracka Obame - bivša zaposlenica Cambridge Analytice - zviždačica i svjedokinja na sudu protiv Cambridge Analytice
David Carrol	- profesor u *Parsons School of Design* - većinski narator filma
Julian Wheatland	- bivši glavni operativni i financijski direktor Cambridge Analytice
Alexander Nix	- bivši glavni izvršni direktor Cambridge Analytice
Carole Cadwalladr	- istražna novinarka (*The Guardian*)
Christopher Wiley	- bivši *data scientist* Cambridge Analytice - zviždač i svjedok na sudu protiv Cambridge Analytice
Steve Bannon	- bivši izvršni voditelj Trumpove predsjedničke kampanje

Dokumentarni film *The Great Hack*, prikazuje nekoliko slučajeva zloupotrebe podataka, a za potrebe ovog diplomskog rada fokus je na zloupotrebi podataka u Trumpovoj predsjedničkoj kampanji, u Brexit kampanji za izlazak Velike Britanije iz Europske unije te će se iznijeti detalji slučaja tužbe privatne osobe Davida Carolla prema Cambridge Analytici do koje je došlo nakon što je Caroll zatražio uvid u osobne podatke koje tvrtka posjeduje o njemu. Analizom sadržaja dokumentarnog filma i odabranih članaka utvrđen je tijek događaja iznesen u nastavku.

2013 – Lansiranje aplikacije „*thisisyourdigitallife*“

Akademik Sveučilišta u Cambridge-u, Aleksandr Kogan, izradio je aplikaciju „*thisisyourdigitallife“* koja je bila vrsta testa osobnosti. Prema sudskim iskazima zviždača i bivšeg zaposlenika CA-e Christophera Wileya, Steve Bannon, izvršni voditelj Trumpove predsjedničke kampanje i bivši suvlasnik CA-e, imao je stav da se „društvo prvo mora slomiti u male dijelove kako bi se ti dijelovi iznova mogli formirati u oblik društva kakav želimo“ i upravo je to bilo *oružje* koje je Bannon htio sagraditi u naumu da se to iskoristi u nadolazećim predsjedničkim izborima. Bannon se obraća Wileyu, koji odlazi profesoru Koganu, koji tada formira ideju o spomenutoj aplikaciji i izrađuje ju. Aplikaciji se pristupalo putem Facebooka, i aplikacija je prikupljala podatke svih ljudi koji su riješili test, ali i svih *Facebook* prijatelja od tih ljudi. Sam test je odavao veoma osobne podatke, kao što su informacije o preferiranom provođenju slobodnog vremena, osobnosti, emocijama i sl. Ukoliko je netko *Facebook* prijatelj s osobom koja je pristupila spornoj aplikaciji, ta osoba je također žrtva prikupljanja podataka. Podaci koji su se prikupljali uključuju: javne objave, like-ove, privatne poruke itd. te su se na temelju tih podataka oblikovale osobnosti tih korisnika, odnosno glasača u Americi. Prema direktnim navodima CA-e, tvrtka je na ovaj način posjedovala 5000 jedinica informacija o svakom glasaču u SAD-u. Wiley potvrđuje kako ljudi nisu znali da su im se podaci prikupljali na taj način, niti su na to pristali. Tvrdi kako se radilo o psihološkoj igri na razini jedne cijele nacije s ciljem manipuliranja demokratskih procesa.

2014 — Promjena sigurnosnih pravila u *Facebooku*

Kako bi se ograničio pristup osobnim podacima koje posjeduje *developer* spomenute aplikacije, tvrtka *Facebook* promijenila je sigurnosne uvjete kako bi osigurala da treća strana više nema uvid u osobne podatke korisnika, bez prethodnog pristanka na to od strane korisnika. Međutim, problem je u tome što promjena ovih sigurnosnih pravila ne može povratiti podatke koji su do tog trenutka već prikupljeni.

2015 – Predsjednička kampanja Ted Cruza

U javnost je krajem 2015. godine proizašla vijest o suradnji Ted Cruza i Cambridge Analytice za vrijeme Cruzove predsjedničke kampanje. Sam Cruz potvrdio je suradnju i korištenje milijuna psiholoških podataka kako bi postigao natjecateljsku prednost među svojim protukandidatima. Kada je priča dospjela u javnost, *Facebook* je optužen za nedovoljne sigurnosne mjere i nedovoljnu kontrolu korištenja osobnih podataka svojih korisnika. Mark Zuckerberg, vlasnik tvrtke *Facebook*, tada je pravnim postupkom zatražio od poduzeća CA-e i *developera* Kogana da se svi *neprimjereno* prikupljeni podaci izbrišu iz njihovih baza podataka. Cambridge Analytica tada daje javno priopćenje kako su podaci izbrisani, što se kasnije pokazalo kao neistinit navod.

2016 — Predsjednička kampanja Donalda Trumpa

U vrijeme kandidature Donalda Trumpa za predsjednika SAD-a, Trumpov tim počeo je ulagati velike iznose u oglašavanje putem Facebooka, oko otprilike 1 milijun dolara dnevno. Ljudi koji su radili na Trumpovoj kampanji surađivali su s Cambridge Analyticom pod projektom imena *Project Alamo*. Dokazi ove suradnje kasnije su za vrijeme sudskog postupka proizašli u javnost, točnije *mailovi* između zaposlenika SCL grupe, Alexandera Nixa i Brittany Kaiser, snimke skrivene kamere i sl. Prema kasnijem svjedočenju Brittany Kaiser, način na koji su se prikupljeni podaci iskorištavali u sklopu Trumpove predsjedničke kampanje je sljedeći. Prvi korak je bilo oblikovanje osobnosti na temelju prikupljenih osobnih podataka kako je navedeno ranije u tekstu. Zatim su se izdvojile oni pojedinci koji su imali osobnost nazvanu *persuadables*, što bi u prijevodu značilo *da ih se može nagovoriti*, odnosno pojedince bez čvrsto određenog stava. U kontekstu političkih izbora, to su bili glasači koji nisu bili u potpunosti sigurni za koga glasati. Zatim su se odabrale savezne države SAD-a koje su u predizbornim anketama pokazivale gotovo izjednačen rezultat između Trumpa i njegove najveće protukandidatkinje Hillary Clinton.

Ciljana populacija na koju se trebalo fokusirati su bile osobe bez čvrstog stava u odabranim saveznim državama. Kreativni tim CA-e kreirao je personalizirani sadržaj koji se tada plasirao *targetiranim* glasačima diljem svih digitalnih platformi koje ti korisnici koriste, sve dok ti pojedinci nisu vidjeli svijet na način koji je Trumpov tim htio, odnosno sve dok nisu odlučili svoj glas dati Trumpu. Spomenuti kreativni sadržaj podrazumijevao je javno sramoćenje H. Clinton, prikazivanje kandidatkinje u lažno negativnom svjetlu, a cijela kampanja protiv Clinton u poduzeću CA nazvana je *„porazimo prevaranticu Hillary“ (eng. „Defeat Crooked Hillary“)*. Agresivnim plasiranjem u javnost sadržaja koji su stvarali negativnu sliku o Hillary Clinton postignuta je manipulacija američkih glasača, a kao rezultat takve manipulacije Clinton gubi predsjedničke izbore od Trumpa.

Slika 4. Logo kampanje "Defeat Crooked Hillary"

Izvor: „Defeat Crooked Hillary“ Facebook stranica. https://www.facebook.com/pg/Defeat-Crooked-Hillary-1739342232972780/posts/?ref=page_internal *(pristupljeno 03.03.2020.)*

17. ožujka 2018. – Javno razotkrivanje od strane zviždača Christophera Wileya

Carole Cadwalldr, istražna novinarka za *The Guardian*, kontaktirala je Christophera Wileya, već tada bivšeg zaposlenika Cambridge Analytice, koji je tada za javnost otkrio sve ilegalne radnje Cambridge Analytice. Wiley je bio jedan od osoba koji je bio uz CA-u od samog početka, pomogao je uspostaviti poduzeće, a kasnije je radio kao znanstvenik koji se bavi obradom podataka.

Prema Wileyu, CA na nepošten je način prikupila osobne podatke od 50 milijuna *Facebook* korisnika (kasnije se dokazalo kako je ta brojka bila i veća – 87 milijuna). Nadalje, tvrdi kako su se podaci koje je CA obrađivala, koristili kako bi se razvila psihografički profili ljudi u Americi koji su tada postali ciljana meta za *online* distribuciju materijala koji idu u prilog Trumpu. Nakon razotkrivanja od strane Wileya, CA zanijekala je da su bilo koji od spomenutih podataka korišteni u svrhu Trumpove kampanje.

20. ožujka 2018. – Otvorena istraga protiv *Facebooka*

Samo 3 dana nakon iskaza C. Wileya, *Federal Trade Commission* SAD-a pokrenula je istragu kako bi se dokazalo je li Facebook prekršio neki od zakona vezanih uz zaštitu privatnosti osobnih podataka njegovih korisnika.

10. travnja 2018 – 23. srpnja 2019. - Daljnji sudski postupak protiv *Facebooka*

Zuckerberg je svjedočio pred kongresom te je izjavio kako su u *Facebooku* došli do novih saznanja kako CA nije izbrisala osobne podatke koje je obećala izbrisati. U nekoliko svjedočenja koja su uslijedila, Zuckerberg je izjavio kako priznaje da u *Facebooku* nisu učinili dovoljno za zaštitu osobnih podataka i da je greška njega i njegovih zaposlenika to što nisu znali za takvu zloupotrebu *Facebookovih* podataka. Grupa odvjetnika pokrenula je sudsku tužbu protiv *Facebooka* i Cambridge Analytice, a kasnije je još jedna tužba protiv *Facebooka* pokrenuta od strane Aleksandra Kogana. U sudskom postupku protiv Cambridge Analytice u javnost su proizašli razni dokazi. Brittany Kaiser je, između ostalog, kao dokaz priložila datoteku s podacima 30 milijuna *Facebook* korisnika u vlasništvu CA-e, na dan 4.3.2016. godine, što je bilo nakon što je tvrtka pred sudom tvrdila kako su ti podaci izbrisani. Nix, glavni izvršni direktor CA-e, pred sudom je zanijekao sve optužbe. Kasnije, za vrijeme trajanja sudskog procesa, u javnost su procurile snimke skrivene kamere na kojima Nix govori i izjavljuje kako je CA zaslužna za sve istraživanje, podatke, analize podataka, *targeting*, cijelu digitalnu kampanju, formiranje komunikacijske

strategije Trumpove predsjedničke kampanje. Nakon tih snimaka, uslijedila je suspenzija Nixa od Cambridge Analytice koja je prekinula s poslovanjem 2. svibnja 2018. godine i pokrenula postupak bankrota. Sudski postupak protiv Facebooka završen je 23. srpnja 2019. godine kada se *Facebook* nagodio i pristao platiti kaznu od 5 milijardi dolara.

Brexit

Tijekom skandala orijentiranog uglavnom na slučaj Cambridge Analytice i Trumpove predsjedničke kampanje, u javnost su proizašli različiti dokazi koji upućuju na suradnju Cambridge Analytice i Nezavisne strane Ujedinjenog Kraljevstva, UKIP, (*United Kindgdom Independent Party*). Kaiser i Wiley svjedočili su protiv CA-e i UKIP-a, uz priložene dokaze *mailova* u kojima je vidljiva povezanost ovih dviju strana. Prema navodima zviždača, Cambridge Analytica provodila je isti postupak kao i u Trumpovoj kampanji, samo s drugačijim ciljem – da navede javnost Velike Britanije na glasanje za izlazak iz Europske unije, što se u konačnici i dogodilo. Iako su dokazi bili brojni i čvrsti, rezultati referenduma nisu poništeni do danas.

Slučaj Davida Carrola protiv Cambridge Analytice

Treća priča prikazana u promatranom dokumentarcu orijentirana je na Davida Carrola koji je pokrenuo sudski postupak protiv poduzeća Cambridge Analytica kako bi dobio uvid u osobne podatke koje CA posjeduje, način na koji su isti prikupljeni i procesuirani te s kime su podijeljeni. Zakonsko pravo svakog čovjeka je znati te podatke, a dužnost svakog poduzeća je pružiti te iste informacije. Suđenje je trajalo dugo, a rezultiralo je priznanjem krivice od CA-e i odbijanjem isporuke Carrollovog zahtjeva. U jednom priopćenju, CA je poručila kako *David Carrol nema ništa više prava na to što traži nego član Talibana koji sjedi u spilji u Afganistanu.*

6.4. Sažetak rezultata istraživanja

Istraživanjem odabranog istraživačkog materijala vidljivo je kako je poduzeće Cambridge Analytica zlouporabilo osobne podatke korisnika društvene mreže *Facebook*. Korisnici nisu znali na koje načine se njihovi podaci iskorištavaju te je stoga logično zaključiti kako nisu dali ni svoj pristanak na takvo korištenje osobnih podataka. Cambridge Analytica surađivala je s velikim političkim kampanjama iznimnog značaja, kao što su predsjednički izbori u SAD-u i referendum Velike Britanije za izlazak iz Europske unije. Cijela afera završila je zatvaranjem spornog poduzeća i kazne od 5 milijardi dolara koju je platilo poduzeće *Facebook* radi nedostatne zaštite osobnih podataka svojih korisnika.

7. DISKUSIJA

7.1. Elaboracija hipoteza

H1: Osobni e-podaci zloupotrebljavaju se s ciljem manipuliranja javnosti.

H2: Društvene mreže su glavni izvor zlouporabe osobnih e-podataka.

H3: Zlouporaba osobnih e-podataka može imati presudnu ulogu u stavovima javnosti.

Izjava Brittany Kaiser i dokazi koje je priložila na sudu opisuju načine prikupljanja osobnih podataka te načine obrade i iskorištavanja istih s ciljem promjena mišljenja i stavova šire javnosti, odnosno manipulacije. Osobni podaci su se prikupljali, razvrstavali i zatim su se na temelju grupiranih skupina podataka o individualnim osobama kreirali psihološki profili korisnika interneta. Izdvajali su se oni pojedinci čije su psihološke karakteristike i osobine odavale kako nemaju čvrst stav. Zatim je Trumpov tim koji je provodio cijeli postupak u suradnji s Cambridge Analyticom, fokus stavljao upravo na te korisnike koje se tada „*bombardiralo*“ s negativnim objavama o kandidatkinji Hillary Clinton u svrhu kreiranja negativnog stava prema Trumpovoj najvećoj protivnici. Kampanja protiv Clinton sadržavala je govore mržnje, laži i izvrnute informacije kako bi javnost *zamrzila* Hillary i dala svoj glas Trumpu, što se na kraju i dogodilo. Osim u Trumpovoj kampanji, Cambridge Analytica je siti proces provodila u raznim drugim političkim kampanjama, od kojih je značajnija kampanja Brexit – kampanja Nezavisne stranke Ujedinjenog Kraljevstva za izlazak Velike Britanije iz Europske unije. Na isti način, Cambridge Analytica je svojim djelovanjem postigla formiranje stava šire javnosti kako na referendumu trebaju glasati za izlazak iz Europske unije. Kao i u ostalim političkim kampanjama na kojima je CA radila, i ova je rezultirala uspješno za to poduzeće, odnosno, cilj je postignut i glasovi za izlazak iz EU su prevagnuli.

Iz navedenog je razvidno da su **prva hipteza H1** i **treća hipoteza H3** ovog rada **potvrđene**, odnosno da se osobni e-podaci zloupotrebljavaju s ciljem manipuliranja javnosti te da zloupotreba osobnih e-podataka može imati presudnu ulogu u stavovima javnosti.

Cambridge Analytica osobne podatke korisnika interneta prikupljala je putem aplikacije koju je izradila treća strana, a koja je bila povezana s društvenom mrežom *Facebook*. Naime, izrađena je aplikacija u obliku testa osobnosti koji su korisnici rješavali. U aplikaciju se prijavljivalo putem *Facebooka*, a jednom kada se korisnik prijavio, aplikacija je tada stekla uvid u osobne podatke tog korisnika i svih *Facebook* prijatelja te osobe. Spomenuta aplikacija tako je ilegalno prikupljala podatke koje je zatim prodala poduzeću Cambridge Analytica. Konkretno, radilo se o osobnim podacima 87 milijuna korisnika *Facebooka* koje je tada CA dalje obrađivala. Vezano uz slučaj Cambridge Analytice i *Facebooka*, i od strane suda je potvrđeno kako i društvena mreža *Facebook* mora snositi svoj dio odgovornosti i platiti kaznu jer je dozvolila ovakvu zloupotrebu osobnih podataka. Ovime je **druga hipoteza H2** ovog diplomskog rada koja govori kako su glavni izvori zloupotrebe osobnih e-podataka društvene mreže **potvrđena**.

7.2. Interpretacija rezultata istraživanja

Istraživanjem odabranog istraživačkog materijala, vidljivo je kako se radi o teškim političkim optužbama velikih razmjera. Sporni slučajevi kroz koje je prolazilo poduzeće Cambridge Analytica sadržavali su mnoštvo dokaza koji su upućivali na ilegalne radnje od strane CA-e i različitih političkih stranaka te utjecajnih političara diljem svijeta. Međutim, usprkos svim svjedočenjima i dokazima, Cambridge Analytica je *tiho* prestala s radom i proglasila bankrot bez ozbiljnijih posljedica i snošenja odgovornosti. Na saslušanju Europskog parlamenta tijekom slučaja Cambridge Analytice, izjavljeno je kako je dokazano da ne više ne postoji dostatan politički sustav za provedbu poštenih i legitimnih političkih izbora, pa ipak, rezultati referenduma za izlazak Velike Britanije iz

Europske unije nisu osporeni. Na temelju promatranog materijala, za zaključiti je kako je potrebno puno više od svega što se dogodilo u navedenim slučajevima, kako bi se svrgnule određene političke stranke, poduzeća i organizacije. Postavlja se pitanje jesu li pošteni demokratski izbori uopće više mogući u današnjem društvu.

7.3. Kritički osvrt, primjena rezultata, preporuke

Provedeno istraživanje potvrdilo je sve tri hipoteze ovog diplomskog rada, što je zapravo zabrinjavajuće jer su potvrđeni najveći strahovi svih korisnika interneta. Ne možemo sa sigurnošću znati da se sve navedeno ne odvija i dalje ili da se neće odvijati u budućnosti, a ono što najviše zabrinjava je to hoće li javnost znati o slučajevima zloupotrebe osobnih podataka u budućnosti. Slučaj Cambridge Analytice iznimno je zanimljiv i rezultati su od interesa široke populacije. Živimo u doba kada su osobni podaci najvrjedniji resurs pa je teško za očekivati da je ovime što se dogodilo okončano bilo kakva daljnja zloupotreba podataka na ovaj način. Zanimljiv je podatak da SCL grupa ima mnogo sestrinskih poduzeća diljem svijeta i za pretpostaviti je da će nastaviti djelovati na isti način u drugim dijelovima svijeta pod drugim imenima. U budućnosti bi bilo zanimljivo provesti istraživanje o sestrinskim poduzećima SCL grupe i njihovim djelatnostima kao nadogradnju ovog istraživanja. Vjerujem kako bi se time došlo do zanimljivih podataka i saznanja.

8. ZAKLJUČAK

S razvojem tehnologije, život je postao nezamisliv bez mobilnih uređaja u našoj svakodnevici. Putem svih aplikacija koje koristimo, postajemo umreženi i odajemo naše osobne podatke bez da smo toga svjesni i bez ikakvog saznanja o tome kome idu ti podaci i na koji ih način druga strana koristi. Živimo u doba velikih podataka, u kojem se velike svjetske kompanije obogaćuju na temelju osobnih informacija čija je zaštita nedovoljno zaštićena propisima i zakonima, a čije upravljanje gotovo da nema nadzora. Digitalna poduzeća korisnicima nude jeftine aplikacije koje su im privlačne, korisne i zabavne u zamjenu za osobne informacije o njima koje mogu prikupiti putem interneta. Mali broj ljudi razumije stvarnu razinu rizika kada se radi o zloupotrebi osobnih podataka, a poduzeća koja se time bave mogu uspješno skrivati zloupotrebu podataka dulje vrijeme prije negoli netko shvati o čemu se zapravo radi. U većini slučajeva, sama poduzeća nisu svjesna svih načina na koje zloupotrebljavaju osobne podatke ljudi, a tada je nekome van tog poduzeća još teže utvrditi raditi li se o dozvoljenim radnjama ili o zloupotrebi.

Godinama se spominje kako se osobni podaci prikupljaju u razne svrhe, međutim, smatram kako tek počinjemo shvaćati dublje ciljeve koji stoje iza toga. Dugo vremena, generalno mišljenje je prevladavalo kako se prikupljeni osobni podaci ipak ne koriste u ozbiljne svrhe, a spomenuti slučajevi u ovom radu, ali i neka druga novija saznanja po pitanju zloupotrebe osobnih podataka u svijetu ukazuju na to kako smo kao društvo općenito bili u zabludi. Kada u potpunosti shvatimo da nikada nećemo moći sa sigurnošću znati što je istina, a što nam se samo prezentira kao istina, možda budemo korak bliže da se manipulaciji na temelju velikih podataka stane na kraj.

9. LITERATURA

Tiskani izvori:

1. Acquisti, Alessandro. 2010. *The economics of personal data and the economics of privacy.* Heinz College. Carnegie Mellon University.
2. Heaney, Catherine; Israel, Barbara. 2008. Social networks and social support. *Health behaviour and health education: Theory, research, and practice.* 4. 189-210.
3. Stafford, Paul. 2012. *Protecting Your Digital Privacy*. Paul Stafford.
4. Cherry, Denny. 2013. *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online*. Elsevier Science. Waltham.
5. Laney, Doug. 2001. *3d data management: Controlling data volume, velocity and variety*. META Group.

Mrežni i elektronički izvori:

1. Agencija za zaštitu osobnih podataka. *Zaštita osobnih podataka u RH*. https://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (pristupljeno 27.02.2020.)
2. Amer, Karim; Noujaim,Jehane. 2019. *The Great Hack.* Dokumentarni film. Netflix.
3. Annual Reports. *Acxiom 2018 Annual Report*. http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ACXM_2018.pdf (pristupljeno 27.02.2020.)
4. BBC News. *Cambridge Analytica's Kenya election role 'must be investigated'.*https://www.bbc.com/news/world-africa-43471707 (pristupljeno 28.02.2020.)
5. Cambridge Analytica. Web arhiva. https://web.archive.org/web/20160624121051/https://cambridgeanalytica.org/about (pristupljeno 27.02.2020.)
6. Cadwalladr, Carole; Graham-Harrison, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (pristupljeno 03.03.2020.)

7. Dellinger, AJ. *Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?* https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#26d72e43567f (pristupljeno 27.02.2020.)
8. Dhawan, Vikas; Zanini, Nadir. 2014. Big data and social media analytics. *Research Matters: A Cambridge Assessment publication 28*. 36-41. https://www.cambridgeassessment.org.uk/Images/465808-big-data-and-social-media-analytics.pdf (pristupljeno 27.02.2020.)
9. European Comission. *What is personal data?*https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (pristupljeno 26.02.2020.)
10. European Commission. *Digital Privacy*. https://ec.europa.eu/digital-single-market/en/online-privacy (pristupljeno 27.02.2020.)
11. Europska unija. *Zaštita podataka i privatnost na internetu*. https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm#shortcut-1 (pristupljeno 27.02.2020.)
12. Facebook. *Pravila o upotrebi podataka.*https://www.facebook.com/policy.php (pristupljeno 26.02.2020.)
13. Fruhlinger, Josh. *Marriott data breach FAQ: How did it happen and what was the impact?* https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (pristupljeno 27.02.2020.)
14. GDPR. *What are the GDPR Fines?*. https://gdpr.eu/fines/ (pristupljeno 27.02.2020.)
15. Gross, Ralph; Acquisti, Alessandro. 2005. Information revelation and privacy in online social networks*. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society.* 71-80. https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf (pristupljeno 18.02.2020.)
16. Grothaus, Michael. *Mexico is investigating companies with links to Cambridge Analytica*. https://www.fastcompany.com/40556882/mexico-is-investigating-companies-with-links-to-cambridge-analytica (pristupljeno 28.02.2020.)
17. Heshmaty, Alex. *What is data misuse?*https://www.infolaw.co.uk/newsletter/2019/11/what-is-data-misuse/ (pristupljeno 18.02.2020)
18. Ingram, David. Factbox: Who is Cambridge Analytica and what did it do? https://www.reuters.com/article/us-facebook-cambridge-analytica-

factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F (pristupljeno 28.02.2020.)
19. Intel IT Center. 2012. *Peer Research Big Data Analytics*. Intel. https://www.intel.com/content/dam/www/public/us/en/documents/reports/data-insights-peer-research-report.pdf (pristupljeno 26.02.2020.)
20. Lang'at, Patrick. *Cambridge Analytica staff Dan Mureşan died while working in Kenya*. https://www.nation.co.ke/news/politics/Cambridge-Analytica-staff-Dan-Mure-an-died-in-Kenya/1064-4351058-11gicwcz/index.html (pristupljeno 28.02.2020.)
21. Leetaru, Kalev. 2018. *Social Media Companies Collect So Much Data Even They Can't Remember All The Ways They Surveil Us.* https://www.forbes.com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/#548681227d0b (pristupljeno 26.02.2020.)
22. Leetaru, Kalev. 2019. *How Big Is Social Media And Does It Really Count As 'Big Data'?* https://www.forbes.com/sites/kalevleetaru/2019/02/11/how-big-is-social-media-and-does-it-really-count-as-big-data/#44d51393f2c1 (pristupljeno 26.02.2020.)
23. Matende, David. *Media, like false preachers*. http://nairobilawmonthly.com/index.php/2018/06/05/media-like-false-preachers/ (pristupljeno 28.02.2020.)
24. Matsakis, Louise. *The WIRED Guide to Your Personal Data (and Who Is Using It).*https://www.wired.com/story/wired-guide-personal-data-collection/ (pristupljeno 26.02.2020.)
25. Meredith, Sam. *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal.*https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html (pristupljeno 03.03.2020.)
26. Naylor, Brian. *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?* https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it?t=1582788767301 (pristupljeno 27.02.2020.)
27. Osborne, Hilary. *What is Cambridge Analytica? The firm at the centre of Facebook's data breach*. https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach (pristupljeno 27.02.2020.)
28. Perlorth, Nicole*. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html (pristupljeno 27.02.2020.)

29. Punit, Itika Sharma. *Cambridge Analytica's parent firm proposed a massive political machine for India's 2014 elections*. https://qz.com/1239561/cambridge-analyticas-parent-firm-proposed-a-massive-political-machine-for-indias-2014-elections/ (pristupljeno 28.02.2020.)
30. Quartz. *Cambridge Analytica's parent firm proposed a massive political machine for India's 2014 elections*. https://qz.com/1239561/cambridge-analyticas-parent-firm-proposed-a-massive-political-machine-for-indias-2014-elections/ (pristupljeno 28.02.2020.)
31. Ragan, Steve. *412 million FriendFinder accounts exposed by hackers*. https://www.csoonline.com/article/3139311/412-million-friendfinder-accounts-exposed-by-hackers.html (pristupljeno 27.02.2020.)
32. Rehman, Ikhlaq. 2019. Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice 2497*. 1-11. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac (pristupljeno 28.01.2020.)
33. Roos, Dave. *How Online Social Networks Work*. https://computer.howstuffworks.com/internet/social-networking/information/how-online-social-networks-work.htm (pristupljeno 26.02.2020.)
34. Salinas, Sara. *Facebook says the number of users affected by Cambridge Analytica data leak is 87 million*. https://www.cnbc.com/2018/04/04/facebook-updates-the-number-of-users-impacted-by-cambridge-analytica-leak-to-87-million-.html (pristupljeno 28.01.2020.)
35. Samsel, Haley; Svitek, Patrick. *Ted Cruz says Cambridge Analytica told his presidential campaign its data use was legal.* https://www.texastribune.org/2018/03/20/ted-cruz-campaign-cambridge-analytica/ (pristupljeno 03.03.2020.)
36. SCL Elections. Web arhiva. https://web.archive.org/web/20110716020144/http://sclelections.com/9/about-scl-elections/what-we-do.html (pristupljeno 27.02.2020.)
37. Scott, Mark. *Cambridge Analytica did work for Brexit groups, says ex-staffer.*https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/ (pristupljeno 28.02.2020.)
38. Scott, Mark. *Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower*. https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/ (pristupljeno 28.01.2020.)

39. Springfield! Springfield*! The Great Hack (2019) Movie Script*. https://www.springfieldspringfield.co.uk/movie_script.php?movie=the-great-hack (pristupljeno 02.03.2020.)
40. Statista. *Forecast of Big Data market size, based on revenue, from 2011 to 2027*. https://www.statista.com/statistics/254266/global-big-data-market-forecast/ (pristupljeno 27.02.2020.)
41. The Guardian. *What is Cambridge Analytica? The firm at the centre of Facebook's data breach*. https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach (pristupljeno 27.02.2020.)
42. The National Supervisory Authority For Personal Data Processing, Romania. *The protection of personal data and the social network websites*. https://www.dataprotection.ro/index.jsp?page=The_protection_of_personal_data_and_the_social_network_websites&lang=en (pristupljeno 27.02.2020.)
43. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ. (Opća uredba o zaštiti podataka). SL EU L119. https://www.zakon.hr/z/1021/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-%28EU%29-2016-679 (pristupljeno 27.02.2020.)
44. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka. Narodne novine, br. 139/04. http://www.propisi.hr/print.php?id=3970 (pristupljeno 27.02.2020.)
45. Ustav Republike Hrvatske. Narodne novine, br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01 i 55/01. Članak 37. https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske(pristupljeno 27.02.2020.)
46. Ward, Jonathan Stuart; Barker, Adam. 2013. *Undefined by data: a survey of big data definitions.* School of Computer Science. University of St Andrews, UK. arXiv preprint arXiv:1309.5821. https://arxiv.org/pdf/1309.5821.pdf (pristupljeno 26.02.2020.)
47. Zakon o provedbi Opće uredbe o zaštiti podataka. Narodne novine, 42/18. https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka (pristupljeno 27.02.2020.)

POPIS ILUSTRACIJA

Slika 1. Predviđanje tržišta velikih podataka na temelju ukupnih godišnjih prihoda za period 2011.-2027.....7
Slika 2. Povezanost ključnih osoba Cambridge Analytice 22
Slika 3. Obećanje većeg broja glasova od strane SCL Elections na njihovoj web stranici .. **Error! Bookmark not defined.**
Slika 4. Projekti SCL grupacije u Indiji.....26

Tablica 1. Glavni likovi dokumentarnog filma (po redoslijedu prikazivanja) 29

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, Josip Rašić pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor diplomskog rada pod naslovom Zloupotreba osobnih e-podataka: Studija slučaja na primjeru Cambridge Analityca te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student:
Josip Rašić

(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, Josip Rašić neopozivo izjavljujem da sam suglasan s javnom objavom diplomskog rada pod naslovom Zloupotreba osobnih e-podataka: Studija slučaja na primjeru Cambridge Analityca čiji sam autor.

Student:
Josip Rašić

(vlastoručni potpis)