# Mehanizmi zaštite, upravljanja i korištenja osobnih podataka

**Saić, Daria**

**Professional thesis / Završni specijalistički**

**2019**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:148:068813

**EKONOMSKI FAKULTET**

**Zagreb**

**Sveučilišni studij POSLOVNA EKONOMIJA**

ZAVRŠNI RAD

# MEHANIZMI ZAŠTITE, UPRAVLJANJA I KORIŠTENJA OSOBNIH PODATAKA

# MECHANISMS FOR THE PROTECTION, MANAGEMENT AND USE OF PERSONAL DATA

Daria Saić

Zagreb, rujan 2019.

**EKONOMSKI FAKULTET**

**Zagreb**

**Sveučilišni studij POSLOVNA EKONOMIJA**

ZAVRŠNI RAD

# MEHANIZMI ZAŠTITE, UPRAVLJANJA I KORIŠTENJA OSOBNIH PODATAKA

# MECHANISMS FOR THE PROTECTION, MANAGEMENT AND USE OF PERSONAL DATA

Daria Saić: 0067470635

Kolegij: Informatika

Mentor: Prof. dr. sc. Ivan Strugar

Zagreb, rujan 2019.

_____

Ime i prezime studenta/ice

# IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____

(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu,_____ _____

(potpis)

# Sadržaj

# 1. Uvod

Suvremeno društvo suočava se s ubrzanim tehnološkim i informacijskim promjenama koje mijenjaju društvene i kulturne navike suvremenog čovjeka. Ubrzani rast zahtijeva i usklađivanje zakonodavnih akata te primjenu modernih metoda u sprječavanju zloupotrebe tehnologije i informacijskih sustava. Jedan od važnih segmenata zaštite privatnosti i sprječavanja zloupotrebe je kontrola i zaštita osobnih podataka. Svijet u kojem je informacija ključna za razmjenu podataka, komunikaciju, ali i upotrebu u marketinške i poslovne svrhe zahtijeva zakonsku regulativu koja će pratiti i određivati pravila korištenja osobnih podataka u virtualnom svijetu prikupljanja i korištenja istih. Ovaj završni rad za svoj cilj ima utvrditi uz pomoć deskriptivne metode i primjera iz prakse mehanizme zaštite, upravljanja i korištenja osobnih podataka u današnjem vremenu.

Cilj ovoga rada je na temelju relevantne znanstvene literature definirati što su to osobni podatci, kako se u Republici Hrvatskoj štiti prikupljanje i korištenje osobnih podataka te jesu li hrvatski zakoni usklađeni s europskim i svjetskim na tom polju. Osim toga, cilj je opisati kako se primjenjuje europska legislativa o zaštiti podataka u svjetskim razmjerima, ali i u Hrvatskoj. Također, rad će upozoriti na opasnosti socijalnog inženjeringa i nakon njegova definiranja navedeni će biti načini kako se od njega zaštiti.

Veliki podatci i rudarenje podataka u suvremenom poslovnom svijetu postavljaju novitete u načinu poslovanja. Iz toga razloga ovaj rad će ukazati na promjene koje se događaju uslijed korištenja suvremenih izvora informacija za poboljšanje poslovanja, posebice u sferi korištenja osobnih podataka u marketinške svrhe te korištenja baza podataka koje olakšavaju oglašavanja i stvaranje potrebe klijentima.

S obzirom, da rad nastaje u vremenu u kojoj je zloupotreba osobnih podatak aktualna problem cilj je opisati najpoznatije slučajeve rudarenja podataka na primjeru korištenja i prikupljanja podataka putem društvene mreže *Facebook*. Ovome dijelu rada kao izvor poslužit će novinski izvještaji jer se radi o aferama u predizbornoj kampanji *Donalda Trumpa* i potpori izlaska Velike Britanije iz Europske unije.

# 1. Osobni podatci

Prema definiciji Europske unije i zakonodavstva kojega je prihvatila i Republika Hrvatska svojim pristupanjem Europskoj uniji 2013. godine osobni podatci su *„sve informacije koje se odnose na pojedinca čije je identitet utvrđen ili se može utvrditi“.*[1] Također, to su i informacije koje zajedno prikupljene mogu dovesti do utvrđivanja identiteta osobe. Pod osobne podatke ubrajaju se i informacije koje su deidentificirane, šifrirane ili pseudonimizirane jer se njihovom upotrebom može utvrditi identitet. Pseudonimizacija označuje obradu osobnih podataka na način da se osobni podatci više ne mogu pripisati određenoj osobi bez upotrebe dodatnih informacija i to pod uvjetom da se takve dodatne informacije drže odvojeno pod određenim kriterijima koji onemogućavaju povezivanje i otkrivanje identiteta.[2]

Konkretno, osobni podaci su: ime i prezime, kućna adresa, e-mail adresa koja je u formi ime.prezime@društvo.com, broj osobne iskaznice, podatci o lokaciji i to primjerice podaci prikupljeni iz funkcija podataka o lokaciji na mobilnom telefonu. Zatim, adresa internetskog porta (*IP*), identifikacijski broj kolačića, oglašavački identifikator telefona te u konačnici podatci kojima raspolažu liječnici opće prakse ili bolnice, a u njima mogu biti simboli iz koji se može utvrditi jedinstveni identitet osobe.[3] Ovdje se pridodaju i genetski podatci, a to su oni koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o pojedincu i njegovoj fiziologiji ili zdravlju te biometrijski podatci koji su dobiveni tehničkom obradom u vezi s fizičkim, fiziološkim obilježjima, primjerice fotografija lica ili daktiloskopski podatci (otisak prsta).[4]

Pod definicijom osobnih podataka ne smatraju se registracijski broj društva, e-mail adrese u formi info@društvo.hr te anonimizirani podatci. Važnosti pravilnog postupanja s osobnim podatcima doprinose i načela obrade osobnih podataka:

- Načelo zakonitosti, poštenosti i transparentnosti
- Načelo ograničavanja svrhe

[1] *Što su to osobni podaci?* [online]: Europska komisija. Dostupno na: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr [ 25. kolovoza 2018.]
[2] prema: Kladar, D. (2018.) *Kako se pripremiti za GDPR*, Zagreb: Forum poslovni mediji, 8.
[3] prema: *Što su to osobni podaci?* [online]: Europska komisija. Dostupno na: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr [ 25. kolovoza 2018.]
[4] Kladar,Ibid., 8.

- Načelo smanjenja količine podataka (ograničenost podataka s obzirom na svrhu)
- Načelo točnosti
- Načelo ograničavanja pohrane (samo onoliko koliko je potrebno u svrhe za koje se koristi)
- Načelo cjelovitosti i povjerljivosti
- Načelo pouzdanosti
- Načelo zakonitosti obrade[5]

Navedena načela i definicija upozoravaju na više načina i mogućnosti za prikupljanje osobnih podataka. Zasigurno najzastupljeniji način prikupljanja, obrade i korištenja, u današnjem vremenu, je onaj putem informacijskih tehnologija, a posebice Interneta. Internet je globalni informacijsko-komunikacijski sustav koji povezuje računalne mreže pojedinih zemalja i organizacija, te omogućava korisnicima da diljem svijeta putem svojih računala, mobitela ili drugih uređaja na kojim se koriste Internetom međusobno komuniciraju, razmjenjuju informacije i koriste brojne druge usluge.[6] Osnovna opasnost i rizik korištenja Interneta je uz brojne reklame, neželjenu elektroničku poštu, sponzorske reklame, praćenje, ilegalno skidanje podataka, financijske prevare i javnost osobnih podataka te veliki potencijala za zloupotrebu njihove objave.

Iz navedenih razloga priopćavanje osobnih podataka ili datoteka osobnih podataka od strane javnih tijela trećoj osobi, a posebice ako se radi o elektroničkoj izmjeni podataka, treba biti regulirano zakonom o zaštiti osobnih podataka i informacija. Iznošenje osobnih podataka ili datoteka osobnih podataka ne smije doći i iz toga razloga se uvažavaju i primjenjuju zakonske odredbe koje određuju pristup informacijama iz javnog sektora, zaštitu iznošenja podataka osobama koja nisu predmet podataka bez pristanka osobe na koju se podatci odnose. Iz toga razloga, dužnosnici i zaposlenici državnih tijela, tijela jedinice lokalne samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim ili neklasificiranim podatcima dužni su čuvati tajnost za vrijeme i nakon prestanka obavljanja dužnosti.[7]

[5] Kladar, Ibid., 22.
[6] prema: Varga, M., Šimović, V. i Milković, M. (2012.): *Zaštita elektroničkih informacija*. Varaždin, 10.
[7] Varga, Ibid., 10.

Kada se govori o elektroničkoj zaštiti podataka na elektroničkim dokumentima to se može postići postavljanjem lozinki te standardiziranim davanjem imena mapama i dokumentima. Tim se postupkom olakšava pretraživanje datoteka, mapa i podmapa vlasniku i to uz pomoć različitih kreiranih filtera za pretraživanje. Takva sistematizacija spremanja podataka najniža je razina kojoj se osobni podatci na računalu mogu zaštiti. Ipak najvažnija zaštita dolazi iz pravnih okvira, odnosno iz zakona koji štite i uređuju prikupljanje, upravljanje i dijeljenje osobnih podataka. U posljednje vrijeme najviše se govori o primjeni *Opće uredbe o zaštiti podataka* (dalje: *Uredba*) koja je poznatija pod engleskim nazivom *General Data Protection Regulation* (*GDPR*) iz svibnja 2018.

## 1.1 Opća uredba o zaštiti osobnih podataka (General Data Protection Regulation, GDPR)

Pravo na zaštitu osobnih podataka predstavlja temeljno ljudsko pravo. Definiranje zaštite prikupljanja i korištenja osobnih podataka unutar Europske unije datira još iz 1995. godine kada je prvi puta donesena odredba *European Union Data Protection Directive* koja je poslužila kao legalni instrument za zaštitu osobnih podataka na tlu Europske unije, ali i Švicarske koja je jedina zemlja van Europske unije koja je prihvatila ovu odredbu. Kao što je ranije spomenuto, napredak tehnologije sve više je ubrzao i protok informacija i osobnih podataka što je i u europskim krugovima postalo vodeća tema razgovora. Promišljanja su išla u smjeru unaprijeđena zastarjele legislative iz 1995. godine i uvođenje novih suvremenijih odredbi. Prvi korak k tome bio je *Lisabonski sporazum* iz prosinca 2009. gdje se u poglavlju o fundamentalnim pravim Europske unije ističe zaštita prikupljanja i korištenja osobnih podataka. Osnovna razlika između definiranja zaštite podataka 2009. od onoga iz 1995. je upravo u upotrebi Interneta i tako zvanog oblačnog računarstva (eng. *cloud computting)*, što označava virtualno zadržavanje, prikupljanje i dijeljenje osobnih podataka putem Interneta.[8]

Osim navedenih zakonskih odredbi kao osnovno ljudsko pravo zaštita podataka navedena je i u *Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda* (dalje: *Konvencija*). Tako se u članku 7.1 *Konvencije* se navodi:“ *kako svatko ima pravo na poštovanje svog privatnog i obiteljskog života, doma i dopisivanja. Javna se vlast neće miješati u ostvarivanje toga prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne*

[8] prema: Škrinjar Vidović,M., (2016.) EU dana Protetion Reform: Challanges for Cloud computing. *Croatian Yearbook of European Law and Policy*, 12., 172.

*sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprečavanja nereda i zločina, radi zaštite zdravlja ili morala ili zaštite prava i sloboda drugih* ."[9] Iako iz ovog navoda nije direktno naznačena zaštita osobnih podataka tumačenjem je lako zaključiti da se navođenjem dopisivanja i poštivanja sfere privatnog života jasno označava potreba za zaštitom privatnosti od virtualnog svijete koji je povoljan za zloupotrebu osobnih podataka. Razvoj komunikacijskih i informacijskih tehnologija otežava zaštitu privatnosti. Najbolji primjeri zadiranja u privatnost su informacijski kanali poput *YouTube*, pojava društvenih mreža *Facebooka, Instagrama, Twittera,* ali i sve veći razvoj online trgovine.[10]

Ideja zaštite ljudskih prava u vidu sigurnosti osobnih podataka i osiguravanje sigurnog korištenja Internetom i ispravna regulacija korištenja Interneta u svrhe prikupljanja i korištenja osobnih podataka rezultirali su stvaranjem *Uredbe* koju je Europski parlament i Vijeće Europe donijelo i prihvatilo 27. travnja 2016. godine. Tim činom sve članice Europske unije postale su obavezne uskladiti svoje zakonodavstvo s Uredbom i započeti s njenom primjenom. Predmet *Uredbe* je :

> *„zaštita pojedinca glede obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka. Uredbom se štite temeljna prava i slobode pojedinca, a posebno njihovo pravo na zaštitu osobnih podataka. Uredba se primjenjuje na svaku obradu osobnih podataka, bilo ona automatizirana bilo neautomatizirana (ako čini sustav pohrane ili su namijenjeni biti dio sustava pohrane)"*[11]

Primjena *Uredbe* u Republici Hrvatskoj započela je 25. svibnja 2018. godine. Od navedenog datuma započela je primjena koja je donijela prilagodbu ponajprije svih organizacija koje u svakom trenutku moraju znati kako raspolažu osobnim podatcima svojih korisnika, klijenata ili zaposlenika. Nužno je da u svakom trenutku znaju gdje se nalaze osobni podatci, kako su pohranjeni te u koje se svrhe smiju koristiti. Važan dio pravilne primjene *Uredbe* je i da ukoliko vlasnik osobnih podatka želi povući vlastitu privolu danu organizaciji da se služi njegovim osobnim podatcima, organizacija mora imati alate i mogućnosti učiniti brisanje i povlačenje osobnih podataka iz upotrebe u zakonskom roku.[12]

---

[9] Klarić M. (2016.) Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda. *Zbornik radova Pravnog fakulteta u Splitu*, 53./4., 975.
[10] Klarić, Ibid., 975.
[11] Kladar, D. *Kako se pripremiti?,* 15.
[12] prema: *Opća uredba o zaštiti podataka 2018: Što donosi GDPR?* [online] , https://gdpr2018.eu/sto-donosi-gdpr/ [24. kolovoz. 2018.]

Osim na tvrtke i organizacije iz Europske unije, *Uredbi* podliježu i sve tvrtke i organizacije koje surađuju ili prikupljaju podatke o građanima Europske unije. Tako je utvrđeno da je 92% tvrtki iz Sjedinjenih Američkih Država koje surađuju s tvrtkama iz Europske unije tijekom 2018. uskladilo svoj rad s *Uredbom*. Iz ovoga je vidljivo da, iako se *Uredba* direktno odnosi na članice Europske unije, ona ima odjeka i u svjetskim razmjerima, a posebice u virtualnom svijetu koji ne poznaje državne, nacionalne i ekonomske granice. Tako *Uredbi* podliježu i društvene mreže kao što su *Facebook* ili pak velike korporacije poput *Googlea* ili *Microsofta*.[13]

*Uredba* sadrži i pravila o drastičnim kaznama za nepoštivanje odredbi koje su njom prihvaćene. Članak 82. i članak 83. *Uredbe* donose pravila o naknadi štete i odgovornosti za osobu koja je pretrpjela materijalna ili druga oštećenja zbog zloupotrebe osobnih podataka te opće uvjete za izricanje upravnih novčanih kazni. Iznosi koji su navedeni kao moguća kazna dokazuju ozbiljnost i važnost ovoga zakona. Tako se za kršenje pravila obrade, prikupljanja ili zloupotrebe voditelja obrade osobnih podataka može donijeti upravna novčana kazna do 10.000.000 eura, a za poduzetnike do 2% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.[14]

Iz toga razloga brojne su tvrtke i organizacije pristupile promjenama svoga načina poslovanja. Neki od primjera prilagodbe poslovanja je implementacija različitih sporazuma koji u međunarodnim i svjetskim razmjerima uređuju pravila poslovanja i razmjene osobnih podataka. Prvi takav primjer su interna pravila između multinacionalnih kompanija za razmjenu podataka *binding corporate rules* što označava interna pravila između multinacionalnih kompanija za razmjenu podataka posebice sa zemljama u kojima još nije dovoljno razvijena i implementirana zaštita prometa osobnim podacima. Drugi primjer je Sporazum između EU i SAD-a o zaštiti privatnosti podataka (eng: *EU-US privacy shield).* Ova uredba primjenjuje se na zaštitu razmjene podataka u komercijalne svrhe između Europske unije i Sjedinjenih Američkih Država.[15]

---

[13] Opća uredba, Ibid.

[14] prema: *Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinca 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)*: Službeni list Europske unije. L 119/1.

**[15]** prema: Peter Sayer (2016.): 5. things you need to know about the EU-US Privacy Shield agreement [online]: https://www.pcworld.com/article/3038688/privacy/five-things-you-need-to-know-about-the-eu-us-privacy-shield-agreement.html [28. kolovoz 2018.]

Prilagodba tvrtki i organizacija zahtijeva multidisciplinarni pristup jer se prije svega treba ostvariti pravna prilagodba, zatim, uskladiti poslovni procesi te u konačnici osigurati tehničke mogućnosti za pravilnu primjenu *Uredbe* i zaštite osobnih podataka. Prvenstveno, potrebno je provjeriti i procijeniti pripremljenosti tvrtke, nakon čega slijedi izrada interne pravne regulacije primjene *Uredbe,* a u konačnici pravno normiranje prema *Agenciji za zaštitu osobnih podataka* (dalje: *AZOP*), koja je u Republici Hrvatskoj nadležna za pravilnu provedbu i nadzor provedbe *Uredbe*. Posljednja etapa prilagodbe *Uredbi* je primjena tehničkih mogućnosti i nove tehnologije u pravilnom prikupljanju, zaštiti i upotrebi osobnih podataka.

## 1.2 Zaštita osobnih podataka u Republici Hrvatskoj

Ranije je već spomenuto nekoliko primjera zaštite podataka u Republici Hrvatskoj, što je razumljivo s obzirom da je Hrvatska ravnopravna članica Europske unije koja primjenjuje europske zakone i ide u korak s europskim standardima. No, osim primjene *Uredbe*, koja je na hrvatskom prostoru u funkciji i primjeni od svibnja 2018., postoje i posebne odredbe hrvatskog zakonodavstva po pitanju reguliranja i normiranja zaštite osobnih podataka. Osim prihvaćanja europske regulative i njene primjenu, Republika Hrvatska je zaštitu podatka postavila i u najvažnijem zakonodavnom spisu, a to je *Ustav Republike Hrvatske*. Naime, poglavlje III. nosi naslov *Zaštita ljudskih prava i sloboda*, a unutar drugog potpoglavlja, koje govori o osobnim i političkim slobodama i pravima, nalazi se definirano u članku 39. i sigurnost i tajnost osobnih podataka. Ističe se važnost privole ispitanika, što je jedini preduvjet za legalno prikupljanje, obradu i korištenje osobnih podataka. Ustavom se propisuje i zaštita podataka te nadzor nad djelovanjem informatičkih sustava u Hrvatskoj.[16]

Neovisno i samostalno tijelo koje se brine o provedbi i nadzoru primjene usklađivanja rada svih koji podliježu *Uredbi* je *AZOP*. Glavni zadatak *AZOP*-a je djelovanje na ispunjavanju svih prava i obveza na području zaštite osobnih podataka u Republici Hrvatskoj.[17]

*AZOP* je osnovan *Zakonom o zaštiti osobnih podataka,* a istim zakonom su joj dane i ovlasti. Ona obavlja upravne i stručne poslove na temelju javnih ovlasti i to iz različitih djelokruga:

[16] prema: Klarić M. (2016.) Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, 983.
[17] prema: *Statut Agencije za zaštitu osobnih podataka* (2004.), Zagreb, 5.

- Nadzire provođenje zaštite podataka
- Ukazuje na uočene zloupotrebe osobnih podataka
- Sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuću uređenu zaštitu osobnih podataka
- Rješava zahtjeve povodom kršenja i povrede korištenja, prikupljanja i čuvanja osobnih podataka
- Vodi središnji registar
- Naređuje uklanjanja nepravilnosti
- Privremeno zabranjuje prikupljanje, obradu i korištenje osobnih podataka
- Naređuje brisanje osobnih podataka prikupljenih bez pravne osnove
- Zabranjuje iznošenje osobnih podataka iz Republike Hrvatske ako se to protivi hrvatskim zakonima
- Predlaže pokretanje postupka kaznene ili prekršajne naravi pred nadležnim tijelima[18]

U konačnici, *AZOP* osigurava da svaka fizička osoba u Republici Hrvatskoj ima pravovaljanu zaštitu osobnih podataka i to bez obzira na državljanstvo, prebivalište, rasu, boju kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.[19] *AZOP* ima i ulogu predlaganja postupka kaznene ili prekršajne prijave pred nadležnim tijelima i protiv njenih odluka nije dozvoljeno ulaganje žalbe. [20]

Osim u Hrvatskoj i ostale zemlje imaju svoje nacionalne zakone kojima naknadno definiranju zaštitu osobnih podataka. Primjerice, u Njemačkoj *Savezni zakon o zaštiti podataka* sadrži odredbe o zaštiti osobnih podataka u javnom i privatnom sektoru, a strogo su definirani i posebni zakoni za informacijsko komunikacijske sustave. Kao i u Hrvatskoj, zaštita osobnih podataka podignuta je i na ustavnu razinu, a osim saveznog povjerenika za zaštitu osobnih podataka postoji još šesnaest zemaljskih tijela koji se brinu za regulativnost prikupljanje, obrade i korištenja osobnih podataka.[21]

[18] Statut, Ibid, 5.,6.

[19] prema: *Statut Agencije za zaštitu osobnih podataka,* 2004.

[20] prema: *Zaštita osobnih podataka u RH*, Agencija za zaštitu osobnih podataka (AZOP) – službeni letak.

[21] prema: Klarić M. (2016.) Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, 986.,987.

Također, zemlje koje u Europi imaju status izrazito liberalnih, kao što je Nizozemska, imaju snažno definiranu upotrebu osobnih podataka, a posebice zaštitu u virtualnom svijetu. Primjerice, u Nizozemskoj je na snazi *Zakon o zaštiti osobnih podataka*, a *Zakon o telekomunikacijama* je posebno posvećen zaštiti na Internetu. Osim toga, odgovornost za kontrolu regularnosti zaštite podataka provodi Nizozemska ustanova za zaštitu osobnih podataka, a posebno je ustanovljeno i *Neovisno poštansko i telekomunikacijsko tijelo Nizozemske* koje se bavi komunikacijskim i telekomunikacijskim sustavima zaštite.[22] Navedeno, upućuje da hrvatska tijela i zakonodavstvo je usklađeno, ne samo s Europskom unijom, već i s praksama zapadnih demokracija koje na nacionalnim razinama provode zaštitu podataka.

# 2. Socijalni inženjering – primjer zloupotrebe osobnih podataka

Suvremeno društvo živi u dobu kada se ustaljeni pojam kriminala mijenja. On više ne označava samo prijestupe poput pljačke prodavaonica, krađe automobila, otmice ili pak puno gore primjere poput ubojstava. Modernom poimanju kriminaliteta treba se nadodati računalni

[22] Klarić, Ibid., 987.

kriminalitet. Pojam je to koji označava sve vrste kriminala koje su počinjene putem računala ili prikupljenih virtualnih podataka. Neke od najčešćih zloupotreba računala i računalnih programa su neželjena elektronička pošta (eng: *spam),* koji su alat brojnih tvrtki koje prikupljanjem adresa elektroničke pošte adresa reklamiraju svoje vlastite proizvode. Korištenje elektroničkih adresa bez privole njenog vlasnika, a posebice ako je u formi ime.prezime@info.hr označava zadiranje i kršenje Opće *uredbe o zaštiti podataka*. Statistika upozorava da u današnjem vremenu dvije od tri poslane elektroničke pošte su neželjena elektronička pošta (eng. *spamovi).*[23]

Osim neželjene elektroničke pošte tu su i maliciozni programi (eng: *malware)* što označava različite vrste računalnih virusa, ali i crve te trojance koji napadaju naša osobna računala i na taj način preuzimaju osobne podatke. Kako bi se spriječili napadi malicioznih programa korisni su antivirusni programi i upotreba sigurnosnih stjenki što je kombinacija programske (eng. *softvera)* zaštite i strojne zaštite (eng. *hardvera)* koje izoliraju unutarnju mrežu organizacije od Interneta.[24] Posebna povreda osobnih podataka se događa kod klasičnih prijevara koje podrazumijevanju najčešće namjerno krivo unošenje osobnih podataka koji nisu pravovaljani. Ovakve prijevare je nekada teško detektirati posebice ako se na više mjesta krivi podatak ponavlja.

Ipak, osim gore navedenih, najzastupljenije zlouporabe informacijsko komunikacijskih sustava na polju osobnih podataka događaju se na društvenim mrežama. Osim što su društvene mreže predmet kriminalnih djelatnosti one su i od velikog interesa i koristi velikim korporacijskim tvrtkama i marketinškim organizacijama. Tako zvani socijalni inženjering predstavlja jednu od najvećih opasnosti u virtualnom svijetu. On označava tehnike kojima se služe pojedinci kako bi iskorištavanjem ljudskih pogrešaka i slabosti utjecali na drugog pojedinca i to u svrhu navođenja da pojedinac učini nešto što nije u njegovom interesu. Socijalni inženjering se koristi u otkrivanju povjerljivih informacija ili dobivanju pristupa nekim informacijama do kojih nije lako doći.[25] Plodno tlo za takve radnje su upravo društvene mreže *poput Facebooka, Instagrama, Tvittera, MySpace* koje otkrivaju pregršt osobnih podataka o pojedincu do kojih je iznimno lako doći jer ih korisnik sam postavlja.

[23] prema: Ćosić,B. (2013.) Prevencija računalnog kriminaliteta: *Policijska sigurnost*. Zagreb, 22., 147.
[24]prema: Varga, Šimović i Milković, *Zaštita elektroničkih informacija*, 40.
[25] prema: *O socijalnom inženjeringu* [online], https://www.cert.hr/socijalni_inzenjering/ [25. kolovoz 2018.]

Prvenstveno, radi se o profilima na društvenim mrežama koji najčešće nose nazive imena i prezimena korisnika, zatim datuma rođenja, podatke o lokacijama na kojima se osoba nalazi. No, osim toga liste prijatelja na društvenim mrežama također otkrivaju mnogo toga o korisniku, a posebno se opasanim smatraju iznošenje razmišljanja i planova za putovanja, što će korisnik u budućnosti raditi te brojna druga iznošenja osobnih stavova i podataka. Ovim javnim podatcima znatno se olakšao posao kriminalcima koji vrlo lako dolaze do svih potrebnih informacija o potencijalnim žrtvama. Otkrivanje i praćenje je postala trivijalna stvar.

## 3.1. Metode socijalnog inženjeringa

Primjeri kriminalnih radnji sežu do toga da se na Internetu mogu kupiti i okupiti različite vrste listi adresa elektroničke pošte, različite baze podataka ili pak validni brojevi kreditnih kartica.[26] Postavljanjem različitih osobnih podataka u virtualnom svijetu, a posebice na društvenim mrežama vlasnici profila se sami izlažu velikim opasnostima da postanu žrtve kriminalnih radnji. Kriminalci koji se služe socijalnim inženjeringom sve više usavršavaju svoje metode, a neke od najpoznatijih su:

- *Pshising*

Ovaj oblik socijalnog inženjeringa poznat je još iz 1987., a u računalnom žargonu dolazi od engleske riječi *fishing* što označava pecanje. Cilj ovog kriminalnog djela je prisvojiti osjetljive podatke trećih osoba. Primjerice korisničko ime, lozinke, broj kreditne kartice, osobni identifikacijski broj (OIB), broj socijalnog osiguranja te još brojne druge. Način kojim se služe ovi kriminalci je zapravo lažno predstavljanje, odnosno korištenje određenog osobnog podatka treće osobe koji je bio lako dostupan putem primjerice društvene mreže. Pravi primjer je slanje elektroničkih poruka poruka u kojima se s lažne elektroničke poštanske adrese upućuje poruka naslovljena na ime i prezime treće osobe i primjerice traži broj kreditne kartice. Da je ovo zaista ozbiljan problem svjedoči i primjerice britansko zakonodavstvo koje za ovu vrstu prekršaja dodjeljuje kazne i do 10 godina zatvora.[27]

- *Vishing*

[26] prema: Ćosić,B. (2013.) Prevencija računalnog kriminaliteta, 139.
[27] Ćosić, Ibid, 155.

Ova vrsta podrazumijeva lažno predstavljanje i pozive putem lažnih telefonskih brojeva. Ovaj oblik socijalnog inženjeringa je u blagom padu s obzirom na sve manje korištenje telefonskih usluga. Dobro je istaknuti da ovaj oblik ilegalnog prikupljanja osobnih podataka u današnjici pogađa stariju populaciju.[28]

- *Impersonation*

Doslovan prijevod na hrvatski jezik označavao bi lažno predstavljanje i to u svrhu prikupljanja osobnih podataka.[29]

Sva tri navedena načina upozoravaju na ustaljeni oblik ponašanja kriminalca, a to je prvenstveno sakupljanje informacija o žrtvi, uspostavljanje veze sa žrtvom, pristupanje žrtvi te realizacija kriminalnog plana. Shematski prikaz vidjeti na slici 1. Upravo iz tih razloga nužno je limitirati objavljivanje osobnih podataka u virtualnom svijetu, provjeravati identitet osoba s kojima stupamo u kontakt i ponajviše se Internetom služiti odgovorno i savjesno.

*Slika 1. Etape socijalnog inženjeringa*


Izvor: CARnet – Hrvatska akademska i istraživačka mreža (2010.) [online]: *Napredne tehnike socijalnog inženjeringa* (brošura), 3. https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-02-292.pdf, [25.kolovoz 2018.]

Socijalni inženjer može biti bilo koja osoba koja se u različite svrhe koristi socijalnim inženjeringom. Tako su to često hakeri koji uz pomoć tehnika inženjeringa dobivaju ključne informacije za upade u računalne sustave. Često su to i osobe koje izvode ispitivanja koja služe za ispitivanje ranjivosti nekog računalnog sustava. Također, to su i lopovi koje kradu osobne identitete i služe se ilegalno osobnim podatcima osoba koje za to nisu dale privolu. Socijalni inženjeri mogu biti i obični ljudi koji u svom svakodnevnom životu prikupljaju podatka što često ne dovodi do ozbiljnih situacija. U konačnici, socijalni inženjering je isplativ u poslovnom

[28] prema: O *socijalnom inženjeringu* [online], https://www.cert.hr/socijalni_inzenjering/ [ 25. kolovoz 2018.]
[29] O socijalnom inženjeringu, Ibid. i Ćosić, Prevencija računalnog kriminaliteta, 155.

i političkom životu. Predstavnici različitih političkih opcija posežu za metodama prikupljanja podataka u svrhu otkrivanja podrške i javnog mijenja o političkom kandidatu. Dok s druge strane u primjerice trgovini prodavači se služe metodama socijalnog inženjeringa kako bi prikupili informacije o željama i kupovnim preferencama potencijalnih i postojećih korisnika.[30]

Neki od najpoznatijih svjetskih socijalnih inženjera su *Kevin David Mitnick,* konzultant za računalnu sigurnost optužen za više kriminalnih djela učinjenih metodama socijalnog inženjeringa. Prva nedjela učinio je u dječačkoj dobi kada je zaobišao plaćanje vožnje u autobusu u *Los Angelesu*, a najviše se služio manipulacijom telefonskih poziva koju je koristio kako bi izbjegavao naplatu skupih međunarodnih poziva. Bavio se upadima u brojne računalne sustave, hakiranjem mobitela. Za svoja kriminalna djela bio je više puta osuđivan i u zatvoru. Nakon što ga *FBI* godine 1995. uhitila odslužio je četiri godine zatvorske kazne nakon čega je otvorio konzultantsku tvrtku za računalnu sigurnost. Osim *Mitnicka* svjetski najpoznatiji socijalni inženjeri su trojica braće *Ramy, Muzher i Shadde Badir*. Ono što je kod njih specifično je da su sva trojica od rođenja slijepi, a njihov najpoznatiji kriminalni akt je bio upadi u telefonske razgovore u području Izraela 1990-ih godina.[31]

## 3.2. Načini zaštite od socijalnog inženjeringa

Posljedice za žrtve socijalnog inženjeringa mogu biti višestruke, od krađe identiteta, neželjenih novčanih transakcija pa sve do nanošenja štete ugledu i dostojanstvu osobe. Postavlja se pitanje kako se zaštititi. Prvenstveno zaštita se olakšava ako postoji jasno definirana sigurnosna politika na državnoj, ali i na razini tvrtke ili organizacije. Osim toga, ta ista politika treba ići u korak s vremenom i nužno ju je ažurirati. Zatim, kako bi se efikasnost zaštite podigla potrebna je konstantna edukacija i obuka zaposlenika i osoblja. To znači obrazovanje o sigurnosnoj politici, podizanje svijesti o rizicima i gubitcima te treniranje koje će za svoj cilj

[30] prema: CARnet – Hrvatska akademska i istraživačka mreža (2010.) [online]: *Napredne tehnike socijalnog inženjeringa* (brošura), 3. https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-02-292.pdf, [25.kolovoz 2018.]
[31] CARnet, Ibid.

imati upoznavanje metoda socijalnog inženjeringa. Kako bi se zaštitili od socijalnog inženjeringa potrebno je i pravilno upravljanje lozinkama.[32]

U konačnici, metode socijalnog inženjeringa su prilagođene tehnološkim dosezima i ubrzanom razvoju komunikacijskih sustava stoga i zaštita treba biti u korak s tim. Podizanje svijesti o važnosti zaštite podataka, kontrole izdavanja podatka, ali i svjesnosti da svaki korisnik Interneta treba provesti mjere vlastite zaštite. U skladu s tim u Republici Hrvatskoj postoje temeljna prava građana/osoba čiji se osobni podatci obrađuju. Poznavanje tih temeljenih prava doprinosi poznavanju sigurnosnih prava.

Prvo temeljno pravo je da osoba ima pravo biti informirana o prikupljanju i daljnjoj obradi osobnih podataka. Drugo je da ima pravo u zakonskom roku od dane privole za obradu osobnih podataka odustati od prikupljanja osobnih podataka i zatražiti prestanak prikupljanja. Treće pravo je da u bilo kojem trenutku osoba ima pravo na uvid u osobne podatke koje se nalaze u zbirkama, također može utjecati i na korekcije uneseni podataka ukoliko su uneseni podatci u zbirci netočni ili nepotpuni. Također, postoji i mogućnost protivljenja korištenja osobnih podataka u marketinške svrhe, ali i potraživanje obeštećenja od voditelja zbirke osobnih podataka ako se povrijedi bilo koja stavka sigurnosnih prava vlasnika osobnih.[33]

Poznavanje ovih pravila samo doprinosi generalnoj zaštiti podataka, ali služi i podizanju svijesti i edukaciji o tome kako se lakše zaštititi od socijalnog inženjeringa. Izvori za saznavanje prava zaštite podataka mogu se pronaći na službenim stranicama *AZOP-a*, ali i službenim biltenima i brošurama *AZOP-a, CARnet*-a te državnih službi. Neki od tih brošura korištene su i u izradi ovoga rada te se mogu pronaći u popisu literature.

[32] CARnet, Ibid.

[33] prema: *Zaštita osobnih podataka u RH*, Agencija za zaštitu osobnih podataka (AZOP) – službeni letak.

# 3. Korištenje baza osobnih podataka u poslovanju

Velike količine prikupljenih podataka koje se nalaze u bazama tvrtki izvrstan su izvor za poslovne prilike. Iskorištavanje baza podataka za formiranje poslovnih planova i okretanje prema zadovoljavanju potreba klijenata dobar su primjer korištenja prikupljenih podataka u legalne svrhe. Iako je do sada rad govorio o nelegalno i kriminalnom dijelu korištenja podataka i osobnih podataka drugi dio rada posvetit će se korištenju velike količine podataka u svrhu

ostvarivanja napretka tvrtki i organizacija te udovoljavanju i prilagodbi želja njihovih klijenata. Pravi primjer za to je kombinacija marketinga, tehnologije, ali i ostalih vještina koja se primjenjuje u upravljanju odnosima s klijentima (eng. *Customer Relationship Management CRM*). Definicija „upravljanja odnosima s klijentima" je da se rade poslovne i prodajne strategije kako bi se poboljšala zainteresiranost i zadovoljstvo klijenta. Ta poslovna i prodajna strategija iskorištava informatičke tehnologije kako bi predstavila opće, pouzdane i iscrpne točke gledišta na klijenta uz korištenje svih procesa i interakcije s klijentom kako bi se plodonosni odnosi zadržali i povećale."[34] Kako bi se isplatio koristiti se metodom upravljanja odnosa s klijentima potrebna je koordinacija baza podataka svih odjela.

Prvi primjeri korištenja metode upravljanja korisnika sežu još u devedesete godine dvadesetog stoljeća i to putem tehnologije govornih automata i pozivnih centara. Smatralo se da će se spajanje podataka o kupcu s terena i o onim podatcima prikupljenim putem automata i pozivnih centara stvoriti bolja interakcija s klijentom. Današnje poimanje upravljanja odnosnima s klijentima podrazumijeva upotrebu sofisticiranih računalnih programa koji integriraju sve prikupljene podatke. Nakon što se velika količina podataka nađe na jednom mjestu potrebno je razlučiti što je od toga korisno za pojedinog klijenta i formiranje poslovnih prilika za njega. Jedna od značajnih tehnika za razlučivanje korisnik informacija iz mase nekorisnih je tako zvano rudarenje podataka o čemu će više biti rečeno u narednim poglavljima.[35]

Upravo upravljanje odnosima s klijentima doprinosi minimalizaciji troškova poslovanja, ali povećava izglede za uspješno poslovanje. Cilj je fokusirati se na kupca/klijenta i točno prepoznati njegove potrebe i iskoristiti priliku za plasiranje proizvoda i ostvarivanje profita. Neki od osnovnih ciljeva *CRM-a* su osiguravanje bržeg protoka informacija u prodaji i izbjegavanje fizičkog zapisivanja podataka što usporava i ostavlja ranjivim prikupljene podatke. Stoga se koriste informacijski sustavi. Cilj je i povećavanje zadovoljstva kupaca te produžetak vjernosti kupca. Također, i olakšava se filtriranje povoljnih poslovnih prilika od onih nepovoljnih, a samim time poboljšava se i kvaliteta analize poslovnih prilika. Iz perspektive djelatnika tvrtke smanjuje se količina administrativnog rada, olakšava se njihovo

[34] prema: Navijalić, M. (2014.) *Informacijski sustavi za upravljanje odnosima s klijentima*. Diplomski rad: Zagreb, Fakultet strojarstva i brodogradnje – Split, 4., 5.
[35] Ibid.

praćenje i mjerenje efikasnosti. Olakšava se i proces traženja odgovora na upite te se uz pomoć standardiziranih obrazaca olakšava potraga za informacijama.[36]

Osim pozitivnih strana korištenja *CRM-a* nekoliko je i nedostataka. Upravljanje odnosima s klijentima zahtijeva velike investicije u tehnologiju tvrtke. Potrebno je nabaviti odgovarajuću računalnu opremu, softverska rješenja, analitičke programe, ali i za programe održavanja i zapošljavanja radnika koji znaju obavljati poslove na novoj tehnologiji. Osim povećanih izdataka za implementaciju sustava ponekad problem predstavlja primjena novih tehnoloških dosega u stari način poslovanja. Posebice je teško promijeniti ustaljene navike zaposlenika, ali pravilna edukacija može prevladati i taj nedostatak.[37]

Kako bi prikupljanje podataka za bazu bilo usklađeno s sigurnosnim pravilima, potrebno je upoznati klijente da će se podatci o njima spremati i koristiti. Jedan od poznatijih primjera kako se može pronevjeriti povjerenje klijenata je primjer financijske tvrtke *American Express* koja je garantirala svojim klijentima sigurnost podataka i ne izdavanje njih trećim stranama. No, dogodila se suradnja s tvrtkom *KnowledgeBase Marketing Inc* što je rezultiralo odljevom velikog broja korisnika *American Expressa*.[38] Pošto se radi o oslanjanju na računalne izračune i pretpostavke donesene pretpostavke ne moraju biti uvijek točne. Moguće je da se dogode određene pogreške sustava i to u favoriziranju lojalnih i većih korisnika. Ovakve pogreške mogle bi dovesti do toga da manje lojalni kupci se osjete manje vrijednima te da to bude okidač za njihovo napuštanje i prekid suradnje.[39] No, bez obzira na negativne strane primjena *CRM-a* u poslovanju unijela je promjena u tehnike poslovanja i prodaje. Kakva je usporedba primjena sustava poslovanja bez *CRM-a* koji je bio usmjeren na transakcije i sa *CRM-om* koji je usmjeren na odnose vidjeti u Tablici 1.

[36] Navijalić, Ibid, 6.
[37] Navijalić, Ibid, 9.
[38] Navijalić, Ibid. 21.
[39] Navijalić, Ibid.

*Tablica 1. Razlike između klasičnog poslovanja i CRM-a*

| **Marketing usmjeren na transakcije** | **Marketing usmjeren na odnose** |
|---|---|
| Fokus na prodaju | Fokus na izgradnji lojalnosti i zadržavanje kupaca |
| Naglasak na oblike proizvoda | Naglasak na koristi od proizvoda koje su značajne za potrošače |
| Mali naglasak na zadržavanju kupca | Naglasak na visoku razinu usluga koje su usmjerene na pojedinačnog kupca |
| Ograničeno povjerenje kupaca | Visoko povjerenje kupaca |
| Umjeren kontakt s kupcima | Veliki kontakt s kupcima kroz koji se pokušava dobiti informacije o kupcima i poboljšati odnos s njima |
| Kvaliteta je isključivo briga proizvodnje | Kvaliteta je briga svih |

Izvor: Vesna Vučemilović, „Prednosti strategije upravljanja odnosom s kupcima“,121.

Najpoznatiji i najrašireniji sustav koji se upotrebljava za *CRM* je *Microsoftov sustav – Microsoft Dynamics CRM.*[40] Ovaj programski paket fokusiran je na prodaju, marketing i korisničku podršku. To je prvenstveno web aplikacija s povezanim sučeljima. Ona je programirana tako da se bavi upravljanjem klijentima, upravljanje prodajom i marketingom. Također aplikacija planira i određuje cijene, popuste te povezuje informacije o klijentima sa njihovim potrebama. Ona osim kreiranja korisničkih profila, pronalazi vezu među njima, analizira te kreira izvješća o potencijalnim prodajnim i marketinškim postupcima. Osnovna platforma *Microsoft Dynamics CRM* se sastoji od:

- Baze podataka *Microsoft SQL Server*
- *Web* servisa
- Sistemskih servisa (za meta podatke, radni tok i integraciju)
- Procesora upita koji podržava entitetske modele
- Sigurnosnih upita koji koriste *XML* stanja za zaštitu fizičke baze podataka
- Pristupa za proširivanje poslovne logike
- Servisa za izvještaje
- Komponenti web sučelja [41]

[40] Navijalić, Ibid, 27.
[41] Navijalić, Ibid.

U Hrvatskoj jedna od prvih tvrtki koja je pristupila korištenju *CRM-a* je *Hrvatski telekom*. Uvođenje *CRM* sustava je trebalo osigurati stjecanje novih korisnika, povećati profitabilnosti postojećih korisnika i zadržati postojeće korisnike. Stvaranje odnosa s korisnikom je imalo tri faze. Prva je značila analiziranje kupovnih navika korisnika i uslužnih kanala koje korisnik najviše koristi te razvoj personaliziranog odnosa s korisnikom. Na temelju tako prikupljenih informacija kategorizirani su klijenti.[42] Prvi korak bilo je otvaranje pozivnih centara u Osijeku i Buzinu te upotreba platforme "*Definity*" što je omogućilo korištenje virtualnog pozivnog centra kako bi se povećao broj poziva, a usluga poboljšala. Ovim načinom prikupljen je i velik broj podataka, ali se i ubrzala usluga što je kao produkt imalo zadovoljstvo korisnika, ali i profit za tvrtku koja je prikupljala podatke.[43]

Korištenje *CRM-a* povećava efikasnost i produktivnost poslovanja jer se sve usmjerava prema željama klijenta i radi se na prikupljanju korisnih informacija kako zadržati postojeće korisnike, kako im udovoljiti, ali istovremeno kako i prodati novu uslugu. S druge strane, kvalitetno korištenje podataka dovodi i do privlačenja novih korisnika i time se ostvaruje potencijalno proširenje poslovanja. Suvremene tvrtke koriste se ogromnim potencijalnom koji se nalazi u mnoštvu „velikih podataka" samo je ključno kako znati izlučiti ono što je korisno.

## 4.1. *Big data* /Veliki podatci i *Data mining* /rudarenje podatcima

Korištenje u poslovnoj praksi prikupljenih podataka samo je jedan od primjera kako se mogu koristiti baze podataka. Veliki podatci /*Big data* nepresušan su izvor informacija, a jedna od metoda pretraživanja i uzorkovanja korisnik podataka je rudarenje podataka. Korištenje podatka i osobnih podataka u poslovne svrhe jedan je od važnih segmenata za koje služi virtualan svijet u kojem se nalaze Veliki podatci. Korištenjem metoda rudarenja podataka (eng. *Data mining*) može se stvoriti određeno znanje. Odnosno, cilj rudarenja podataka je identificirati nove, potencijalno korisne veze i uzroke u postojećim podatcima. Pomoću alata za rudarenje otkrivaju se matrice ponašanja, predviđaju se budući trendovi temeljem čega se u poslovnom svijetu donose odluke. Uz pomoć takvog način prikupljanja podataka može se raslojavati tržište, pronaći profil tipičnog klijenta za određenu vrstu proizvoda, otkriti sličnosti među tržištima.[44]

[42] prema: Vučemilović, V. (2015.) Prednosti strategije upravljanja odnosom s kupcima, *Zbornik radova Veleučilišta u Šibeniku*, 123.
[43] Vučemilović, Ibid.
[44] prema: Ćulum, S. (2016.), *Poslovna inteligencija,* Rijeka, 35.

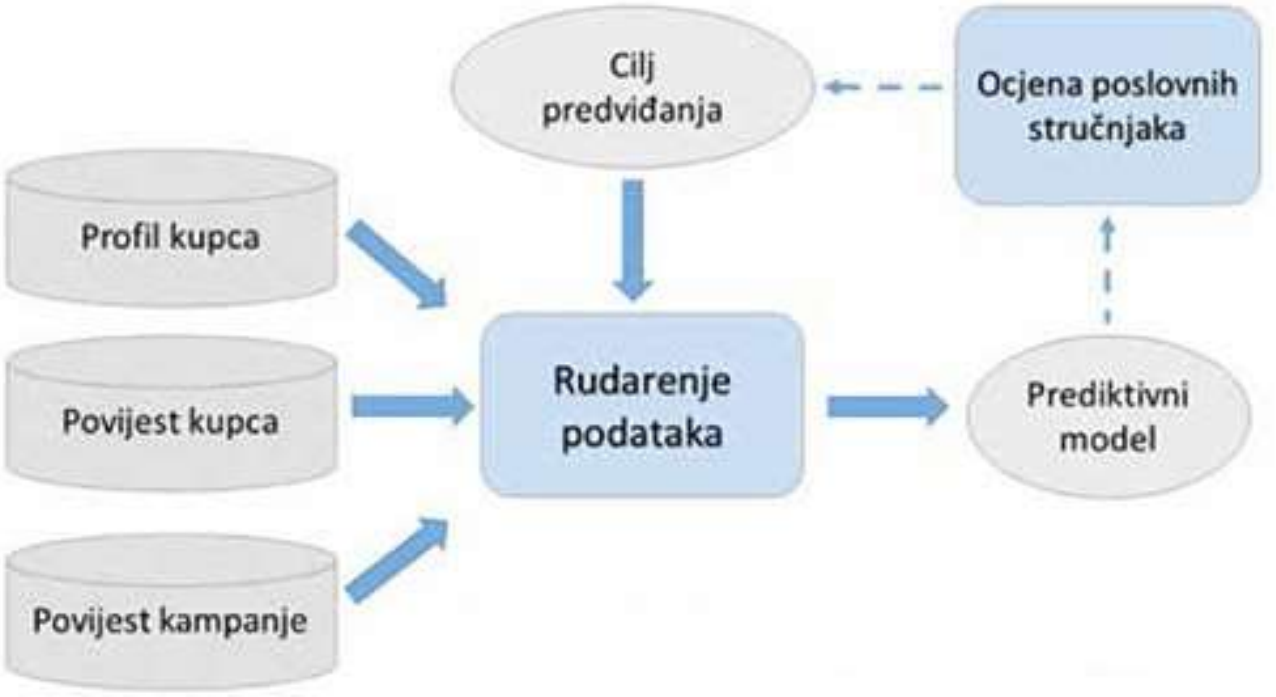
Sam naziv metode o rudarenju podataka ukazuje na traganje za zlatom što podatci u suvremenom svijetu i jesu.[45] Metodologija rudarenja podataka zahtijeva definiranje problema poslovanja, zatim određivanje potrebitih podataka, transformaciju podataka i njihovo uzorkovanje i vrednovanje.

Ono čemu u poslovnom svijetu rudarenje iznimno pomaže je zadržavanje klijenata jer putem prikupljanja podataka o njima profiliraju se njihove potrebe. Osim toga, prodaja dodatnih proizvoda postojećim klijentima te segmentacija što označava stvaranje profila klijenta. Rudarenje također donosi i racionalizaciju troškova, a samim time olakšava okretanje i aktivaciji novih klijenata.[46]

Jedan od poznatijih primjer korištenja novih informacija prikupljenih rudarenjem podataka je o prodaji proizvoda za tvrtku *P&G* u kojem je ustanovljeno da petkom poslijepodne očevi kupuju pelene i uz to najčešće pivo za nadolazeću večernju ili vikend utakmicu. Korisnost otkrića bila je u tome što je tvrtka usmjerila svoje marketinške poruke o prodaji pelena prema očevima. Osim toga  punjenje zaliha pelena u prodavaonici najveće su bile petkom. [47] Kao što je i vidljivo na slici 2., ali i iz navedenog primjera rudarenje podataka označava prikupljanje svih informacija u svrhu skupljanja znanja koje će doprinijeti valjanoj i dobroj prosudbi, odnosno predikciji, kako treba postupiti.

[45] prema: Pejić Bach, M. (2005.) Rudarenje podataka u bankarstvu, *Zbornik Ekonomskog fakulteta u Zagrebu*, 3., 182.
[46] Pejić Bach, Ibid.
[47] prema: Ćulum, S. *Poslovna inteligencija*, 35.

*Slika 2. Shematski prikaz „rudarenja podataka“*

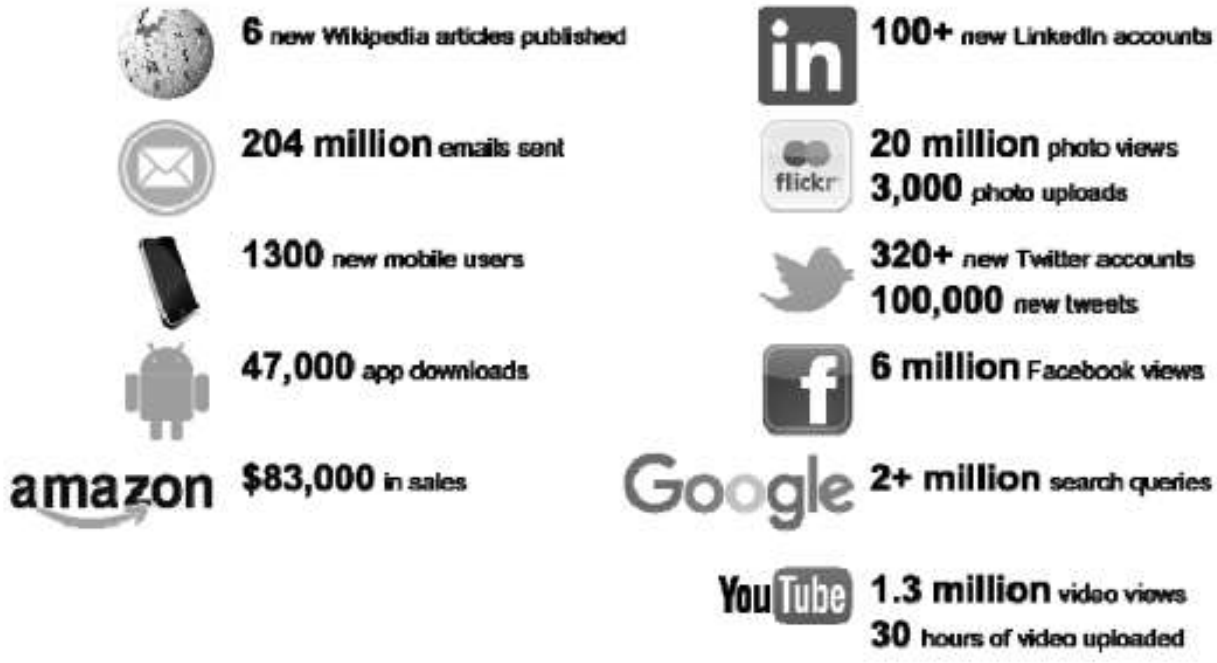



**Izvor**: Zekić- Sušac, M., *Prediktivna analitika- 2-koraka bliže* [online] http://www.infotrend.hr/clanak/2017/6/prediktivna-analitika---2---korak-,90,1308.html [25.kolovoza 2018.]

Kojom brzinom u današnjem svijetu nastaju podatci svjedoči istraživanje *IBM-a* koje donose brojke o tome da je 90% podataka u virtualnom svijetu stvoreno od 2014. do 2016. Načini prikupljanja podataka su se drastično izmijenili, a njihove skladištenje i čuvanje postalo je jednostavno i jeftino. Gotovo svaka osoba svakodnevno ostavlja virtualni trag. A na slikovit način o tome govori slika 3. koja donosi izračun prikupljenih podataka putem Interneta.[48]

[48] prema: Šebalj, D., Živković, A. i Hodak, K. (2016.) Big data: changes in data management: *Ekonomski vjesnik*, 487.

*Slika 3. Nastanak virtualnih podataka u jednoj minuti*




Izvor: Šebalj, D., Živković, A. i Hodak, K., Big data: changes in data management, 488.

Ta velika količina virtualnih podataka predstavlja sve što se u svijetu bilježi i sprema. No, ne predstavlja problem velika količina podataka i njihov prostor za spremanja već što se sve s tim podatcima može učiniti. Kroz rad je već navedeno nekoliko primjera zloupotrebe podataka, a posebno osobnih podataka. Iako osnovna namjena *Big data* predstavlja nepresušan izvor za tvrtke ili organizacije za unaprjeđenje njihova poslovanja. Podatci mogu biti spremljeni u virtualne arhive tvrtki ili van njih. Definicija Velikih podataka stvorena je 2000. godine i ona govori o tome da: *„Veliki podatci odnose se na eksploziju u količini (a katkad i kvaliteti) dostupnih i potencijalno relevantnih podataka, a sve kao posljedica napretka u tehnologiji zapisivanja i pohranjivanja podataka*."[49]

Način prikupljanja Velikih podataka je putem podatkovnih tragova web pretraživanja, putem komunikacije na društvenim mrežama, podatcima koji su skupljeni senzorima, ali i onih koje sakupljaju nadzorni sustavi. Posjedovanje Velikih podataka ne znači i prednost u poslovanju, ali je to odlična polazna točka za promjenu i unaprjeđenje poslovanja. Podatci se prikupljaju u današnjem vremenu brže i više nego ikada. Virtualni svijet omogućio je brojne alate putem

[49] Kocijan, K. (2014.) Big Data: how we got to the BigData and where are they taking us, *Komunikacijski obrasci i informacijska znanost*, Zagreb, 3.

kojih se Veliki podatci prikupljaju. Osim ranije spomenutih društvenih mreža, tu su i mrežne stranice za virtualnu kupovinu poput *Amazona, E-baya* pa sve to *Googla* i ostalih pretraživača. Ovome se također pridodaju aplikacije koje služe orijentaciji, poput *GPS-a, Gooogle maps* i brojnih drugih.[50]

Kolika je količina Velikih podataka nastala u suvremenom dobu ilustrativno prikazuje slika 2. no, kako bi se taj dojam još više približio potrebno je to opisati usporedbama. Tako primjerice slikovito prikazano da se svi prikupljeni podatci nalaze u tiskanom knjižnom obliku s njima bi se moglo podići pet stupova od Zemlje do Mjeseca. Dok primjerice u svijetu astronomije gdje je *Sloan Digital Sky Survey* teleskop, koji je izgrađen u *New Mexicu,* samo u prvih nekoliko tjedana prikupio više podataka nego što je prikupljeno u cijeloj povijesti astronomije. U periodu od 2000. do 2010., arhivirano je 140 terabajta informacija prikupljenih ovim teleskopom. No zasigurno u trenutku pisanja ovoga rada ovi podatci slove već kao zastarjeli jer ubrzani razvoj tehnologije je nezamislivo unaprijedio prikupljanje i spremanje podataka.[51]

Kolika je vrijednost Velikih podataka pokazuje i činjenica da postoje tvrtke koje se bave njihovom prodajom. Prva takva nastala je na Islandu 2008. i nosi naziv *DataMarket.* Ostale koje su među poznatijima *su Factual, Windows Azure Market i Import.io*. Postojanje ovakvih tvrtki samo svjedoči tome da su podatci „gorivo“ za eru u kojoj trenutno živimo. Primjer iz britanske prakse govori o tome da se u istraživanje i inovacije na polju istraživanja Velikih podataka ulaže veliki novac. Tako je 2013. engleska vlada za istraživanja na tom polju dodijelila 189 milijuna funti što je veliki novac s obzirom da je primjerice prva sljedeća znanost iza ovog iznosa bila sintetička biologija s 88 milijuna funti.[52]

Upotreba Velikih podataka ne odnosi se samo na one koji su prikupljeni u današnjem vremenu. Velike tvrtke koriste se često zapisima o svojim zaposlenicima koji su nastali kao zabilješke u povijesti njihovog zaposlenja. Osim toga, u vremenu razvoja električnih automobila tvrtke *IBM, Honda, Pacific Gas i Eletric Company* u Kaliforniji su pokušali na temelju starih spisa o modelima potrošnje električne energije, trajanja putovanja, vremenskih prognoza predvidjeti gdje će biti potrebno izgraditi električne punionice automobila. Zanimljiva i korisna upotreba Velikih podataka je i u američkoj policiji koja je u gradovima *Santa Cruz, Richmond, Chicago,*

[50] Kocijan, Ibid, 5.
[51] Kocijan, Ibid, 7.
[52] Kocijan, Ibid, 8., 9.

*Los Angeles* i *Memphis* uz pomoć starih podataka o danima u tjednu, vremenskoj prognozi, praznicima, posebnim događanjima u gradu predvidjela moguća mjesta u gradovima gdje će se dogoditi prekršaji. Na temelju tih podataka slale su se policijske kontrole i patrole koje su za cilj imale spriječiti eskalacije .[53]

Veliki podatci otvaraju prostor brojnim malverzacijama i prevarama ukoliko se ne poštuju zakonske odredbe koje reguliraju njihovu upotrebu. Internet i njegovo korištenje ugrožavaju privatnost korisnika, ali nekontrolirano i protuzakonito korištenje Velikih podataka više ugrožava osobnu privatnost.

[53] Kocijan, Ibid, 10., 11.

# 5. Slučaj Cambridge Analytica – Facebook

Velika i nedavno otkrivena afera nelegalnog korištenja Velikih podataka svakako je ona s najpoznatije društvene mreže *Facebook,* vlasnika *Mark Zuckerberga*. Cjelokupni slučaj povezan je s tvrtkom koja se bavi analizom podataka i svoje usluge prodaje na području politike i marketinga. *Cambridge Analytica* tvrtka je sa sjedištima u *Londonu, New Yorku* i *Washingtonu* i kao svoju osnovnu poslovnu djelatnost ističe analize podataka koji trebaju poslužiti za otkrivanje i razumijevanje motivacije i angažiranosti ciljane publike kako bi se ona usmjerila prema određenom cilju. Najbolji primjeri korištenja usluga ovog tipa tvrtke je u političkim kampanjama. Dobro je spomenuti da *Cambridge Analytica* u svom poslovanju ima dva sektora prvi je onaj koji se isključivo bavi politikom, a drugi je komercijalni . Osim toga ističu i svoje suradnje s nevladinim organizacijama. [54]

Ovaj rad na više mjesta navodi društvene mreže kao prostor u kojem korisnici svojevoljno postavljaju veliki broj osobnih podataka. Upravo iz toga razloga one su i često meta nelegalnog prikupljanja i korištenja podataka u različite svrhe. Definicija društvenih mreža je usluga temeljena na *webu* koja omogućuje pojedincu da izgrade javni ili polu javni profil unutar omeđenog sustava. No, ono što upotrebu društvenih mreža daje opciju društvenosti je mogućnost stvaranja različitih veza putem različitih profila. Društvene mreže omogućuju korištenje vlastitih popisa veza i popise drugih veza unutar sustava.[55] *Facebook* je trenutačno najpopularnija društvena mreža koju je u drugom dijelu 2018. godine aktivno koristilo preko 2.23 bilijuna korisnika.[56] Toliko veliki broj korisnika diljem svijeta predstavlja veliki broj podataka koji se na dnevnoj, odnosno u minuti prikuplja. Ovo je više nego dovoljan razlog da se brojne tvrtke poput *Cambridge Analytica* zainteresiraju za podatke koji se nalaze u vlasništvu *Facebooka.*

Tijekom 2016. godine u Sjedinjenim Američkim Državama odvijala se jedna od najzanimljivijih predsjedničkih kampanja u kojima je uz ustaljene političke kandidate poput Hilarry Clinton najjači protukandidat bio *Donald Trump*, američki poduzetnik i TV zvijezda. *Trump* je osvojio predsjednički mandat i time postao jedan od najkontroverznijih predsjednika

[54] prema: *Cambridge Analytica službene stranice* [online], https://cambridgeanalytica.org/ [ 24. kolovoz 2018.]
[55] prema: Kušić, S. (2010.) Online društvene mreže i društveno umrežavanje, *Život i škola*, 2., 104.
[56] prema: *Facebook statistika* [online], https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [preuzeto 30. kolovoza 2018.]

u američkoj povijesti. Nakon pobjede u javnosti su se počele otkrivati marketinški i politički trikovi koje je *Trumpov* izborni tim koristio kako bi došao do pobjede. Ključnu ulogu imala je tvrtka *Cambridge Analytica* koja je svojim uslugama radila na formiranju stavova i pravilno usmjeravala tijek izborne kampanje.

*Cambridge Analytica* je otkupila podatke s preko osamdeset sedam milijuna *Facebook* profila. Vlasnik tvrtke *Steve Banonn* u 2016. godini blizak je *Donaldu Trumpu* i jedan od glavnih pokretača njegove političke kampanje. Način na koji su podatci s *Facebook* profila prikupljani je putem kviza kojega je izradio *Aleksandr Kogano* suradnik tvrtke *Cambridge Analytica*. Kviz stvoren da osim podataka koje je prikupljao direktno od ispitanika također je prikupljao različite podatke i *Facebook* prijatelja osoba koje su riješile kviz u obliku aplikacije pod nazivom „*thisisyourdigitallife*". Osobe koje su rješavale test bile su plaćene i složile su se da njihovi podatci budu korišteni u akademske svrhe. Naime, *Kogano* je osim kao suradnik tvrtke *Cambridge Analytica* djelovao i kao znanstvenik na Sveučilištu u *Cambridgeu* gdje je radio na projektu *Global Science Reaserch* u sklopu kojeg je aplikacija i napravljena.[57] Ovakva primjer prevare pripada i socijalnom inženjeringu jer su sve komponente te vrste zloupotrebe podataka zastupljene u ovom primjeru. Tijek ovog procesa moguće je vidjeti i na slici 4.

Ovaj propust *Facebook* administracije dogodio se zbog pogreške u *Facebook API,* odnosno u njegovom sustavu zaštite privatnosti svojih korisnika.[58] *Trump* je osvojio predsjedničke izbore i u ovom skandalu jedini je izašao sa pozitivnim rezultatom jer je *Cambridge Analytica* nakon ovoga počela gubiti klijente te zbog javnog linča postala tvrtka koju prati glas „kradljivice podataka".

Ovaj slučaj otvorio je i pitanje sigurnosti korisnika *Facebooka* i njihovih podataka. Posebice se dovodi u pitanje prodaja podataka korisnika trećim stranama. Nezamisliv je profit koji *Facebook* može imati od prodaje podataka korisnika u različite svrhe. Sam osnivač i vlasnik

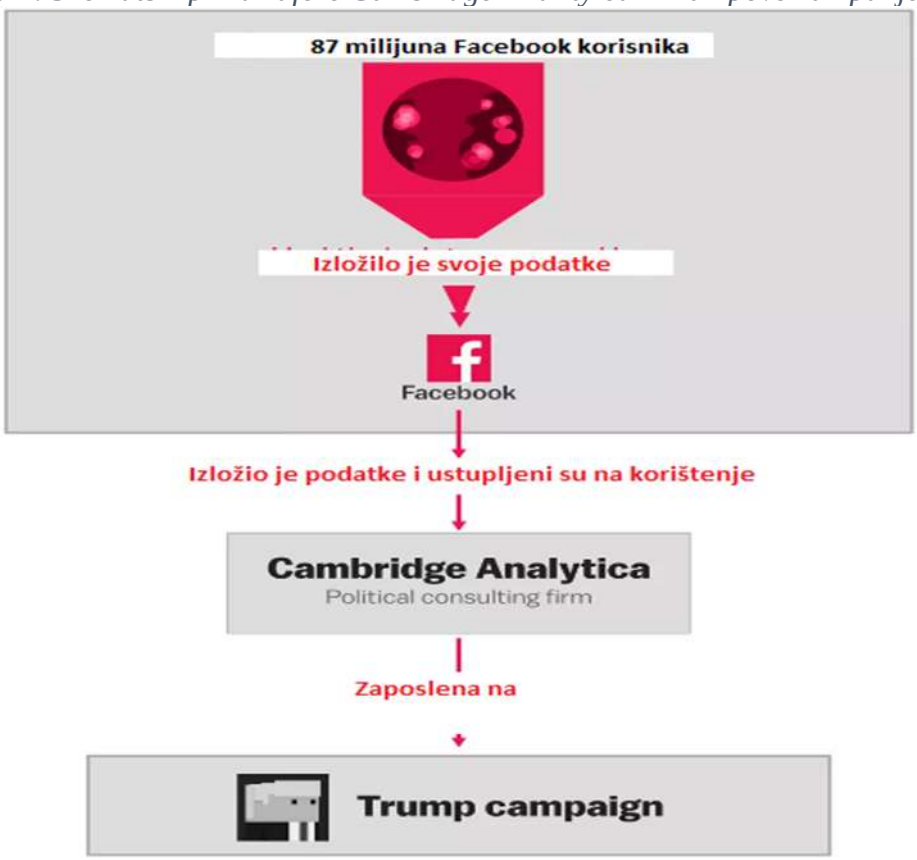
---

[57] prema: *Reveald: 50 milion Facebook profiles harvested for Cambridge Analytica in major dana breach* [online], https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [26. kolovoz 2018.]

[58] prema: *The Facebook and Cambridge Analytica scandal, explained with a simple diagram* [online], https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram [ 30. kolovoz 2018.]

*Mark Zuckerberg* u slučaju *Cambridge Analitytica* izjavio je: *"We have a responsibility to protect your information. If we can't, we don't deserve it."* (*Mi imamo odgovornost za zaštitu vaših podataka. Ako to ne možemo, onda ih i ne zaslužujemo.*).[59]

*Slika 4. Shematski prikaz afere Cambridge Analityica i Trumpove kampanje*




**Izvor:** *The Facebook and Cambridge Analytica scandal, explained with a simple diagram* [online], https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram [ 30. kolovoz 2018.]

Osim političke afere američkih predsjedničkih izbora 2016. godine otkriveno je sudjelovanje nezakonitog korištenja podataka prikupljanih s *Facebooka* i u kampanji za izlazak Velike Britanije iz Europske unije, popularno zvani *Brexit*. Ovaj puta u tome je sudjelovala tvrtka koja je bliska ranije spomenutoj *Cambridge Analytica*, a to je kanadska tvrtka *AggregateIQ*. Kanađani su surađivali s organizacijom koja se zalagala za izlazak Velike Britanije iz Europske unije pod nazivom „*Vote Leave*". Vođe organizacije su *Matthew Elliot* i *Dominic Cummings.*

[59] *The Facebook*, Ibid.

Nakon što je Velika Britanija izglasala svoj izlazak iz Europske unije istraga o legalnosti predizborne promidžbe dovela je do saznanja o propustima u korištenju oglašavanja na *Facebooku* i korištenju podataka koji su nezakonito korišteni u političke svrhe. *Facebook* kažnjen je s novčanim iznosom od 500.000 britanskih funti. Odluku o tome donijela je Britanska agencija za informacije (*The Information Commissioner's Office*) i to s odlukom u kojoj je utvrđeno da *Facebook* nije učinio sve kako bi zaštitio osobne podatke svojih korisnika i također nije bio transparentan u odnosima s trećim stranama. Ovo posljednje odnosi se na suradnju s tvrtkama koje se bave prikupljanjem i analizom podataka.[60]

Evidentno je da najveća društvena mreža ima sigurnosne propust koji i u najvećim političkim i poslovnim krugovima podižu nezamislive skandale. Sve ovo samo upućuje i potvrđuje da posjedovanje Velikih podataka predstavlja posjedovanje i velike poslovne moći. Pitanje koje se postavlja je samo kako na legalan način ustupati podatke prikupljane putem društvenih mreža i na koji se način zaštiti od zloupotrebe primjerice putem metoda socijalnog inženjeringa.

Internet i društvene mreže u svijetu trgovine podataka imaju značajnu ulogu. One su prostor gdje se gotovo besplatno podatci prikupljaju, a participacija u njima je izrazito visoka, ali isto tako i potencijalna manipulacija.[61] Raširena upotreba Interneta obavezuje i edukaciju korisnika o zaštiti podatak, a primjena zakona, kao što je *Uredba*, treba poslužiti kao instrument testiranja ispravnosti upravljanja podatcima.

# 6. Zaključak

[60] prema: *Reveald: 50 milion Facebook profiles harvested for Cambridge Analytica in major dana breach* [online], https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [26. kolovoz 2018.]

[61] prema: Nenadić, I., (2017.) Kako su mainstream mediji otvorili vrata alternativnim činjenicama?, *Političke analize,* 18.

Cilj ovoga rada je ispunjen te je opisana zaštita prikupljanja, obrade i korištenja podataka i osobnih podataka koja u današnjici zahtijeva veliku angažiranost brojnih dijelova društva. Prvenstveno svaki čovjek treba biti osobito oprezan prilikom davanja svojih osobnih podataka, ali i educira o svojim pravima za zaštitu privatnosti. S druge strane organizacije i tvrtke koje na bilo koje način prikupljaju, obrađuju ili koriste podatke i osobne podatke obavezni su prilagoditi se zakonodavnim okvirima. Osobni podatci su sve što može dovesti do identifikacije osobe. Tako osim klasičnog poimanja osobnih podataka poput imena i prezimena u tu kategoriju pripada i primjerice *IP* adresa vlastitog računala ili pak liječnički karton. Pravilno ophođenje s osobnim podatcima osigurava se putem osam načela koja nalažu sigurnost prikupljanja, obrade i korištenja. Velika opasnost od zloupotrebe i nepravilnog korištenja je u virtualnom, odnosno računalnom svijetu. Izazovi zaštite podataka stoga zahtijevaju i osobne intervencije za zaštitu. Primjer za to je sistematizirano nazivlje osobnih datoteka na osobnim računalima. Osim ovog osnovnog primjera zaštite, postoji i razvijena zaštita koja dolazi iz državnih okvira. Radi se o zakonima koji štite i propisuju pravilno rukovanje podatcima i osobnim podatcima.

Europska unija, a Hrvatska kao njena članica, imaju ususstavljen zakonodavni okvir za ovu problematiku. Svakako najznačajniji zakon, koji se od svibnja 2018. godine primjenjuje i u Hrvatskoj, je *Opća uredba o zaštiti podataka*. Koliko je potrebno poštovati privatnost i anonimnost podataka svjedoče i propisane kazne unutar *Uredbe*, ali i postojanje *Agencije za zaštitu osobnih podataka* koja radi na kontroli i edukaciji o zaštiti podataka u Republici Hrvatskoj. Održivost pravilnog korištenja osobnih podataka ovisi o primjeni Uredbe, ali i nepristranog djelovanja *AZOP-a*. Garancije pravilnog korištenja, prikupljanja i obrade osobnih podataka leži u funkcioniranju institucija koje imaju zadaću time se baviti i kontrolirati pravilnu primjenu zakona. Posebni izazovi se nalaze u informatizaciji i tehnološkom napredovanju društva zato je Republika Hrvatska pitanje zaštite podataka i privatnosti inkorporirala u svoj vrhovni zakon – Ustav.

Rad osim što definira osobne podatke te zaštitu podataka upozorava i na brojne načine zloupotrebe i kriminalnog korištenja podataka. Prvenstveno, to se odnosi na tehnološko-komunikacijske kanala kao što su telefon i Internet. Posebna pozornost stavljena je na zloupotrebe putem Interneta jer ipak danas je to najraširenije tehnološko – komunikacijsko sredstvo. Brojni su načini kako se putem njega mogu nezakoniti koristit podatci. Neke od mogućnosti koje su opisane su računalni virusi, neželjena elektronička pošta te posebno

socijalni inženjering i njegove metode. Korištenje socijalnog inženjeringa je kažnjivo, ali je sveprisutno. Iz toga razloga ključno je znati koje su metode socijalnog inženjeringa i kako ih izbjegavati u svakodnevnom životu. Stoga, poglavlje o tome iznosi i obrazlaže potencijalne opasnosti, prije svega na društvenim mrežama.

Informacije se prikupljaju brzo i u velikim količinama. Pojam Veliki podatci ukazuje na nepregledne količine podataka koje mogu biti iznimno korisne u sustavima poslovanja, a posebice marketinga. Izlučivanje korisnih podataka vrši se metodom rudarenja podataka. Stručnjaci i računalni programi koji se ovime bave iznimno su sofisticirani i predstavljaju okosnice današnjih suvremenih tvrtki. Usmjeravanje poslovanja na klijenta i njegove potrebe donosi i povoljnije financijske rezultate za vlasnika tvrtke, a smamim time i zadovoljnije radnike. Primjenjivanje pravilnog korištenja Velikih podataka dovodi do unaprijeđena poslovanja, a to sve vodi i k većem profitu. Poglavlje Veliki podatci i rudarenje podataka donosi primjere iz prakse i pravilnoj upotrebi Velikih podataka i rudarenja u poslovnom svijetu.

Rudarenje podataka u kombinaciji sa socijalnim inženjeringom otvaraju i prostor za manipulacije podatcima njihovom legalnom upotrebom. Poglavlje *Cambridge Analytica* iznosi zaključke o upotrebi metode rudarenja podataka u političkim kampanjama. Informacije iz 2016. godine i predizborne kampanje američkog predsjednika *Trump*a te slučaja britanskog *Brexita* upozoravaju i na opasnosti koje nam donosi korištenje društvenih mreža i Veliki podatci koji se putem njih prikupljaju. *Facebook* je najpopularnija društvena mreža čiji korisnici ostavljaju i svojevoljno postavljaju mnoštvo osobnih podataka koji mogu poslužiti u različite svrhe. Svakako tako velik broj podataka privlačan je istraživanju i formiranju političkog mijenja. No slučaj upotrebe Velikih podataka u političke svrhe nije samo narušio pravne sustave i izborna pravila u SAD-u i Velikoj Britaniji već je nepovratno umanjio povjerenje korisnika *Facebooka* zbog nekontroliranog korištenja korisničkih podataka i nedovoljnu zaštitu istih.

Zaključno, može se ustvrditi da su mehanizmi zaštite, prikupljanja i obrade podataka, a posebice osobnih podataka u 21. stoljeću veliki izazov za sve strukture društva. Kako se napredak tehnologije nezaustavljivo odvija ova problematika zasigurno ostaje nedovršena i biti će potrebno praćenje tehnološkog napretka i usavršavanje metoda zaštite privatnosti i podataka korisnika i privatnih osoba.

# 7. Literatura

# Knjige


1. Kladar, D. (2018.) *Kako se pripremiti za GDPR*, Zagreb: Forum poslovni mediji

2. Varga,M., Šimović, V. i Milković, M. (2012.): *Zaštita elektroničkih informacija*. Varaždin

3. Ćulum, S. (2016.), *Poslovna inteligencija*, Rijeka


# Članci, bilteni, brošure i objavljeni zakoni


1. Škrinjar Vidović,M., (2016.) EU dana Protetion Reform: Challanges for Cloud computing. *Croatian Yearbook of European Law and Policy*, 12.

2. Klarić M. (2016.) Zaštita osobnih podataka i Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda. *Zbornik radova Pravnog fakulteta u Splitu*, 53./4., 975.

3. *Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinca 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)*: Službeni list Europske unije. L 119/1.

4. *Statut Agencije za zaštitu osobnih podataka* (2004.), Zagreb, 5.

5. *Zaštita osobnih podataka u RH*, Agencija za zaštitu osobnih podataka (AZOP) – službeni letak.

6. Ćosić, B. (2013.) Prevencija računalnog kriminaliteta: *Policijska sigurnost*. Zagreb, 22.

7. *Zaštita osobnih podataka u RH*, Agencija za zaštitu osobnih podataka (AZOP) – službeni letak.

8. Navijalić, M. (2014.) *Informacijski sustavi za upravljanje odnosima s klijentima*. Diplomski rad: Zagreb, Fakultet strojarstva i brodogradnje – Split, 4.

9. Pejić Bach, M. (2005.) Rudarenje podataka u bankarstvu, *Zbornik Ekonomskog fakulteta u Zagrebu*, 3.

10. Vučemilović, V. (2015.) Prednosti strategije upravljanja odnosom s kupcima, *Zbornik radova Veleučilišta u Šibeniku*

11. Šebalj, D., Živković, A. i Hodak, K. (2016.) Big data: changes in data management: *Ekonomski vjesnik*

12. Kocijan, K. (2014.) Big Data: how we got to the BigData and where are they taking us, *Komunikacijski obrasci i informacijska znanost*, Zagreb, 3.

13. Kušić, S. (2010.) Online društvene mreže i društveno umrežavanje, *Život i škola*, 2.

14. Nenadić, I., (2017.) Kako su mainstream mediji otvorili vrata alternativnim činjenicama?, *Političke analize*

# Internetski izvori

1. *Što su to osobni podaci?* [online]: Europska komisija. Dostupno na: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_hr [ 25. kolovoza 2018.]

2. Peter Sayer (2016.): 5. things you need to know about the EU-US Privacy Shield agreement [online]: https://www.pcworld.com/article/3038688/privacy/five-things-you-need-to-know-about-the-eu-us-privacy-shield-agreement.html [28. kolovoz 2018.]

3. *Opća uredba o zaštiti podataka 2018: Što donosi GDPR?* [online] , https://gdpr2018.eu/sto-donosi-gdpr/ [24. kolovoz. 2018.]

4. CARnet – Hrvatska akademska i istraživačka mreža (2010.) [online]: *Napredne tehnike socijalnog inženjeringa* (brošura), 3. https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-02-292.pdf, [25.kolovoz 2018.]

5. *O socijalnom inženjeringu* [online], https://www.cert.hr/socijalni_inzenjering/ [25. kolovoz 2018.]

6. *Facebook statistika* [online], https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [preuzeto 30. kolovoza 2018.]

7. *The Facebook and Cambridge Analytica scandal, explained with a simple diagram* [online], https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram [ 30. kolovoz 2018.]

8. *Reveald: 50 milion Facebook profiles harvested for Cambridge Analytica in major dana breach* [online], https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [26. kolovoz 2018.]

9. *Cambridge Analytica službene stranice* [online], https://cambridgeanalytica.org/ [ 24. kolovoz 2018.]

# 8. Popis priloga