Dopuštenja aplikacijama pametnih telefona i privatnost podataka

Stanišić, Anđela

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Anđela Stanišić

DOPUŠTENJA APLIKACIJAMA PAMETNIH TELEFONA I PRIVATNOST PODATAKA

ZAVRŠNI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 6186

Pristupnik: **Anđela Stanišić (0135254481)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Dopuštenja aplikacijama pametnih telefona i privatnost podataka**

Opis zadatka:

Navesti statistike korištenja aplikacija pametnih telefona. Pojasniti koncept dopuštenja aplikacijama pametnih telefona. Izvijestiti o privatnosti podataka aplikacija pametnih telefona. Opisati mogućnosti zaštite podataka prikupljenih aplikacijama.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

DOPUŠTENJA APLIKACIJAMA PAMETNIH TELEFONA I PRIVATNOST PODATAKA

SMARTPHONE APPLICATIONS PERMISSIONS AND DATA PRIVACY

Mentor: doc. dr. sc. Siniša Husnjak

Student: Anđela Stanišić

JMBAG: 0135254481

Zagreb, 2021.

DOPUŠTENJA APLIKACIJAMA PAMETNIH TELEFONA I PRIVATNOST PODATAKA

SAŽETAK

Korištenje mobilnih aplikacija postala je rutina i neophodna potreba svakog korisnika te razvoj i rast aplikacija se iz dana u dan povećava. Svrha ovog rada je osvijestiti korisnike da obrate pozornost na uvjete korištenja aplikacija prilikom same instalacije. Rad se temelji na statističkim podacima koji prikazuju porast broja korisnika na globalnoj razini najkorištenijih društvenih mreža. Korisnici većinu svog vremena provode na društvenim mrežama i tako odaju više informacija o sebi. Neke tvrtke, poput *Facebooka*, posjeduju više aplikacija i kako bi pružili što bolji sadržaj, svi podaci se dijele međusobno. Osim što koriste podatke u vlastite svrhe, također aplikacije dijele osobne podatke sa trećim stranama. Većina država ima propisane zakone koji postavljaju uvjete koje podatke aplikacije mogu prikupljati te zajedno sa zaštitom operativnog sustava, korisnici su barem jednim dijelom zaštićeni. Prije instaliranja aplikacija, korisnici trebaju obratiti pozornost na aplikacije koje instaliraju i koje podatke uzimaju od njih.

Ključne riječi: podaci, aplikacije, korisnik, mobilni uređaji

SMARTPHONE APPLICATIONS PERMISSIONS AND DATA PRIVACY

SUMMARY

The use of mobile applications has become a routine and a necessary need of every user, and the development and growth of applications is increasing day by day. The purpose of this thesis is to make users aware of the conditions of use of applications during installation. The thesis is based on statistical data showing the increase in the number of users globally of the most used social networks. Users spend most of their time on social media and, on that way, reveal more informations about themselves. Some companies, like Facebook, own multiple applications and in order to provide the best possible content, all the data is shared mutually. In addition to using the data for their own purposes, the applications also share personal data with third parties. Most states have prescribed laws that set the conditions about which data applications can collect, and thus, along with operating system protection, users are at least partially protected. Before installing applications, users should pay attention to the applications they install and what data they take from them.

Keywords: data, applications, user, mobile devices

SADRŽAJ

1. UVOD

Društvene mreže omogućuju korisnicima brz način komuniciranja putem Interneta. Sadržaj koji se prenosi može biti u obliku poruka, video zapisa, fotografija, dokumenata i slično. Način komuniciranja najčešće se odvija putem aplikacija ili *web* stranica. Prvobitna ideja društvenih mreža bila je način interakcije s prijateljima i obitelji, ali kasnije su ih usvojile tvrtke koji su takav oblik komuniciranja pretvorili u marketinške svrhe. Za pojedine tvrtke, društveni mediji su postali nezamjenjiv alat. Tvrtke koriste platforme za oglašavanje i promicanje prodaje, mjerenje potrošačkih trendova i pružanje korisničkih usluga.

Društvene mreže prate kako korisnici gledaju, dijele i stupaju u interakciju s pruženim sadržajem. Pomoću tih podataka smišljaju sadržaj koji bi mogao stvoriti veći interes kod korisnika kako bi proveli više vremena na njihovoj platformi. Osim toga, prikupljaju osobne podatke korisnika, a više informacija znači bolji sadržaj te bolju zaradu.

Cilj i svrha završnog rada je prikaz podataka koje prikupljaju određene aplikacije i narušava li se time privatnost korisnika.

Rad se sastoji od 6 poglavlja:

1. Uvod
2. Korištenje aplikacija pametnih telefona
3. Dopuštenja aplikacija pametnih telefona
4. Privatnost podataka aplikacija pametnih telefona
5. Mogućnost zaštite podataka prikupljenih aplikacijama
6. Zaključak

U drugom poglavlju prikazani su statistički podaci na globalnoj razini koji su potkrijepljeni grafovima. Prikazat će se porast broja korisnika kroz određeno razdoblje i razvoj najpopularnijih društvenih mreža.

U trećem poglavlju opisat će se Uvjeti i odredbe aplikacija koje vlasnici aplikacija moraju ispuniti prije slanja aplikacije na tržište. Opisat će se dva najpoznatija operativa sustava: *Android* i *iOS* te kako s novijim generacijama operativnog sustava dolaze i nova pravila. Prikazat će se razlike u ovlastima sljedećih aplikacija: *Instagram*, *Facebook*, *Facebook Messenger*, *WhatsApp*, *Telegram*, *Viber* i *TikTok*.

U četvrtom poglavlju prikazat će se pravila o zaštiti privatnosti korisnika koje također vlasnici aplikacija moraju poštovati prije slanja aplikacija na tržište. GDPR je Europska zakonska regulativa koja pruža korisnicima veću kontrolu nad svojima podacima od vlasnika aplikacija. Nadalje, bit će opisane aplikacije koje unatoč svojim postavljenim Uvjetima i dalje prikupljaju podatke od korisnika. Također, bit će navedeni slučajevi kršenja i prikupljanja podataka.

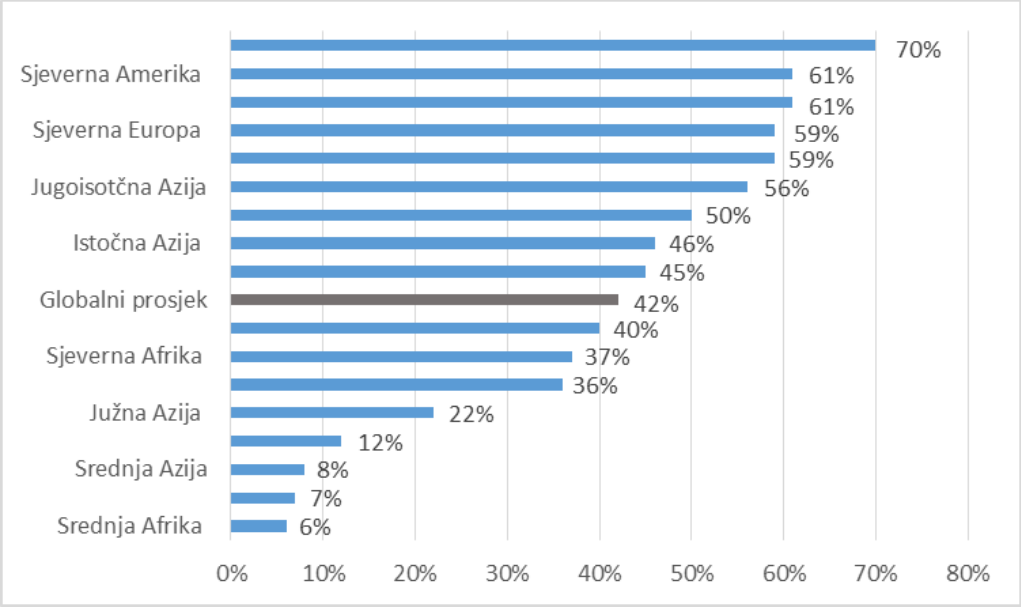
U petom poglavlju prikazat će se način zaštite korisnika od prikupljanja podataka. Zaštita se odvija na razini operativnog sustava i digitalne distribucije. Svaki operativni sustav ima svoj zaštitni sustav koji ne dopušta instaliranje zlonamjernih aplikacija i slično. Isto tako, trgovine aplikacijama provode različite sigurnosne mjere kako bi sve aplikacije na toj platformi bile sigurne za korištenje.

2. KORIŠTENJE APLIKACIJA PAMETNIH TELEFONA

Sve više je korisnika koji preuzimaju aplikacije i provode više vremena baveći se aplikacijama. To ukazuje da rast ukupno utrošenog vremena potiče više ukupnih korisnika, kao i više vremena provedenog po korisniku dnevno. S obzirom na to da se povećava broj preuzetih aplikacija, platforme za preuzimanje aplikacija šalju sve više aplikacija na tržište. Raznolikost u kategorijama aplikacija omogućuje korisnicima korištenje aplikacija za različite svrhe, kao što su društvene mreže, igre, glazba, financije i mnoge druge.

2.1. Statistički podaci globalne razine

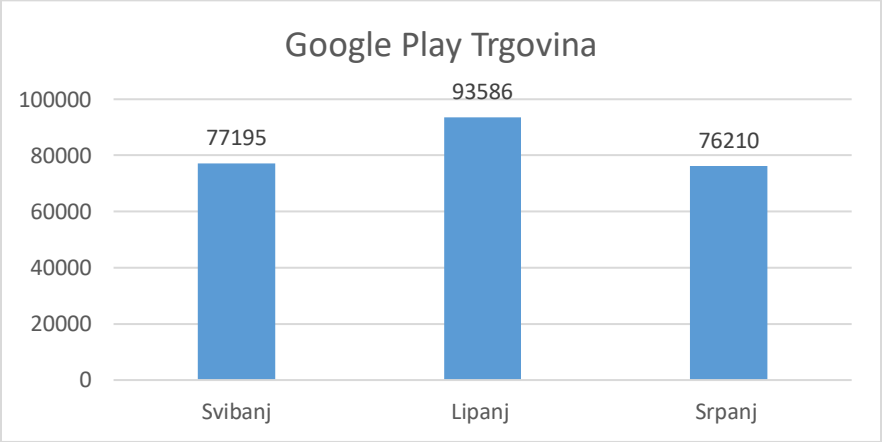
Nekoliko milijuna ljudi svakodnevno koristi mobilne uređaje. Uređaji poput pametnih telefona i tableta, evoluirali su u ključne alate za informacije, komunikaciju i zabavu. Budući da mobilne tehnologije postaju pristupačnije, predviđa se porast nad korištenjem interneta i mobilnih uređaja. Mobilne mreže su primarno sredstvo za pristup internetu te danas mobilni internetski promet čini više od 55% ukupnog *web* prometa. Korištenje interneta širom svijeta i revolucija mobilnih uređaja nastavlja preoblikovati ponašanje i frekvencije korištenja interneta. Jedna od najpopularnijih mrežnih aktivnosti među korisnicima mobilnih uređaja su društvene mreže. Grafikon 1 prikazuje podatke od siječnja 2019. godine gdje je stopa korištenja mobilnih društvenih mreža u svijetu iznosila 42%, [1].



Grafikon 1. Statistički podaci korištenja društvenih mreža na globalnoj razini

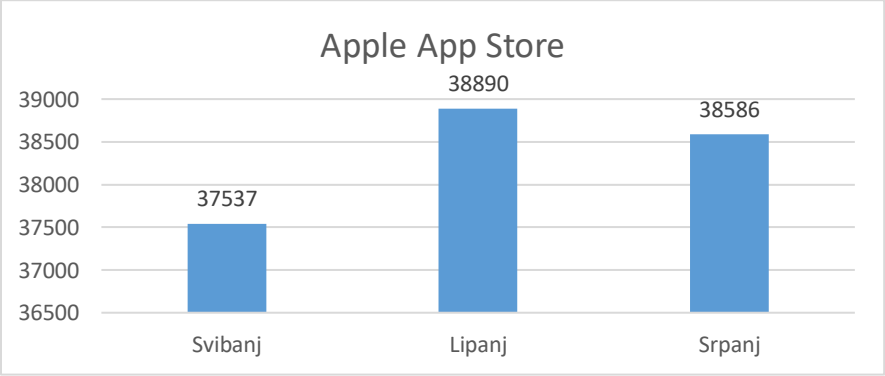
Izvor: https://www.statista.com/statistics/412257/mobile-social-penetration-rate-region/

Iako su na nekim mobilnim uređajima aplikacije unaprijed instalirane, korisnici mogu odabrati aplikacije putem trgovine aplikacija, kao što su *Google Play* trgovina za *Android* i *Apple App Store* za *iOS*. Prema podacima od srpnja 2020. u *Apple App Storeu* objavljeno je oko 4,37 milijuna aplikacija, dok trgovina *Google Play* od lipnja 2020. godine ima dostupno oko 2,96 milijuna aplikacija. Trgovina *Google Play* u prosjeku svakog mjeseca izbaci na tržište više od 100 000 novih aplikacija za *Android*. Za razliku od *Google Play* trgovine, *Apple App Store* u prosjeku svakog mjeseca izda više od 30 000 novih aplikacija za *iOS*. Smatra da je *Google Play* trgovina jeftinija i u svijetu ima mnogo više korisnika *Androida* nego *iOS* korisnika, stoga nove *iOS* aplikacije se izdaju sporije od *Android* aplikacija. Grafikoni 2 i 3 prikazuju podatke novih aplikacija trgovine *Google Play* i *Apple App Storea* od svibnja, lipnja i srpnja 2021. godine



Grafikon 2. Statistika novih aplikacija *Google Play* Trgovine

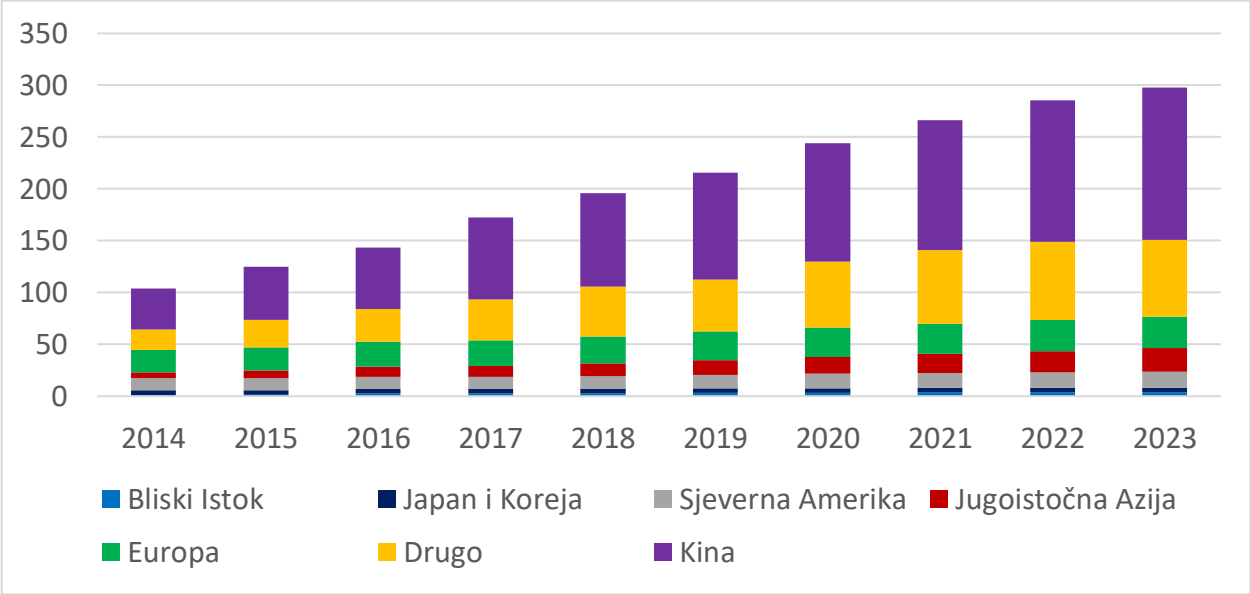
Izvor: https://42matters.com/google-play-statistics-and-trends



Grafikon 3. Statistika novih aplikacija *Apple App Storea*

Izvor: https://42matters.com/google-play-statistics-and-trends

Trenutno je oko 92% aplikacija u *Apple App Storeu* besplatno dok *Google Play* trgovina ima 96% besplatnih aplikacija, što ujedno i povećava broj korisnika. Iako je većina mobilnih aplikacija besplatna na tržištu, mnoge od tih aplikacija i dalje zarađuju na oglasima, dodacima i nadogradnjama. Kako globalni broj korisnika mobilnih uređaja neprestano raste, predviđa se i porast broja preuzimanja aplikacija, [2]. Grafikon 4 prikazuje porast te predviđen porast preuzimanja mobilnih aplikacija od 2014. godine do 2023. godine po regijama diljem svijeta.



Grafikon 4. Preuzimanje mobilnih aplikacija u milijardama

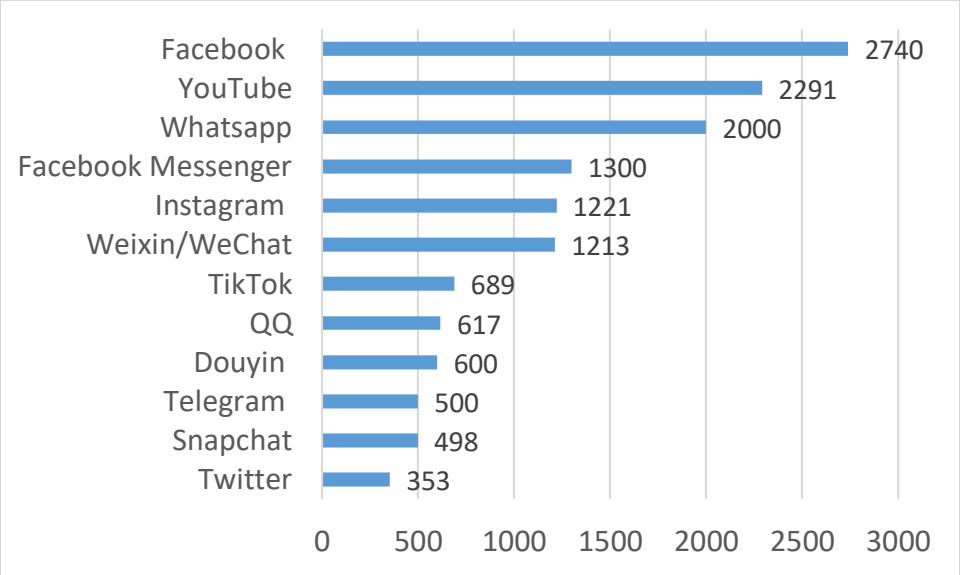
Izvor: https://www.statista.com/statistics/266488/forecast-of-mobile-app-downloads/

2.2. Statistički podaci društvenih mreža

Društvene mreže su jedne od najkorištenijih aplikacija diljem svijeta. Dostupne su na više jezika i omogućuju povezivanje s prijateljima ili ljudima preko geografskih, političkih ili ekonomskih granica. Procjenjuje se da trenutno ima oko 2.784.143,6 milijardi korisnika društvenih mreža. S obzirom na rast upotrebe mobilnih uređaja i popularnost mobilnih društvenih mreža očekuje se i porast korisnika.

Facebook je trenutno prva društvena mreža koja broji više od 2,6 milijardi aktivnih korisnika mjesečno te prema podacima od siječnja 2021. je trenutno najkorištenija društvena mreža kao što je vidljivo iz grafikona 5. Također, tvrtka trenutno posjeduje četiri najveće platforme za društvene

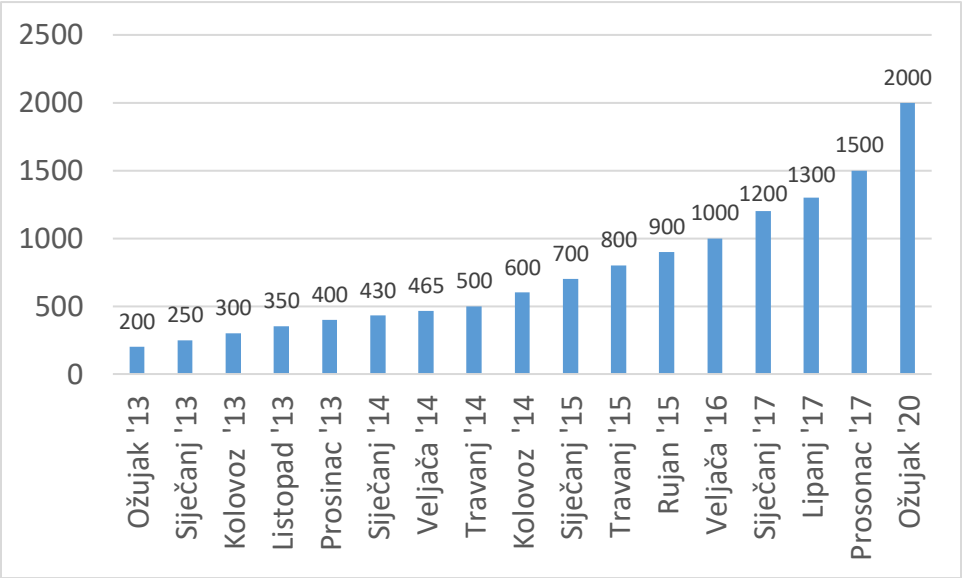
medije, a to su: *Facebook*, ujedno i osnovna platforma, *WhatsApp*, *Facebook Messenger* i *Instagram*. Dostupnost *Facebooka* na mobilnim uređajima omogućila je tvrtki da rano postavi pravo na internetska tržišta koja su prva za mobilne uređaje, poput Indije. *Facebook* također objavljuje aplikacije temeljene na originalnim *Facebook* značajkama kao što je *Facebook Messenger*. To je platforma koja omogućuje komunikaciju *Facebook* korisnicima putem tekstualnih poruka, glasovnih poruka ili videopoziva. Širok raspon aplikacija povezanih s *Facebookom* osigurava da je tvrtka jedna od najpopularnijih izdavača aplikacija u svijetu na temelju preuzimanja, [3].



Grafikon 5. Najpopularnije društvene mreže širom svijeta od siječnja 2021. rangirane po broju aktivnih korisnika u milijunima

Izvor: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

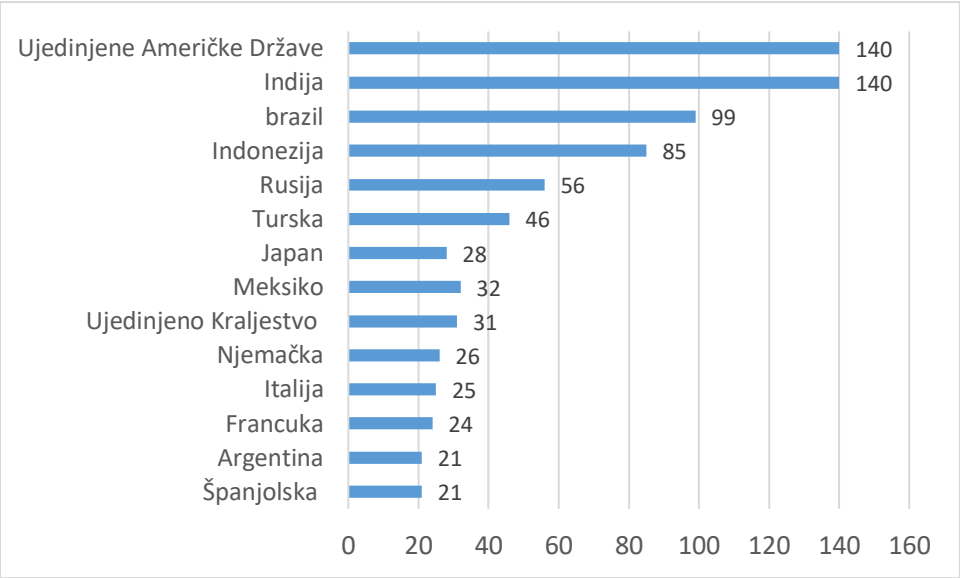
WhatsApp je platforma koja većinom služi za komunikaciju putem poruka. Jedna je od najpopularnijih aplikacija za razmjenu poruka putem cijelog svijeta te se uostalom suočava i s jakom konkurencijom. Aplikacija je zasnovana na jeftinom modelu preplate. Korisnicima se omogućuje dijeljenje tekstualnih, slikovnih i video poruka, a naplaćuje se putem mobilnog operatera, [4]. *WhatsApp* od ožujka 2020. godine broji dvije milijarde aktivnih korisnika mjesečno. Porast broja korisnika prikazan je u grafikonu 6.



Grafikon 6. Broj mjesečno aktivnih *WhatsApp* korisnika u milijunima od travnja 2013. do ožujka 2020.

Izvor: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

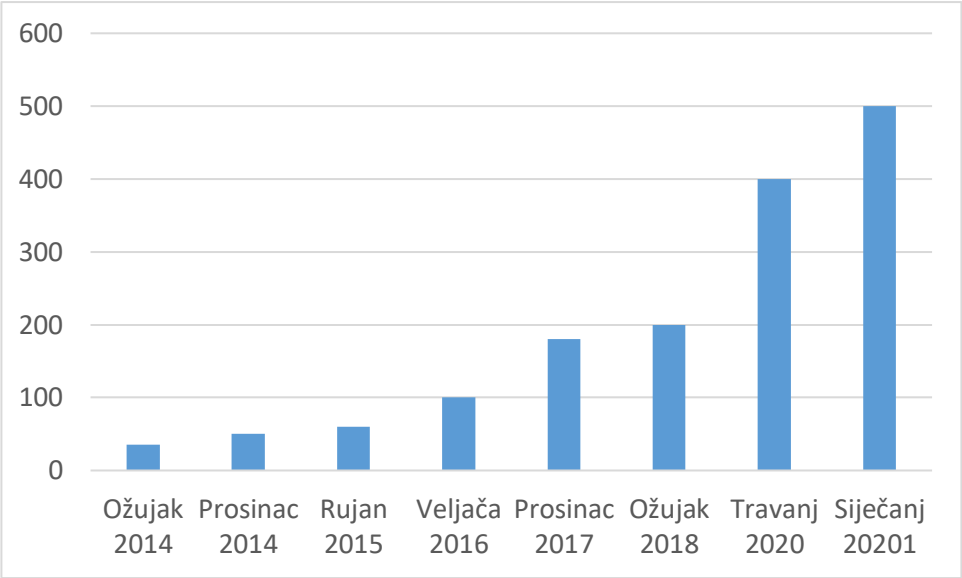
Instagram je društvena mreža koja služi za razmjenu fotografija i kratkih videozapisa. Trenutno se vodi kao šesta najveća društvena mreža na svijetu te broji 4,18 milijardi aktivnih svjetskih korisnika. Prema podacima o *Instagram* stopi rasta, između rujna 2017. i lipnja 2018. godine, platforma za razmjenu medija je ostvarila rast od 200 milijuna novih korisnika, dok od 2018. do 2019., rast korisnika bio je povećan za 6,7%, [5]. Sjedinjene Američke Države, Indija i Brazil su trenutno države s najvećim brojem mjesečnih korisnika, vidljivo na grafikonu 7.



Grafikon 7. Broj *Instagram* korisnika u milijunima od siječnja 2021.

Izvor: https://www.statista.com/statistics/578364/countries-with-most-instagram-users/

Jedna od najpopularnijih aplikacija u svijetu je *Telegram*. Prvi put je pokrenuta 2013. godine kao aplikacija za razmjenu poruka. Na samim počecima aplikacija je bila dostupna samo na *iOS*-u, a kasnije se mogla koristiti i na *Androidima*. Od samog pokretanja aplikacije stopa rasta korisnika je 40% svake godine. Najveći porast korisnika bio je tijekom 72-satnog skoka u siječnju 2021. gdje se pridružilo 25 milijuna novih korisnika. Također, aplikacija broji više od 63 milijuna preuzimanja u siječnju 2021. te nosi titulu najviše preuzimane aplikacije u tom razdoblju. *Telegram* danas broji oko 500 milijuna aktivnih korisnika mjesečno, [6]. Porast broja korisnika od 2014. godine do 2021. godine, vidi se na grafikonu 8.



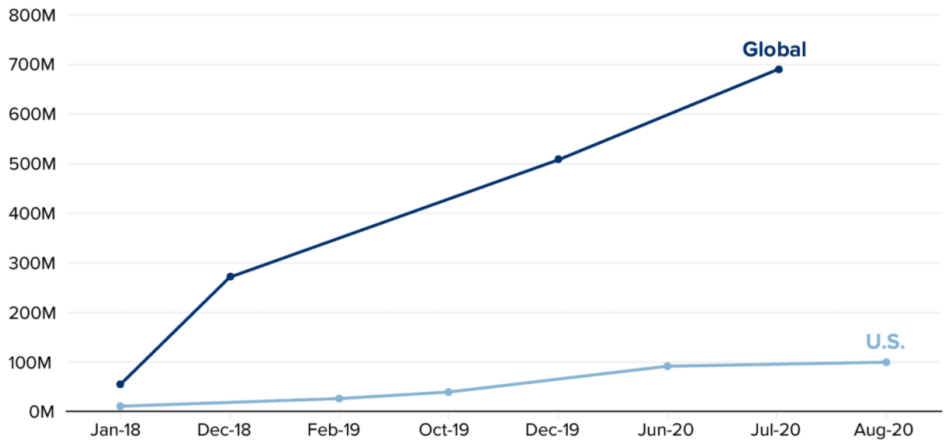
Grafikon 8. Porast broja *Telegram* korisnika (u milijunima) do siječnja 2021. godine

Izvor: https://backlinko.com/telegram-users

Viber je također jedna od aplikacija koja nudi besplatne usluge poziva i razmjenu poruka mobilnim korisnicima. Platforma omogućuje upućivanje poziva, slanje teksta, slika ili videozapisa, a za to sve jedino je potreban pristup internetu. U ožujku 2018. *Viber* je dosegao milijardu korisnika, a do rujna se pridružilo još 50 milijuna korisnika. Iako ima velik broj korisnika, *WhatsApp* je i dalje ovoj platformi najveća konkurencija. Aplikacija se koristi u 193 zemlje diljem svijeta i dostupna je na nekoliko jezika kako bi se prilagodila globalnoj publici. Premda *Viber* trenutno ima 1,05 milijardi korisnika, samo 260 milijuna aktivno koristi aplikaciju. Da bi se korisnici mogli smatrati aktivnima, aplikaciji treba pristupiti najmanje jednom mjesečno, [7].

TikTok je aplikacija koja omogućuje korisnicima stvaranje kratkih videozapisa s glazbom, filtrima i nekim drugim značajkama u trajanju od 15 sekundi. Od pokretanja, dakle 2017. godine, *TikTok* u roku od nekoliko mjeseci postaje jedna od najbrže rastućih aplikacija u svijetu. *TikTok* je preuzet preko 738 milijuna puta u 2019. godini te postaje jedna od vodećih aplikacija na trgovini *Google Play* i *Apple App Storeu*. Premda *TikTok* ima konkurenciju poput *YouTube*a, *Facebooka* i *Instagrama*, prema statistici od siječnja 2021. platforma ima 689 milijuna mjesečno aktivnih korisnika diljem svijeta. Od travnja 2020., aplikacija je preuzeta više od dvije milijarde puta te popularnost i dalje ne prestaje rasti. Unatoč popularnosti, neke zemlje, poput Pakistana, su zabranile korištenje aplikacije zbog „nemoralnog/nepristojnog sadržaja“ na platformi, [8]. Na

grafikonu 9 vidljiv je rast *TikTok* korisnika na globalnoj razini i u Sjedinjenim Američkim Državama.

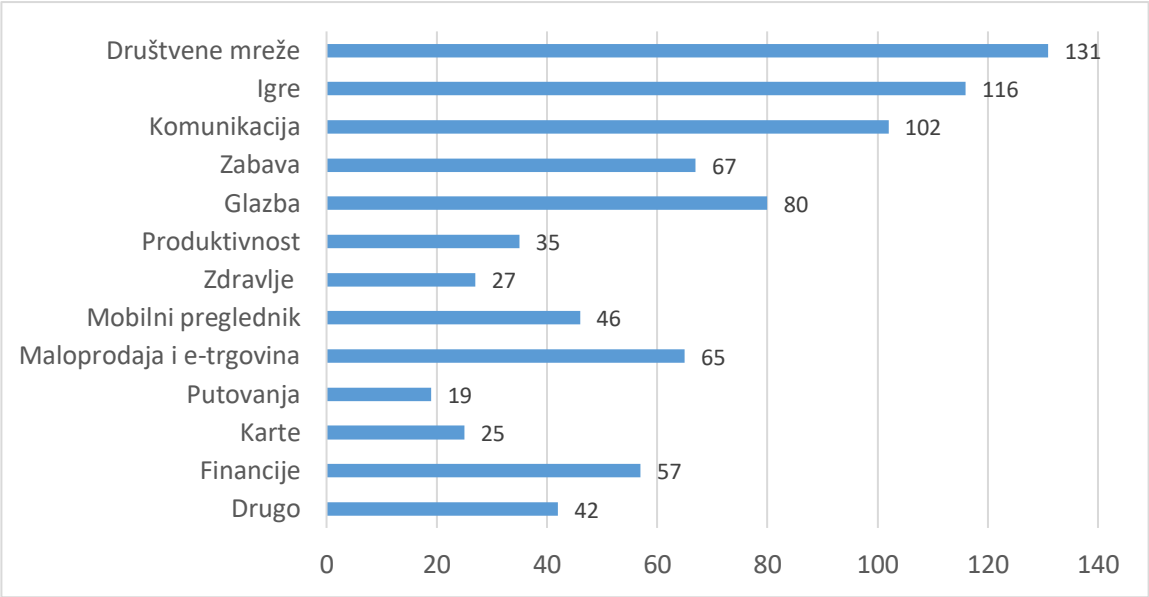


Grafikon 9. Rast *TikTok* mjesečnih aktivnih korisnika

Izvor: https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html

2.3. Vrijeme provedeno na zaslonu

Ljudi provode više vremena na društvenim mrežama nego baveći se svakodnevnim aktivnostima. Svjetska zdravstvena organizacija procjenjuje da je prosječni globalni životni vijek 72 godine te se procjenjuje da će ljudi provesti gotovo šest godina i osam mjeseci svog života na društvenim mrežama. Prema podacima iz 2020. godine dnevno prosječno vrijeme provedeno na društvenim mrežama iznosi 2 sata i 24 minute, [9]. Korisnici prosječno tjedno potroše 131 minutu koristeći društvene mreže, kao što se vidi na grafikonu 10.



Grafikon 10. Prosječno tjedno vrijeme utrošeno koristeći aplikacije (u minutama)

Izvor: https://www.simform.com/the-state-of-mobile-app-usage/

Iako kod nekih mobilnih uređaja korisnik može vidjeti vrijeme koje je provedeno na mobilnom uređaju, sada to može vidjeti i kod nekih društvenih mreža u sklopu aplikacije. Neke od tih aplikacije su *Facebook* i *Instagram*. Naime, u postavkama aplikacije postoji opcija gdje se može vidjeti dnevna aktivnost i prosječno vrijeme provedeno na aplikaciji. Također, jedna od opcija je da se postavi granica koliko korisnik svakodnevno želi provesti na aplikaciji. Nakon što korisnik prijeđe postavljeni limit, dolazi obavijest koja upozorava korisnika da je prešao postavljenu granicu te korisnik može zanemariti obavijest ili odjaviti se sa svog računa, [10]. Na taj način korisnik može smanjiti vrijeme provedeno na društvenim mrežama i iskoristiti ga za neke druge aktivnosti.

3. DOPUŠTENJA APLIKACIJA PAMETNIH TELEFONA

U današnje vrijeme skoro svaka aplikacija ima svoje Uvjete i odredbe korištenja. Postavlja se skup pravila kojih se korisnici moraju pridržavati da bi pristupili aplikaciji, koristili je ili nastavili koristiti aplikaciju. Prema tim pravilima, vlasnici aplikacije imaju pravo isključiti korisnika iz svoje aplikacije u slučaju zloupotrebe aplikacije, imaju ograničenu odgovornost prema korisnicima, zadržavaju pravo raskida korisničkih računa ukoliko to žele i mnoge druge. Uvjeti i odredbe korištenja aplikacije nisu zakonski propisane i nisu nužno potrebni za pokretanje mobilne aplikacije u trgovini aplikacija.

3.1. Uvjeti i odredbe aplikacija

Uvjeti korištenja ili Uvjeti pružanja usluge su pravne okosnice odnosa između mobilne aplikacije i korisnika. Definira se način na koji se aplikacija, usluga ili sadržaj može koristiti te se zaštićuje sadržaj s aspekta autorskih prava, kao i zaštita od potencijalnih obveza. Postavljaju se klauzule koje utjelovljuju pravila, zahtjeve i ograničenja koje korisnik mora prihvatiti da bi koristio mobilnu aplikaciju. Postoji nekoliko važnih klauzula koje većina vlasnika aplikacija uključuje u svoje Uvjete i odredbe.

Klauzula o nedopuštenom korištenju informira korisnika o aktivnostima i ponašanjima koja su strogo zabranjena unutar aplikacije. To uključuje stvari poput prikupljanje podataka od drugih korisnika bez njihova pristanka, slanje neželjene pošte drugim korisnicima, prenošenje uznemirujućeg, nepristojnog ili nezakonitog materijala i mnoge druge.

Klauzula o intelektualnom vlasništvu odnosi se na korištenje logotipa, dizajna, umjetničkih kreacija, simbola i slika. To znači da korisnici ne smiju koristiti nikakve zaštitne znakove aplikacije, logotipe ili nešto slično, ali također nisu dopuštene izmjene, poboljšanja, izvedena djela i njihove nadogradnje vezane za intelektualno vlasništvo.

Većina platformi koja služi za razmjenu sadržaja za korisnike uključuje klauzulu koja se odnosi na sadržaj koji generiraju korisnici. Ta klauzula usredotočuje se na vlasnike korisničkog sadržaja, ali uključuje pravo vlasnika aplikacije na uklanjanje neprimjerenog ili ilegalnog sadržaja kojeg generiraju korisnici.

Također jedna od bitnih stavki je kršenje autorskih prava. Korisnicima se omogućuje prijava kršenja autorskih prava koja se događaju unutar aplikacije. Zaštita od kršenja autorskih prava može

se uključiti pomoću DMCA (eng. *Digital Millennium Copyright Act*) odjeljka ukoliko postoji u aplikaciji. DMCA pomaže u izolaciji aplikacije od pravne odgovornosti za bilo kakvo kršenje autorskih prava koje se događa zbog radnje njihovih korisnika. Neki od DMCA zahtjeva su: uključenje klauzule koja navodi da se ukloni sav materijal za koji se ispostavi da je prekršeno autorsko pravo, obavijest korisnicima kako se točno može prijaviti kršenje autorskih prava i uspostavljanje plana koji izvršava uklanjanje materijala na zahtjev korisnika. Iako je DCMA američki zakon, većina zemalja širom svijeta ima zakone koji se odnose na kršenje autorskih prava.

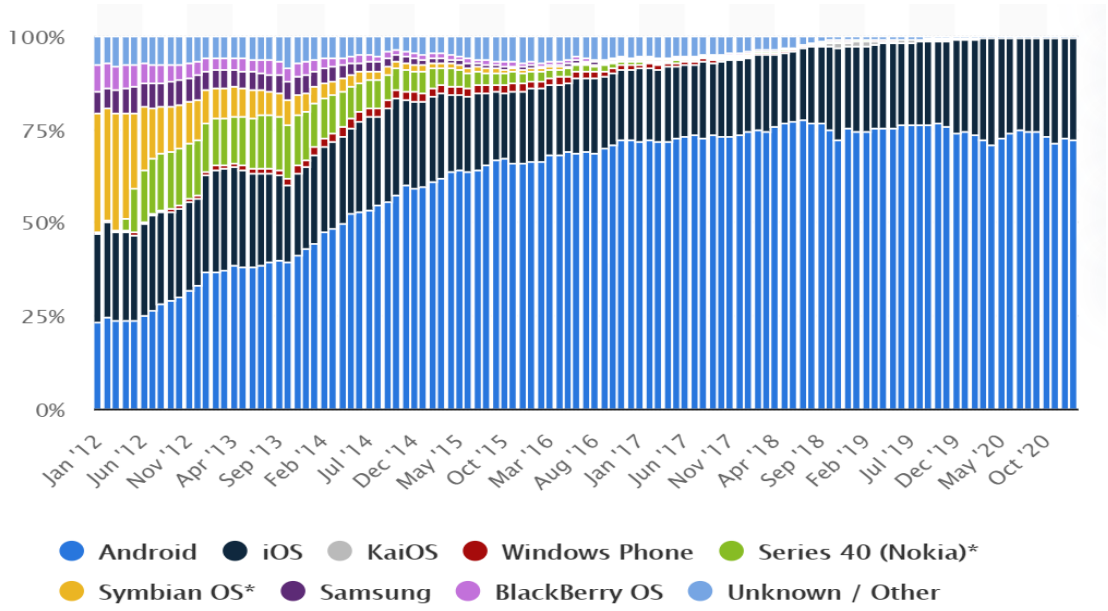
Ukoliko aplikacija zahtijeva plaćanja, dakle ako se radi o pretplati, nadogradnji aplikacije ili e-trgovine, uključuje se klauzula koja se svodi na način plaćanja koji se prihvaća, naknade koje se naplaćuju, kada se očekuje plaćanje i druge relevantne stvari.

Klauzula o pravu na ukidanje računa daje mobilnoj aplikaciji ovlaštenje da ukine ili suspendira račune korisnika pod određenim okolnostima na koje se odnose Uvjeti i odredbe. S ovom klauzulom omogućuje uvid u detalje koje radnje i ponašanja se ne dopuštaju te kako se postupa s bilo kojim korisnikom koji generira nedopušteni sadržaj.

Klauzulom o jamstvu / ograničenju odgovornosti u kojoj vlasnik prikazuje svoju aplikaciju kao „takvu kakvu jest“ i bez priloženog jamstva. Također, ograđuje se od odgovornosti poput pogrešaka, slučajnih šteta, propusta, uvredljivog sadržaja, zlonamjernog softvera i drugih stvari koje se ne mogu kontrolirati, [11].

3.2. Specifičnosti operativnih sustava

Jedni od najpoznatijih i najkorištenijih operativnih sustava su *Android* OS i *Apple iOS*. Iako ta dva operativna sustava imaju dosta sličnosti, najveća razlika je u tipu koda. *Apple iOS* ima zatvoren programski kod, što znači da je sustav manje fleksibilan, ali i manje ranjiv. *Android* OS je otvorenog programskog koda, temeljem toga korisnici mogu mijenjati kod prema svojim potrebama. Oba operativna sustava predstavljena su 2007. godine te redovito ažuriraju svoje usluge i softver. Trenutno posjeduju oko 99% globalnog tržišnog udjela. Prema podacima od siječnja 2021. godine, *Android* OS trenutno posjeduje oko 71,93% mobilnog tržišta te se smatra kao vodeći operativni sustav u svijetu, dok *iOS* posjeduje oko 27,47% svjetskog mobilnog tržišta. Udio mobilnih operativnih sustava od siječnja 2012. do siječnja 2021. prikazan je na grafikonu 11, [12].



Grafikon 11. Udio mobilnih operativnih sustava

Izvor: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/#statisticContainer

3.2.1. Apple iOS

Apple iOS je operativni sustav koji je dizajniran za umrežavanje između *Appleovih* mobilnih terminalnih uređaja. Mobilni terminalni uređaji temeljeni na *iOS* sustavu su *iPhone*, *iPad* i *iPod Touch*. Operativni sustav temeljen je na *Unixu* koji pokreće sve *Appleove* mobilne terminalne uređaje, a kratica *iOS* označava *iPhone Operating System*. Naziv *iOS* službeno se počeo primjenjivati 2008. godine kada je *Apple* omogućio svim proizvođačima aplikacije kreiranje aplikacije za tu platformu te su objavili *iPhone* razvojni paket za razvoj softvera (SDK, eng. *Software development kit*) koji pruža alate za razvoj *iOS* aplikacija, [13].

Kod podrške za *Apple ID* korisnici se prijavljuju na *web* stranice i aplikacije koristeći svoj postojeći *Apple ID*. Također, *Apple ID*-ovi zaštićeni su dvofaktorskom autentifikacijom i korisnici se mogu prijaviti pomoću biometrijske metode provjere autentičnosti koja podržava prijavu pomoću *Face ID*-a ili *Touch ID*-a.

iOS upotrebljava kontrole pomoću kojih aplikacije mogu spriječiti dobivanje podataka o lokaciji ili prihvaćanje sadržaja od nepoznatih pošiljatelja. Bez odobrenja korisnika, aplikacijama se može zabraniti korištenje *WiFi*-a ili *Bluetootha*. Prilikom pokretanja uređaja koriste se

sigurnosni lanci pokretanja i izvršava se samo pouzdani kod. Na taj način se provjerava integritet bilo kojeg koda pokrenutog uređaja.

Iako *Apple* štiti svoje korisnike od drugih malicioznih korisnika, *Apple* prikuplja, koristi i dijeli osobne podatke korisnika zbog vlastitih svrha. Prikupljaju se samo osobni podaci koji su im potrebni. Prilikom izrade *Apple ID*-a, preuzimanja ažuriranja softvera, povezivanje s pruženim uslugama, korištenje društvenih mreži ili neki drugi oblik komunikacije s *Appleom*, mogu se prikupljati razne informacije. Podaci koji se prikupljaju uključuju:

- informacije o računu
- informacije o uređaju
- podaci za kontakt
- informacije o plaćanju
- podaci o transakciji
- informacije o sprječavanju prijevara
- informacije o lokaciji
- zdravstvene informacije
- financijske informacije
- podaci državne iskaznice
- podaci o aktivnosti
- korištenja ponuđenih usluga kao što su povijest pregledavanja i pretraživanja.

Korisnik ne mora dati sve osobne podatke koje se od njega zatraže, a ne učini li to, neće biti u mogućnosti koristiti pojedine usluge ili proizvode u nekim slučajevima. Također podaci se prikupljaju kako bi se korisnicima poboljšale usluge koje se nude, ali i za zaštitu i sprječavanje prijevara i za poštivanje zakona. Povremeno se koriste osobni podaci za slanje važnih obavijesti, kao što su promjena uvjeta i pravila. Između ostalog, *Apple* prima osobne podatke i iz drugih izvora. Zaprimaju se podaci od drugih pojedinaca ili trećih strana koji dijele podatke s *Appleom*. Može se koristiti sadržaj poput slike, glasovne poruke ili neki drugi podaci vezani za korisnika u svrhe istraživanja i razvoja, [15].

Appleovo izdanje *iOS* 14 izdaje nove promjene koje se odnose na prikupljanje podataka i načina na koji se koriste. S ovim ažuriranjem uvodi se transparentnost praćenja aplikacija (ATT,

eng. *App Tracking Transparency*) gdje se kod programera zahtijeva da objave u *App Storeu* točne podatke koji se prikupljaju, dok istovremeno korisnicima se dopušta uključenje/isključenje dijeljenja podataka. Novija ažuriranja obuhvaćaju: upravljanje dozvolama za lokaciju, upit za prijavu za pristup IDFA-i (eng. *Identifier for Advertisers*) i prikupljanje podataka u aplikaciji.

U postavkama aplikacije korisnik može upravljati dozvolama za lokaciju. Korisniku se pojavljuje skočni prozor gdje postoji mogućnost uključenja ili isključenja precizne lokacije. Ukoliko se odabere opcija „uključi“, prikazuje se točna lokacija korisnika na karti. Ako se odabere opcija „isključi“, tada se prikazuje otprilike mjesto gdje se nalazi korisnik. Također, programeri mogu zatražiti jednokratni pristup preciznoj lokaciji u slučaju da se pojavi važna značajka koja to zahtijeva.

Koristeći identifikator oglašavanja, tj. IDFA, aplikacije moraju zatražiti dopuštenje za praćenje korisnika u web lokacijama i drugim aplikacijama. Korisniku se nudi na izbor „Dopusti praćenje“ ili „Zatraži da aplikacije ne prati“. Uz to, korisnici će imati nadzornu ploču za „Privatnost aplikacija“ kako bi vidjeli kojim dopuštenjima njihove aplikacije imaju pristup.

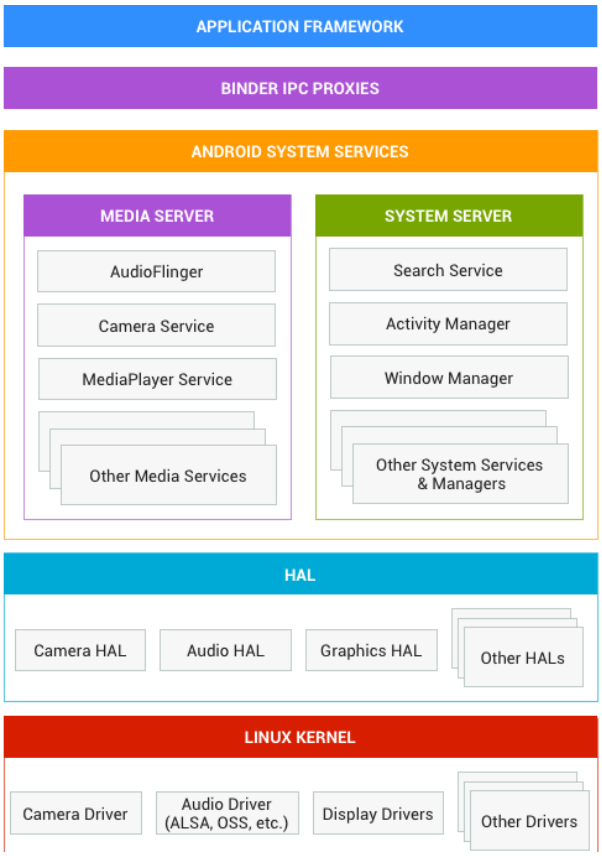
Između ostalog, programeri aplikacija moraju navesti koje podatke prikupljaju o korisnicima, što uključuje pregled pristupanja, korištenja i dijeljenja korisnikovih podataka. Međutim, programer aplikacije sam prijavljuje te podatke i prikazuje ih u *App Storeu,* [16].

3.2.2. Android OS

Android je operativni sustav kojeg je *Google* stvorio za upotrebu na mobilnim uređajima, poput pametnih telefona i tableta. Operativni sustav je otvorenog koda i zasnovan je na *Linuxu* za mobilne uređaje. Otvoreni izvorni kod i dopušteno licenciranje, omogućuje proizvođačima uređaja, mobilnim operaterima i programerima da slobodno prilagode i distribuiraju platformu. To ujedno i pruža korisnicima veći izbor stila uređaja i cijena.

Arhitektura *Android* sustava sastoji se od okvira aplikacije, vezivo IPC (eng. *Binder Inter-Process Communication*), usluge sustava, sloj apstrakcije hardvera (HAL, eng. *Hardware abstraction layer*) i *Linux kernel*. Okvir aplikacije najčešće koriste programeri aplikacija. Zatim, vezivo IPC omogućuje aplikacijskom okviru da prelazi granice procesa i poziva u kod usluga sustava *Android*. To omogućuje API-ju (eng. *Application Programming Interface*) visoke razine za interakciju s uslugama *Android* sustava. *Android* uključuje dvije skupine usluga sustava:

sustavne, poput *Window Managera* i *Notification Managera* i medijske usluge koje su uključene u reprodukciju i snimanje medija. HAL definira standardno sučelje koje dobavljači hardvera mogu implementirati, što omogućuje *Androidu* da bude agnostičan u pogledu implementacija upravljačkih programa niže razine. Korištenje HAL-a omogućuje implementaciju funkcionalnosti bez utjecaja ili mijenjanja sustava više razine. Operativni sustav *Androida* koristi verziju jezgre *Linuxa* s nekoliko posebnih dodataka, kao što je *Low Memory Killer,* [17]. Na slici 1 prikazana je arhitektura *Android* OS-a



Slika 1. Arhitektura *Android* operativnog sustava

Izvor: https://source.android.com/devices/architecture?hl=cs

Android svake godine izda nekoliko ažuriranih verzija svog operativnog sustava. Verzije *Android* sustava nazvane su temom deserta, a početkom 2009. godine izdana je verzija *Android* 1.5 *Cupcake*. Trenutno postoji 11 različitih verzija *Androida*, a neke od naziva su: *Cupcake, Donut, Gingerbread, Lollipop, Marshmallow* itd.

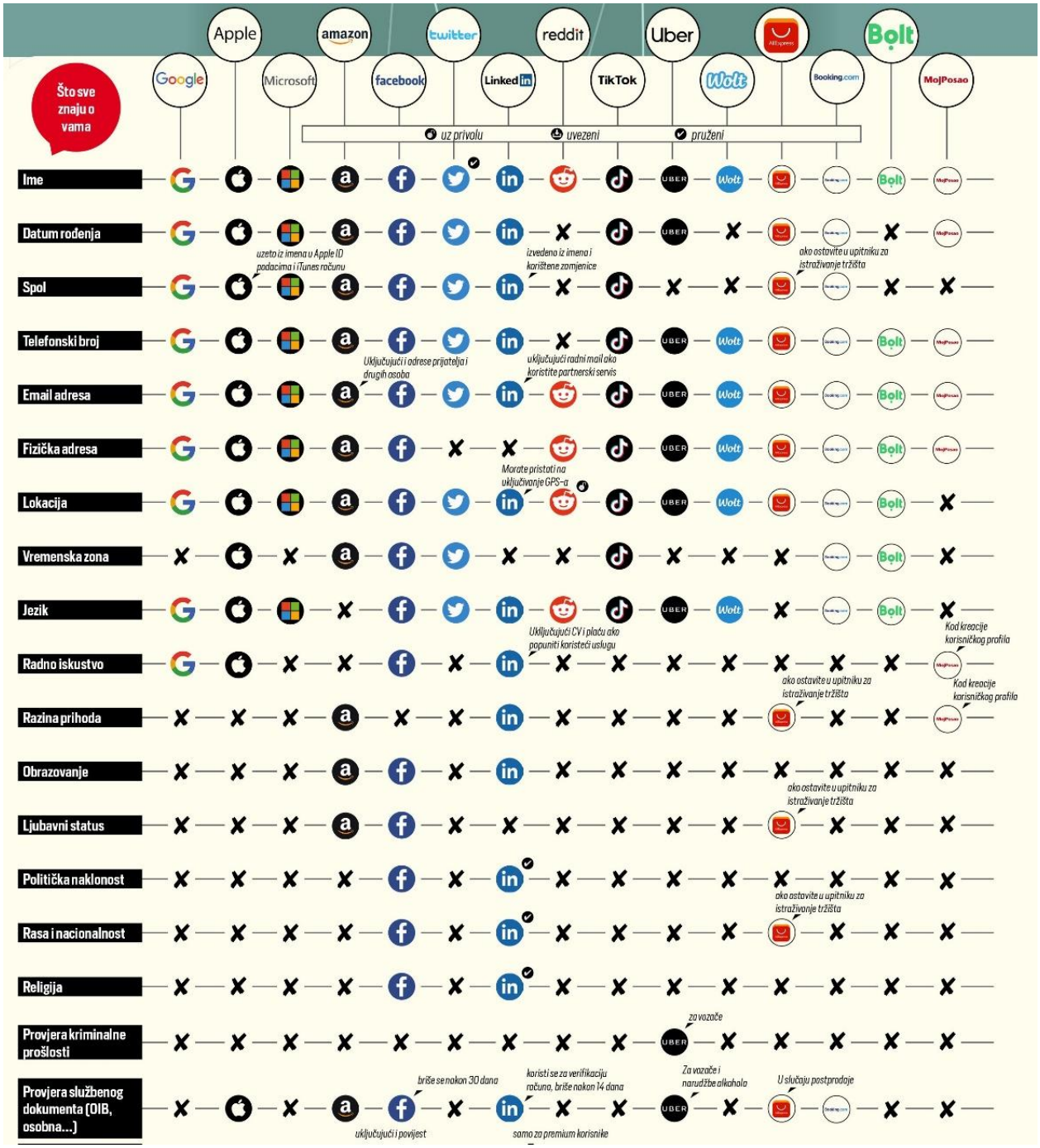
Početkom rujna 2020. godine izdana je *Android* 11 verzija. Najvažnije promjene vezane su za privatnost. Nadogradnja se nadovezuje na proširenu sustav dozvola uveden u *Androidu* 10 i dodaje se mogućnost korisnicima da aplikacijama daju određena dopuštenja koja se odnose na pristup lokaciji, kameri i mikrofonu. Uvedena je i nova značajka u kojoj se aplikacijama koje su otvorene nekoliko mjeseci automatski ukinu dozvole, osim ako ih korisnik aktivno ne odobri. Također, uklanja se mogućnost aplikacijama da vide koje su druge aplikacije instalirane na mobilnom uređaju korisnika i ograničavaju se načini na koje aplikacije mogu komunicirati s lokalnom pohranom kako bi se bolje zaštitile informacije korisnika.

Neka od ažuriranja za Android 11 su nadalje navedena. Postavljaju se granice što aplikacije mogu, a što ne smiju raditi u pozadini. Korisnik sam odabire kada će dijeliti osobne podatke s aplikacijama koje preuzima. Daje jednokratna dopuštenja aplikacijama koje trebaju pristup kameri, mikrofonu ili lokaciji. Aplikaciji se može dodijeliti jednokratno dopuštenje, umjesto postojećih opcija da se na primjer lokacija dijeli cijelo vrijeme, postoji i opcija da se lokacija dijeli samo dok se aplikacija upotrebljava. Sljedeći put kad aplikaciji zatreba pristup, aplikacija mora ponovno zatražiti dopuštenje. Ako već neko vrijeme korisnik nije koristio neku aplikaciju, *Android* resetira dozvole za nekorištenje aplikacije te korisnik uvijek može ponovno uključiti dopuštenja. Također, *Android* ograničava širok pristup zajedničkoj pohrani za sve aplikacije tako da podaci korisnika ostaju bolje zaštićeni. Ukoliko korisnik više puta odbije dozvole nekih aplikacije, blokira se zahtjev da aplikacija ponovno zatraži dopuštenje. *Google Play Protect* svaki dan skenira aplikacije, ako se otkrije aplikacija koja može oštetiti uređaj ili preuzeti podatke, šalje se obavijest korisniku. Svaka aplikacija se čuva na razini operativnog sustava, tako da druge aplikacije ne nadgledaju što korisnik radi, [18].

Google je predstavio prvu preglednu verziju *Android* 12 u veljači 2021. godine. Ta verzija će imati veći fokus na sigurnosti s novim kontrolama za nadzor pristupa mikrofonu i kameri. Uvode se brojne značajke koje povećavaju sigurnosti, kao i veća privatnost i produktivnost za korisnike. Očekuje se da će *Google* objaviti ukupno tri programa za programere prije nego što prijeđe na cjelovitu i reprezentativniju javnu beta verziju u svibnju, [19].

3.3. Razlike ovlasti aplikacija društvenih mreža

Društvene mreže postale su dio svakodnevice gotovo svakog korisnika u svijetu. Da bi se pojedine aplikacije mogle koristiti potrebno je prihvatiti Uvjete korištenja te aplikacije. Mnogi korisnici prihvaćaju Uvjete i odredbe korištenja aplikacije bez daljnjeg čitanja, a nisu ni svjesni koje uvjete su prihvatili. Samim pristankom na Uvjete i odredbe aplikacije, aplikacije dobivaju dopuštenje u prikupljanju osobnih podataka korisnika, kao i ostala dopuštenja koje su navedena u tim uvjetima. Prikupljaju se podaci o lokaciji, podaci o kontaktima, povijesti pregledavanja i mnoge druge. Aplikacije prikupljaju podatke iz više razloga, a jedan od osnovnih razloga je poboljšanje korisnikovog iskustva kako bi se ispravile pogreške i poboljšao rad određene platforme. Najčešće se prikupljaju podaci koji se koriste za praćenje korisnika (eng. *Data Used to Track You*) i podaci koji su povezani s korisnikom (eng. *Data Linked to You*). Na slici 2 prikazan je dio podataka koje prikupljaju aplikacije, a neke od njih opisane su u nastavku.



Slika 2. Količina prikupljenih podataka
Izvor: https://bgr.com/tech/app-privacy-labels-facebook-messenger-vs-imessge-signal-whatsapp/

Mnoge aplikacije dijele podatke sa „trećim stranama“. Treće strane mogu biti povezane s tvrtkom koja pokreće aplikacije ili mogu samo platiti naknadu za pristup podacima korisnika. S

obzirom na velik broj korisnika, društvene mreže prikupljaju najviše podataka zbog njihovog vlastitog marketinga, [20].

3.3.1. Instagram

Instagram kao jedna od najvećih društvenih mreža prikuplja podatke koji se unose prilikom upotrebe same aplikacije, kao što su podaci koji se upisuju prilikom registracije na korisnički račun. Ukoliko se kreira i dijeli sadržaj, prikupljaju se podaci o:

- osobama
- lokaciji fotografija
- datum izrade dokumenata
- korisničkim računima
- stranicama i grupama s kojima je korisnik povezan
- podaci za kontakt ako ih korisnik odluči prenijeti, sinkronizirati ili uvesti s uređaja

Ukoliko korisnik upotrebljava proizvode za kupnje ili druge financijske transakcije koje se vrše putem *Instagrama*, prikupljaju se podaci o kupnji ili transakciji. To uključuje podatke o plaćanju, npr. broj kreditne ili debitne kartice, ostali podaci o kartici, podaci o računu i provjeri autentičnosti, kao i podaci za slanje računa i pošiljke te podatke za kontakt. Također, prikupljaju se podaci s računala, telefona, povezanih televizora i drugih uređaja koji su povezani na internet. Podaci koji se prikupljaju s tih uređaja uključuju:

- svojstva uređaja, kao što je operacijski sustav
- verzija hardvera i softvera
- radnje na uređaju
- identifikatori
- signali *Bluetootha*
- podaci o obližnjim *Wi-Fi* pristupnim točkama
- davatelj usluge mobilne mreže
- jezik
- broj mobitela
- IP adresa
- brzina veze

- podaci iz kolačića (eng. *Cookies*).

Ako se uključi opcija prepoznavanja lica, *Instagram* upotrebljava tu tehnologiju kako bi prepoznali korisnike na fotografijama, videozapisima i pri korištenju kamere. Svi ti podaci se većinom koriste kako bi platforma *Instagram* kreirala sadržaj prema korisnicima, uključujući ponude i sponzorirane sadržaje koji bi mogli biti zanimljivi korisnicima, [21].

Instagram koristi podatke za otkrivanje sumnjivih pokušaja prijave, npr. koji uređaj korisnik upotrebljava za prijavu. Izvješća o padu s korisnikovog telefona pomaže im da prepoznaju greške u kodu i da se identificiraju dijelovi aplikacije koje nitko ne koristi. Osim potpunog brisanja aplikacije, nije moguće spriječiti *Instagram* da prati ponašanje korisnika na svojoj platformi, [22].

3.3.2. *Facebook*

Facebook detaljno proučava sitnice internetskog života svojih korisnika, a njegovo praćenje proteže se izvan poznatih ciljanih reklama tvrtke. Pojedinosti koje ljudi često dobrovoljno „odaju“ kao što su dob, ime, prezime, status veze, lokacija, samo su dio koje *Facebook* prikuplja. *Facebook* prati svoje korisnike na drugim *web* mjestima i aplikacijama.

Prikuplja biometrijske podatke o licu bez izričitog pristanka korisnika na „prijavu“. I dok je od 2012. godine u Europskoj uniji zabranjeno koristiti tehnologiju prepoznavanja lica, izvan Unije *Facebook* koristi tehnologiju prepoznavanja lica za značajku označavanja imena koja automatski može predložiti imena ljudi na korisnikovim fotografijama. Nadalje, aplikacija prikuplja i sadržaj, komunikaciju i druge podatke koje korisnik unosi prilikom upotrebe platforme. To uključuje:

- registraciju za korisnički račun
- kreiranje i dijeljenje sadržaja
- komunikaciju s drugim korisnicima
- informacije o sadržaju koji se objavljuje
- lokacija fotografije
- datum izrade dokumenta

Facebook koristi brojne softverske alate za praćenje korisnika. Primjerice, kada se korisnici interneta odvaže na druge *web* stranice, njihovi podaci se i dalje mogu nadgledati pomoću softvera. Praćenje aktivnosti odvija se klikom na gumb „Sviđa mi se“ i „Dijeli“, ali i pomoću *Facebook*

Pixela. To je nevidljivi kod koji pada na druge *web* stranice što omogućuje tu *web* lokaciju, a ujedno služi i za praćenje aktivnosti korisnika. *Facebook* također prikuplja podatke poput:

- IP adrese
- preglednik kojeg korisnik upotrebljava
- reklamni oglas kojeg je korisnik posjetio
- učestalost posjeta *web* lokaciji.

Neki regulatori u Europi tvrde da *Facebook* nije dobio izričit i informiran pristanak korisnika da ih prati na drugim *web* lokacijama i aplikacijama, čime se stvara sve veća nelagoda kao posljedica nepravednog manipuliranja korisnika od strane tehnoloških divova, odnosno, većina njihovih korisnika ne zna koliko *Facebook* može prikupiti podataka i koje bi ih tvrtke mogle koristiti, [23].

Pomoću virtualne privatne mreže (VPN, eng. *Virtual Private Network*) postoji mogućnost ograničavanja količine podataka koje *Facebook* može prikupiti o korisnicima. VPN funkcionira spajanjem na drugi poslužitelj na drugom mjestu, što će promijeniti IP adresu korisnika i zadržava kodiranje podataka. Na taj način *Facebook* neće moći pratiti podatke korisnika, iako *Facebook* i dalje vidi novu IP adresu, svi podaci su šifrirani, što korisnike čini zaštićenijima, [24].

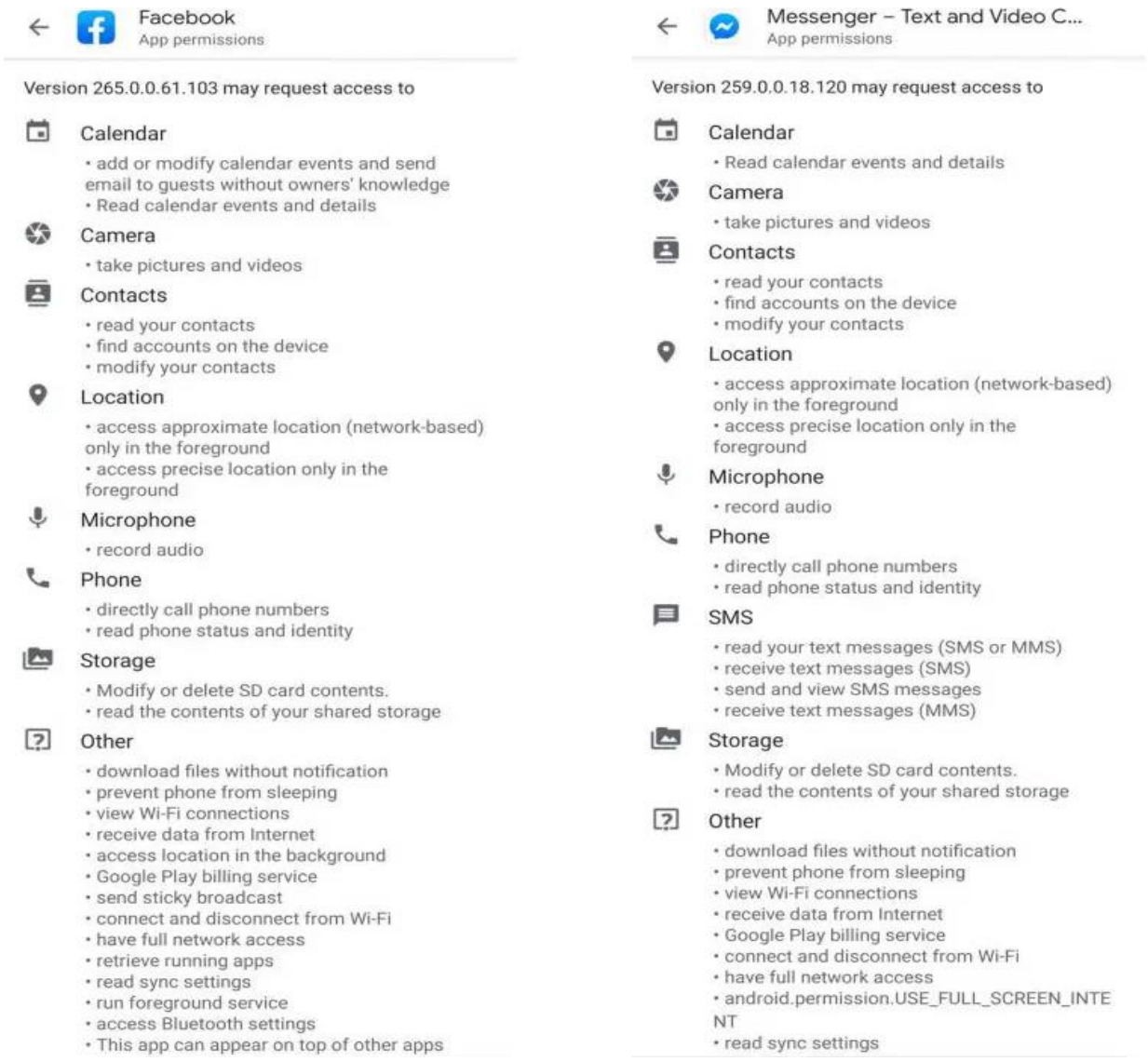
3.3.3. Facebook Messenger

Facebook Messenger je platforma koja služi za razmjenu poruka, ali ujedno i prikuplja veliku količinu podataka od korisnika za razliku od drugih aplikacija koje pružaju slične usluge. S obzirom na to da je *Facebook Messenger* pod vlasništvom tvrtke *Facebook*, oni također imaju uvid u podatke koje prikupljaju i mogu ih koristiti. Kako *Facebook* većinu prihoda ostvaruje preko reklama te da bi to učinili učinkovito, koriste i podatke prikupljene od strane *Facebook Messenger* korisnika.

Poruke koje se šalju putem aplikacije *Facebook Messengera* nisu šifrirane *end-to-end* enkripcijom kao na primjer kod *WhatsAppa*. *End-to-end* enkripcija znači ako se s mobilnog uređaja pošalje poruka, a poruka je šifrirana, ona se šalje kao gomila zbrkanih slova i brojeva prije nego što dođe do primatelja. Na taj način, uključujući hakere, nitko neće moći znati kako poruka glasi i što poručuje. Budući da aplikacija *Facebook Messenger* prema zadanim postavkama ne šifrira poruke korisnika, *Facebook* može vidjeti sve slike i poruke koje se šalju. I dok je od 2016. godine

Facebook najavio novu značajku koja nudi šifrirane, tajne i samouništavajuće *Messenger chatove*, mnogi korisnici danas ni ne znaju da ta značajka postoji, [25].

Na slici 3 se vidi samo dio podatka koje prikupljaju *Facebook* i *Facebook Messenger*. Nadalje su navedeni ostali podaci koje prikuplja *Facebook Messenger*: ime i prezime, broj telefona, *e-mail* adresa, korisnički ID, ID uređaja, povijest pretraživanja, lokacija, informacije o kontaktima ostalih korisnika, fotografije ili videozapisi, audio podaci, financijske informacije i mnoge druge, [26].



Slika 3. Dio podataka koje prikupljaju *Facebook* i *Facebook Messenger*

Izvor: https://crambler.com/truth-about-facebook-messenger-app-privacy/

3.3.4. WhatsApp

WhatsApp ima više od 2 milijarde korisnika širom svijeta i to je čini jednom od najpopularnijih aplikacija za komunikaciju putem poruka. Stvorena je s idejom pružanja privatne i sigurne platforme za razmjenu poruka. Od 2014. godine aplikacija se nalazi pod vlasništvom tvrtke *Facebook,* no *WhatsApp* je naznačio da će i dalje raditi kao neovisna tvrtka i poštivati sve obaveze u pogledu sigurnosti i privatnosti. Iako tvrtka *Facebook* prikuplja podatke korisnika pomoću oglasa i drugih načina kako bi korisnicima pružili što zanimljiviji sadržaj, *WhatsApp* je aplikacija koja nema oglase s obzirom na to da je to platforma koja služi za osobnu komunikaciju.

Poruke koje se razmjenjuju putem ove aplikacije su zaštićene enkripcijom. Poruke su šifrirane i nitko drugi osim pošiljatelja ili primatelja nije u mogućnosti vidjeti ili pročitati sadržaj poruka, fotografija, videozapisa, glasovnih poruka ili privitaka. Kako bi mogao pružati uslugu *WhatsApp* mora prikupiti neke osnovne informacije. Dakle, *WhatsApp* sprema telefonski broj korisnika jer se on koristi za prijavu na uslugu i omogućuje povezivanje s drugim korisnicima. Također, prikupljaju se podaci o:

- davatelju mobilne usluge
- vrsta mobilnog uređaja
- operativni sustav
- brzina veze i jačina signala
- podaci o oglašavanju
- povijest kupovine
- interakcija proizvoda
- podaci o izvedbi
- podaci o plaćaju
- dijagnostički podaci
- lokacija korisnika kroz obližnje Wi-Fi pristupne točke i *Bluetooth* signale

Budući da je komunikacija s mobilnim tornjevima i internetskim pristupnim točkama neophodna za upotrebu uređaja, gotovo je nemoguće spriječiti *WhatsApp* da prikuplja te podatke. Tvrtka vodi evidenciju o tome koliko vremena korisnik provodi u razgovoru s određenim korisnicima. Sve dok korisnik ima aplikaciju i dopušta joj da pregledava popis kontakata, *WhatsApp* može sadržavati telefonski broj, e-mail i druge podatke za kontakt u svojoj bazi

podataka, iako neki drugi korisnik nikad nije instalirao aplikaciju. *Facebook* uzima podatke o tim kontaktima i uspoređuje ih s kontakt podacima koji se koriste u drugim *Facebook* proizvodima. Na primjer, ako tvrtka otkrije da jedan od *WhatsApp* kontakata još nije na *Instagramu*, možda će početi prikazivati *Instagram* oglase na mreži, [27].

3.3.5. Telegram

Telegram je besplatna aplikacija koja služi za brzu i jednostavnu razmjenu poruka. Kao i ostale platforme za komunikaciju, na *Telegramu* se također mogu slati poruke, fotografije, videozapisi ili datoteke. Poruke, glasovni i video pozivi, kao i glasovni razgovori u grupama su zaštićeni *end-to-end* enkripcijom, što daje dodatnu sigurnost korisniku da bezbrižno komunicira. Za razliku od *WhatsAppa, Telegram* je zasnovan na oblaku s neometanom sinkronizacijom. Kao rezultat toga može se koristiti na svim uređajima i korisnik može pristupiti porukama iz nekoliko uređaja odjednom, uključujući tablete i računala, kao i dijeljenje neograničenog broja fotografija, videa i datoteka. Jedna od zanimljivih značajki *Telegrama* je način rada „tajnog *chata*“ koji je šifriran protokolom MTProto. Poruke koje su poslane u tajnom *chatu* može pristupiti samo uređaj putem kojeg je tekst poslan ili primljen. Tekst poruke se mogu obrisati u bilo kojem trenutku, a po želji se mogu i samouništiti. Tajni *chat* se može pokrenuti samo putem pozivnice, nakon čega korisnici razmjenjuju „ključeve za šifriranje“ i tada komunikacija može započeti. Za razliku od prije navedenih aplikacija, *Telegram* je jedna od rijetkih aplikacija koja prikuplja mali broj podataka korisnika. Podaci koji se prikupljaju su: ime, broj telefona, kontakti i korisnički ID, [28].

3.3.6. Viber

Viber je još jedna aplikacija za razmjenu trenutnih poruka koja podržava *end-to-end* enkripciju, stoga su poruke, videozapisi, fotografije, video i glasovni pozivi zaštićeni. Platformom upravlja japanska tvrtka MNC Rakuten i platforma omogućuje izradu sigurnosnih kopija podataka iz aplikacije. Kao i *Telegram, Viber* nudi poruke koje mogu nestajati. Korisnik može postaviti određeno vrijeme i tekst korisnika nestaje. Iako je *Viber* besplatna aplikacija, pojedini oglasi se prikazuju na platformi. Međutim, tvrtka objašnjava kako im oglasi pomažu da aplikacija ostane besplatna za upotrebu te da se nikakvi korisnički podaci ne dijele s pružateljima oglašavanja. Podaci koje aplikacija prikuplja su: ime, korisnički ID, telefonski broj, ID uređaja, lokacija, ID *e-maila* i kontakte, [29].

3.3.7. TikTok

TikTok je aplikacija za dijeljenje videozapisa kratkog oblika koja korisnicima omogućuje stvaranje i dijeljenje videozapisa na bilo koju temu. Aplikacija nudi korisnicima širok izbor zvukova i isječaka pjesama, zajedno s opcijom dodavanja specijalnih efekata i filtera. *TikTok* prikuplja ogromnu količinu podataka o svojim korisnicima, uključujući: koje videozapise gledaju i komentiraju, podaci o lokaciji, model mobilnog uređaja i operativni sustav, IP adresa korisnika, mobilni operater koje korisnik koristi, povijest pregledavanja i pretraživanja, sadržaj poruka koji se razmjenjuju s drugim korisnicima u aplikaciji, dob, telefonski broj i još mnogo toga. Također prikupljaju informacije o prirodi zvuka i tekstu izgovorenih riječi u sadržaju korisnika kako bi se omogućili posebni video efekti za moderiranje sadržaja za demografsku klasifikaciju, sadržaje i preporuke za oglase te za druge radnje koje ne omogućuju osobnu identifikaciju, [30]. Na tablici 1 prikazana je usporedba potrebnih ovlasti pojedinih aplikacija koje prikupljaju podatke.

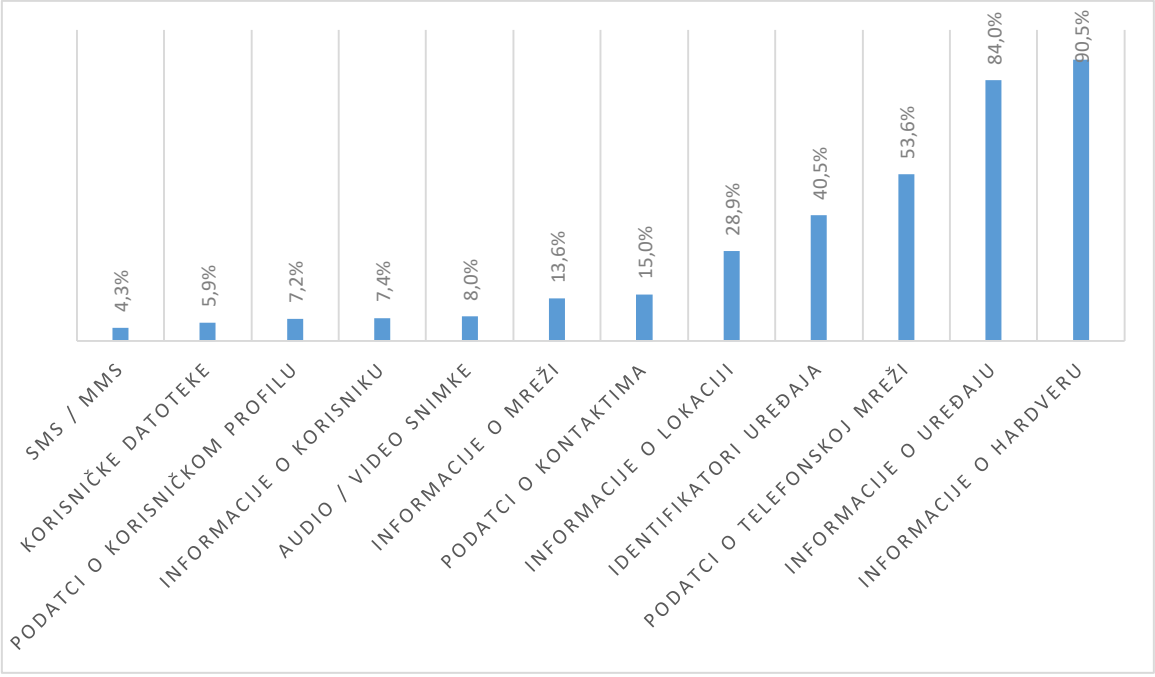
Tablica 1. Uporedba potrebnih ovlasti pojedinih aplikacija za prikupljanje podataka

Aplikacije / Podaci/Ovlasti	Instagram	Facebook	Facebook Messenger	WhatsApp	Telegram	Viber	TikTok
Ime	x	x	x	x	x	x	x
Korisnički ID	x	x	x	x	x	x	x
Telefonski broj	x	x	x	x	x	x	x
ID uređaja	x	x	x	x		x	x
Lokacija	x	x	x	x		x	x
E-mail	x	x	x	x	x	x	x
Kontakti	x	x	x	x		x	
Podaci o oglašavanju	x	x	x				x
Kupnja ili financijske transakcije	x	x	x	x			
Povijest pretraživanja	x	x	x				x
Prepoznavanje lica	x	x					x
Operativni sustav	x	x	x	x			
IP adresa	x	x	x				x
Davatelj mobilne usluge	x	x		x			x
Sadržaj na platformi	x	x	x				x
Svojstva uređaja	x		x				
Podaci iz kolačića	x	x	x				x
Registracija za korisnički račun	x	x					
Komunikacija s drugim korisnicima	x	x	x	x		x	x
Podaci o korisničkom računu	x	x	x				x
Brzina veze i jačina signala	x			x			
Signali Bluetootha i Wi-Fi-a	x			x			

4. PRIVATNOST PODATAKA APLIKACIJA PAMETNIH TELEFONA

Napretkom prethodnih godina tehnologija je dostigla veliku razinu zaštite podataka, ali i dalje postoji rizici napada, stoga možemo kazati da mobilnim aplikacijama privatnost je strogi neprijatelj. Prosječno provedeno vrijeme na mobilnim aplikacijama dok koristimo mobilni uređaj iznosi oko 90%, zbog čega postaje izravan izvor napada na privatnost samog korisnika. Mobilne aplikacije stoga mogu biti zlonamjerno izrađene u svrhu nelegitimne zarade. Postoje slučajevi s nekoliko aplikacija koje su povezane na službenoj trgovini aplikacija, ali pretežito većinski udio takvih zlonamjernih aplikacija nalazi se u *third party stores*. Takve aplikacije nastoje propuštati podatke te ostvaruju manipulaciju nad korisnikom te ih izlaže napadima, zato u svim slučajevima imaju moć nanijeti veliku štetu korisniku i samoj organizaciji koja provodi pravila o korisničkoj privatnosti.

Zlonamjerne aplikacije su danas najmanje raširena prijetnja mobilnim uređajima i utječe samo 5% na Android aplikacija i 2% iOS aplikacija. Suprotno tome, neautorizirani prijenos podataka je daleko najizraženiji oblik svega 67% u Android i 61% u iOS aplikacijama. Neautorizirani prijenos podataka prikazan je na grafikonu 12.



Grafikon 12. Neautorizirani prijenos podataka

Izvor: [31]

Prvom instalacijom aplikacije na pametne telefone ili tablete, aplikacija traži dozvolu za pristupom raznim izvorima podataka s korisničkog uređaja poput lokacije, audio i video snimke, zapisniku poziva, SMS-a itd. Najčešći slučaj je da korisnik daje dozvolu bez da obrati pažnju. Rezultirajući time puno aplikacija može dostići manipulaciju nad korisnikom tako da zapravo prikupljaju podatke u jedinstvenu svrhu preprodaje nekim drugim privatnim tvrtkama. Besplatne aplikacije implementiraju u prosjeku šest marketinških knjižnica koje pretvaraju u oglasni prostor putem kojega prikupljaju korisničke podatke. To predstavlja najveći izazov softverskih tvrtki kako bi spriječili širenje podataka putem mobilnih aplikacija, [31].

4.1. Pravila o zaštiti privatnosti (*Privacy policy*)

Pravila o zaštiti privatnosti je pravni dokument koji navodi kako tvrtka ili *web* mjesto prikuplja i obrađuje podatke svojih kupaca i posjetitelja. Izričito se opisuje drže li se ti podaci povjerljivima ili se dijele ili prodaju trećim stranama. Osobni podaci o pojedincu mogu uključivati sljedeće: ime, adresa, *e-mail*, dob, spol, broj telefona, bračni status, nacionalnost, vjerska uvjerenja i mnoge druge informacije koje aplikacija može prikupljati. Dakle, Politika privatnosti je dokument koji korisnicima daje do znanja o tome kako su korisnici osigurani prilikom korištenja neke aplikacije i poštuje li se njihova privatnost.

Širom svijeta razvijeni su zakoni i propisi za zaštitu podataka koji se odnose na vladu, obrazovanje, djecu, potrošače, financijske institucije itd. Ti podaci su kritični za osobu kojoj pripadaju. Od brojeva kreditnih kartica i brojeva socijalnog osiguranja do adrese *e-maila* i telefonskih brojeva, važni su osjetljivi podaci korisnika koji otkrivaju identitet. Takve informacije u nepouzdanim rukama mogu potencijalno imati dalekosežne posljedice. Ugovori o zaštiti privatnosti informiraju korisnike koje se informacije od njih prikupljaju. To uključuje podatke koje korisnici dobrovoljno i aktivno pružaju prilikom registracije za korištenje usluga, kao i podatke koji se od njih mogu automatski prikupiti, npr. upotrebom kolačića.

Tvrtke ili aplikacije koje obrađuju podatke o korisnicima, dužni su objaviti svoja pravila privatnosti na *web* mjestima ili omogućiti pristup cjelovitom ugovoru o zaštiti privatnosti unutar aplikacije. Većina zemalja je već donijela zakone kako bi zaštitila sigurnost podataka i privatnost svojih korisnika. Ti zakoni zahtijevaju od tvrtki da dobiju izričit pristanak korisnika čiji će se podaci pohranjivati ili obrađivati. Neki od tih zakona su: GDPR (eng. *General Data Protection Regulation*) u EU, CalOPPA u SAD-u i PIPEDA u Kanadi. Ako aplikacija dosegne korisnike širom

svijeta, bez obzira na to gdje se tvrtka nalazi ili ima sjedište, moraju se poštovati zakoni o privatnosti u svim zemljama gdje se nalaze njihovi korisnici. Iako se zakoni o zaštiti podataka i privatnosti razlikuju od regije do regije, Politika privatnosti mora sveobuhvatno informirati svoje korisnike o tome kako će se njihovi podaci koristiti. Primjerice, GDPR je trenutno najsnažnije zakonodavstvo o privatnosti na svijetu i jedan od njihovih glavnih zahtjeva za bilo koju tvrtku koja spada pod njihovu nadležnost je imati pravila o privatnosti u skladu s GDPR-om koja sadrže neke vrlo specifične podatke i napisana su na jednostavan i razumljiv način.

Usluge trećih strana također zahtijevaju pravila o privatnosti. Neki pružatelji usluga poput *Applea, Googlea* i *Amazona* zahtijevaju da vlasnici aplikacija objave ugovor o privatnosti ako koriste bilo koju od njihovih usluga. Mnoge aplikacije koriste oglašavanje na stranici ili u aplikaciji za stvaranje prihoda od trećih strana. Budući da ovi oglasi također prikupljaju korisničke podatke, treće strane zahtijevaju da aplikacije zatraže dopuštenja svojih korisnika za dijeljenje njihovih osobnih podataka. Smjernice o pravilima privatnosti zahtijevaju da se korisnike obavijesti o tome koji podaci se prikupljaju, zašto se prikupljaju i što se s njima radi. Također zahtijeva se da vlasnici aplikacija obavijeste svoje korisnike koriste li značajke oglašavanja, kolačiće ili usluge praćenja na svojim aplikacijama kako bi pružili bolja korisnička iskustva temeljena na prethodnim ponašanjima korisnika prilikom pregledavanja, [32].

4.2. GDPR

Opća uredba o zaštiti podataka zakonodavstvo je Europske unije čiji je cilj stanovnicima EU pružiti veću kontrolu nad njihovim podacima. GDPR je postao potpuno provediv 25. svibnja 2018. godine. Prema ovoj uredbi, organizacije koje obrađuju podatke stanovnika EU moraju se pridržavati pravila o podacima i privatnosti. Jedan od ključnih zahtjeva i promjena je ažuriranje Pravila o privatnosti kako bi se održavali zahtjevi GDPR-a.

Glavni ciljevi i zahtjevi GDPR-a je informiranje građana EU o tome kako tvrtke prikupljaju, koriste, dijele, osiguravaju i obrađuju svoje osobne podatke. Korisnici moraju biti obaviješteni o tome zašto se obrađuju njihovi podaci i koliko dugo ih vlasnici aplikacije čuvaju. Dakle, većina Pravila o privatnosti sadrže sljedeće: koji osobni podaci se skupljaju, kako se prikupljaju, za što se koriste, sigurnost prikupljenih podataka, podjela podataka s trećim stranama te kakve kontrole korisnici imaju nad bilo čime od navedenog.

Osobni podaci u kontekstu GDPR-a odnose se na sve podatke koji se odnose na identificiranu ili utvrdivu živuću osobu. To uključuje dijelove podataka koji kada se prikupe zajedno mogu dovesti do identifikacije osobe. To se odnosi čak i na podatke koji su pseudonimizirani ili šifrirani sve dok je šifriranje/anonimizacija reverzibilna. Što se tiče ispunjavanja obveza zaštite podataka prema uredbi, to znači da će ključeve za dešifriranje trebati čuvati odvojeno od pseudonimiziranih podataka.

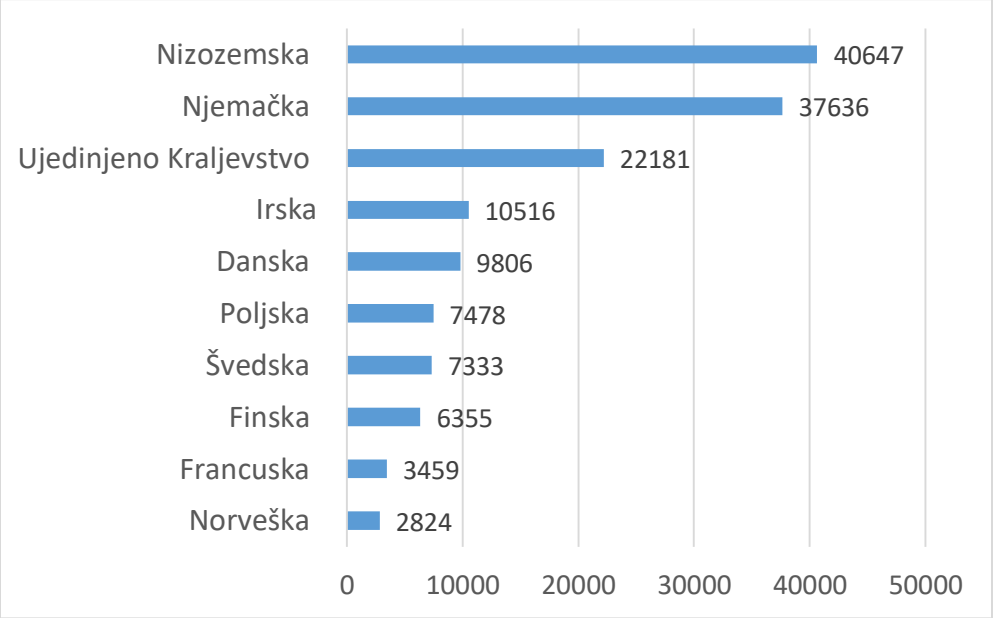
Ovaj opseg učinkovito pokriva gotovo sve tvrtke i prema tome GDPR se može primijeniti bez obzira ima li organizacija sjedište u EU ili ne. Uobičajena zabluda je da su samo korisnici iz EU obuhvaćeni zaštitom GDPR-a, međutim proteže se i na korisnike izvan EU ako je kontrolor podataka sa sjedištem u EU. Dakle, kontrolor podataka sa sjedištem u EU mora prema zadanim postavkama primijeniti GDPR standarde na sve korisnike.

Općenito, prilikom dobivanja pristanka za obradu podataka, organizacije ne smiju koristiti pretjerano složene ili neodgonetljive izraze. To uključuje nerazumljiv sadržaj i nepotreban žargon. Dakle, Uvjeti i Pravila o zaštiti privatnosti trebaju biti postavljeni čitko, koristeći razumljiv jezik i klauzule tako da korisnici budu potpuno svjesni na što pristaju i koje su posljedice njihovog pristanka.

Prema GDPR-u korisnici imaju pravo prigovarati određenim aktivnostima obrade u vezi s njihovim osobnim podacima koje provode vlasnici aplikacije. Korisnik se može usprotiviti obradi svojih podataka kad god se obrada temelji na legitimnom interesu upravljača ili izvršavanju zadatka u javnom interesu, izvršavanju službene vlasti ili us vrhu znanstvenog ili povijesnog istraživanja i statistika. Ako se primi prigovor na obradu osobnih podataka i nema osnova za odbijanje, aktivnost obrade mora prestati. Iako se aktivnost obrade, uključujući pohranu, mora zaustaviti za određene aktivnosti obrade kojima se prigovara, brisanje možda neće biti prikladno ako se podaci obrađuju u druge svrhe, uključujući ispunjenje zakonske ili ugovorne obveze. U većini slučajeva organizacije moraju uvažiti prigovor bez naplate naknade, međutim ako se utvrdi da je zahtjev neutralan ili pretjeran, može se zatražiti naknada da bi se zahtjev odbio. Ako se zahtjev odbije, korisnik mora biti obaviješten zajedno s obrazloženjem nez nepotrebnog odgađanja i to u roku od mjesec dana od primitka zahtjeva.

Kada podaci više nisu relevantni za svoju izvornu svrhu, ako su korisnici povukli pristanak ili ako su osobni podaci nezakonito obrađeni, korisnici imaju pravo zatražiti brisanje njihovih

podataka i prestanak širenja. Pravo na brisanje podataka može se odbiti: ako se osobni podaci obrađuju za potrebe arhiviranja u javnom interesu, ako su podaci potrebni za pravnu obranu, poštivanje zakonske obveze i u izvršavanju službenih ovlasti dodijeljenih kontroloru, [33]. Na grafikonu 13 nalaze se države u kojima se najviše događa nepoštivanje GDPR zakona.



Grafikon 13. Države koje krše GDPR zakon

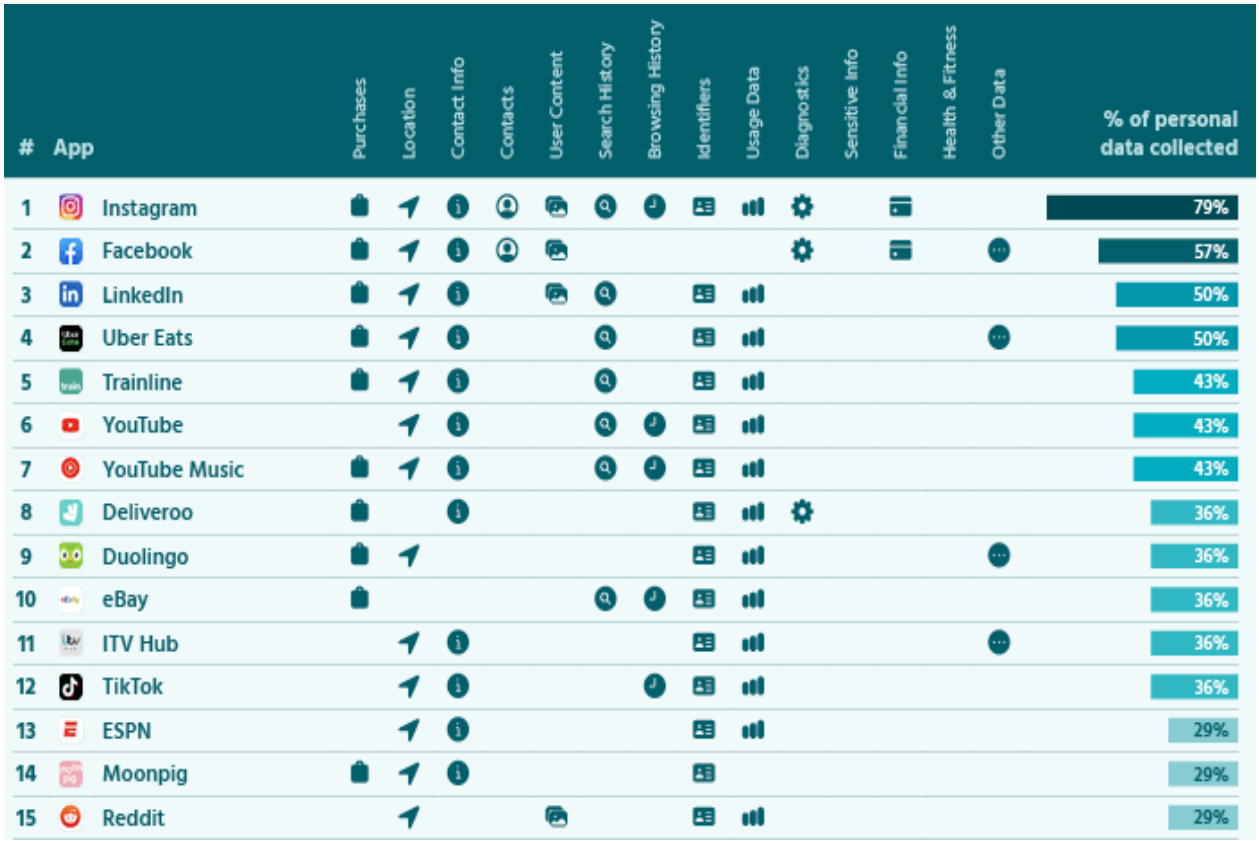
Izvor: https://www.statista.com/chart/20566/personal-data-breaches-notified-per-eea-jurisdiction/

4.3. Potencijalno opasne aplikacije

Globalni internetski divovi oslanjaju se na činjenicu da korisnici vrlo rijetko ili nikad ne čitaju njihove Uvjete korištenja koje prihvaćaju prilikom same instalacije aplikacije, a pritom njihova Pravila o privatnosti nisu u skladu s onim što je napisano u Uvjetima korištenja. Aplikacije mogu prikupljati i dijeliti bilo što od osobnih podataka korisnika i korisničkog sadržaja, pretraživati i pregledavati povijest i analizirati kao profil za sebe i druge aplikacije. Gotovo 80% aplikacija koristi podatke korisnika za plasiranje vlastitih proizvoda u aplikaciji i šire. To uključuje stvari poput aplikacija koje poslužuju vlastite oglase na drugim platformama, kao i promocije u aplikacijama u vlastitu korist ili za treće strane koje plaćaju uslugu.

Prema podacima iz 2021. godine, *Instagram* dijeli 79% podataka, dok Facebook dijeli 57% podataka korisnika s drugim tvrtkama. Dijele se gotovi svi podaci od kupnje podataka, osobnih podataka i povijesti pregledavanja te još mnogo drugih. *Facebook* i *Instagram* dijele infrastrukturu,

sustave i tehnologije s drugim *Facebook* tvrtkama kako bi pružili inovativno, relevantno, dosljedno i sigurno iskustvo korisnicima u svim proizvodima tvrtke *Facebook*. Na primjer, obrađuju se podaci iz *WhatsAppa* o računima koji šalju neželjenu poštu na toj platformi te se poduzimaju odgovarajuće mjere protiv tih računa na *Facebooku*, *Instagramu* ili *Facebook Messengeru*. *Facebook Messenger* štiti sadržaj poruka kada korisnici koriste tajni *chat*, što znači da sadržaj poruke čitaju samo primatelj i pošiljatelj, no ujedno *Facebook* čita sadržaj *Messenger* poruka, uključujući metapodatke, fotografije koje se dijele, lokacija, pa čak i živu sliku s kamera pametnih telefona korisnika. Na slici 4 nalaze se aplikacije koje dijele podatke sa trećim stranama.



Slika 4. Aplikacije koje dijele podatke s trećim stranama

Izvor: https://www.pcloud.com/invasive-apps

Iako su *WhatsApp* poruke zaštićene potpunom enkripcijom te tvrtka *WhatsApp* tvrdi da sadržaj poruka njihovih korisnika nitko ne može čitati, no ako se detaljnije prouče postavke *WhatsAppa*, vidi se da *Facebook* ipak čita sadržaj poruka. Dakle, *WhatsApp* poruke se neće dijeliti na *Facebooku* kako bi ih drugi korisnici mogli vidjeti, nego koriste sadržaj poruka za pomoć u radu i

pružanju usluga. Drugim riječima, privatnost korisnika na *WhatsAppu* je zaštićena tako da nikome ne dijeli sadržaj poruka osim *Facebooku*.

Korištenjem *Viber* usluga korisnici dopuštaju da se prikupljaju, koriste, otkrivaju i zadržavaju osobni podaci ili neki drugi podaci. Iako u Pravilima privatnosti piše da se sadržaj koji se dijeli privatno ne čita i ne sluša, u Uvjetima i odredbama aplikacija piše malo drugačije. Da bi zaštitili svoje korisnike i da njihovo korištenje aplikacije bude pozitivno, vlasnici pridržavaju pravo u svakom trenutku ukloniti ili odbiti distribuciju bilo kojeg sadržaja na usluzi, stoga imaju mogućnost suspendirati ili ukinuti korisnike i blokirati sudionike *Viber* javnih *chatova*. Dakle, sadržaj korisnika se ipak skenira i čita kako bi otkrili moguća kršenja moralnih pravila na *Viberu* i kako bi blokirali distribuciju neprikladnog sadržaja, [34].

U najnovijim Uvjetima i odredbama aplikacije uvodi se da platforma *TikTok* može prikupljati biometrijske podatke poput otiska lica i glasovnih otisaka iz sadržaja kojeg korisnici objavljuju na platformi. Za sada, takvo prikupljanje podataka nalazi se samo u SAD-u. S obzirom na to da samo nekolicina država u SAD-u ima biometrijske zakone o privatnosti, pa se smatra da je *TikTok* tražio pristanak samo „tamo gdje to nalaže zakon“, [35].

4.4. Kršenje podataka (*Data Breach*)

Kršenje podataka uključuje incident u kojem se kradu ili preuzimaju informacije od korisnika iz sustava bez znanja ili odobrenja vlasnika sustava. Ukradeni podaci mogu uključivati osjetljive, vlasničke ili povjerljive podatke kao što su brojevi kreditnih kartica, podaci o klijentima, poslovne tajne ili pitanja nacionalne sigurnosti.

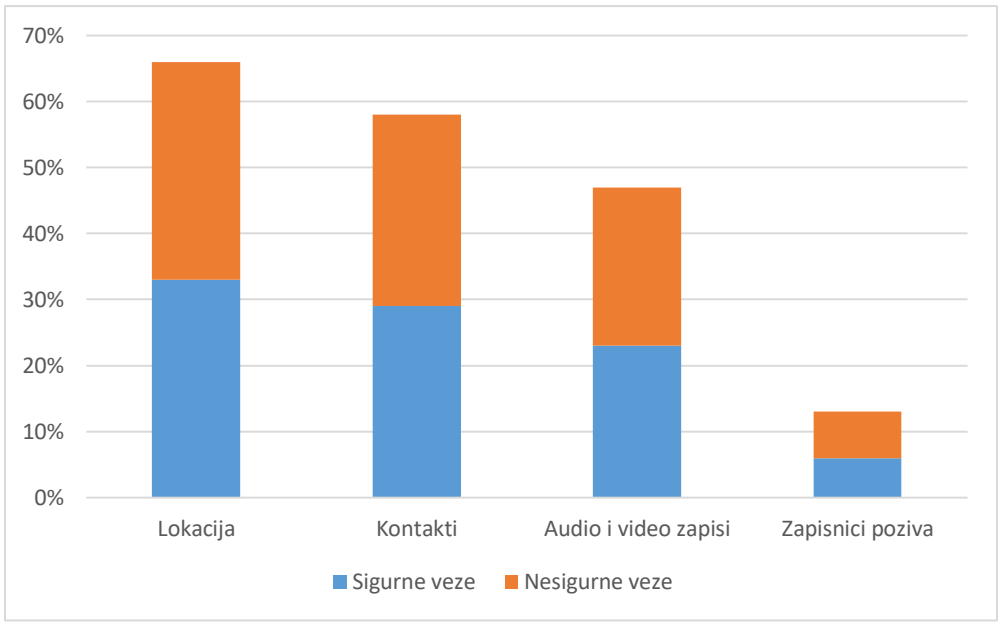
Aplikacije prikupljaju veliku količinu podataka te se obično nalaze na meti hakera. 2019. godine otkriveno je da su hakeri prikupili od *Facebooka* ogromnu bazu podataka te je javno objavili na *webu*. Podaci koji su prikupljeni uključuju: imena i prezimena korisnika, *Facebook* ID, e-mail adrese, brojevi mobitela, lokacija i još mnogi drugi podaci koji bi se mogli iskoristiti za napredno hakiranje putem socijalnog inženjeringa, prevare, ali i u razne marketinške tvrtke. Dvije godine kasnije, 2021. godine, ponovno su hakirani sustavi *Facebooka* i podaci su objavljeni na *webu*. Objavljeno je i koliko je korisničkih računa s *Facebooka* kompromitirano u kojoj zemlji svijeta te za Hrvatsku taj broj iznosi 659.115 korisnika, [36].

S obzirom na to da *WhatsApp* nudi potpunu enkripciju poslanog sadržaja hakeri vrlo često pokušavaju pronaći druge načine kako bi pristupili sadržaju korisnika. *WhatsApp* je u svojoj VOIP (eng. *Voice over Internet Protocol*) funkciji sadržavao ranjivost koja je napadačima omogućavala ubacivanje zlonamjernog softvera tako da se pozove korisnika na njegov mobilni uređaj. Greška je otkrivena u jednom od napada gdje je instaliran zlonamjerni softver na mobilne uređaje britanskih odvjetnika. Nakon toga, 2014 godine, *Facebook* je kupio *WhatsApp*, koji je radio na otklanjanju greške pa se sa sadašnjom razinom zaštite slične situacije ne bi trebale događati u budućnosti, [37].

4.5. Prikupljanje podataka (*Data Collection*)

Google poslužitelj prikuplja oko 20 puta više telemetrijskih podataka s *Android* uređaja nego *Apple* iOS-a. Isto tako oba operativna sustava dijele podatke sa svojim središnjim poslužiteljima kada korisnici pregledavaju zaslone njihovih postavki. Kada se mobilni uređaj ne koristi, postupak prikupljanja podataka je gotovo svake četiri i pol minute. Nadalje, kada se nova SIM kartica umetne u iOS i *Android* uređaje, detalji o SIM-u se automatski dijele s *Appleom* i *Googleom*. Telemetrija se može koristiti za povezivanje fizičkih uređaja s osobnim podacima i podacima koje obje tvrtke koriste u reklamne svrhe. Također, taj postupak prikupljanja telemetrije omogućuje proizvođačima OS-a da prate lokaciju korisnika na temelju IP adrese koja povezuje i prenosi telemetriju uređaja na njihove poslužitelje. Smatra se da postoji vrlo mala mogućnost da korisnici spriječe prikupljanje telemetrije sa svojih uređaja, [38].

Društvene mreže, osim za komunikaciju koriste se i za kupnju i prodaju proizvoda te oko 82 % internetskih korisnika kupuje putem interneta preko svojih mobilnih uređaja. Programi za kupnju obrađuju podatke o kreditnim karticama korisnika, ali ujedno i prikupljaju osobne podatke poput popisa kontakata, audio i video zapisa i zapisnika poziva. Grafikon 14 prikazuje da aplikacije za kupnju prikupljaju i šalju podatke o lokaciji korisnika mreže (58%), audio i video zapisima (47%) i zapisnicima poziva (13%). Osim toga, prikazana je raspodjela osobnih podataka poslanih putem sigurnih veza, HTTPS (eng. *HyperText Transfer Protocol Secure*) s pouzdanim certifikatom ili nesigurnih veza, HTTP (eng. *HyperText Transfer Protocol*) ili nepouzdani certifikat, [39].



Grafikon 14. Podaci koji se prenose putem internetske mreže
Izvor: https://blog.pradeo.com/google-play-most-downloaded-shopping-apps-process-users-data

5. MOGUĆNOSTI ZAŠTITE PODATAKA PRIKUPLJENIH APLIKACIJAMA

Gotovo sve aplikacije prikupljaju veliku količinu podataka te kako ti podaci ne bi dospjeli do malicioznih korisnika potrebno je zaštititi sustav, a ujedno i korisnike. Osim što postoje razne zakonske regulative na razini države kojih se trebaju držati proizvođači aplikacija i terminalnih uređaja, isto tako proizvođači terminalnih uređaja pokušavaju zaštititi svoje sustave raznim nadogradnjama i ažuriranjima. Većina terminalnih uređaja imaju već ugrađen sigurnosni sustav koji štiti uređaj te daje dodatnu sigurnost korisnicima. Također, trgovine aplikacija provode razne sigurnosne mjere prije nego što aplikacija dođe na tržište, ali i korisnici trebaju obratiti pozornost na aplikacije koje instaliraju. Na slici 5 se nalaze aplikacije koje prikupljaju najmanje podataka.

Slika 5. Aplikacije koje prikupljaju najmanje podataka

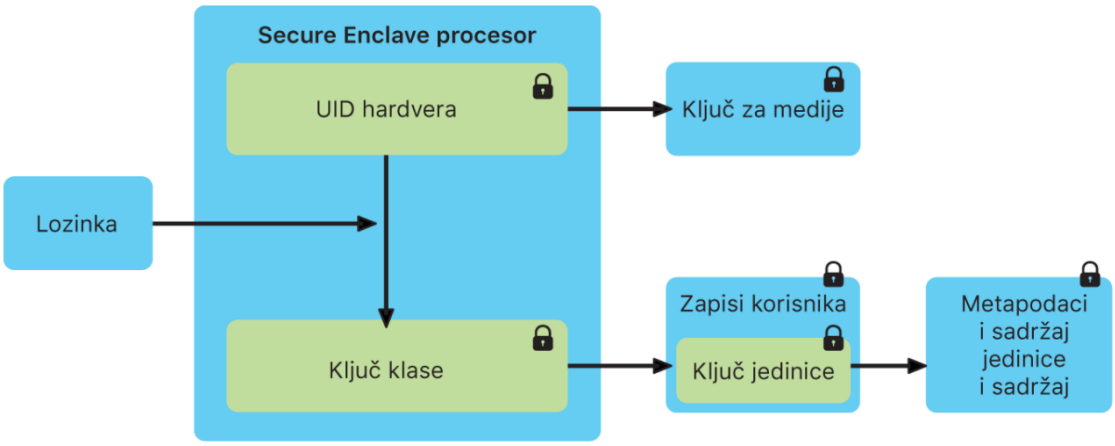
Izvor: https://www.pcloud.com/invasive-apps

5.1. Na razini operativnog sustava

5.1.1. Apple iOS

Sigurnosne značajke koje su ugrađene u sustav pomažu spriječiti da netko drugi pokuša pristupiti podacima na *iPhoneu* ili *iCloudu* korisnika. Te značajke smanjuju mogućnost dijeljenja podataka te korisnik može podesiti koje informacije se dijele i kada.

Secure Enclave je hardverska značajka koja pohranjuje kriptografske ključeve na izoliranom mjestu kako bi se spriječilo da ti ključevi budu ugroženi. Nasumični generator brojeva dio je *Secure Enclave* sustava na čipu (SoC, eng. *System on a Chip*) i putem njega se kriptiraju ključni podaci. Ukoliko je jezgra uređaja ugrožena također se održava integritet kriptografskih postupaka. Komunikacije između procesora aplikacije i modula *Secure Enclave* odvija se tako što se izolira podatak u sandučić koji zatim pokreće prekid i pokreću se međuspremnici dijeljenih memorijskih podataka, [14]. Na slici 6 prikazan je *Secure Enclave* procesor.



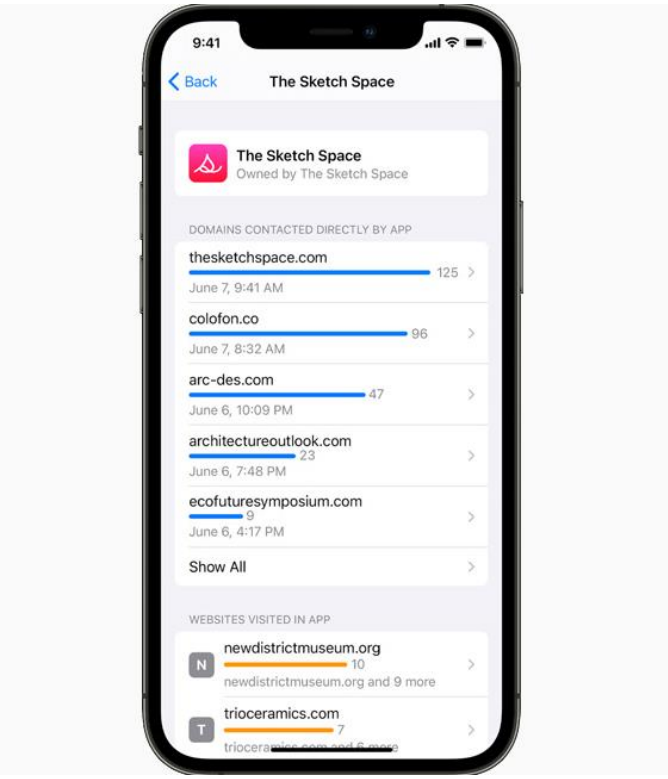
Slika 6. *Secure Enclave* procesor

Izvor: https://support.apple.com/hr-hr/guide/security/sec59b0b31ff/web

2017. godine tvrtka *Apple* je prvi put predstavila značajke protiv praćenja korisnika, no 2021. godine najnovija verzija mobilnog softvera, iOS 14, natjerala je programere aplikacija da budu transparentniji u pogledu podataka koje prate i što rade s tim podacima. Aplikacije traže dopuštenja korisnika da prate njihove aktivnosti na drugim *web* stranicama te korisnici ponekad mogu odbiti zatražena dopuštenja.

Druga značajka iOS 15 bi spriječila marketinške stručnjake da prate podatke, na primjer, otvara li primatelj marketinšku e-poštu ili pristupa njihovoj IP adresi korištenjem skrivene grafike koju učitava klijent e-pošte, što omogućuje pošiljateljima prikupljanje podataka o aktivnostima korisnika. U aplikaciji *Mail*, zaštita privatnosti e-pošte sprječava pošiljatelje da koriste nevidljive piksele za prikupljanje podataka o korisniku. Nova značajka pomaže korisnicima spriječiti pošiljatelje da znaju kada otvaraju e-poštu te prekriva IP adresu korisnika tako da se ne može povezati s drugim mrežnim aktivnostima ili koristiti za određivanje lokacije korisnika.

Pomoću Izvješća o privatnosti aplikacije korisnici mogu vidjeti koliko je često svaka aplikacija koristila dozvolu koju je prethodno dala za pristup svojoj lokaciji, fotografijama, kameri, mikrofonu i kontaktima u posljednjih sedam dana. Korisnici također mogu saznati s kime se njihovi podaci mogu podijeliti ako vide sve domene trećih strana s kojima aplikacija kontaktira, kao što je prikazano na slici 7.



Slika 7. *Secure Enclave* procesor

Izvor: https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/

Tvrtka *Apple* želi ukazati na razlike između svojih proizvoda i usluga i proizvoda svojih konkurenata. *Apple* se, na primjer, ne oslanja na prihod od oglasa kao izvor prihoda, već svojim korisnicima naplaćuje usluge. Jedna od tih usluga je *iCloud*. Pretplatnici usluge *iCloud* moći će koristiti *iCloud+* bez dodatnih troškova. To uključuje *Private Relay* koji šifrira podatkovni promet tako da ga ne mogu vidjeti treće strane, uključujući *Apple*. No neke od novih značajki privatnosti koje *Apple* proširuje svojim korisnicima neće biti dostupne svugdje, na primjer *iCloud+ Private Relax* neće biti dostupan u brojnim zemljama.

Korisnici mogu podijeliti svoju trenutnu lokaciju s aplikacijom samo jednom, bez davanja razvojnom programeru daljnji pristup nakon te sesije. Programeri mogu prilagoditi gumb za dijeljenje trenutne lokacije i integrirati ga izravno u svoje aplikacije. S obzirom na to da korisnici ponekad kopiraju osjetljive podatke, poput lozinki, *Apple* je izbacio novu funkciju „Sigurnog lijepljenja“ koja se može ugraditi u aplikaciju. Nakon omogućavanja sigurnog lijepljenja, programeri aplikacija neće moći u potpunosti vidjeti sadržaj međuspremnika, osim ako korisnik ne odluči kopirati neki sadržaj iz druge aplikacije i zalijepiti je u aplikaciju koja se trenutno koristi. U tom procesu programeri ne mogu izravno doći do kopiranog sadržaja sve dok korisnik ne dopusti da se zalijepi u trenutnu aplikaciju, [40].

5.1.2. Android OS

Jezgra *Linux* pruža *Androidu* niz sigurnosnih mjera. omogućuje operacijskom sustavu model dopuštenja na temelju korisnika, izolaciju procesa, siguran mehanizam za IPC i mogućnost uklanjanja svih nepotrebnih ili potencijalno nesigurnih dijelova jezgre. Nadalje radi na sprječavanju više korisnika sustava u međusobnom pristupu resursima i njihovom iscrpljivanju. Svakoj aplikaciji za *Android* dodjeljuje se jedinstveni korisnički ID, a svaka se izvodi kao zaseban proces. Stoga se svaka aplikacija provodi na razini procesa putem jezgre *Linuxa*, što aplikacijama ne dopušta međusobnu interakciju i daje im samo ograničen pristup operacijskom sustavu *Android*. Na taj način korisnik dobiva kontrolu pristupa temeljenu na dopuštenjima te dobiva popis aktivnosti koje će *Android* aplikacija izvesti i što će od njih zahtijevati prije nego što se aplikacija uopće preuzme.

Android nudi skladište ključeva podržano hardverom koje omogućuje generiranje ključeva, uvoz i izvoz asimetričnih ključeva, uvoz neobrađenih simetričnih ključeva, asimetrično šifriranje i

dešifriranje s odgovarajućim načinima dodavanja i još mnogo toga. Nakon što je uređaj šifriran, svi podaci koje je stvorio korisnik automatski se šifriraju prije nego što se pošalju na disk. Šifriranje osigurava da čak i ako neovlaštena strana pokuša pristupiti podacima, neće ih moći pročitati.

Sigurnosne funkcije rade na pouzdanom okruženju izvođenja (TEE, eng. *Trusted Execution Environment*) kako bi se osiguralo da operativni sustav ostane siguran. *Trusty OS* radi na istom procesoru kao i *Android OS*, ali *Trusty* je odvojen od ostatka sustava hardverom i softverom te rade paralelno jedno s drugim. *Trusty* ima pristup punoj snazi glavnog procesora i memorije uređaja, ali je potpuno izolirani njegova izolacija ga štiti od zlonamjernih aplikacije koje je instalirao korisnik i potencijalnih ranjivosti koje bi se mogle otkriti na *Androidu*. Kritične sigurnosne funkcije događaju se u TEE-u odvojeno od OS-a. *Verified Boot* upozorava korisnike na kompromise OS-a pri pokretanju te nastoji osigurati da sav izvedeni kod dolazi iz pouzdanog izvora (obično OEM-a (eng. *Original Equipment Manufacturer*) uređaja), a ne od napadača ili korupcije. On uspostavlja cijeli lanac povjerenja, počevši od hardverski zaštićenog korijena povjerenja do pokretačkog programa.

Google također dopušta samo provjerene i sigurne *Android* aplikacije na svoje tržište i na taj način korisnik ima manje šanse instalirati zlonamjernu aplikaciju. Između ostalog, sigurnosni sustav *Androida* traži od korisnika da dopusti instalaciju aplikacije, što znači da je nemoguće daljinski instalirati i pokrenuti aplikaciju, [41].

5.2.Na razini digitalne distribucije

5.2.1. Apple App Store

App Store je platforma koja je razvijena za trgovinu mobilnih aplikacija za operativne sustave iOS i iPadOS. Aplikacije kupljene u *Apple App Storeu* pohranjuje se u *iCloud*, to je *Appleova* usluga pohrane u oblaku i računarskom oblaku za lak pristup s bilo kojeg prijavljenog uređaja.

Prije postavljanja aplikacija na platformu, sve aplikacije se automatski provjeravaju da se vidi radi li se o poznatom zlonamjernom softveru. Svaka aplikacija mora zatražiti dopuštenje korisnika kako bi mogli odabrati koje podatke korisnici žele dijeliti. Prvi put kada aplikacija treće strane želi pristupiti podacima korisnika, poput lokacije, kontakata, kalendara ili fotografija, korisnik automatski prima upozorenje. Čak i ako jednom odobri pristup, kasnije ga može opozvati. Također, osigurava se korisnicima *App Storea* da aplikacijama uskrate pristup određenim osjetljivim podacima na mobilnom uređaju, da ne mogu podešavati mobilni uređaj ili OS te da im je zabranjen

potpuni pristup korisnikovim podacima. Nadalje, zaštite na razini sustava onemogućuju aplikaciji pristup podacima iz drugih aplikacija bez izričitog dopuštenja korisnika. Ljudi koji pregledavaju aplikacije na *App Storeu* moraju se pridržavati strogih standarda pregleda aplikacije. Smjernice za pregled *App Storea* zahtijevaju da aplikacije budu sigurne, da pružaju dobro korisničko iskustvo, da su u skladu s pravilima privatnosti, da zaštite uređaje od zlonamjernog softvera i prijetnji te da koriste odobrene poslovne modele.

Na ovoj platformi svaka aplikacija ima dodijeljenu dobnu kategoriju pa roditelji mogu odrediti što je prikladno za njihovu djecu. Odbacuju se aplikacije s bilo kakvim sadržajem ili ponašanjem koje su iznad postavljenih granica, osobito ako dovode djecu u opasnost. Aplikacije moraju slijediti odobreni poslovni model i jasno prikazati cijenu, objasniti što korisnici dobivaju kupnjom i razjasniti uvjete obnove pretplate. *Apple* šalje potvrdu svaki put kada se koristi značajku kupnje u aplikaciji, a te kupnje i pretplate vide se na računu korisnika.

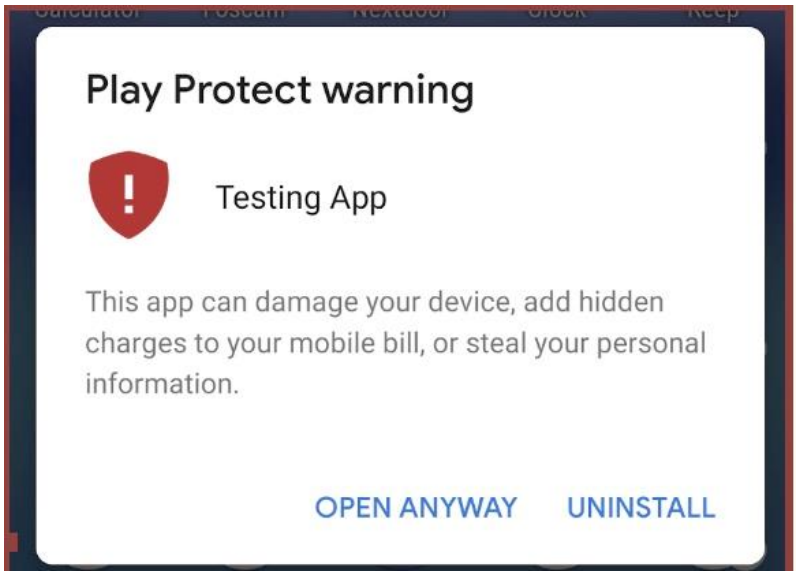
Korisnici mogu izraditi siguran račun sa željenim načinom plaćanja koji je zapisan i lako dostupan na svim uređajima i na *webu*. Račun je zaštićen autentifikacijom u dva faktora, osiguravajući da je korisnik jedina osoba koja može pristupiti svom računu, čak i ako netko drugi zna lozinku. Dodatni sloj sigurnosti uključuje i *Touch* ID *i Face* ID koje su ugrađene izravno u mobilne uređaje, [42].

5.2.2. Google Play Store

Google Play Store je *Googleova* platforma koja nudi različiti digitalni sadržaja svojim korisnicima. Služi kao službena trgovina aplikacija za certificirane uređaje koji rade na *Android* operativnom sustavu i njegovim izvedenicama, kao OS *Chrome*. Omogućavaju korisnicima pregledavanje i preuzimanje aplikacija razvijenih s kompletom za razvoj softvera za *Android* i objavljenih putem *Googlea*. Trgovina *Google Play* unaprijed je instalirana na pametnim telefonima koji se isporučuju s GSM-a (eng. *Google Mobile Services*). *Googleove* mobilne usluge uključuju brojne aplikacije koje su već unaprijed instalirane. Iz tog razloga, gotovo svi proizvođači mobilnih uređaja koji prodaju *Android* mobilne uređaje imat će unaprijed instalirane neke aplikacije. Predinstalirane aplikacije najčešće se ne mogu deinstalirati.

Google Play Protect je *Googleova* ugrađena zaštita od zlonamjernog softvera za *Android*. *Google Play Protect* neprestano radi na zaštiti uređaja, podataka i aplikacija. Automatski se skenira uređaj i osigurava se korisniku da ima najnovije sigurnosne sustave za mobilne uređaje. Dnevno

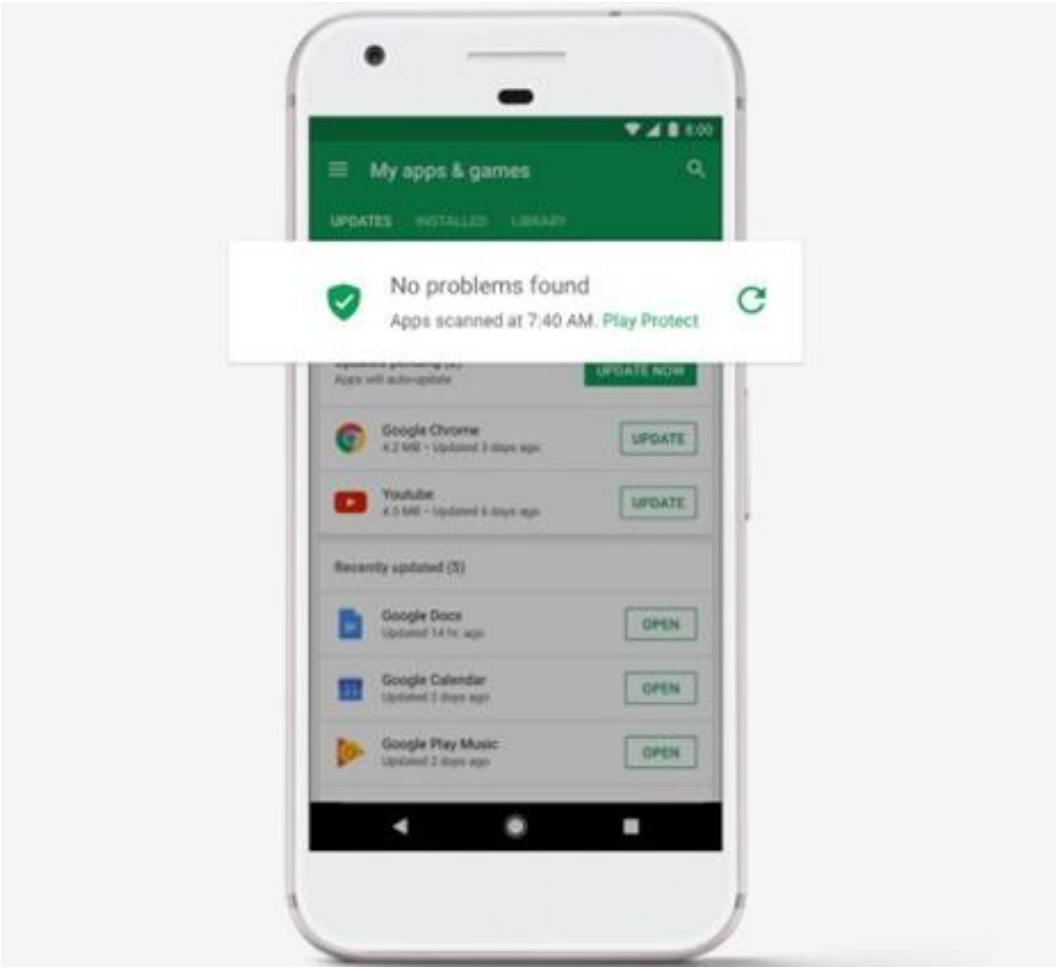
skeniranje omogućuje *Google Play Protectu* da brzo reagira na otkrivenu prijetnju, smanjujući koliko dugo bi korisnici mogli biti izloženi prijetnji i koliko bi uređaja moglo biti pogođeno. Sve *Android* aplikacije prolaze kroz sigurnosno testiranje prije nego što se pojave u Trgovini *Google Play*. Svaka aplikacija se provjerava i obustavljaju se sve aplikacije koje krše postavljena pravila. Na slici 8 se nalazi upozorenje koje se pojavljuje kada se primijeti štetna aplikacija na uređaju



Slika 8. Upozorenje na štetne aplikacije

Izvor: https://androidcommunity.com/google-play-protect-updated-to-better-secure-android-against-malicious-apps-20190227/

Aplikacije koje se smatraju najštetnijima uklanjaju se s uređaja, dok se manje štetne aplikacije onemogućuju. Onemogućene aplikacije su neupotrebljive, ali ostaju na uređaju, a svi podaci povezani s aplikacijom mogu se oporaviti. Iako *Google Play Protect* radi u pozadini, korisnici mogu provjeriti kada je zadnji put skeniran njihov uređaj i pregledati popis skeniranih aplikacija. Kada je uređaj izvan mreže ili ako je izgubio mrežnu vezu, *Google Play Protect* ima izvanmrežno skeniranje koje sprječava instaliranje štetnih aplikacija. Na slici 9 vidi se obavijest koja se pojavljuje kada je uređaj uspješno skeniran i kad nisu pronađene zlonamjerne aplikacije.



Slika 9. Skeniranje uređaja

Izvor: https://beebom.com/what-is-google-play-protect-enable-disable/

SafetyNet API je aplikacijsko programsko sučelje za sprječavanje zloupotrebe koji razvojnim programerima omogućuje procjenu *Android* uređaja na kojem se njihova aplikacija izvodi. API bi trebao biti korišten kao dio sustava za otkrivanje zloupotrebe kako bi se utvrdilo jesu li poslužitelji u interakciji s izvornom aplikacijom koja se izvodi na originalnom *Android* uređaju. API za provjeru pruža kriptografski potpisanu ocjenu, procjenjujući integritet uređaja. Kako bi se stvorila potvrda, API ispituje softversko i hardversko okruženje uređaja, tražeći probleme s integritetom i uspoređujući ih s referentnim podacima za odobrene *Android* uređaje. *SafetyNet* API omogućuje programerima poboljšanje sigurnosti aplikacija pružajući niz usluga kako bi se zaštitile aplikacije protiv sigurnosnih prijetnji, uključujući potencijalno štetne aplikacija i lažne korisnike, [43].

6. ZAKLJUČAK

Mobilni uređaji postali su predmeti bez kojih većina nas ne može zamisliti život. Ljudi su oduvijek tražili načine međusobnog povezivanja i umrežavanja. S obzirom na to da doba digitalizacije stalno napreduje, pojavljuju se brojne platforme i aplikacije za društveno umrežavanje. Vlasnici aplikacije stalno ažuriraju svoje aplikacije i dodaju novitete kako bi zadržali svoje korisnike, ali i privukli nove.

Jedne od najpopularnijih aplikacija su društvene mreže. One omogućuju ljudima i korporacijama da se povežu jedno s drugima kako bi mogli razviti odnose i razmjenjivati informacije, ideje i poruke. Kao i većina stvari, korištenje društvenih mreža ima svoje pozitivne, ali i negativne strane. Društvene mreže pružaju mogućnost povezivanja s obitelji i prijateljima širom svijeta te brz pristup informacijama i istraživanju.

Uz sve svoje prednosti, priroda društvenih mreža predstavlja niz potencijalnih problema. Povećano korištenje društvenih mreža znači više vremena provedenog na zaslonu što može prouzrokovati ovisnost. To može dovesti do internetskog zlostavljanja, socijalne anksioznosti, izloženosti sadržaju koji nije primjeren dobi ili upoznavanje „prijatelja“ koji možda i nisu prijatelji, pa čak i stranci. Ljudi postaju socijalno aktivni na društvenim mrežama, a sve manje razvijaju komunikaciju uživo pa čak i dok komuniciraju uživo povremeno gledaju na mobilne uređaje te nisu dovoljno fokusirani na razgovor.

S obzirom na to da broj korisnika na društvenim mrežama stalno raste, one postaju najlakša meta za prikupljanje podataka. Gotovo svaka aplikacija ima svoje Uvjete i odredbe u kojima piše koje podatke prikupljaju od korisnika i u koje svrhe koriste te podatke. Mnoge aplikacije se ne mogu koristiti bez da korisnik prihvati postavljene Uvjete. Većina korisnika prilikom instalacije prihvaća ponuđene Uvjete bez daljnjeg čitanja te na taj način odobravaju vlasnicima aplikacija legalno prikupljanje osobnih podataka, iako pojedine tvrtke dijele podatke s trećim stranama.

Vlasnici aplikacija tvrde da prikupljaju podatke kako bi korisnicima pružili što bolji sadržaj na platformi i na taj način pokušavaju zadržati svoje korisnike. Većina operativnih sustava ima razvijen sigurnosni sustav koji sprječava maliciozne korisnike da pristupe sustavu. Bez obzira na taj sigurnosni sustav uvijek postoji mogućnost da maliciozni korisnik „upadne“ u sustav ili aplikaciju te da napravi nešto na štetu korisnika. Aplikacije zadiru duboku u našu privatnost no svjesno ili nesvjesno smo dali pristanak za to. Najbolji način obrane od prikupljanja podataka je

potpuno deinstaliranje aplikacija ili čitanje postavljenih Uvjeta kako bismo bili sigurni da aplikacija prikuplja što manje osobnih podataka.

LITERATURA

[1] Statista Research Depertment; STATISTICS AND FACTS ON MOBILE INTERNET USAGE WORLDWIDE. 2021. Preuzeto sa: https://www.statista.com/topics/779/mobile-internet/#dossierSummary__chapter2 [Pristupljeno: 13.04.2021]

[2] MindSea Team; 28 MOBILE APP STATISTICS TO KNOW IN 2021. 2021. Preuzeto sa: https://mindsea.com/app-stats/ [Pristupljeno: 13.04.2021]

[3] Statista Research Depertment; GLOBAL SOCIAL NETWORKS RANKED BY NUMBER OF USERS 2021. 2021. Preuzeto sa: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [Pristupljeno: 13.04.2021]

[4] Statista Research Depertment; NUMBER OF MONTHLY ACTIVE WHATSAPP USERS 2013-2020. 2021. Preuzeto sa: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ [Pristupljeno: 15.04.2021]

[5] Dean B.; INSTAGRAM DEMOGRAPHIC STATISTICS: HOW MANY PEPOPLE USE INSTAGRAM IN 2021? 2021. Preuzeto sa: https://backlinko.com/instagram-users [Pristupljeno: 15.04.2021]

[6] Dean B.; HOW MANY PEOPLE USE TELEGRAM IN 2021? 55 TELEGRAM STATS. 2021. Preuzeto sa: https://backlinko.com/telegram-users [Pristupljeno: 18.04.2021]

[7] 99Content; VIBER STATISTICS. Preuzeto sa: https://99firms.com/blog/viber-statistics/ [Pristupljeno: 18.04.2021]

[8] Mohsin M; 10 TIKTOK STATISTICS THAT YOU NEED TO KNOW IN 2021 [INFOGRAPHIC]. 2021. Preuzeto sa: https://www.oberlo.com/blog/tiktok-statistics [Pristupljeno: 18.04.2021]

[9] AVERAGE TIME SPENT DAILY ON SOCIAL MEDIA (LATEST 2020 DATA). 2020. Preuzeto sa: https://www.broadbandsearch.net/blog/average-daily-time-on-social-media [Pristupljeno: 24.04.2021]

[10] Buxton M.; YOU CAN NOW SEE HOW MUCH TIME YOU SPEND ON INSTAGRAM, BUT DO YOU WANT TO KNOW? 2018. Preuzeto sa: https://www.refinery29.com/en-us/2018/08/206008/instagram-time-spent-reminder [Pristupljeno: 24.04.2021]

[11] TERMS AND CONDITIONS FOR MOBILE APPS. Preuzeto sa: https://www.termsfeed.com/blog/terms-conditions-mobile-apps/ [Pristupljeno: 24.04.2021]

[12] S. O'Dea; MARKET SHARE OF MOBILE OPERATING SYSTEMS WORLDWIDE 2012-2021. 2021. Preuzeto sa: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/#statisticContainer [Pristupljeno: 24.04.2021]

[13] Kenton W.; APPLE IOS. 2020. Preuzeto sa: https://www.investopedia.com/terms/a/apple-ios.asp#citation-3 [Pristupljeno: 28.04.2021]

[14] Posey B.; APPLE IOS. Preuzeto sa: https://searchmobilecomputing.techtarget.com/definition/iOS [Pristupljeno: 28.04.2021]

[15] Preuzeto sa: https://www.apple.com/legal/privacy/en-ww/ [Pristupljeno: 29.04.2021]

[16] Morin T.; AN APP DEVELOPER'S GUIDE TO IOS 14 CHANGES. 2020. Preuzeto sa: https://gimbal.com/app-developers-guide-ios-14-changes/?utm_source=pardot&utm_medium=email&utm_campaign=ios_14.5_update [Pristupljeno: 29.04.2021]

[17] ANDROID ARCHITECTURE. Preuzeto sa: https://source.android.com/devices/architecture?hl=cs

[18] ANDROID 11: THE OS THAT GETS TO WHAT'S IMPORTANT. Preuzeto sa: https://www.android.com/android-11/#a11-privacy-security-article [Pristupljeno: 19.05.2021]

[19] JR Raphael; ANDROID VERSIONS: A LIVING HISTORY FROM 1.0 TO 12. 2021. Preuzeto sa: https://www.computerworld.com/article/3235946/android-versions-a-living-history-from-1-0-to-today.html [Pristupljeno: 19.05.2021]

[20] Dimiitrov I.; INVASIVE APPS. 2021. Preuzeto sa: https://blog.pcloud.com/invasive-apps/ [Pristupljeno: 27.04.2021]

[21] INSTAGRAM. Preuzeto sa: https://help.instagram.com/519522125107875#how-we-use-information [Pristupljeno: 14.06.2021]

[22] Burges M.; HOW TO STOP INSTAGRAM FROM TRACKING EVERYTHING YOU DO. 2020. Preuzeto sa: https://www.wired.com/story/how-to-stop-instagram-from-tracking-everything-you-do/ [Pristupljeno: 14.06.2021]

[23] Singer N.; WHAT YOU DON'T KNOW ABOUT HOW FACEBOOK USES YOUR DATA. 2018. Preuzeto sa: https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html [Pristupljeno: 15.06.2021]

[24] Dvorak C.; WHAT DATA DOES FACEBOOK COLLECT? 2020.Preuzeto sa: https://www.reviews.org/internet-service/what-data-does-facebook-collect/ [Pristupljeno: 15.06.2021]

[25] Pfohl J.; THE SCARY TRUTH ABOUT THE FACEBOOK MESSENGER APP AND YOUR PRIVACY. 2020. Preuzeto sa: https://crambler.com/truth-about-facebook-messenger-app-privacy/ [Pristupljeno: 18.06.2021]

[26] Rilloraza B.; THE AMOUNT OF DATA FACEBOOK MESSENGER COLLECTS FROM USERS IS STAGGERING. 2021 Preuzeto sa: https://www.technobaboy.com/2021/01/07/facebook-messenger-data-collect-users/ [Pristupljeno: 18.06.2021]

[27] Marks T.; WHAT DOES WHATSAPP KNOW ABOUT ME? 2021. Preuzeto sa: https://vpnoverview.com/privacy/social-media/what-does-whatsapp-know-about-me/ [Pristupljeno: 25.06.2021]

[28] TELEGRAM. Preuzeto sa: https://telegram.org/ [Pristupljeno: 25.06.2021]

[29] TELEGRAM, SIGNAL, VIBER: ALL YOU NEED TO KNOW ABOUT THE TOP ALTERNATIVES TO WHATSAPP. 2021. Preuzeto sa: https://economictimes.indiatimes.com/magazines/panache/telegram-signal-viber-all-you-need-to-know-about-the-top-alternatives-to-whatsapp/a-detailed-look-at-best-whatsapp-alternatives/slideshow/80247998.cms [Pristupljeno: 25.06.2021]

[30] Tidy J.; TIKTOK: WHAT IS THE APP AND HOW MUCH DATA DOES IT COLLECT? 2020. Preuzeto sa: https://www.bbc.com/news/technology-53476117 [Pristupljeno: 26.06.2021]

[31] The Pradeo Lab; MOBILE SECURITY REPORT. 2019. [Pristupljeno: 26.06.2021]

[32] Maria P.; SAMPLE PRIVACY POLICY TEMPLATE. Preuzeto sa: https://www.privacypolicies.com/blog/privacy-policy-template/ [Pristupljeno: 15.07.2021]

[33] WHAT IS THE GDPR? A COMPLETE GUIDE ON EVERYTHING YOU NEED TO KNOW TO COMPLY. Preuzeto sa: https://www.iubenda.com/en/help/5428-gdpr-guide [Pristupljeno: 20.07.2021]

[34] GDPR Croatia (Facebook) [Pristupljeno: 20.07.2021]

[35] Lakshmanan R.; TIKTOK QUIETLY UPDATED ITS PRIVACY POLICY TO COLLECT USERS' BIOMETRIC DATA. 2021. Preuzeto sa: https://amp.thehackernews.com/thn/2021/06/tiktok-quietly-updated-its-privacy.html [Pristupljeno: 20.07.2021]

[36] Vrbanus S.; OSOBNI PODACI 660 TISUĆA HRVATSKIH KORISNIKA FACEBOOKA PROCURILI U JAVNOST. 2021 Preuzeto sa: https://www.bug.hr/sigurnost/osobni-podaci-660-tisuca-hrvatskih-korisnika-facebooka-procurili-u-javnost-20366 [Pristupljeno: 24.07.2021]

[37] Prateek P.; SIX OF THE LARGEST APP-RELATED DATA BREACHES. 2020. Preuzeto sa: https://www.intertrust.com/blog/six-of-the-largest-app-related-data-breaches/ [Pristupljeno: 24.07.2021]

[38] Cimpanu C.; GOOGLE COLLECTS 20 TIMES MORE TELEMETRY FROM ANDROID DEVICES THAN APPLE FROM IOS. 2021. Preuzeto sa: https://therecord.media/google-collects-20-times-more-telemetry-from-android-devices-than-apple-from-ios/?__cf_chl_jschl_tk__=0ac0516654ef57e96b5c2283cfdcaf59ddc7d5b2-1620499397-0-Ad5Hyx3GDjzHK6z-17rA1eQj21Py7o6uo7HHLWosLvq3uu7EOBCl5T5I9fvrS8E7UnqgorM_WxkSGZcMoIG0VGtTx5hlc4X6SYN83IthSLaJvEu_P5fFiEdhE7K6AohfgqS2TCXK-Vy0LqHw6hi6Adyyb6Tz-WrC-W4-zL4O7wJLUoWQq_DjfPkkA3Dpi4LrmXsDjLu2HI1X_pBRpakInP1tKGVhTmQH_IZE4T29W

8ezLdT7rAhJozhCFH8EVgXWRbdxcgjTDeqgZbUdgHZzvZVKsV51BggLeXoZbv-HAH2gaJzCB6_wQHCVjbKQwWxo1JBKHh3NOTrD3XodLsrJzUxS_mTnUKS81ubETQahqBFK8IE6Ert52GeC9SjrZKQ2uNJjxZ1dMySkgINW9uBpyXc03lKWlyF4juFF9c8e6S4hiUS9W_u4hQydeZTwSvZqDHP7XXE4GDejiJm-txy5bKudeXs23aVfhyQbF5mCLTeO0u15EG0gfeQAGMJ9_U81cQ [Pristupljeno: 26.07.2021]

[39] The Pradeo Lab; GOOGLE PLAY'S MOST DOWNLOADED SHOPPING APPS IRRESPONSIBLY PROCESS USERS' DATA. 2019. Preuzeto sa: https://blog.pradeo.com/google-play-most-downloaded-shopping-apps-process-users-data [Pristupljeno: 26.07.2021]

[40] O'Brein C.; WHAT EXACTLY IS APPLE DOING TO PROTECT USERS' PRIVACY? 2021. Preuzeto sa: https://www.irishtimes.com/business/technology/what-exactly-is-apple-doing-to-protect-users-privacy-1.4594876 [Pristupljeno: 01.08.2021]

[41] ANDROID. Preuzeto sa: https://www.android.com/intl/en_uk/enterprise/security/ [Pristupljeno: 01.08.2021]

[42] APPLE APP STORE. Preuzeto sa: https://www.apple.com/app-store/ [Pristupljeno: 05.08.2021]

[43] GOOGLE PLAY PROTECT. Preuzeto sa: https://www.android.com/intl/en_us/intl/en_uk/play-protect/ [Pristupljeno: 05.08.2021]

POPIS GRAFIKONA

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.
Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.
Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Dopuštenja aplikacijama pametnih telefona i privatnost podataka**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 4.9.2021 Anđela Stanišić
(potpis)