AGREGIRANJE RIZIKA NARUŠAVANJA PRIVATNOSTI OSOBNIH PODATAKA NA MOBILNIM UREĐAJIMA

Stepić, Andrea

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

AGREGIRANJE RIZIKA NARUŠAVANJA PRIVATNOSTI OSOBNIH PODATAKA NA MOBILNIM UREĐAJIMA

Andrea Stepić

Zagreb, listopad 2019.

Predgovor

Ovim putem želim se prvenstveno zahvaliti svojoj obitelji na potpori, razumijevanju i nesebičnoj pomoći koju mi je pružala tijekom cjelokupnog trajanja studija i izrade diplomskog rada.

Svojem mentoru, mr. sc. Mariju Volareviću zahvaljujem na trudu koji je uložio u ovaj rad, a posebno na njegovom razumijevanju i riječima podrške.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Hrvatski:

Digitalnoj transformaciji društva svjedočimo kroz brzi rast digitalizacije usluga i pojavu velikog broja online servisa i aplikacija kojima svojevoljno i bez puno razmišljanja dajemo velike količine svojih osobnih i drugih privatnih podataka. Rad istražuje kakvi su trenutni trendovi u industriji mobilnih aplikacija vezano za privatnost te pojašnjava kriterije transparentnosti izjava o privatnosti proizašle iz Opće uredbe o zaštiti podataka (GDPR). Slijedi pregled dozvola mobilnih aplikacija i povezanih rizika nakon čega analizira izjave o privatnosti šest popularnih mobilnih aplikacija u Republici Hrvatskoj (RH) vezano za transparentnost izjava i dozvole odabranih aplikacija. Na kraju putem ankete istražuje koliko su građani RH svjesni rizika narušavanja svoje privatnosti putem mobilnih aplikacija i sprječava li ih to saznanje u preuzimanju istih te daje uvid u neka od istraživanja vezana za paradoks privatnosti.

Ključne riječi: privatnost, izjava o privatnosti, dozvole aplikacija, mobilni uređaji, paradoks privatnosti, Opća uredba o zaštiti podataka (GDPR).

English:

Digital transformation is evident in the fast growth of service digitalization and an occurrence of a large number of online services and applications to which we freely and without much thought give a great deal of personal and other private information. This paper deals with current trends in the mobile applications industry regarding privacy and explains the transparency criteria of privacy policies set out in the General Data Protection Regulation (GDPR). This is followed by an explanation of mobile applications' permissions and related risks after which privacy policies of six popular mobile applications in the Republic of Croatia are analysed with regards to their transparency and permissions of the chosen applications. In the last part an online survey is used to gain insight about awareness of privacy intrusions of mobile applications among the Croatian population as well as whether knowledge of such intrusions prevents them from downloading certain applications. In the end insight is given into some of the research regarding the privacy paradox.

Key words: privacy, privacy policy, app permissions, mobile devices, privacy paradox, General Data Protection Regulation (GDPR).

Sadržaj

1. Uvod

Digitalnoj transformaciji društva svjedočimo kroz brzi rast digitalizacije usluga i pojavu velikog broja servisa i aplikacija kao što su Gmail, web tražilice, online trgovine, Facebook i druge. Mijenjaju se navike, potrebe i očekivanja korisnika koji u želji za trenutačnom komunikacijom, virtualnim druženjem, boljom organizacijom i snalaženjem te brojnim drugim prednostima, svojevoljno i bez puno razmišljanja raznim aplikacijama i servisima daju velike količine svojih osobnih i drugih privatnih podataka.

Brojna istraživanja pokazala su kako većina ljudi privatnost smatra važnom i svjesni su da aplikacije na mobilnim uređajima prikupljaju razne podatke kroz pristup mikrofonu, fotoaparatu, lokaciji i dr. Unatoč tome preuzimaju aplikacije koje im tu privatnost narušavaju.

Ovim radom namjeravam (I) istražiti koji su potencijalni rizici za privatnost korisnika mobilnih uređaja uzrokovani korištenjem različitih mobilnih aplikacija općenito, a ujedno i analizom nekih od popularnijih aplikacija (II) steći uvid u transparentnost njihovih izjava o privatnosti kako je propisano Općom uredbom o zaštiti podataka (engl. *General Data Protection Regulation* - GDPR). U prvom dijelu rada kratko ću navesti trenutačne trendove u industriji mobilnih aplikacija što se tiče privatnosti nakon čega ću u drugom dijelu pojasniti što je to GDPR kao i što transparentne izjave o privatnosti moraju sadržavati. U trećem dijelu pojasnit ću dozvole koje mobilne aplikacije zahtijevaju kao i rizike koje te dozvole nose. Zatim ću analizirati izjave o privatnosti šest popularnih mobilnih aplikacija koje koriste građani Republike Hrvatske (RH) kako bih dobila uvid u transparentnost njihovih izjava o privatnosti temeljem Članaka 13. i 14. GDPR-a, kao i koje podatke prikupljaju i s kojom svrhom. Na kraju ću (III) pojasniti fenomen paradoksa privatnosti te putem ankete istražiti koliko su građani RH svjesni narušavanja svoje privatnosti putem mobilnih aplikacija te sprječava li ih to saznanje u preuzimanju istih.

Rezultate dobivene ovim istraživanjem mogli bi iskoristiti entiteti u RH koji već imaju ili će tek imati izjave o privatnosti, ali i prilikom kreiranja vlastitih aplikacija vodeći računa o privatnosti korisnika. Razvojem svijesti i mehanizama zaštite očekujemo stvaranje podloge za uspješniji razvoj novih poslovnih modela u kojima korisnik u potpunosti stavlja pod kontrolu uporabu i monetizaciju svojih osobnih podataka.

2. Privatnost i industrija mobilnih aplikacija

Industriju mobilnih aplikacija obilježavaju različiti trendovi kao što su strojno učenje, proširena i virtualna stvarnost, nosive tehnologije, Internet stvari, instant aplikacije i dr., no ovdje ću izdvojiti neke od trendova i značajne događaje koji utječu na industriju mobilnih aplikacija vezano za privatnost. To su:

- Monetizacija podataka
- Korisničko dijeljenje osobnih i privatnih podataka
- Rast svijesti o privatnosti i
- Opća uredba o zaštiti podataka (GDPR).

2.1. Monetizacija podataka

Digitalne platforme[1] ili mreže posredovane platformom koriste se diljem svijeta već duži niz godina, a svoj stalni rast mogu zahvaliti lakoći korištenja i inovativnim rješenjima, sve većem broju korisnika Interneta i mobilnih uređaja, efektu mreža[2], ali i mogućnosti monetizacije podataka korisnika kroz personalizirano oglašavanje (ACCC - Australian Competition & Consumer Commission, 2019: str. 43). Primjeri takvih platformi su Facebook i Google, dvostrane digitalne platforme gdje su s jedne strane korisnici njihovih usluga (trenutačne poruke, e-mail, pretraživanje Interneta i dr.), a s druge strane oglašivači. S porastom broja mobilnih uređaja tj. pametnih telefona povećao se i broj korisnika raznih digitalnih platformi na istima.

Kako je navedeno u izvješću o digitalnim platformama Australske komisije za tržišno natjecanje i potrošače (ACCC, 2019: str. 7, 46), razne popularne platforme svoj izniman profit ostvaruju kroz izrazito personalizirano oglašavanje, a koje je moguće zbog velike količine podataka koje prikupljaju o svojim korisnicima. Za to je značajna veličina baze korisnika jer što je broj korisnika veći, veća je mogućnost personaliziranog oglašavanja,

[1] Digitalne platforme su aplikacije čije usluge koriste različite skupine korisnika, a vrijednost aplikacije za svakog pojedinog korisnika raste što je broj korisnika veći (ACCC, 2019: str. 41). To su npr. portali koji spajaju iznajmljivače apartmana i turiste koji traže smještaj, web preglednici kao što je Google Chrome koji koriste razne osobe za traženje informacija, ali i oglašivači koji će tim osobama prikazivati personalizirane oglase, zatim društvene mreže i dr.

[2] Efekt mreža označava fenomen gdje vrijednost mreže i platforme raste s porastom broja korisnika platforme. Iz prezentacije Ane Mihalić, *Platform mediated business networks*, 1. 4. i 5. 4. 2017. godine, kolegij Disruptivne tehnologije, Visoko učilište Algebra, slajd 14.

a samim time veći je i profit. Zbog navedenoga, i tvrtke koje se bave prikupljanjem i prodajom podataka su postale važan dio digitalne ekonomije.

Osim Googlea (odnosno njegove krovne tvtke Alphabet) i Facebooka, dviju tvrtki koje posjeduju neke od najpoznatijih digitalnih platformi (web tražilica Google i društvena mreža Facebook), brojne druge tvrtke putem društvenih mreža, web preglednika, pretraživanja na web tražilicama, programa, elektroničke pošte, aplikacija i dr. prikupljaju osobne podatke korisnika koje zatim koriste kako bi poboljšali svoje proizvode i usluge, dok neke od njih te podatke prodaju trećim stranama. I prve i treće strane na temelju prikupljenih podataka izrađuju profile korisnika odnosno njihove virtualne, ali i fizičke identitete koji im omogućuju serviranje ciljanih, personaliziranih oglasa u skladu s interesima korisnika. Putem mobilnih uređaja i aplikacija prikuplja se još veća količina podataka jer svoje pametne telefone nosimo svuda sa sobom i oni sadrže veliku količinu podataka o nama bilo to u kalendarima, porukama, pretraživanim stranicama, e-pošti, galerijama fotografija i dr.

Osim toga, zbog GPS značajke pametnih telefona, tvrtke imaju podatke o tome gdje se i kada krećemo, zbog naših objava na društvenim mrežama znaju i kada spavamo, zbog termina pretraživanja u web tražilicama znaju od kakvih bolesti patimo mi ili članovi naše obitelji, znaju s kim se družimo i brojne druge informacije, a što se može zaključiti iz vrsta podataka koje brojne digitalne platforme i mobilne aplikacije prikupljaju i koje su navedene u njihovim izjavama o privatnosti. Vrste podataka koje prikupljaju aplikacije odabrane za potrebe ovoga rada nabrojane su u podpoglavlju 5.3. pod nazivom *Prikupljanje podataka od strane voditelja obrade odabranih aplikacija*. Zbog svega navedenoga, monetizacija podataka je svakako jedan od najznačajnijih trendova koji izravno utječu na privatnost korisnika mobilnih uređaja i aplikacija.

2.2. Trend dijeljenja privatnih podataka

Prema mađarskom psihologu Abrahamu Maslowu, treća najvažnija ljudska potreba nakon primarnih fizioloških potreba (zrak, voda, hrana, spavanje) i potrebe za sigurnošću je potreba za pripadanjem (Pavuna, 2019: str. 76; prema Maslow, 1943), dok Harcourt navodi kako ljudi žele biti voljeni, željeni i popularni, a to im digitalne platforme kao što su društvene mreže omogućuju na svjetskoj razini (Pavuna, 2019: str. 77; prema Harcourt, 2015).

Gore navedena monetizacija podataka ne bi bila moguća bez razvoja raznih tehnologija, no ni bez novih trendova u ponašanju ljudi koje su takve tehnologije omogućile. Naime, ljudi različitih godina, od najmlađih do najstarijih, su se vrlo brzo prilagodili konceptu društvenih mreža i dijeljenju osobnih i drugih privatnih podataka. Na raznoraznim društvenim mrežama i putem svojih mrežnih stranica ili blogova, kao i aplikacija za trenutačnu komunikaciju oni objavljuju svoje fotografije kao i fotografije svoje djece, pišu i izrađuju video zapise o svojim dnevnim aktivnostima, informiraju svoje prijatelje i rodbinu o svojim razmišljanjima, putovanjima, dogodovštinama, receptima koje isprobavaju i dr. Pri tome koriste računala, ali još više svoje pametne telefone na kojima im za to služe brojne mobilne aplikacije kao što su Facebook, Viber, Snapchat, WhatsApp, Instagram i druge, na kojima kao da se trude podijeliti što više svojih osobnih podataka i privatnih informacija. Osim komunikacije i dijeljenja navedenih vrsta sadržaja, sve više koristimo pametne telefone i za Internet kupovinu, slušanje i gledanje audio i video sadržaja, Internet odnosno mobilno bankarstvo, za plaćanje u trgovinama i dr. Harvardski profesor Bernard E. Harcourt je takvo društvo nazvao „društvom izlaganja“ te ga opisao kao „novo političko i društveno stanje koje radikalno transformira međuljudske odnose, našu političku zajednicu i nas same; novu virtualnu transparentnost koja dramatično preoblikuje odnose moći u cijelom društvu, koja iznova dizajnira naš društveni krajolik, koja stvara dramatično novi protok moći u društvu“ (Pavuna, 2019: str. 72-73; prema Harcourt, 2015).

Istina je da mnoge od tih podataka ljudi svojevoljno daju tvrtkama čije proizvode ili usluge koriste, no veliki broj ljudi čini se nije niti svjestan rizika namjernog odavanja ili nesvjesnog pružanja mnogobrojnih osobnih podataka.

Prema Posebnom Eurobarometru 487b QB11 (Europska komisija, 2019: str. 2), istraživanju koje je 2019. godine provedeno na 27.000 stanovnika Europe, 43 % ispitanika nije nikada pokušalo promijeniti svoje postavke privatnosti na nekoj društvenoj mreži, a kao glavne razloge za to naveli su kako vjeruju da će stranice same postaviti odgovarajuće postavke privatnosti (29 %) te da ne znaju kako to učiniti (27 %). Petina njih izjavila je da nije mijenjala postavke jer se ne brine zbog dijeljenja osobnih podataka, 17 % njih nije niti znalo da ih mogu promijeniti, a 14 % izjavilo je kako za to nema vremena (Europska komisija, 2019: str. 2).

2.3. Rast svijesti o privatnosti

2018. godinu obilježio je skandal u kojemu su sudjelovale društvena mreža Facebook i privatna britanska tvrtka Cambridge Analytica koja je, navodno, pomoću podataka ilegalno prikupljenih s Facebooka sudjelovala u kreiranju mišljenja američkih građana tijekom američkih predsjedničkih izbora 2016. godine. Naime, dr. Aleksandr Kogan, profesor psihologije na Sveučilištu Cambridge, izradio je aplikaciju, kviz osobnosti pod nazivom „thisisyourdigitallife“ u akademske svrhe, koju je preuzelo oko 320 000 korisnika Facebooka. Međutim, svaki od tih korisnika nesvjesno je, u prosjeku, dao pristup podacima još 160 profila svojih prijatelja koji za to nisu znali (Cadwalladr, 2018). Podaci milijuna korisnika čije je prikupljanje od strane Facebooka bilo dozvoljeno isključivo u akademske svrhe prodani su putem Koganove tvrtke Global Science Research bez privole svih korisnika tvrtci Cambridge Analytica, a o cijelom skandalu u javnost je 2018. godine izišao jedan od osnivača tvrtke Cambridge Analytica, Christopher Wylie (Cadwalladr, 2018).

Ovaj skandal doprinio je tome da privatnost korisnika digitalnih platformi, odnosno Interneta dođe u prvi plan te su razne vlade (Kanada, Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske, SAD, Europski parlament) i organizacije reagirale i odlučile istražiti Facebookovo narušavanje privatnosti korisnika, ali i kršenje zakona u nekim državama (ACCC, 2019; Keach, 2018.). U srpnju 2019. godine američka Savezna trgovinska komisija (Federal Trade Commission – FTC) je donijela odluku o kazni za Facebook od pet milijardi američkih dolara koju još treba odobriti Ministarstvo pravosuđa SAD-a (BBC News, 2019). U listopadu 2018. godine britanski Ured povjerenika za informacije (Information Commissioner's Office - ICO) je kaznio Facebook s 500 000 funti jer je razvojnim programerima omogućio pristup podacima korisnika bez da su dobili izričitu i informiranu privolu korisnika (ACCC, 2019: str. 420, prema UK Information Commissioner's Office, 2018).

2.4. Nova regulativa Europske unije

Cambridge Analytica skandal dogodio se samo dva mjeseca prije nego je u Europskoj uniji na snagu stupila Opća uredba o zaštiti podataka. Opća uredba o zaštiti podataka[3] (Uredba (EU) 2016/679) ili GDPR (General Data Protection Regulation) donesena je 27. travnja 2016. godine, a na snagu je stupila 25. svibnja 2018. godine. Uredba se odnosi na sve organizacije koje prikupljaju osobne odnosno identificirajuće podatke građana EU bez obzira nalaze li se te organizacije u Europskoj uniji (EU), a njome su utvrđena pravila koja se odnose na zaštitu pojedinaca/ispitanika u smislu obrade njihovih osobnih podataka kao i pravila koja uređuju pitanje slobode kretanja osobnih podataka pojedinaca (GDPR, 2016: Članak 1). Odnosi se na sve fizičke i pravne osobe koje osobne podatke obrađuju kako bi pružile svoje proizvode ili usluge tim istim ispitanicima i pri tome prate ponašanje pojedinaca (Bateman, 2019). Obrada se prema GDPR-u „odnosi na kreiranje, prikupljanje, skladištenje, dijeljenje i brisanje podataka“ (European Union Agency for Network and Information Security - ENISA, 2017: str. 51).

Prema Članku 25. Opće uredbe o zaštiti podataka, razvojni programeri tj. voditelji obrade prilikom određivanja načina obrade kao i u trenutku obrade trebaju provoditi odgovarajuće tehničke i organizacijske mjere, odnosno trebaju se voditi konceptima privatnosti po dizajnu (engl. *Privacy by Design*[4]) i predefinirane privatnosti (engl. *Privacy by Default*). Kada govorimo o mobilnim aplikacijama, privatnost po dizajnu znači da je već prilikom kreiranja aplikacije potrebno voditi računa o privatnosti korisnika i ugraditi ju u dizajn razvijane tehnologije (ENISA, 2017: str. 47). Koncept predefinirane privatnosti znači da postavke privatnosti trebaju biti predefinirane na način da se prikupljaju samo oni osobni podaci koji su potrebni za svaku specifičnu svrhu (ENISA, 2017: str. 21, 56). Cilj ovih koncepata je osigurati korisnicima privatnost i kontrolu nad vlastitim osobnim podacima (O'Neil, 2016) *Privacy by Design* je 2010. godine na Međunarodnoj konferenciji o zaštiti podataka i povjerenika za privatnost prihvaćen kao međunarodni standard (O'Neil, 2016).

Prema Ann Cavoukian (Cavoukian, 2009; Burns, 2017), kreatorici koncepta privatnosti po dizajnu, taj koncept počiva na sedam temeljnih načela:

---

[3] Puni naziv Uredbe je Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ.

[4] Pojam *Privacy by design* razvila je 1990-tih godina Ann Cavoukian, tadašnja Povjerenica za informacije i privatnost kanadske pokrajine Ontario.

1. **Privatnost mora biti proaktivna**, a ne reaktivna, odnosno onaj koji kreira aplikaciju mora očekivati moguće probleme s privatnošću i spriječiti ih te stoga niti ne nudi postupke koji bi riješili probleme s privatnošću nakon što bi se dogodili;
2. **Privatnost mora biti predefinirana** (*Privacy by Default*), odnosno mora se automatski štititi u bilo kojoj informacijskoj tehnologiji ili poslovnoj praksi, a pojedinac ne mora poduzeti ništa kako bi zaštitio svoju privatnost. Jednako tako, privola za davanje osobnih podataka se ne podrazumijeva;
3. **Privatnost ugrađena u dizajn** – ona je sastavni dio sustava i njezinom primjenom ne smije biti smanjena funkcionalnost;
4. **Potpuna funkcionalnost** – potrebno je ispuniti sve legitimne interese i ciljeve na način koji neće umanjiti neke druge interese kao što je sigurnost. Dakle, potrebno je pokazati kako je moguće imati i sigurnost i privatnost u isto vrijeme;
5. Potrebna je **cjelovita zaštita osobnih podataka** korisnika od početka prikupljanja do njihovog brisanja;
6. **Vidljivost i transparentnost** – tvrtke moraju voditi računa o tome da su njihovi standardi vezani za privatnost vidljivi i transparentni, da se sve dokumentira te da je isto moguće neovisno potvrditi;
7. **Poštivanje privatnosti korisnika**, odnosno da su interesi korisnika na prvom mjestu na način da su predefinirane značajke privatnosti na visokoj razini, da ih se obavještava na vrijeme te da na raspolaganju imaju opcije koje idu u prilog njihovoj privatnosti. Potrebno je osigurati sljedeće:
    a. Potrebna je izričita privola korisnika za prikupljanje osobnih podataka;
    b. Osobni podaci moraju biti točni i ažurni;
    c. Korisnici moraju imati pristup svojim osobnim podacima i biti obaviješteni o načinima njihovog korištenja;
    d. Usklađenost – organizacije moraju korisnicima omogućiti mehanizme za postupke žalbe i obeštećenja i dati im informacije o istima.

U sljedećem poglavlju pobliže će biti pojašnjen GDPR i u njemu navedeno načelo transparentnosti kao jedno od najvažnijih načela kojega se tvrtke koje nude svoje proizvode i usluge putem Interneta trebaju pridržavati u svom poslovanju i prilikom kreiranja svojih izjava o privatnosti. Ovo poglavlje poslužit će kao uvod u kasniju analizu nekih od najpopularnijih mobilnih aplikacija u Republici Hrvatskoj kako bi se dobio uvid u

transparentnost njihovih izjava o privatnosti i dozvola koje zahtijevaju na mobilnim uređajima.

3. Opća uredba o zaštiti podataka i izjave o privatnosti

U prethodnom poglavlju navedeno je kako se Općom uredbom o zaštiti podataka (GDPR) utvrđuju pravila vezana za zaštitu pojedinaca, a vezano za obradu osobnih podataka kao i slobodu kretanja istih (GDPR, Članak 1.). GDPR prema Recitalu 23 štiti fizičke osobe koje se nalaze u Europskoj uniji (EU) bez obzira na to gdje je poslovni nastan voditelja obrade tih osobnih podataka (GDPR, Recital 23). Dakle, ukoliko neka američka tvrtka nudi proizvode građanima bilo koje države EU ili obrađuje podatke građana EU (npr. Facebook), ona se također mora pridržavati odredbi GDPR-a. Prema Recitalu 39 GDPR-a, obrada osobnih podataka mora biti zakonita, poštena i transparentna gdje transparentnost znači da informacije o obradi podataka moraju biti „lako dostupne i razumljive“ te da je za komunikaciju tih informacija potrebno koristiti „jasan i jednostavan jezik“ (GDPR, Recital 39).

Pojašnjenja Opće uredbe o zaštiti podataka iz ovog poglavlja poslužit će kao temelj za analizu transparentnosti odabranih mobilnih aplikacija u petom poglavlju ovoga rada.

3.1. Osobni podaci

Pravo na zaštitu osobnih podataka „je pravo zaštite legitimnih interesa građanina (pojedinca) koje se odnosi na sprječavanje i sankcioniranje zlouporaba osobnih podataka, a zajamčeno je međunarodnim i nacionalnim propisima“ (AZOP, Pravo na zaštitu osobnih podataka) i ono je jedno od temeljnih ljudskih prava. Pojedinac je „fizička osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi jednog ili više obilježja specifičnih za njegov fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet“ (AZOP, Pravo na zaštitu osobnih podataka).

Pravo na zaštitu osobnih podataka nije novi pojam, no trenutno je jedno od vrućih pitanja zbog razvoja digitalnih tehnologija. Ujedinjeni narodi su u Općoj deklaraciji o ljudskim pravima još prije 80 godina naveli kako se „Nikoga ne smije uznemiravati samovoljnim miješanjem u njegov privatni život, njegovu obitelj, njegov stan, njegovo privatno dopisivanje niti napadom na njegovu čast i ugled." (AZOP, Pravo na zaštitu osobnih podataka).

Pod osobnim podacima smatramo sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi izravno ili neizravno pomoću nekih identifikatora. U osobne podatke tako ubrajamo (AZOP, Pravo na zaštitu podataka; AZOP, Vodič kroz opću uredbu o zaštiti podataka; Burns, 2018; GDPR, Članak 4.)

- Ime i prezime
- E-mail adresu
- Telefonski broj
- Adresu stanovanja
- OIB, JMBG, odnosno identifikacijski broj
- Podatke o zdravstvenom stanju
- Brojeve kreditnih kartica i druge financijske podatke
- Ocjene učenika u školi i evidencije o njihovom ponašanju
- Porezne prijave
- Podatke o posudbi
- Broj putovnice, osobne iskaznice i dr.
- Podatke o lokaciji
- Popis omiljenih pjesama ili literature
- Fotografiju
- Glas
- Mrežne identifikatore kao što su IP adrese, identifikatori mobilnih uređaja, zatim podatke o web pregledniku, RFID *tagove*[5], kolačiće, MAC adrese i korisnička imena[6]
- Čimbenike vezane uz razne vrste identiteta pojedinca kao što su mentalni, ekonomski, fizički, socijalni, fiziološki i kulturni identitet.

Osim toga, postoje i **posebne kategorije osobnih podataka** u koje ubrajamo podatke o političkim stajalištima, vjerskim ili drugim uvjerenjima, podatke o podrijetlu (rasnom ili etničkom), o članstvu u sindikatima, o zdravlju, spolnom životu i seksualnoj orijentaciji, genetske i biometrijske podatke te podatke o kaznenom i prekršajnom postupku (GDPR, Članak 9.; AZOP, Pravo na zaštitu osobnih podataka).

[5] RFID (engl. *Radio frequency identification*) *tag* je vrsta sustava za praćenje koja koristi pametne barkodove za identifikaciju. RFID transponder nosi serijski broj koji je jedinstven samo za taj određeni proizvod. (MARCO, Automatska identifikacija: RFID; Pontius, 2017).
[6] U kombinaciji s drugim podacima mogu se iskoristiti kako bi se nekoga identificiralo.

3.2. Izjave o privatnosti

U GDPR-u se nigdje izrijekom ne spominje kako voditelji obrade (engl. *data controllers*) trebaju imati dokument pod nazivom „Politika privatnosti“ ili nešto slično, no u Smjernicama o transparentnosti navodi se izjava ili obavijest o privatnosti (engl. *Privacy Policy* ili *Data Protection Notice*). Prema tome, svaki poslovni subjekt kao i svaka mrežna stranica i mobilna aplikacija koja prikuplja i obrađuje osobne podatke svojih korisnika mora imati jasno istaknutu izjavu o privatnosti.

Članci 12., 13. i 14. GDPR-a su ključni jer Članci 13. i 14. navode koje informacije se ispitanicima moraju pružiti vezano za obradu njihovih osobnih podataka, dok Članak 12. navodi na koji način je te informacije potrebno pružiti ispitanicima. Članak 13. primjenjuje se ukoliko se podaci prikupljaju izravno od ispitanika u slučajevima kada ispitanik svoje podatke svjesno daje voditelju obrade (kao kada ispuni određeni obrazac na mrežnoj stranici) ili voditelj obrade podatke prikuplja opažanjem (npr. putem video nadzora, mrežne opreme, praćenjem Wi-Fi signala, upotrebom automatiziranih uređaja za prikupljanje podataka i dr.). Članak 14. se primjenjuje u slučajevima kada voditelj obrade osobne podatke ispitanika prikuplja iz drugih izvora kao što su npr. voditelji obrade podataka neke treće strane, javno dostupnih izvora, drugih ispitanika ili posrednika podataka (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 14-15).

Uvažavajući Članke 13. i 14., ispitanicima je putem izjave o privatnosti potrebno dostaviti sljedeće informacije (GDPR, Članci 13. i 14; Radna skupina za zaštitu podataka iz Članka 29., 2018: str 14-15, 35-40):

- Identitet voditelja obrade kao i informacije o tome kako ga kontaktirati;
- Kontakt podatke službenika za zaštitu podataka;
- Koja je svrha i pravna osnova obrade osobnih podataka (bez obzira jesu li prikupljeni na način da ih ispitanik sam da voditelju obrade podataka ili se oni prikupljaju automatski, zatim putem kamera, praćenjem Wi-Fi signala, putem mrežne opreme, RFID ili drugih senzora ili se prikupljaju iz nekih drugih izvora kao što su treće strane, javno dostupni izvori, posrednici podataka ili od drugih ispitanika);
- Koji su legitimni interesi voditelja obrade ili treće strane kojoj će podaci biti preneseni;

- Koji su primatelji[7] ili kategorije primatelja osobnih podataka;
- Ukoliko podaci nisu dobiveni od ispitanika, koji su izvori osobnih podataka te dolaze li iz javno dostupnih izvora;
- Hoće li podaci biti preneseni trećoj zemlji ili nekoj međunarodnoj organizaciji te koje su zaštitne mjere u tom slučaju kao i kako je moguće dobiti kopiju prenesenih podataka;
- Razdoblje na koje će se podaci čuvati;
- Informacije o pravima pojedinaca koja se odnose na pristup osobnim podacima, ispravak ili brisanje osobnih podataka kao i mogućnost ograničavanja obrade te pravo na prigovor i prenosivost podataka;
- Informacije o pravu povlačenja privole u bilo kojem trenutku ukoliko se obrada temelji na privoli;
- Informacije o pravu podnošenja pritužbe nadzornom tijelu;
- Informacije o tome jesu li osobni podaci nužni i koje su posljedice ukoliko ih pojedinac ne pruži;
- Informacije o tome da postoji automatizirano donošenje odluka (nakon izrade profila pojedinca) te kojom se logikom služe kao i kakve su posljedice takve obrade za pojedinca; te
- Informacije o daljnjoj obradi u neke druge svrhe kao i informacije o kojoj je svrsi te sve druge informacije ovdje navedene.

Poslovni subjekti trebali bi se pridržavati i sedam načela obrade osobnih podataka navedenih u GDPR-u, u Članku 5. (GDPR, Članak 5.; Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 23-24):

1. **Načelo zakonitosti, poštenosti i transparentnosti** - osobni podaci moraju se obrađivati na zakonit, pošten i transparentan način;
2. **Načelo ograničavanja svrhe** - osobni podaci smiju se prikupljati samo u „posebne, izričite i zakonite svrhe“ i smiju se obrađivati samo za tu svrhu, a također se smiju dalje obrađivati[8] za znanstvena i povijesna istraživanja, u svrhu statistike, ali i arhiviranja koje je u javnom interesu. Vezano za ovo načelo, često se mogu u

[7] GDPR, Članak 4., točka 9. definira „primatelja“ kao „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana“.
[8] Informacije vezane za daljnju obradu ispitanici moraju dobiti prije početka takve obrade (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 24).

izjavama o privatnosti vidjeti svrhe kao što je „pružanje usluge i razvoj novih značajki i novih usluga“, a što se prema GDPR-u smatra preopćenitom svrhom (ENISA, str. 17);

3. **Načelo smanjenja količine podataka** - podaci koji se prikupljaju moraju biti „primjereni, relevantni i ograničeni na ono što je nužno“ za svrhu za koju se prikupljaju odnosno obrađuju;
4. **Načelo točnosti** - prikupljeni osobni podaci moraju biti točni i ažurni, a ukoliko nisu točni, potrebno ih je što prije izbrisati ili ispraviti;
5. **Načelo ograničenja pohrane** - osobni podaci smiju se čuvati samo dok traje svrha za koju su prikupljeni u obliku putem kojeg će se moći identificirati pojedinca, a dulje se mogu čuvati ukoliko će se obrađivati u druge svrhe spomenute u stavku 2.;
6. **Načelo cjelovitosti i povjerljivosti** - prilikom obrade osobnih podataka potrebno je osigurati odgovarajuću sigurnost istih; i
7. **Načelo pouzdanosti** - voditelj obrade koji se mora pridržavati ovih načela mora tu usklađenost s načelima moći i dokazati.

Načelo zakonitosti kao prvo načelo obrade osobnih podataka navodi kako je obrada podataka zakonita ukoliko je pojedinac dao privolu za obradu podataka ili je obrada nužna (Radna skupina za zašttu podataka iz Članka 29., 2014: str. 4):

a. U svrhu sklapanja ili izvršavanja ugovora;
b. U svrhu ispunjavanja pravnih obveza voditelja obrade;
c. U svrhu zaštite ključnih interesa ispitanika;
d. U svrhu izvršavanja zadaća od javnog interesa; ili
e. Zbog legitimnih interesa voditelja obrade ili neke treće strane pri čemu je potrebno napraviti test ravnoteže[9]. Međutim, do obrade ne smije doći ukoliko su interesi ili temeljna prava i slobode ispitanika jači od legitimnih interesa voditelja obrade.

U legitimne interese voditelja obrade ubrajaju se slučajevi kada između ispitanika i voditelja obrade postoji neki odnos kao npr. kada je ispitanik klijent voditelja obrade (dakle, potrebno je procijeniti može li ispitanik s obzirom na odnos očekivati obradu podataka u određenu

[9] Potrebno je legitimne interese voditelja obrade ili trećih strana razmotriti nasuprot interesa ili temeljnih prava i sloboda ispitanika te o rezultatu ovisi mogu li legitimni interesi biti pravna osnova za obradu podataka ispitanika (Radna skupina za zaštitu podataka iz Članka 29., 2014: str. 9).

svrhu), zatim zbog sprječavanja prijevara, zbog pružanja sigurnosti mreže ili informacijskog sustava, kao i za potrebe izravnog marketinga (GDPR, Recital 47, Recital 49). Prema Mišljenju Radne skupine za zaštitu podataka iz Članka 29. (2014: str. 18) o legitimnim interesima, izravni marketing može predstavljati legitiman interes ukoliko je opravdanost utvrđena testom ravnoteže, no ukoliko se radi o značajnom profiliranju, dijeljenju podataka, personaliziranom oglašavanju ili izravnom marketingu putem Interneta, potrebna je suglasnost odnosno privola ispitanika. (Radna skupina za zaštitu podataka iz Članka 29., 2014: str. 25-26). Kako pojašnjavaju, prikupljanje podataka o preferencijama korisnika kako bi im kreirali personalizirane ponude i stvarali proizvode i usluge koji će u konačnici biti bolji za korisnika, može biti legitiman interes ukoliko postoje određene zaštite, od kojih je jedna i mogućnost ispitanika da odbije takvo prikupljanje podataka. Međutim, nije dozvoljeno kontinuirano praćenje aktivnosti korisnika, prikupljanje i kombiniranje podataka iz različitih izvora i prikupljenih za druge svrhe kako bi se korisnike profiliralo, a da za to voditelji obrade nisu dobili izričitu informiranu privolu korisnika. U ovom slučaju test ravnoteže išao bi u prilog ispitaniku i njegovim interesima i temeljnim pravima i slobodama (Radna skupina za zaštitu podataka iz Članka 29., 2014: str. 25-26).

3.3. Transparentnost obrade podataka prema GDPR-u

Radna skupina za zaštitu podataka iz Članka 29.[10] je na temelju Opće uredbe o zaštiti podataka 29. studenoga 2017. godine donijela, a 11. travnja 2018. godine revidirala Smjernice o transparentnosti na temelju Uredbe 2016/679[11] (dalje u tekstu: Smjernice o transparentnosti).

Transparentnost se prema GDPR-u smatra obvezatnom i to u trima područjima (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 4):

1. davanje informacija pojedincima, a koje se odnose na poštenu obradu njihovih podataka;
2. način na koji se pojedincima objašnjavaju njihova prava temeljem GDPR-a od strane voditelja obrade podataka; te

[10] Radna skupina osnovana je na temelju Članka 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnost. Njezine su zadaće opisane u Članku 30. Direktive 95/46/EZ i Članku 15. Direktive 2002/58/EZ.

[11] Smjernice o transparentnosti na temelju Uredbe 2016/679 mogu se pronaći na sljedećoj poveznici: https://azop.hr/images/dokumenti/217/smjernice-o-transparentnosti.pdf.

3. način na koji pojedinci mogu ostvariti svoja prava, a što im trebaju omogućiti voditelji obrade podataka.

U Općoj uredbi o zaštiti podataka transparentnost nije definirana, no Poglavlje III. o pravima ispitanika u Članku 12. navodi kako pojedincima jasnim i jednostavnim jezikom treba iskomunicirati kako se njihovi osobni podaci prikupljaju, obrađuju, upotrebljavaju i čuvaju te kako informacije i komunikacije u vezi s obradom podataka trebaju biti lako dostupne i razumljive te pisane jasnim i jednostavnim jezikom (GDPR, Članak 12.). Osim toga, pojedincima bi trebao biti jasan identitet voditelja obrade njihovih podataka te bi trebali biti upoznati s „rizicima, pravilima, zaštitnim mjerama i pravima“ vezano za obradu njihovih podataka. Svrha obrade podataka mora biti jasno naznačena, a razdoblje čuvanja podataka na minimumu, odnosno trebao bi se odrediti neki rok za brisanje podataka ili razdoblja kada će se preispitati jesu li prikupljeni podaci i dalje potrebni. U Smjernicama o transparentnosti se također navodi kako bi pojedinci morali znati koje su posljedice obrade njihovih podataka te da ne bi smjeli biti iznenađeni načinima na koji se njihovi podaci koriste (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 7) kao što je to bio slučaj s Cambridge Analyticom i Facebookom. Također, podaci se ne bi smjeli prikupljati i obrađivati samo u svrhu odgovora na potencijalne zahtjeve (GDPR, Recital 64).

Jednako tako, prije same obrade osobnih podataka pojedinci bi trebali dati svoju privolu i to nekakvom „jasnom potvrdnom radnjom“ kao što je pisana ili usmena izjava, dok u slučaju digitalnih tehnologija, npr. aplikacija, to uključuje i elektroničku pisanu izjavu. Neaktivnost, šutnja ili polje koje je već unaprijed označeno kvačicom ne smatraju se privolom (GDPR, Recital 32). Pojedinac dakle mora biti svjestan da je dao privolu i do koje mjere, a ako pojedinac nema istinski izbor odbiti ili povući privolu, a da to bude bez posljedica, to se ne smatra dobrovoljnim davanjem privole (GDPR, Recital 42).

Smjernice o transparentnosti dodatno pojašnjavaju navedena pravila (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 6-8).

„Sažet i transparentan način“ pružanja informacija znači da pojedincima tj. ispitanicima ne treba davati prekomjerne informacije te da je potrebno koristiti slojevite izjave/obavijesti o privatnosti s poveznicama na različite informacije kako bi na jednostavan način mogli pristupiti odjeljku koji ih zanima, a ne čitati velike količine teksta u jednoj

cjelovitoj obavijesti[12] . Osim toga, izjave o privatnosti bi morale na jasan način biti odijeljene od drugih informacija kao što su uvjeti korištenja[13] ili neke druge informacije koje nisu povezane s privatnošću (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 7).

Pod **„razumljivošću“** se smatra kako bi te informacije trebao moći razumjeti prosječan pripadnik ciljne skupine čiji se osobni podaci namjeravaju prikupljati (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 7). Razumljivost je time vezana za pravilo jasnog i jednostavnog jezika.

„Laka dostupnost“ informacija znači da bi ispitanici trebali moći vrlo lako uočiti informacije/izjavu o privatnosti odnosno poveznicu na te informacije, tj. da te informacije trebaju biti jasno označene ili biti u obliku odgovora na pitanje. Navedene informacije vezane za privatnost ispitanici ne bi trebali biti prisiljeni sami tražiti (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 7-8). U Smjernicama o transparentnosti je posebno navedeno kako bi se te informacije ukoliko se radi o mobilnim aplikacijama trebale moći pronaći u internetskoj trgovini i prije preuzimanja aplikacija, ali i dalje biti lako dostupne unutar aplikacije i to unutar dva „dodira“ odnosno dva „klika“. Osim toga, izjava o privatnosti morala bi se odnositi samo na tu specifičnu mobilnu aplikaciju, a ne općenito na tvrtku koja je vlasnik aplikacije. Radna skupina iz Članka 29. je također preporučila da poveznica na izjavu o privatnosti bude dostupna u trenutku prikupljanja osobnih podataka, (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 8).

„Jasan i jednostavan jezik“ se u Smjernicama objašnjava kao jezik u kojem se izbjegavaju „složene rečenice i jezične strukture“, a informacije su „konkretne i jasne“ što znači da nema dvosmislenosti ili apstraktnih formulacija. Navodi se kako posebno jasno mora biti napisana svrha i pravna osnova obrade osobnih podataka (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 8-9). Osim toga, potrebno je izbjegavati riječi kao što su „neki“, „često“, „može“, „možda“ i slično, pravilno strukturirati odlomke i rečenice, koristiti aktivni oblik i ne koristiti pretjerano legalističke, stručne ili tehničke pojmove (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 9-10). Rječnik, ton i stil jezika koji se

[12] Radna skupina iz Članka 29. smatra kako se i dalje mogu razvijati i primjenjivati druge inovativne metode kojima će se postići transparentnost (Radna skupina za zaštitu podataka iz Članka 29., 2018; str. 19).
[13] Uvjeti korištenja (engl. *Terms and Conditions, Terms of Service, Terms of Use*) su skup pravila, zahtjeva, specifikacija i standarda koji čine sastavni dio nekog ugovora. Za mrežne stranice je to skup pravila koja korisnici moraju prihvatiti kako bi tu stranicu mogli koristiti. Ukoliko se ne nude nikakve usluge niti proizvodi, za web stranice to je često samo Izjava o odricanju od odgovornosti (engl. *Disclaimer*). Uvjeti korištenja pojašnjavaju što tvrtka očekuje od svojih korisnika kao i što korisnici mogu očekivati od tvrtke (TermsFeed, BusinessDictionary i FreePrivacyPolicy).

koriste u izjavama o privatnosti u mobilnim aplikacijama za djecu[14] trebaju biti primjereni uzrastu (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 10).

Izjave o privatnosti moraju biti predočene u pisanom obliku, tj. u elektroničkom obliku ukoliko se radi o mobilnim aplikacijama i to u obliku slojevitih izjava o privatnosti, ali i na jednom mjestu ili u jednom cjelovitom dokumentu kojemu ispitanici mogu lako pristupiti. Osim navedenoga, informacije o transparentnosti ispitanici mogu dobiti i putem drugih elektroničkih sredstava kao što su videozapisi, glasovne obavijesti, nadzorne ploče za privatnost, obavijesti u pravom trenutku[15] (engl. *just-in-time*) i dr. (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 12).

Kako je u Smjernicama o transparentnosti navedeno (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 15), ključan element obveze transparentnosti i poštene obrade podataka je pravodobno pružanje informacija i to „u trenutku prikupljanja osobnih podataka“ ili unutar „razumnog roka“ do mjesec dana ukoliko su osobni podaci dobiveni neizravno (iz javno dostupnih izvora, od trećih strana, od posrednika ili od drugih ispitanika).

Sva navedena načela i pravila trebala bi biti na snazi i prilikom pružanja početne izjave/obavijesti o privatnosti i prilikom svih budućih izmjena iste, a ispitanici bi o bitnim ili materijalnim promjenama trebali biti obaviješteni na pravilan način koji će ispitanici doista i uočiti. Bitnim ili materijalnim promjenama smatraju se promjena svrhe obrade, promjena načina ostvarivanja prava, promjena identiteta voditelja obrade i slično (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 16-17). Ukoliko se radi o velikim promjenama koje imaju značajan utjecaj na ispitanika, ispitanici bi trebali biti upućeni na buduće promjene znatno prije same promjene i to na način koji će ispitanici vidjeti, a kako bi mogli razmotriti navedene promjene i odlučiti slažu li se s takvom obradom njihovih osobnih podataka ili žele povući danu privolu (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 17).

---

[14] Radna skupina za zaštitu podataka iz Članka 29. djetetom smatra osobu mlađu od 18 godina što je u skladu s Konvencijom UN-a o pravima djeteta (Radna skupina za zaštitu podataka iz Članka 29., 2018: str 10).

[15] Obavijesti „u pravom trenutku“ koriste se za posebne informacije vezane za privatnost na način da se pojedini blokovi informacija prikazuju ispitaniku u trenutku kada su njemu relevantne kao što je to npr. slučaj s davanjem adrese prilikom kupnje preko mobilne aplikacije kada u skočnom prozoru može stajati objašnjenje da je taj podatak potreban samo u svrhu kontakta vezano za tu specifičnu kupnju te da će adresa biti dana dostavnoj službi. U nadzornim pločama za privatnost ispitanici mogu u svakom trenutku pročitati informacije vezane za privatnost i upravljati svojim postavkama privatnosti, a informacije o privatnosti mogu biti personalizirane s obzirom na podatke koji se prikupljaju vezano za tog pojedinca (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 20-21).

I Radna skupina za zaštitu podataka iz Članka 29. i američka Savezna trgovinska komisija (FTC) su zaključile kako je upravo transparentnost jedan od glavnih problema kada govorimo o mobilnim uređajima (ENISA, 2017: str. 19; prema Radna skupina za zaštitu podataka iz Članka 29., 2013; prema Federal Trade Commission, 2013).

3.4. Uredba o privatnosti i elektroničkim komunikacijama (*e-Privacy Regulation*)

Donošenje Opće uredbe o zaštiti podataka bilo je dio stvaranja okruženja u kojem se pokušava „povećati povjerenje u digitalne usluge i njihovu sigurnost“ u cilju stvaranja jedinstvenog digitalnog tržišta. U tu svrhu, a kako bi se išlo u korak s tehnološkim[16] i gospodarskim razvojem, najavljeno je i preispitivanje Direktive 2002/58 EZ nazvane „Direktiva o e-privatnosti“ kojom bi se osigurala visoka razina zaštite povjerljivosti osobnih podataka u elektroničkoj komunikaciji i na uređajima (GDPR štiti osobne podatke, a ovom Uredbom štitila bi se povjerljivost komunikacija) (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: str. 2, 5). Stoga su Europski parlament i Vijeće 10. siječnja 2017. godine predložili Uredbu o privatnosti i elektroničkim komunikacijama[17] kraće nazvanu *e-Privacy Regulation*. Uredba je trebala na snagu stupiti u isto vrijeme kada i GDPR, odnosno u svibnju 2018. godine, no Prijedlog Uredbe još je u zakonodavnom postupku u Europskom parlamentu i Vijeću. Prema Uredbi, sva elektronička komunikacija fizičke osobe smatrala bi se osobnim podacima, a zaštitu bi uživala i komunikacija pravnih osoba (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: str. 4, 12). Primjenjivala bi se i na internetske glasovne usluge kao i na usluge slanja poruka putem Interneta (*E-Privacy Factsheet*, svibanj 2018: str. 1). To bi značilo kako mobilne aplikacije ili usluge koje pružaju mogućnost komunikacije na Internetu ne smiju ni na koji način prisluškivati, snimati ili presretati komunikaciju korisnika. Za korištenje bilo kakvih informacija s uređaja kao što su fotografije, kalendar, kontakti i ostalo, ali i postavljanje kolačića prilikom korištenja mrežnih stranica potrebno je zatražiti dopuštenje (*E-Privacy Factsheet*, 2018: str. 2). U tekstu Prijedloga Uredbe stoji kako krajnji korisnici moraju imati

[16] Kako stoji u Recitalu 6 Prijedloga Uredbe, misli se na komunikacijske usluge koje zamjenjuju tradicionalne usluge kao i nove tehnike koje omogućuju praćenje korisnika na Internetu, a koje nisu bile uključene u Direktivu 2002/58 EZ. (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: str. 12).
[17] Puni naziv je Prijedlog Uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ.

veći izbor te da je potrebno centralizirati privolu u samom softveru i ujedno obavijestiti korisnike o postavkama privatnosti tog softvera (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: str. 5).

Anonimizirani osobni podaci nisu obuhvaćeni GDPR-om, ali pseudonimizirani[18] jesu jer se pomoću dodatnih informacija opet mogu povezati s pojedincem pa se tako i dalje smatraju osobnim podacima (ENISA, 2017: str. 15). Dakle, prema načelu povjerljivosti gdje se podaci o komunikaciji smiju otkrivati samo strankama koje u toj komunikaciji sudjeluju, sva sadašnja i buduća sredstva komunikacije bit će obuhvaćena ovom Uredbom, a radi se o aplikacijama za trenutačnu razmjenu poruka, „običnim" i telefonskim pozivima preko Interneta, porukama koje korisnici šalju putem društvenih medija, elektroničkoj pošti i pristupu Internetu (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: Recital 1). Ovime su obuhvaćeni i metapodaci iz elektroničke komunikacije kao što su lokacija, vrijeme, datum poziva, pozivani broj i trajanje poziva, mrežne stranice koje je osoba posjećivala i dr. Jednako tako, Uredbom bi se štitila i komunikacija između uređaja koji čine Internet stvari (IoT) (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: Recital 2, Recital 12). S obzirom da je za obradu podataka iz elektroničke komunikacije potrebna privola, ona „neće biti valjana ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica" (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: Recital 18). Osim toga, s obzirom na učestale obavijesti o kolačićima na svakoj mrežnoj stranici koju ispitanici posjećuju, u Uredbi je predloženo da se već u postavkama aplikacije može urediti davanje privole (Recital 22).

[18] Pseudonimizacija je u GDPR-u definirana kao „obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi. GDPR, Članak 4, stavka 5.

4. Dozvole mobilnih aplikacija u operativnom sustavu Android

Tržište mobilnih aplikacija sastoji se od brojnih malih tvrtki i pojedinaca, a broj aplikacija na tržištu kontinuirano raste. 2008. godine kada su nastali Appleov App Store i Googleov Android Market (sadašnji Google Play), na tržištu se nalazilo oko 60 000 aplikacija. U ožujku 2013. godine, App Store je sadržavao više od 827.000 aplikacija, dok je Android Market sadržavao oko 670 000 aplikacija. Bili su tu i Blackberry, Windows Mobile i Symbian koji su zajedno imali oko 95.000 aplikacija (OECD, 2013: str. 8). Prema stranici statista.com, u lipnju 2019. godine u Google Play trgovini nalazilo se oko 2 700 000 aplikacija, dok je na App Storeu bilo oko 1 960 000 aplikacija (Statista, 2019).

Prema OECD-ovom izvješću iz 2012. godine, u 36 zemalja članica OECD-a[19] među kojima su Sjedinjene Američke Države (SAD), Velika Britanija, Australija, Francuska, Njemačka i druge, prosječan broj aplikacija na mobilnom uređaju je 26 (osim za Švedsku, Švicarsku i Francusku gdje u prosjeku imaju preko 30 aplikacija) dok u Japanu imaju najviše, u prosjeku 41 aplikaciju (OECD, 2013: str. 5). Veliki broj mobilnih aplikacija na uređaju zbog različitih dozvola i prikupljanja velike količine osobnih podataka predstavlja povećani rizik za privatnost korisnika mobilnih uređaja.

Mobilni uređaji su postali naša svakodnevica i nikamo ne idemo bez njih. Koristimo ih za pretraživanje Interneta, video pozive, komunikaciju na društvenim mrežama ili instant poruke, gledanje video sadržaja, fotografiranje, kupnju putem Interneta, Internet bankarstvo, elektroničku poštu i drugo, a sve to nam omogućuju razne mobilne aplikacije. S obzirom na količinu osobnih i privatnih podataka koji se nalaze u našim mobilnim uređajima, postavlja se pitanje tko sve ima pristup tim podacima, u koju svrhu se prikupljaju i koriste li se u neželjene svrhe kao što je to, npr. činila aplikacija „Brightest Flashlight Free“ koja je slala lokaciju i identifikatore uređaja trećim stranama, uključujući oglašivačke mreže (Mangset, 2018: str. 1). Običnom korisniku koji ne posjeduje znanje o tome kako testirati izvorni kod

[19] OECD je kratica za Organizaciju za ekonomsku suradnju i razvoj te ima 36 zemalja članica: Australija, Austrija, Belgija, Kanada, Čile, Češka Republika, Danska, Estonija, Finska, Francuska, Njemačka, Grčka, Mađarska, Island, Irska, Izrael, Italija, Japan, Južna Koreja, Latvija, Litva, Luksemburg, Meksiko, Nizozemska, Novi Zeland, Norveška, Poljska, Portugal, Slovačka Republika, Slovenija, Španjolska, Švedska, Švicarska, Turska, Velika Britanija, Sjedinjene Američke Države.

mobilne aplikacije u biti je gotovo nemoguće saznati što točno aplikacija na njegovom mobilnom uređaju radi, odnosno koje podatke prikuplja.

S obzirom da je udio operativnog sustava Android na tržištu pametnih mobilnih uređaja krajem 2017. godine bio oko 85,9 % (Gartner, Inc., 2018) te da se radi o operativnom sustavu otvorenog koda, lakše je provesti istraživanja nego na Apple iOS-u te će u ovom poglavlju iz tih razloga naglasak biti na dozvole aplikacija na mobilnim uređajima s operativnim sustavom Android. Appleov operativni sustav je krajem 2017. godine imalo 14 % korisnika dok preostalih 0.1 % otpada na ostale operativne sustave (Gartner, Inc., 2018).

4.1. Sustav dozvola

Sve mobilne aplikacije na operativnom sustavu Android pokreću se unutar *sandboxa*[20] te na taj način ne mogu pristupiti drugim resursima na uređaju i ne mogu naštetiti operativnom sustavu. Za pristup resursima i funkcionalnostima uređaja na koji je aplikacija preuzeta koristi se sustav dozvola, a neke od tih dozvola mogu se isključiti u postavkama samog uređaja te aplikacija tu funkcionalnost neće moći koristiti iako joj je dana dozvola (Nacionalni CERT, 2018: str. 7, 8). Lokacija je primjer takve funkcionalnosti i ona se može isključiti općenito za uređaj i za same aplikacije.

Kako je navedeno na Googleovoj mrežnoj stranici posvećenoj razvojnim programerima, svrha dozvola je zaštita korisnika (Android Developers). Svaka Android aplikacija ukoliko želi pristupiti nekim osjetljivim podacima korisnika kao što su kontakti ili SMS poruke ili nekim značajkama uređaja kao što su pristup Internetu ili fotoaparatu, mora zatražiti dopuštenje korisnika (Android Developers). Osobni podaci spremljeni na uređaju su npr. kontakti, popis poziva, SMS poruke i fotografije, a značajke ugrađene u mobilne uređaje pomoću koji se mogu prikupiti razni osobni podaci su fotoaparat, mikrofon, telefon, GPS, žiroskop i tjelesni senzori. Dozvole aplikaciji daju mogućnost pristupa određenim podacima ili joj daju kontrolu nad ranije navedenim značajkama (Alawajy, 2018: str. 10).

Ovisno o tome o kojoj se verziji Android operativnog sustava (OS) radi, traženje dopuštenja odvija se na dva načina. Ukoliko uređaj ima Android 6.0 ili noviji[21] OS, u

[20] *Sandbox* je „virtualno okruženje koje služi kako bi se operacijski sustav i podatke na računalu zaštitilo od zlonamjernih programa, slučajnih izmjena postavki operacijskog sustava ili namjernog nanošenja štete samom operacijskom sustavu.“ (CARNet, 2009, str. 5).
[21] Najnovija verzija je Android 10, izdana 3. 9. 2019. godine.

trenutku preuzimanja aplikacija neće zatražiti nikakve dozvole, već će to učiniti nakon pokretanja aplikacije i to kada joj ta dozvola zatreba. Osim toga, korisnik na svom uređaju u Postavkama može za svaku aplikaciju regulirati dozvole i uključivati i isključivati ih po želji. Ukoliko se radi o operativnom sustavu Android 5.1.1 ili starijem, sustav će automatski prilikom preuzimanja aplikacije pitati korisnika za sve „rizične“ dozvole odjednom. Ukoliko ih korisnik prihvati (ili sve ili ništa), preuzimanje aplikacije će se nastaviti, no ukoliko ih odbije, preuzimanje aplikacije će biti prekinuto (Android Developers – Permissions Overview). Otprilike 25 % korisnika Androida još uvijek ima verzije niže od 6.0 što znači da ne mogu regulirati dozvole aplikacija (Android Developers - Distribution Dashboards).

4.2. Razine dozvola

Na Googleovoj stranici za razvojne programere (Android Developers – Permissions overview) navedeno je kako u operativnom sustavu Android postoje različite vrste tj. razine dozvola pa tako razlikujemo „normalne“, „*signature*“ i „rizične“ dozvole. „Normalne“ (engl. *normal*) dozvole kao što je postavljanje vremenske zone predstavljaju nizak rizik za privatnost korisnika ili operaciju uređaja ili drugih aplikacija i aplikaciji se daju automatski što znači kako za njih nije potrebno dopuštenje korisnika. „*Signature*“ dozvole aplikaciji se daju prilikom preuzimanja aplikacije, ali samo ako ta aplikacija koristi dozvolu koja ima isti certifikat kao i aplikacija koja definira tu dozvolu. „Rizične“ (engl. *dangerous*) dozvole definiraju se kao dozvole koje imaju pristup privatnim informacijama korisnika ili koje bi mogle potencijalno utjecati na pohranjene podatke korisnika ili na funkcioniranje drugih aplikacija. Jedna od takvih dozvola je pristup kontaktima korisnika. Korisnik mora izričito dopustiti aplikaciji korištenje te dozvole, a ukoliko to ne učini, aplikacija ne može pružiti funkcionalnost temeljenu na tom dopuštenju. Postoje još i posebne dozvole koje ne bi trebala koristiti većina aplikacija, a to su SYSTEM_ALERT_WINDOW i WRITE_SETTINGS (Android Developers – Permissions overview).

Android 9.0 Pie ima ukupno 91 dozvolu na tri razine (36 „normalnih“ dozvola, 29 „*signature*“ dozvola i 26 „rizičnih“ dozvola) (Android Developers – Permissions overview). Za usporedbu, Android 4.4 je imao 145 različitih dozvola (Achara et al., 2014: str. 1). S obzirom da na mobilnim uređajima s operativnim sustavom Android 6.0 i novijim korisnici mogu regulirati samo „rizične“ dozvole, ovdje će uglavnom one biti obrađene kao i rizici vezani za njih, ali će biti navedene i određene „normalne“ dozvole (za starije verzije i za Android 9.0) koje predstavljaju rizik za privatnost korisnika. Popis svih dozvola za Android

9.0 Pie može se pronaći na Googleovoj stranici za razvojne programere[22]. Dozvole na toj stranici preuzete su 19. kolovoza 2019. godine i odnose se na operativni sustav Android 9.0 te su na taj način obrađene u ovom diplomskom radu. Potrebno je imati na umu kako su dozvole različite za različite verzije operativnog sustava Android.

4.2.1. „Rizične“ dozvole i povezani rizici

Android 9.0 ima 26 rizičnih dozvola grupiranih u 10 skupina. Davanje pristupa jednoj dozvoli iz skupine automatski odobrava druge dozvole iz skupine ukoliko se npr. aplikacija ažurira i u novoj verziji traži novu dozvolu iz već odobrene skupine dozvola (Weeks, 2018).

U istraživanju koje je Symantec proveo 2018. godine (Cleary, 2018) na 100 najpopularnijih Android i iOS aplikacija ustanovili su kako je pristup fotoaparatu najčešće zatražena rizična dozvola koju je zatražilo 46 % aplikacija na Androidu i 25 % na iOS-u dok je druga najčešća dozvola pristup lokaciji i to kod 45 % aplikacija na Androidu i 25 % na iOS-u. Snimanje zvuka, odnosno pristup mikrofonu zatražilo je 25 % aplikacija na Androidu i 9 % na iOS-u. Čitanje popisa poziva i čitanje SMS poruka na iOS-u nije dopušteno, no na Androidu je to zatražilo 10 % aplikacija za pozive i 15 % za poruke. Osim toga, uočili su i kako iste aplikacije ponekad traže više rizičnih dozvola na Androidu nego na iOS-u (Cleary, 2018). Tablica 4.1 prikazuje „rizične“ dozvole u operativnom sustavu Android 9.0.

22 https://developer.android.com/guide/topics/permissions/overview#permissions_for_optional_hardware_features

Tablica 4.1 Pregled "rizičnih" dozvola u operativnom sustavu Android 9.0. Izvor: Prilagođeno prema Android Developers – Permissions overview

Skupina dozvola	Originalni naziv
CALENDAR / Kalendar	read_calendar
	write_calendar
CALL_LOG / Zapisi poziva	read_call_log
	write_call_log
	process_outgoing_calls
CAMERA / Fotoaparat	Camera
CONTACTS / Kontakti	read_contacts
	write_contacts
	get_accounts
LOCATION / Lokacija	access_fine_location
	access_coarse_location
MICROPHONE / Mikrofon	record_audio
PHONE / Telefon	read_phone_state
	read_phone_numbers
	call phone
	answer phone calls
	add voicemail
	use SIP
SENSORS / Tjelesni senzori	body sensors
SMS	send_sms
	receive SMS
	read SMS
	receive WAP push
	receive MMS
STORAGE / Pohrana	read_external_storage
	write_external_storage

4.2.1.1. Telefon

Ova dozvola služi kako bi aplikacije mogle pozivati brojeve bez toga da idu kroz Birač koji se nalazi na korisničkom sučelju samog uređaja (Saish, 2019). Aplikacije putem ove dozvole imaju uvid u telefonski broj korisnika, podatke o kojoj se mobilnoj mreži radi, uvid u status telefona, mogu pozivati brojeve, vidjeti popis poziva koji ujedno mogu i

mijenjati, mogu dodati glasovnu poštu, koristiti SIP tehnologiju[23] ili preusmjeriti pozive. Status telefona trebaju npr. igrice da mogu staviti igricu u pozadinu ukoliko dolazi telefonski poziv (Hildenbrand, 2017).

Rizik – zlonamjerne aplikacije mogu pozivati brojeve bez znanja korisnika, uključujući i brojeve s dodanom vrijednosti (engl. *premium*) kao što su 060 brojevi (Weeks, 2018), podaci se mogu prodavati, a jednako tako onaj koji prikuplja te podatke može dobiti uvid u socijalnu mrežu korisnika. Osim toga, zlonamjerne aplikacije mogu kontaktima korisnika slati *malware* s korisnikovog telefonskog broja i na taj način uštedjeti novac i prikriti svoj identitet (Cooper, 2018).

4.2.1.2. SMS

Aplikacija može pristupiti porukama na svim aplikacijama koje koriste SMS poruke, može primati, čitati i slati SMS poruke, primati MMS i WAP push poruke (Cooper, 2018). Ovu dozvolu trebaju sve aplikacije koje su predviđene za slanje poruka, dijeljenje medija i slično. Od 8. listopada 2018. godine, Google je ograničio pristup ovoj skupini dozvola samo na predefinirane aplikacije za SMS poruke (Cimpanu, 2018).

Rizik – Postoji mogućnost da zlonamjerne aplikacije čitaju pa čak i mijenjaju sadržaj poruka (Cooper, 2018). Osim toga, aplikacije mogu iskoristiti uređaj korisnika za slanje neželjenih poruka (engl. *spam*) drugima ili za pretplatu na neke usluge (Weeks, 2018). Također mogu pročitati i poruke koje sadrže kodove vezane za Internet bankarstvo i potvrdu transakcije (Drozhzin, 2018).

4.2.1.3. Pohrana

Ovdje se ne radi o micro SD kartici koju korisnik po izboru stavlja u svoj uređaj kako bi proširio memoriju, već je to pohrana samog telefona. Naziv je ostao od ranih dana kada su se podaci sustava još spremali na vanjsku memoriju, a nije mijenjan jer mnoge aplikacije tada ne bi radile (Hildenbrand, 2017). Dakle, aplikacija koja ima pristup ovoj SD kartici može čitati ili dodavati nešto na tu „vanjsku“ pohranu, ali i brisati. Ovu dozvolu trebaju

[23] SIP je kratica od engl. *Session Initiation Protocol*, tehnologiju koja se koristi za glasovne i video pozive putem Interneta (Saish, 2019).

aplikacije koje nešto spremaju na pohranu telefona kao npr. za preuzimanje sadržaja s Interneta ili za spremanje fotografija koje korisnik primi preko društvenih mreža, kao i aplikacije koje služe za obradu fotografija, za izradu audio i video zapisa, za izradu dokumenata i drugo (Trend Micro).

Rizik – zlonamjerne aplikacije mogu čitati, mijenjati ili brisati sadržaj pohrane uređaja, npr. fotografije, video zapise i dr. (Weeks, 2019), pa i podatke koje su ondje spremile druge aplikacije (Saish, 2019), mogu preuzeti fotografije za npr. analizu lica i slično. Jednako tako, mogu pohranu iskoristiti za spremanje kopiranih osobnih podataka prije slanja tih podataka na svoj server (Trend Micro). Osim toga, *ransomware* može kriptirati sve što se nalazi u prostoru za pohranu i zatražiti od korisnika da plati prije nego mu otključa sadržaj (Cooper, 2018).

4.2.1.4. Kontakti

Aplikacije koje koriste ovu dozvolu mogu čitati, kreirati i mijenjati popis kontakata te mogu vidjeti i sve račune koje korisnici imaju na svom uređaju kao što su korisnički računi društvenih mreža (Facebook, Twitter, Instagram). Pristup kontaktima trebaju aplikacije koje šalju poruke bilo kakve vrste, e-mail, trenutne poruke i slično (Hildenbrand, 2017).

Rizik – zlonamjerne aplikacije mogu preuzeti popis kontakata korisnika i zatim im slati razne vrste poruka kao što su *phishing*[24] ili neželjena pošta (engl. *Spam*) (Weeks, 2018). Također mogu steći uvid u socijalnu mrežu korisnika, koliko često nekoga zovu, šalju elektroničku poštu ili na drugi način s nekim komuniciraju (F-Droid). Osim toga, mogu proslijediti ili prodati popis kontakata oglašivačima (Stegner, 2018).

4.2.1.5. Kalendar

Aplikacije s ovom dozvolom mogu čitati, kreirati, mijenjati ili brisati podatke iz kalendara. Pristup kalendaru trebaju aplikacije koje služe za vođenje kalendara, ali i aplikacije koje npr. trebaju dodati neke događaje ili pozivnice u kalendar korisnika kao što to čine aplikacije za društvene mreže (Weeks, 2018).

[24] *Phishing* – „vrsta socijalnog inženjeringa koja se odnosi na prijevare, kojima se služe zlonamjerni korisnici šaljući lažne poruke koristeći pritom postojeće internet servise“ (Nacionalni CERT- Phishing).

Rizik - zlonamjerne aplikacije mogu steći uvid u rutine korisnika, uvid u podatke o tome kada će netko npr. biti odsutan od kuće, mogu obrisati podatke iz kalendara (Weeks, 2018) ili slati događaje iz kalendara drugim korisnicima (AndroidPermissions, 2018).

4.2.1.6. Lokacija

Lokacija se može odrediti na više načina – pomoću GPS-a na uređaju, Wi-Fi mreža, odašiljača mobilnih mreža i dr. Aplikacije koje se temelje na lokaciji često niti ne trebaju preciznu lokaciju koja se određuje putem GPS-a i to s preciznošću od oko 5 m, već je dovoljna i općenita lokacija (ENISA, 2017: str. 52; Van Diggelen, Want i Wang, 2018). Ova dozvola potrebna je aplikacijama koje služe kao karte, za upute do odredišta i slično, zatim aplikacijama koje geotagiraju fotografije kako bi se znala lokacija fotografije ili aplikacijama za kupnju koje će odrediti približnu lokaciju kamo korisniku poslati pošiljku (Weeks, 2018). Razvojnim programerima može služiti za ostvarivanje profita pomoću oglašavanja temeljenog na lokaciji (Trend Micro).

Rizik – zlonamjerne aplikacije mogu pratiti lokaciju korisnika kako bi imale uvid u rutine i aktivnosti korisnika, a neke bi mogle i obavijestiti lopove o tome kada vlasnik nije kod kuće (Weeks, 2018). Aplikacije također na taj način dobivaju uvid u to gdje korisnik živi i radi i kakvim se aktivnostima bavi (Drozhzin, 2018). Osim toga, može se koristiti za napade ili *malware* koji su temeljeni na lokaciji (Trend Micro), a neke mrežne stranice posjetitelje putem određivanja lokacije mogu blokirati jer se ne nalaze u njihovom području djelovanja (Cooper, 2018).

S obzirom da lokacija na brojne načine može ugrožavati privatnost korisnika, bilo bi poželjno omogućiti korisnicima da sami odrede koju razinu preciznosti žele u kojem trenutku na različitim aplikacijama (ENISA, 2017: str. 52).

4.2.1.7. Fotoaparat

Ovu dozvolu trebaju aplikacije koje snimaju fotografije i video zapise.

Rizik – zlonamjerne aplikacije mogu bez znanja korisnika uključiti fotoaparat ili kameru te snimati što se događa. Osim toga, ukoliko aplikacija ima pristup Internetu, može spremiti te fotografije na razna mjesta (Stegner, 2018).

4.2.1.8. Mikrofon

Putem ove dozvole aplikacija može snimati audio zapise, glasovne poruke, a potrebna je i aplikacijama kao što je Shazam koja na temelju audio zapisa korisniku može prikazati o kojoj se pjesmi radi (Weeks, 2018).

Rizik – zlonamjerne aplikacije mogu uključiti mikrofon bez znanja korisnika i snimati njegove razgovore (Weeks, 2018).

4.2.1.9. Tjelesni senzori

Aplikacije s ovom dozvolom imaju pristup raznim podacima s tjelesnih senzora, npr. za praćenje otkucaja srca, a podatke koriste za davanje savjeta o zdravlju, praćenje napretka u vježbanju i slično (Weeks, 2018).

Rizik – zlonamjerne aplikacije mogu pratiti korisnikovo zdravstveno stanje (Weeks, 2018), što se ubraja u posebne kategorije osobnih podataka.

4.2.1.10. Zapisi poziva

Ovu skupinu dozvola kao i SMS skupinu smiju koristiti samo one aplikacije koje su predefinirane za pozive i poruke. Putem ove dozvole aplikacija može dobiti uvid u pozivane brojeve, može dodavati na popis poziva, može preusmjeriti pozive ili ih prekinuti.

Rizik – zlonamjerne aplikacije mogu dobiti uvid u pozivane brojeve, ali i manipulirati pozivima što predstavlja narušavanje privatnosti korisnika.

4.2.2. Rizici vezani za „normalne“ dozvole

Različite „normalne“ dozvole mogu se kombinirati kako bi se identificiralo i pratilo korisnike jer različite aplikacije mogu imati različite razine dozvola, a ponekad mogu komunicirati jedna s drugom (ENISA, 2017: str. 44). Opet je potrebno imati na umu da određene dozvole iz ranijih verzija operativnog sustava Android i dalje postoje iako ih nema u verziji 9.0. Slijedi pregled „normalnih“ dozvola koje također prikupljaju osobne podatke korisnika.

Read phone status and identity (Hildenbrand, 2017). Status telefona trebaju aplikacije kako bi imale informaciju o tome je li korisnik uređaja usred poziva pa npr. igrice mogu otići u pozadinu ukoliko dolazi telefonski poziv. Identitet telefona odnosi se na jedinstvene identifikatore kao što su *DEVICE IDENTIFIER* i IMEI broj. *Device identifier* ne odaje nikakve privatne informacije, samo vrstu uređaja i softvera. Međutim, IMEI broj (*International Mobile Equipment Identity*) služi pružatelju osnovne telekomunikacijske usluge da identificira vlasnika telefona – ime i prezime, adresa ili nešto drugo. Taj broj nije potreban aplikacijama, no korisnik uređaja ne može znati koji od ta dva identifikatora aplikacija traži (Hildenbrand, 2017).

Full Internet access. Ovo dopuštenje omogućuje aplikaciji da se poveže na Internet, a koriste ga razne aplikacije kao što su web preglednici, aplikacije koje služe za komunikaciju, igrice i druge. Zlonamjerne aplikacije mogu preuzeti *malware*, razna ažuriranja i drugo (Trend Micro). Prema Srikaru Reddyju (2018), ovo dopuštenje prvotno je bilo „rizično“, a s verzijom Androida 6.0 prebačeno je u „normalna“ dopuštenja te korisnik mobilnog uređaja nema mogućnost odlučiti može li se neka aplikacija spajati na Internet ili ne, a samim time ne može niti spriječiti pojavljivanje oglasa u toj aplikaciji.

View network state (ACCESS_NETWORK_STATE). Aplikacije imaju uvid u mobilne i Wi-Fi mreže. Aplikacijama ova dozvola služi kako bi preuzele ažuriranja te kako bi se spojile na server ili neku mrežnu stranicu. Koriste ga aplikacije za lokacije, aplikacije za *check-in*, društvene mreže i druge. Zlonamjerne aplikacije se mogu priključiti na mreže bez znanja korisnika i koristiti podatkovni promet i trošiti bateriju, moguće preuzimati *malware* ili slati poruke (Trend Micro).

View Wi-Fi state (ACCESS_WIFI_STATE). Aplikacije imaju uvid u Wi-Fi mreže i na koju je mrežu korisnik priključen. Koriste ga npr. web preglednici i aplikacije za komunikaciju. Putem ove dozvole, aplikacija može prikupiti sljedeće podatke (Achara et al., 2014: str. 2-3): jedinstveni identifikator uređaja; MAC adresu; geolokaciju koja je u urbanim sredinama točna na oko 20 metara (Achara et al., 2014: str. 2; prema LaMarca et al., 2005) ukoliko je ujedno omogućeno i dopuštenje za pristup Internetu, a što je često slučaj; povijest kretanja jer se popis Wi-Fi mreža koji se ažurira svakih 15 sekundi čuva na uređaju, a ujedno se tu nalazi i SSID (engl. *Service Set Identifier* odnosno naziv bežične mreže); socijalne mreže korisnika uspoređujući popise SSID-eva uređaja (Achara et al., 2014: str. 2; prema Cunche, Kaafar i Boreli, 2013); i potencijalno imena institucija, pojedinaca ili lokacija koji se mogu izvući iz SSID-a (Achara et al., 2014: str. 3; prema Lindqvist et al., 2009). U istraživanju

koje su Achara et al. proveli 2014. godine, dakle prije izlaska Androida 6.0 i mogućnosti pojedinačne regulacije dozvola, ustanovljeno je kako je u to vrijeme od 2 700 najpopularnijih aplikacija iz Google Play trgovine njih 41 % koristilo tu dozvolu. Na kraju su analizirali 88 takvih aplikacija i ustanovili kako neke tvrtke na taj način prikupljaju podatke koji mogu identificirati osobe. S obzirom na osobne informacije koje se tim putem prikupljaju, Achara et al. smatraju kako ova dozvola treba biti ubrojana među „rizične“ dozvole (Achara et al., 2014: str. 1). U svom izvješću također navode kako tu dozvolu koristi sve više oglašivačkih biblioteka (Achara et al., 2014: str. 2; prema Book, Pridgen i Wallach, 2013). Pomoću te dozvole moguće je također i ukrasti Wi-Fi lozinke i priključiti se na mrežu (Trend Micro).

Retrieve running apps. Aplikacije mogu vidjeti koje se aplikacije trenutno koriste i koji se procesi odvijaju. Koriste ih aplikacije za prekid zadataka, za praćenje baterije, kao i sigurnosne aplikacije. Zlonamjerne aplikacije mogu na taj način krasti informacije iz ostalih aplikacija koje su trenutno pokrenute, a mogu i ugasiti sigurnosne aplikacije (Trend Micro).

Run at startup. Ova dozvola služi aplikacijama kako bi se mogle pokrenuti čim korisnik uključi svoj uređaj, npr. aplikacije koje prate potrošnju baterije, sigurnosne aplikacije i druge. Zlonamjerne aplikacije ju mogu iskoristiti kako bi se pokretale odmah pri pokretanju uređaja (Trend Micro).

Control vibration. Ova dozvola omogućuje kontrolu vibriranja telefona, a koriste ga razne aplikacije kao što su igrice i aplikacije za komunikaciju. Zlonamjerne aplikacije mogu isključiti vibraciju koja bi korisnika inače obavijestila o korištenju nekih *premium* usluga ili o tome da je stigla poruka s kodom za verifikaciju te na taj način zlonamjerna aplikacija može presresti takve poruke prije nego ih korisnik vidi (Trend Micro).

Prevent device from sleeping (sprječavanje telefona da prijeđe u stanje mirovanja). Ova dozvola omogućuje da se ekran ne zatamni ili da procesor ne prijeđe u stanje mirovanja, a koriste ga aplikacije za igrice, aplikacije za reprodukciju zvuka i slike kao i web preglednici. Zlonamjerne aplikacije mogu ovu dozvolu iskoristiti kako bi spriječile mirovanje uređaja i na taj način omogućile sebi kontinuiran rad u pozadini (Trend Micro).

U istraživanju provedenom na Massachusetts Institute of Technology (MIT) utvrđeno je kako određene „normalne“ dozvole mogu poslužiti za „identifikaciju uređaja, ranjivih aplikacija i lokacije privatnih podataka koji se mogu eksploatirati“ (ENISA, 2017: str. 44; prema Yerukhimovich et al., 2016). ENISA navodi kako su istraživanja pokazala da se problemi s dozvolama javljaju zbog nerazumijevanja istih od strane razvojnih programera

koji kroz neznanje omogućavaju aplikacijama s različitim razinama dozvola međusobnu komunikaciju (ENISA, 2017: str. 44).

4.3. Prikupljanje podataka putem dozvola aplikacija

Razlozi za prikupljanje osobnih podataka o mobilnim uređajima i putem mobilnih aplikacija su višestruki. Tako se podaci prikupljaju zbog mogućnosti analize korištenja aplikacije, zbog dijagnostike i rješavanja problema, za istraživanje i razvoj, ali i u svrhu ostvarivanja profita putem personaliziranog oglašavanja ili prodaje podataka.

Ukoliko je aplikacija besplatna, kao što je to slučaj s većinom aplikacija na Android platformi i 50 % aplikacija na iOS platformi, vlasnik aplikacije, odnosno razvojni programeri ili voditelji obrade neće ostvariti profit pukim preuzimanjem aplikacije od strane korisnika te u svrhu zarade moraju iskoristiti neki od sljedećih poslovnih modela (OECD, 2013: str. 22-23):

- Plaćanje same aplikacije
- Oglašavanje unutar aplikacije
- Kupnje unutar aplikacije
- Freemium (kratica od engl. *Free-to-premium*)
- Promocija proizvoda
- Prodaja podataka prikupljenih putem aplikacije
- Aplikacija je dio neke druge usluge (kao self-care)
- Aplikacija se naplaćuje od trećih strana kroz uslugu koju pruža (npr. Uber, Amazon).

Podacima na mobilnim uređajima moguće je pristupiti kroz sam operativni sustav na uređaju (putem dozvola u postavkama uređaja), kroz interakciju s korisnikom i promatranjem ponašanja korisnika na aplikaciji (ENISA, 2017: str. 18).

Kada govorimo o dozvolama putem samog uređaja, odnosno operativnog sustava, kod preuzimanja aplikacije nisu dana pojašnjenja zašto se pristup tim podacima traži, a pojašnjenja često nema niti u izjavama o privatnosti. Neki senzori ili podaci mogu biti grupirani, a također nije moguće vidjeti koje treće strane odnosno koje funkcionalnosti trećih strana[25] su integrirane u aplikaciju (ENISA, 2017: str. 20) pa ni samim time razdvojiti određene dozvole (ENISA, 2017: str. 18). Ponekad pristup određenim podacima traži upravo

[25] Npr. mjerenja, alati razvojnih programera, oglašavanje.

ta treća strana, a razvojni programeri, tj. voditelji obrade bi trebali zbog obveze transparentnosti iz GDPR-a biti u potpunosti transparentni o tome koje podatke obrađuje treća strana, a što bi trebalo biti na temelju neke pravne osnove (ENISA, 2017: str. 20).

Mobilni uređaji često sadrže podatke i o drugim osobama, kao što su npr. brojevi telefona, fotografije, poruke i dr. pa se javlja problem privole od strane tih osoba. Mnoge aplikacije traže pristup kontaktima pa i SMS porukama od strane korisnika aplikacije, no ti kontakti nisu dali privolu za korištenje njihovih podataka.

Ukoliko se putem aplikacije može pristupiti mrežnim stranicama na Internetu, pojavljuje se i problem postavljanja kolačića od strane administratora mrežnih stranica i od strane voditelja obrade preuzetih aplikacija. Tako je u Prijedlogu Uredbe o privatnosti i elektroničkim komunikacijama navedeno kako će web preglednici i drugi softveri koji omogućuju elektroničku komunikaciju morati integrirati opciju kojom će se moći spriječiti treće strane u postavljanju kolačića na uređaje krajnjih korisnika. Moguće je i kako će prema predefiniranim postavkama takvo prikupljanje podataka od strane trećih strana biti zabranjeno (ENISA, 2017: str. 19).

Vrste dozvola (ENISA, 2017: str. 42-43):

- Statične dozvole – ove dozvole ugrađuje razvojni programer, a korisnik regulira nakon preuzimanja aplikacije;
- Dinamične dozvole – također ih ugrađuje razvojni programer, a reguliraju se tijekom korištenja aplikacije, npr. kada korisnik želi putem aplikacije Viber nekome poslati fotografiju koja je spremljena na njegov uređaj, Viber će u tom trenutku zatražiti pristup korisnikovim fotografijama/medijima/datotekama; i
- Prilagođene dozvole – ovim dozvolama upravljaju razvojni programeri ili različiti timovi u organizaciji u slučajevima kada su jedni ili drugi odgovorni za različite aplikacije koje međusobno komuniciraju ili razmjenjuju podatke, npr. aplikacije istog razvojnog programera ili organizacije.

Dozvole programskih biblioteka trećih strana (engl. *Third-Party Libraries*) – ovim dozvolama upravljaju navedene biblioteke kao što su npr. oglašivačke biblioteke (engl. *Ad libraries*) koje razvojni programeri koriste pri kreiranju aplikacija. S obzirom da u Android operativnom sustavu nije moguće posebno dati dozvole različitim komponentama aplikacije, često se događa da baš zbog tih biblioteka aplikacije zahtijevaju prekomjerne dozvole koje nisu potrebne za osnovnu funkcionalnost aplikacije, a razvojni programeri ponekad čak niti

ne znaju koje sve dozvole treće strane traže, kao ni kako to utječe na privatnost korisnika (ENISA, 2017: str. 43).

Za statične i dinamične dozvole potreban je pristanak korisnika uređaja, dok prilagođene dozvole kao i one programskih biblioteka za oglašavanje ne traže pristanak korisnika za prikupljanje podataka (ENISA, 2017: str. 43). Prema Symantecovom istraživanju, „rizične“ dozvole su u čak 40 % Android mobilnih aplikacija povezane s trećim stranama (prikazuju se oglasi ili poveznice na druge aplikacije), dok je postotak iOS aplikacija povezanih s trećim stranama puno manji, „samo“ 16 % (Cleary, 2018).

Nije u potpunosti jasno koje dozvole su doista potrebne kako bi neka aplikacija pravilno funkcionirala s obzirom da slične aplikacije mogu imati vrlo različit raspon dozvola (OECD, 2013: str. 41).

4.4. Agregiranje rizika za privatnost kroz korištenje mobilnih uređaja i aplikacija

Rizici za korisnika, odnosno za njegovu privatnost i osobne podatke povećani su prilikom korištenja mobilnih uređaja zbog velike količine podataka koje mobilni uređaji sadrže o svojim vlasnicima, zbog različitih vrsta identifikatora, zbog ekosustava mobilnih aplikacija koji je prilično kompleksan, zbog ograničenja razvojnih programera aplikacija kao i zbog brojnih usluga i softvera trećih strana kojima korisnici mobilnih uređaja pristupaju (ENISA, 2017: str. 5).

Rizici koji mogu proizići iz obrade osobnih podataka i osobne elektroničke komunikacije mogu biti fizički, materijalni ili nematerijalni, a tu se ubrajaju (GDPR, Recital 75; Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, str. 11-12):

- Narušavanje privatnosti dobivanjem uvida u privatne živote korisnika
- Diskriminacija
- Krađa identiteta
- Prijevara
- Financijski gubici
- Šteta za ugled osobe o čijoj se komunikaciji radi ili neke druge osobe koja je predmet komunikacije
- Gubitak povjerljivosti osobnih podataka zaštićenih poslovnom tajnom
- Neovlašteni obrnuti postupak pseudonimizacije

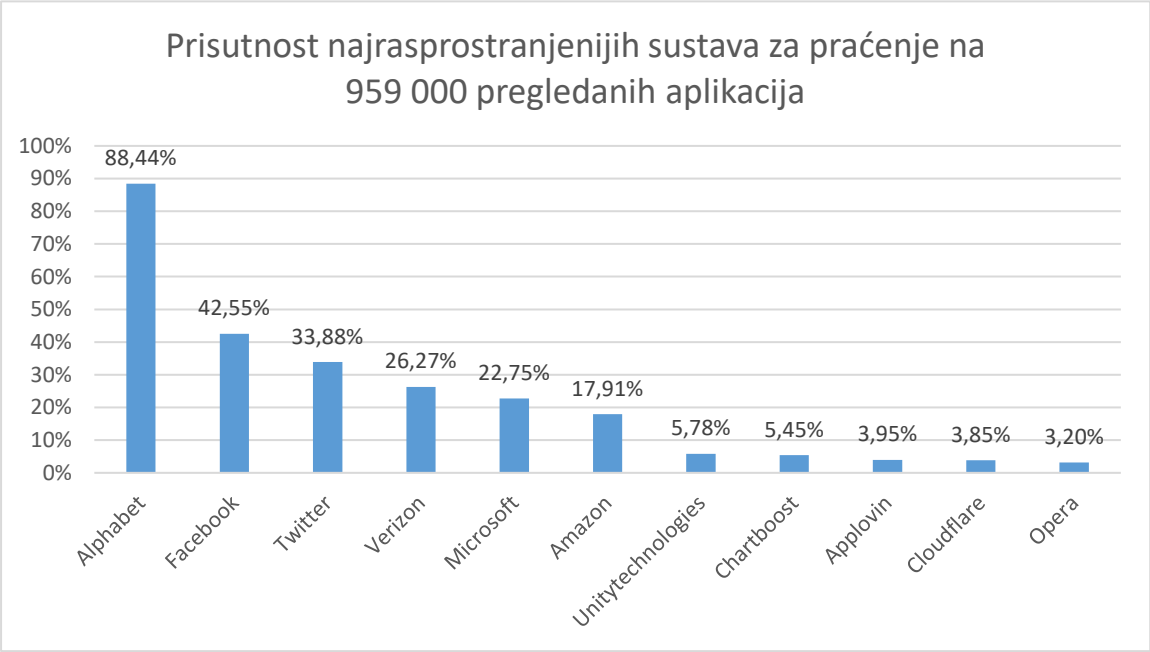
- Neke druge opasnosti - financijske, društvene itd.

Osim toga, Recital 75 GDPR-a kao rizik navodi i situacije gdje ispitanicima mogu biti oduzeta neka prava i slobode, kada nemaju mogućnost kontrole nad svojim osobnim podacima ili kada se njihovi osobni podaci koriste za izradu osobnih profila, ali i korištenje posebnih kategorija podataka, podataka o djeci, zatim korištenje velikih količina podataka ili podataka o velikom broju ispitanika (GDPR, Recital 75).

Podaci prikupljeni putem aplikacija ponekad se prodaju u svrhu personaliziranog oglašavanja, a podatke prodaju razvojni programeri aplikacija, pružatelji platformi ili telekomunikacijske tvrtke. Tvrtke koje kupuju te podatke (npr. Mobclix) na temelju njih izrađuju profile korisnika kako bi mobilno oglašavanje bilo što učinkovitije, a korisnici dobili relevantne informacije (OECD, 2013: str. 25). Poslovni model tvrtki kao što su Google i Facebook je davanje besplatnih usluga korisnicima koji zauzvrat daju pristup svojim osobnim podacima, a na temelju kojih će takve tvrtke oglašivačima moći prodati priliku za oglašavanje i na taj način stvarati profit. Dakle, iako su usluge besplatne kada govorimo o financijskim resursima, ipak ih korisnici na kraju plaćaju svojim podacima i gledanjem oglasa (ACCC, 2019: str. 61). Osim davanja marketinških prilika oglašivačima, rizik predstavlja i dijeljenje podataka s trećim stranama koje su ugrađene u aplikaciju.

Međutim, iznimno je česta i obrnuta situacija gdje aplikacije trećih strana prikupljaju podatke o korisnicima i zatim ih dijele s npr. Googleom i Facebookom (ACCC, 2019: str. 608). Tako je istraživanje Sveučilišta Oxford iz 2018. godine na 959 000 aplikacija na Google Playu ustanovilo kako 88,44 % aplikacija šalje podatke Googleu odnosno njihovoj krovnoj tvrtki Alphabet, 42,55 % Facebooku, 33,88 % Twitteru, a zatim i Verizonu, Microsoftu i Amazonu (26,27 %, 22,75 % i 17,91 %) (Binns et al., 2018: str. 5), a što je prikazano na Slika 4.1. Možemo zaključiti kako Google, Facebook i Twitter prikupljaju značajno više podataka od trećih strana nego ostale tvrtke. Osim toga, ustanovili su kako prema kategoriji aplikacije, najviše sustava za praćenje (engl. *tracker*) imaju aplikacije za djecu i novinski portali, njih sedam (sedam tvrtki u prosjeku dobiva podatke korisnika), dok one iz kategorije igre i zabava u prosjeku imaju šest sustava za praćenje (Binns et al., 2018: str. 6). Prema Recitalu 38 GDPR-a, potrebna je posebna zaštita kada se radi o djeci, a osobito ako se radi o obradi njihovih podataka za profiliranje i marketing.

Pogreška! Izvor reference nije pronađen.



Slika 4.1 Prisutnost najrasprostranjenijih sustava za praćenje na 959 000 pregledanih mobilnih aplikacija. Izvor: prilagođeno prema Binns et al., 2018: str. 5

Osim toga, podaci koji se prikupljaju putem pratilica[26] (engl. *tracker*) se često (od 959 000 aplikacija njih oko 100 000) šalju u različite države s različitim regulativama (Binns et al., 2018: str. 8). Oko 90 % svih analiziranih aplikacija sadržavalo je barem jednu pratilicu tvrtke sa sjedištem u Sjedinjenim Američkim Državama. Nakon toga slijede: Kina u kojoj je sjedište tvrtke barem jedne pratilice u 5,1 % aplikacija; Norveška s 3,2 %; Rusija s 2,6 %, Njemačka s 2,6 %; Singapur s 2.0 %; i Velika Britanija s 1,5 %. Tu su još i Austrija, Južna Koreja i Japan kao sjedišta tvrtki barem jedne pratilice u 0,5 % ili manje aplikacija (Binns et al., 2018: str. 6). S obzirom da se Kina, Rusija, Singapur, Južna Koreja i Japan ne smatraju prikladnima što se tiče razine zaštite osobnih podataka (Binns et al., 2018: str. 7), potrebne su dodatne zaštite kako bi transfer podataka u te države bio legitiman i to u obliku posebnih sporazuma kao što su standardne ugovorne odredbe i obvezujući sporazumi između organizacija u obje jurisdikcije (Binns et al., 2018: str. 3, 7).

[26] Pratilice su male elektronske slike koje se ugrađuju i preuzimaju s mrežnih stranica, aplikacija ili elektroničke pošte koje pružaju informacije o uređaju kao što su IP adresa, URL i drugo (HBO GO).

U GDPR-u u Recitalu 71 navedeno je kako bi ispitanik trebao imati pravo na to da se odluke koje imaju pravne učinke na njega ne donose samo na temelju profiliranja[27], a kao primjeri takvih odluka dani su odbijanje *online* zahtjeva za kreditom ili zapošljavanje gdje se cijeli postupak provodi na Internetu „bez ljudske intervencije“ (GDPR, Recital 71). Međutim, kako navode Binns et al. (2018: str. 7), pratilica pod nazivom DoubleClick koji je prisutan na 60 % od gotovo milijun analiziranih aplikacija, odgovorna je za prikazivanje oglasa za bolje plaćene poslove muškarcima u većem omjeru nego što se isti oglasi prikazuju ženama (Binns et al., 2018: str. 7; prema Datta, Amit, Tschantz, M.C. i Datta, Anupam, 2015). Osim toga, na temelju pratilica česta je i cjenovna diskriminacija (Binns et al., 2018: str. 7; prema Hannak et al., 2014 i Mikians, J., 2012).

Prema istraživanju koje je između kolovoza i prosinca 2018. godine proveo Privacy International na 34 aplikacije koje u Google Play trgovini imaju 10 do 500 milijuna preuzimanja, najmanje 61 % aplikacija je u trenutku pokretanja aplikacije automatski slalo podatke Facebooku bez obzira na to ima li taj korisnik korisnički račun na Facebooku i je li prijavljen na Facebook. Takvo dijeljenje podataka događa se na svim stranicama koje koriste Facebookove poslovne alate (engl. *Facebook Business Tools*) i putem Facebookovog razvojnog programskog okruženja (engl. *Software Development Kit* - SDK) kojeg koriste mobilne aplikacije (Privacy International, 2018a). SDK-evi su alati za razvoj softvera koji pomažu razvojnim programerima u izradi aplikacija za određene operativne sustave (Privacy International, 2018b; str. 3). Za početak, te aplikacije slale su podatak o tome da je aplikacija preuzeta i svaki put kada je pokrenuta. Osim toga, svaki put je poslan i Googleov oglašivački identifikator (AAID) čija je svrha mogućnost povezivanja ponašanja korisnika na različitim aplikacijama i tijekom pretraživanja Interneta u sveobuhvatan profil tog korisnika koji obuhvaća podatke o korisnikovom ponašanju, interesima, aktivnostima, a često i podatke koji se ubrajaju u posebne kategorije osobnih podataka kao što su podaci o zdravstvenom stanju, vjerska i politička opredjeljenja i drugo (Privacy International, 2018b: str. 3-4). Slično istraživanje Mobilsichera je testiralo popularne iOS aplikacije iz App Storea i pronašlo kako i mnoge od njih automatski Facebooku šalju podatke čim se aplikacija pokrene, a veliki broj tih aplikacija prikuplja podatke iz posebne kategorije osobnih podataka kao što su seksualna

[27] „'Izrada profila' se odnosi na svaki oblik automatizirane obrade osobnih podataka kojom se procjenjuju osobni aspekti u vezi s pojedincem, osobito analizu i predviđanje aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja kada ona proizvodi pravne učinke koji se odnose na ispitanika ili na njega snažno utječu.“ (GDPR, Recital 71).

orijentacija, informacije o zdravlju, vjerska uvjerenja i dr. (ACCC, 2019: str. 608-609; prema Ruhenstroth, 2019).

Vrlo je zanimljiva činjenica kako je Privacy International također testirao opcije koje Facebook daje za onemogućavanje prikupljanja kolačića za osobe koje nisu registrirane kao Facebookovi korisnici gdje su pronašli kako te opcije nisu imale značajan utjecan na količinu dijeljenja njihovih podataka s Facebookom (Privacy International, 2018: str. 4).

Kako je navedeno u ENISA-inom izvješću, rizici za privatnost i zaštitu podataka na mobilnim uređajima vezano za mobilne aplikacije proizlaze iz dvije dimenzije od kojih je jedna sama priroda mobilnih aplikacija odnosno činjenica da se radi o softveru na privatnim uređajima, a druga su specifičnosti okruženja u kojem se mobilne aplikacije razvijaju i distribuiraju. **ENISA tako navodi 12 čimbenika rizika** (ENISA, 2017: str. 11-13):

1. **Raznovrsnost podataka i senzora**
    - Razne aplikacije prikupljaju brojne podatke bilo da se radi o kontaktima, fotografijama, podacima o zdravstvenom stanju i dr., a osim toga se koriste raznim senzorima kao što su mjerač brzine, GPS, mikrofon, žiroskop i dr. kako bi prikupili podatke i metapodatke (npr. temperatura, vrijeme, lokacija i datum fotografije i dr.) Pomoću navedenih relativno je jednostavno identificirati korisnika pri čemu su za primjer dali identifikaciju pomoću mjerača brzine i žiroskopa, ali i praćenje na temelju napunjenosti baterije (ENISA, 2017: str. 11-13; prema Gadaleta, M. i Rossi, M., 2016; i prema Vaughan-Nichols, 2016).
2. **Stalna prisutnost mobilnih uređaja**
    - Mobilne uređaje koristimo svakodnevno i u brojnim prilikama pa već nakon kratkog razdoblja korištenja sadrže veliku količinu osobnih i privatnih podataka. ENISA spominje pojam „*liquid surveillance*“ koji označava kontinuirano bilježenje svih pa i najmanjih pojedinosti o našim životima (ENISA, 2017: str. 11-13).
3. **Različite vrste identifikatora**
    - To su ID uređaja, spremljeni dokumenti i njihovi metapodaci (prema Achara et al., 2016), ali i konfiguracijski (ENISA, 2017: str. 11-13; prema Kurtz et al., 2016) i ponašajni otisci (engl. *configuration or behavioural fingerprints*) (ENISA, 2017: str. 11-13; prema Achara et al., 2014; i prema Hilts, Parsons i Knockel, 2016). Prema istraživanju de Montjoye et al. samo četiri prostorno-

vremenske (engl. *spatio-temporal)* točke dovoljne su da se identificira čak 95 % pojedinaca (ENISA, 2017: str. 11-13; prema de Montjoye et al., 2013). Osim toga, bilo koje četiri aplikacije preuzete na mobilni uređaj dovoljne su da se identificira pojedinac s vjerojatnošću od 95 % (ENISA, 2017: str. 11-13; prema Achara, J., Acs, G. i Castellucia, C., 2015). ENISA također navodi kako je vrlo teško, a ponekad i nemoguće resetirati te ponašajne otiske.

4. **Mobilnost i povezanost**
    - S obzirom na ugrađene GPS-ove, praćenje IP adresa, dostupnih mreža i dr., moguće je geolocirati i pratiti mobilne uređaje, a samim time i prikupiti razne osjetljive podatke. Tako npr. ako netko svake nedjelje ide na određenu lokaciju gdje se nalazi katolička crkva može se zaključiti koje je vjere, a što spada u posebne kategorije osobnih podataka. Jednako tako može se pratiti da netko često ide u određenu bolnicu pa je moguće prikupiti osjetljive podatke o zdravlju i slično (ENISA, 2017: str. 11-13; prema Blumberg, A., i Eckersley, P., 2009). Također se pojavljuje i rizik za sigurnost i privatnost zbog mogućeg povezivanja na razne nesigurne mreže, npr. javni Wi-Fi u kafićima, autobusnim postajama, studentskim domovima i slično (ENISA, 2017: str. 11-13; prema Zou, Y., Zhu, J. i Hanzo, L., 2016).
5. **Mogućnost praćenja**
    - Ranije spomenuto fizičko praćenje uređaja može se kombinirati s praćenjem radnji na Internetu te se tako mogu kreirati kompleksniji profili korisnika mobilnih uređaja. Tako postoji i praćenje uređaja gdje treće strane pokušavaju odrediti koji sve uređaji pripadaju korisniku i zatim kombiniraju sve prikupljene podatke (ENISA, 2017: str. 11-13; prema Brookman, J., Rouge, P. i Alva, A.e.a., 2017; prema Mavroudis et al., 2017), ali i praćenje aplikacija gdje jedna aplikacija identificira ili prati ostale preuzete aplikacije na uređajima. Tako su Seneviratne et al. (2014.) prikazali kako se prema preuzetim aplikacijama mogu prikupiti različite informacije o korisniku kao što je status veze, jezici kojima se služi, je li ta osoba roditelj male djece, koje je vjere korisnik i dr. (ENISA, 2017: str. 11-13; prema Seneviratne et al., 2014).
6. **Ograničena fizička sigurnost**
    - Mobilni uređaji su male veličine te ih je lako ukrasti ili razbiti. Osoba koja dođe u posjed uređaja može lako pristupiti podacima na istom.

7. **Ograničena korisnička sučelja**
    - Za razliku od računala, ekrani na mobilnim uređajima su manje veličine i to utječe na privatnost, transparentnost i sigurnost (spominje se istraživanje Melicher et al. (2016) koji su pokazali kako su lozinke na mobilnim uređajima slabije). Zbog veličine ekrana ENISA predlaže korištenje slojevitog pristupa kada se radi o izjavama o privatnosti na mobilnim uređajima s istaknutim najvažnijim točkama (ENISA, 2017: str. 11-13), a što je predloženo i u Smjernicama o transparentnosti (Radna skupina za zaštitu podataka iz Članka 29., 2018: str. 11).
8. **Ograničenja razvojnih programera**
    - Razvojni programeri često imaju ograničeno iskustvo vezano za sigurnost ili privatnost te im je potrebno dati jasnije smjernice o tome kako zahtjeve za većom privatnošću i sigurnošću ugraditi u aplikacije (ENISA, 2017: str. 6).
9. **Korištenje softvera trećih strana**
    - Pri izradi mobilnih aplikacija koriste se različite programske biblioteke (engl. *third-party libraries*“) koje se kombiniraju, a koje izrađuju razne tvrtke različite od samog razvojnog programera. Te biblioteke odnose se npr. na analitiku odnosno praćenje interakcije korisnika s aplikacijom, spajanje na društvene mreže i dr. One također prikupljaju podatke i za sebe i kombiniraju ih s podacima s drugih mobilnih aplikacija (npr. kontakti iz jedne aplikacije i fotografije iz druge aplikacije, a obje aplikacije koriste istu programsku biblioteku) na temelju kojih mogu izrađivati detaljne profile korisnika. Navedene biblioteke često su zatvorene po prirodi i privatne te ih je teško analizirati pa razvojni programeri često niti ne znaju kakve sve podatke korištene biblioteke prikupljaju (ENISA, 2017: str. 11-13).
10. **Trgovine aplikacijama**
    - Trgovine aplikacijama nude ne samo aplikacije, već i razne informacije o aplikacijama, a trebale bi brisati one aplikacije koje predstavljaju sigurnosni rizik za korisnike. ENISA pri tome napominje kako korisnici moguće nemaju dovoljno informacija o potencijalnom prikupljanju osobnih podataka od strane vlasnika trgovine aplikacijama, a koji mogu pratiti kakve aplikacije netko preuzima (ENISA, 2017: str. 11-13).

11. Pohrana u oblaku

- Osobni podaci koje aplikacije prikupljaju često se pohranjuju u oblaku što također predstavlja rizik jer netko može probiti zaštitu i pristupiti osobnim podacima milijuna korisnika (ENISA, 2017: str. 11-13).

12. Društvene mreže

- Dodatnu opasnost za privatnost podataka korisnika predstavlja i mogućnost da će određeni privatni podaci biti vidljivi drugim korisnicima te mreže i kada to korisnik ne želi (ENISA, 2017: str. 11-13).

Kombiniranje podataka predstavlja specifičan rizik zbog stvaranja sveobuhvatnih profila korisnika. Neki od podataka koji se prikupljaju su serijski brojevi uređaja i jedinstveni oglašivački identifikatori. Ovi identifikatori su na samom početku prikupljanja anonimni te za njih nije potrebna privola korisnika, ali moguće ih je kombinirati s prikupljenim osobnim podacima čime i identifikatori prestaju biti anonimni (ACCC, 2019: str. 609; prema Egelman, 2019; prema Ruhenstroth, 2018; prema Whittaker, 2019).

ENISA (2017: str. 28) također navodi i rizik od napada i prikupljanja osobnih i privatnih podataka zbog „*webifikacije*“ (engl. *webification*) kada se mobilna aplikacija integrira sa sadržajem s mrežnih stranica putem tehnologija kao što je *WebView* pa tako napad može doći i od aplikacije i od sadržaja na mrežnoj stranici (npr. maliciozan *JavaScript* koji može povećati razinu dozvola aplikaciji i prikupljati osobne podatke). Jednako tako, rizik predstavljaju i greške koje može napraviti razvojni programer prilikom razvoja aplikacije. Kako navodi ENISA (2017: str. 28), razvojni programeri često imaju problema već s osnovnim funkcionalnostima aplikacija koje izrađuju pa privatnost korisnika odlazi u drugi plan.

Rizik za privatnost predstavlja i mogućnost preuzimanja aplikacija s različitih trgovina koje možda neće provjeriti samu aplikaciju prije njezinog stavljanja u „prodaju“ pa se u njima može nalaziti maliciozan kod koji će npr. prikupljati osobne podatke korisnika i slati skupe SMS poruke (ENISA, 2017: str. 28).

Osim navedenoga, rizik predstavljaju i razne prilagodbe operativnih sustava koje rade tvrtke koje izrađuju mobilne uređaje što rezultira velikim brojem mobilnih aplikacija s previše dozvola, odnosno s velikim pristupom osobnim podacima na mobilnom uređaju, kao i duga razdoblja bez omogućenog ažuriranja operativnih sustava (ENISA, 2017: str. 28).

S obzirom na brojne tehnologije i mogućnosti mobilnih uređaja kao što su bežične mreže, Bluetooth i ostalo, teško je identificirati sve moguće rizike za privatnost. Brojni su i drugi rizici na koje korisnik jednostavno ne može utjecati kao što je prikupljanje podataka od strane pružatelja mrežnih usluga, loša konfiguracija rutera i dr. (ENISA, 2017: str. 30).

Osim toga, poražavajući su rezultati istraživanja na 88 000 Android mobilnih aplikacija koje su proveli Reardon et al., a u kojem su ustanovili kako stotine popularnih aplikacija unatoč tome što nemaju dozvole i dalje prikupljaju osobne podatke korisnika kao što su jedinstveni identifikatori i geolokacija i to tajnim ili zaobilaznim putevima. Tajni način prikupljanja podataka je onaj gdje dvije aplikacije od kojih jedna ima potrebne dozvole, a druga ne, surađuju i dijele podatke. Zaobilazni put je onaj gdje aplikacija bez dopuštenja prikuplja podatke i to je moguće jer se zaobilazni putevi nalaze izvan sigurnosnog mehanizma zbog greške u dizajnu ili načina implementacije dizajna (Reardon et al., 2019: str. 2-3). Primjeri zaobilaznih puteva su korištenje senzora na uređaju kako bi se otkrio spol korisnika ili kako bi se jedinstveno identificiralo korisnika (Reardon et al., 2019: str. 2-3; prema Michalevsky, Boneh i Nakibly, 2014; prema Simon, Xu i Anderson, 2016). Google je najavio kako će taj propust biti popravljen u najnovijoj verziji Androida, Android 10 Q (Ng, 2019).

5. Analiza dozvola i transparentnosti izjava o privatnosti odabranih mobilnih aplikacija

Prvi dio praktičnog rada odnosi se na analizu šest popularnih mobilnih aplikacija različitih proizvođača i namjene i obuhvaća dva područja:

1. **Pregled transparentnosti izjava o privatnosti po pitanju informacija iz Članaka 13. i 14. GDPR-a; te**
2. **Uvid u transparentnost po pitanju prikupljanja osobnih podataka temeljem usporedbe izjava o privatnosti i dozvola aplikacija.**

Aplikacije su odabrane temeljem njihove popularnosti u Republici Hrvatskoj i temeljem okvirnog broja preuzimanja u Google Play trgovini (odabrane su aplikacije s više od 100 000 preuzimanja), a radi se o sljedećim aplikacijama:

1. Otvoreni – zabava/radio
2. Njuškalo – oglasi/prodaja i kupnja
3. PBZ mobilno bankarstvo – financije
4. Moj A1 – korisnička služba
5. Facebook – društvene mreže
6. Gmail – komunikacija.

Analiza je provedena na temelju pronađenih informacija o aplikacijama i pripadajućih izjava o privatnosti putem Google Play trgovine[28] (na dan 2. srpnja 2019. godine) ili na mrežnim stranicama razvojnih programera aplikacija kao i temeljem opažanja prikupljenih nakon preuzimanja navedenih aplikacija[29]. Izjave o privatnosti preuzete su 2. srpnja 2019. godine. Potrebno je napomenuti kako odgovornost za usklađenost s GDPR-om leži na voditelju obrade, odnosno vlasniku aplikacije, a ne na razvojnom programeru koji ju je izradio.

Rezultat analize je pregled transparentnosti i svrhe prikupljanja podataka o korisniku putem odabranih aplikacija te uvid u tražene dozvole i usporedba istih s podacima navedenima u izjavama o privatnosti.

---

[28] Google Play, https://play.google.com/store?hl=hr.
[29] Aplikacije su preuzete na pametni telefon autorice diplomskog rada, a koji sadrži Android operativni sustav 8.0 Oreo.

5.1. Pregled transparentnosti izjava o privatnosti po pitanju informacija iz Članaka 13. i 14. GDPR-a

Sukladno Člancima 13. i 14. Opće uredbe o zaštiti podataka, a kako je navedeno u podpoglavlju 3.2. ovog rada pod nazivom Izjave o privatnosti na str. 10-11, voditelj obrade dužan je u svojoj izjavi o privatnosti navesti 13 vrsta informacija vezanih za prikupljanje i obradu osobnih podataka ispitanika. Za potrebe analize transparentnosti izjava o privatnosti odabranih aplikacija navedenih 13 informacija raščlanjeno je na manje dijelove te su tako određene 22 vrste informacija. Za potrebe analize kreirana je ljestvica (Tablica 5.1) koja će poslužiti kao referenca za uvid u transparentnost pojedinih izjava na način da se nedovoljno transparentnom smatra izjava koja sadrži do 11 zahtijevanih informacija, srednje transparentnom smatra se izjava koja sadrži od 12 do 18 zahtijevanih informacije te se zadovoljavajuće transparentnom smatra ona izjava koja sadrži najmanje 19 od ukupno 22 zahtijevane informacije. Pregled ocjena transparentnosti odabranih aplikacija nalazi se u Tablica 5.3 na str. 70.

Tablica 5.1 Ljestvica transparentnosti izjava o privatnosti

Broj danih informacija (od ukupno 22)	**Ocjena transparentnosti izjave o privatnosti**
0-11	Nedovoljno transparentna
12-18	Srednje transparentna
19-22	Zadovoljavajuće transparentna

Pri analizi transparentnosti u obzir su uzeta pojašnjenja pojedinih vrsta informacija iz Opće uredbe o zaštiti podataka, iz Smjernica o transparentnosti Radne skupine za zaštitu podataka iz Članka 29., kao i iz Mišljenja 06/2014 o legitimnim interesima voditelja obrade[30] iste Radne skupine.

[30] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

Osim toga, razmatrani su i sljedeći dodatni kriteriji (pregled je dan u Tablica 5.4 na str. 71):

1. Traži li aplikacija potvrdnu radnju o čitanju izjave o privatnosti?
2. Traži li aplikacija privolu kojom korisnik potvrđuje da je suglasan s prikupljanjem i obradom podataka kako je navedeno u izjavi o privatnosti? (prema GDPR-u, Recital 32)
3. Nalazi li se izjava o privatnosti u aplikaciji unutar dva „dodira“? (prema Smjernicama o transparentnosti Radne skupine za zaštitu podataka iz Članka 29., str. 8).

Tablica 5.2 na sljedećoj stranici prikazuje koje je informacije (od ukupno 22) u svojoj izjavi o privatnosti pružila svaka od šest odabranih aplikacija.

Tablica 5.2 Pregled pruženih informacija prema Člancima 13.i 14. GDPR-a u izjavama o privatnosti odabranih aplikacija („X“ označava danu informaciju)

R.br.	Zahtijevane informacije prema Člancima 13. i 14.	OTVORENI	NJUŠKALO	PBZ mobilno bankarstvo	Moj A1	Facebook	Gmail
1	Identitet voditelja obrade		X	X	X	X	X
1.a	Kontakt podaci voditelja obrade		X	X	X	X	neizravna poveznica
2	Kontakt podaci službenika za zaštitu podataka		X	X	X	X	neizravna poveznica
3	Svrha i pravna osnova obrade osobnih podataka?	X	X	X	X	X	X
4	Legitimni interesi voditelja obrade ili treće strane?	X	X	X	X	X	X
5	Primatelji ili kategorije primatelja osobnih podataka?		X	X	X	X	X
6	Izvori osobnih podataka (ako ne od ispitanika) te dolaze li iz javno dostupnih izvora?		X	X		X	X
6.a	Hoće li informacije o podacima prikupljenim iz drugih izvora dostaviti u roku propisanom Člankom 14. GDPR-a?			X			
7	Hoće li podaci biti preneseni trećoj zemlji ili nekoj međunarodnoj organizaciji?		X	X	X	X	X
7.a	Koje su zaštitne mjere prilikom prijenosa podataka?		X				izravna poveznica
7.b	Kako je moguće dobiti kopiju prenesenih podataka?						
8	Razdoblje na koje će se podaci čuvati?	Nepotpune informacije	X	X	X	nepotpune informacije, izravne poveznice, potrebno pogledati Uvjete pružanja usluge	izravna poveznica
8.a	Što se događa nakon brisanja korisničkog računa ili prestanka poslovnog odnosa'		X	X	X	u Uvjetima pružanja usluge	X
8.b	Koriste li se prikupljeni podaci nakon brisanja računa u neke druge svrhe kao što su pravne ili transakcijske?		X	x	X	X	X
9	Prava pojedinaca koja se odnose na pristup osobnim podacima, ispravak ili brisanje osobnih podataka kao i mogućnost ograničavanja obrade te pravo na prigovor i prenosivost podataka.		X	X	X	X	nepotpune informacije
10	Pravo povlačenja privole u bilo kojem trenutku		X	X	X	X	X
11	Jesu li osobni podaci nužni i koje su posljedice ukoliko ih pojedinac ne pruži		X	X	X	X	X
12	Izrađuje li voditelj obrade profil ispitanika?	Da, ali nije izrijekom navedeno	X	X	X	Da, ali nije izrijekom navedeno	Da, ali nije izrijekom navedeno
12.a	Postoji li automatizirano donošenje odluka nakon izrade profila i kojom se logikom služe?			X	X		
12.b	Kakve su posljedice takve obrade za pojedinca?			X	X		
13	Informacije o daljnjoj obradi u neke druge svrhe			X		X	X
13.a	O kojoj se daljnjoj svrsi radi?			X		X	X

5.1.1. Otvoreni

Otvoreni je aplikacija hrvatskog Otvorenog radija putem koje korisnici mogu u realnom vremenu slušati Otvoreni radio, pregledavati popis pjesama, pretraživati stihove odabranih pjesama te vidjeti prikaz relevantnih YouTube video zapisa vezanih za odabranu pjesmu. Razvojni programer je hrvatska tvrtka Globaldizajn d.o.o., a aplikaciju je do sada preuzelo preko 100 000 ljudi (Otvoreni, Google Play).

Naziv izjave o privatnosti je *Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir* i sastoji se od 710 riječi što se u prosjeku može pročitati za oko šest minuta (računamo li prosječnu brzinu čitanja od oko 120 riječi u minuti). Poveznica na Opće uvjete zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir nalazi se u trgovini Google Play kao što bi i trebala prema Smjernicama o transparentnosti (Radna skupina za zaštitu podataka, 2018: str. 8), a sama izjava se nalazi na mrežnoj stranici razvojnog programera, odnosno Globaldizajna (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir). Od šest analiziranih aplikacija, jedino Otvoreni ima poveznicu na izjavu o privatnosti koja se odnosi samo na aplikaciju, a ne i na korištenje mrežne stranice Otvorenog radija.

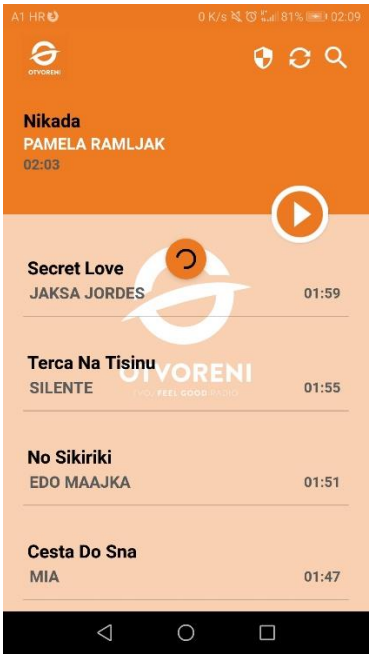
Od 22 zahtijevane vrste informacija prema Člancima 13. i 14. u Općim uvjetima Otvorenog čak 18 vrsta informacija uopće nije navedeno. Tri stavke nisu jasno napisane:

- Svrha i pravna osnova obrade osobnih podataka. Kao svrhu prikupljanja i obrade podataka navode kako će im to omogućiti da „kvalitetnije, preciznije i osobnije“ odaberu „podatke za korisnika, odnosno kako bi poboljšali aplikaciju i njezine sadržaje dodatno usmjerili i prilagodili publici koja ga posjećuje“ (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir). Također navode kako će tako znati koji su sadržaji najpopularniji među određenom publikom. Pravna osnova nije navedena.
- Legitimni interesi. Gore navedeno poboljšanje aplikacije se može smatrati legitimnim interesom.
- Razdoblje na koje će se podaci čuvati. U izjavi se navodi kako će u slučaju poništenja registracije trajno ukloniti osobne podatke unesene prilikom registracije, no nisu naveli što će se dogoditi s ostalim podacima.

Osim toga, Recital 12 GDPR-a nalaže da se ispitanicima pruže informacije o tome izrađuje li voditelj obrade profil ispitanika, a u Općim uvjetima Otvorenog to nije navedeno iako se iz teksta može zaključiti kako profil ipak izrađuju s obzirom da prikupljaju podatke o „preferencijama, hobijima, interesima, aktivnostima“ korisnika (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir).

Prema tekstu navedenom u Općim uvjetima stječe se dojam kako osobnim podacima smatraju samo ime i prezime, OIB, kućnu i e-mail adresu te broj telefona. Kasnije u tekstu navode kako prikupljaju podatke koji se ne smatraju osobnim podacima, a u koje ubrajaju i podatke o mobilnom uređaju i gore navedenim preferencijama i sl. (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir). S obzirom da se prema GDPR-u i neki podaci o mobilnom uređaju smatraju osobnim podacima, njihov navod nije točan. Osim toga, s obzirom da ne navode koje to sve podatke prikupljaju, moguće je da prikupljaju i neke druge osobne podatke.

Nakon preuzimanja aplikacije ne pojavljuju se Opći uvjeti zaštite osobnih podataka. Nakon otvaranja aplikacije vidljiv je glavni ekran s popisom pjesama (Slika 5.1), a odabirom štita u gornjem desnom uglu dolazi se do teksta njihove izjave o privatnosti. Pregledom stavki na ekranu, dolazi se do zaključka kako nigdje nema mogućnosti registracije koja se spominje u izjavi o privatnosti.



Slika 5.1 Prikaz aplikacije Otvoreni nakon preuzimanja i otvaranja. Izvor: aplikacija Otvoreni.

5.1.1.1. Privola i potvrda o čitanju izjave o privatnosti

Aplikacija ne traži potvrdnu radnju o tome da je pročitana izjava o privatnosti te ne traži nikakvu privolu kojom korisnik potvrđuje da je suglasan s prikupljanjem i obradom podataka opisanom u izjavi o privatnosti. Posljednja rečenica je loše konstruirana: „Ti podaci se mobilne aplikacije dajete svoju suglasnost za gore opisani način provođenja analize korištenja ove mobilne aplikacije.“ (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir). Bez obzira na konstrukciju rečenice, može se zaključiti kako samim korištenjem aplikacije korisnik pristaje na obradu svojih osobnih podataka.

5.1.1.2. Transparentnost predočenih informacija

S obzirom na navedeno, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir nisu dovoljno transparentni iz sljedećih razloga:

- Nisu predočene sve potrebne informacije prema Člancima 13. i 14. GDPR-a;
- Netočno su definirani osobni podaci;
- Nije navedeno što se događa s osobnim podacima prikupljenim tijekom korištenja aplikacije, a nakon što korisnik zatraži poništenje svoje registracije;
- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „primjerice“, „može“ i „uključujući“ te se iz toga može zaključiti kako prikupljaju i neke druge podatke koji ovdje nisu navedeni.

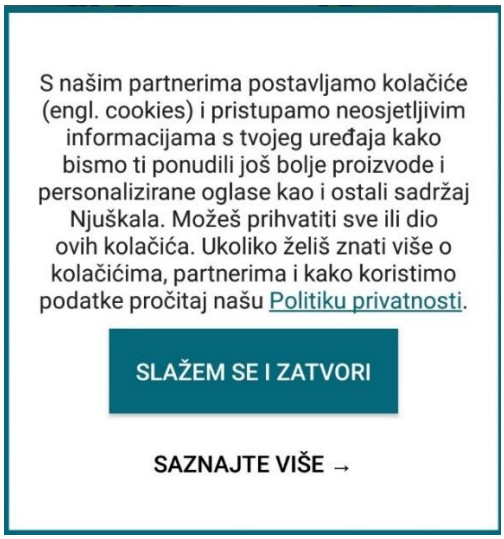
5.1.2. Njuškalo

Njuškalo je mjesto za online trgovanje u Republici Hrvatskoj gdje ljudi objavljuju oglase (sadrži preko milijun oglasa) te prodaju i kupuju razne proizvode i usluge. Sve to može se raditi i u aplikaciji Njuškalo, odnosno mogu se pretraživati i predavati oglasi s fotografijama, može se kontaktirati prodavače i korisničku podršku, uplaćivati sredstva, pregledavati račune i promet i dr. (Njuškalo, Google Play). Razvojni programer je hrvatska tvrtka Undabot, a aplikacija je do sada preuzeta preko 640 000 puta (Njuškalo, Undabot).

Naziv izjave o privatnosti je *Politika privatnosti* (Njuškalo, Politika privatnosti) i sastoji se od 1 934 riječi što se u prosjeku može pročitati za oko 15 do 18 minuta. Poveznica se nalazi unutar Google Play trgovine, dok se tekst nalazi na mrežnoj stranici Njuškala, a ne razvojnog programera kao što je to slučaj s aplikacijom Otvoreni.

Politika privatnosti sadrži većinu potrebnih informacija (16) koje su prilično jasno napisane i dani su primjeri. Problematična je njihova definicija osobnih podataka. U odjeljku „Koje kolačiće i alate koristim?“ navodi se kako alati koji analiziraju korištenje Njuškala „mogu prikupljati“ tehničke podatke kao što su kolačići, IP adresa, identifikator mobilnog uređaja i ostalo, a koji ne identificiraju osobu (Njuškalo, Politika privatnosti). S obzirom da su svi navedeni tehnički podaci osobni podaci prema GDPR-u, ovaj navod nije točan. Jednako tako, navode kako je moguće odbiti ili izbrisati kolačiće te da u tom slučaju korisnik neće moći koristiti neke funkcije aplikacije, no ne navodi se koje.

Nakon preuzimanja i otvaranja aplikacije, pojavljuje se skočni prozor prikazan na Slika 5.2.



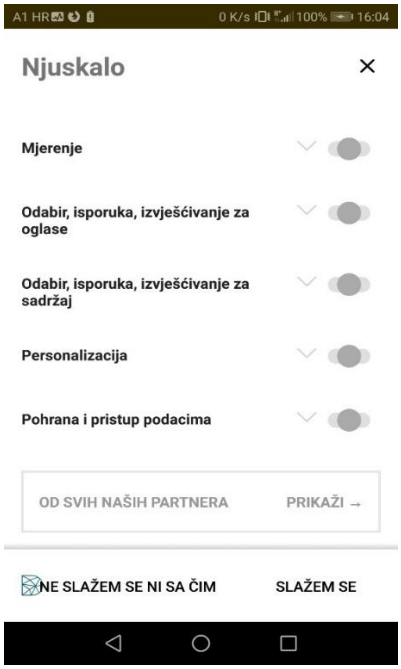
Slika 5.2 Skočni prozor koji se pojavljuje nakon preuzimanja aplikacije Njuškalo. Izvor: aplikacija Njuškalo.

Odabirom „Saznajte više“ korisnik može uključiti ili isključiti sljedeće (Slika 5.3):

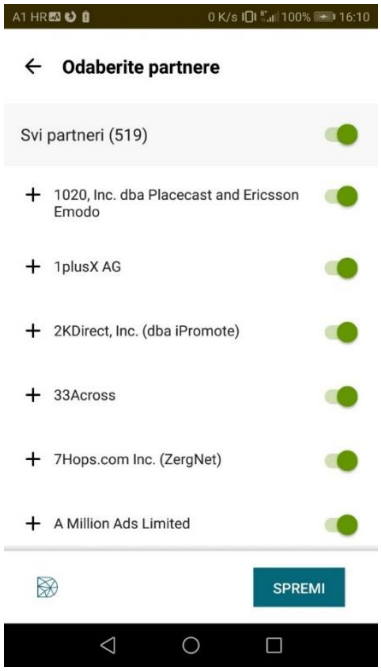
1. Mjerenje
2. Odabir, isporuka, izvješćivanje za oglase
3. Odabir, isporuka, izvješćivanje za sadržaj
4. Personalizacija
5. Pohrana i pristup podacima.

Nakon toga, korisnik može pregledati koji su to partneri koji prikupljaju razne podatke (ima ih 519). Značajno je to da su poveznice na odabir prikaza partnera slabije vidljive od ostatka prozora, korisniku je lako previdjeti tu mogućnost, a k tome su svi partneri

već označeni zelenom bojom, što znači da korisnik ukoliko ne želi da Njuškalovi partneri prikupljaju podatke, mora to prikupljanje aktivno isključiti. Ukoliko isključi pet parametara pod „Saznajte više“, podaci od partnera i dalje su označeni zelenom bojom kao na Slika 5.4.



Slika 5.3 Prikaz mogućnosti uključivanja ili isključivanja prikupljanja podataka od strane aplikacije Njuškalo i Njuškalovih partnera. Izvor: aplikacija Njuškalo.



Slika 5.4 Prikaz mogućnosti uključivanja ili isključivanja prikupljanja podataka od strane aplikacije Njuškalo i Njuškalovih partnera. Izvor: aplikacija Njuškalo.

5.1.2.1. Privola i potvrda o čitanju izjave o privatnosti

Aplikacija ne traži potvrdnu radnju o tome da je pročitana izjava o privatnosti te ne traži nikakvu privolu kojom korisnik potvrđuje da je suglasan s prikupljanjem i obradom podataka opisanom u izjavi o privatnosti. Privola se pojavljuje vezano samo za kolačiće. Problematična je sljedeća rečenica koja se pojavljuje u aplikaciji nakon preuzimanja: „Registracijom ili nastavkom korištenja Njuškala nakon promjene Politike potvrdio si da si upoznat s važećim pravilima i da pristaješ na obradu podataka u navedene svrhe."

5.1.2.2. Transparentnost predočenih informacija

S obzirom na gore navedeno, Politika Privatnosti je srednje transparentna iz sljedećih razloga:

- Nisu predočene sve potrebne informacije prema Člancima 13. i 14. GDPR-a;
- Netočno su definirani osobni podaci;
- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „npr.", „i sl.", „i ostale podatke koje upisuješ", „mogu prikupiti" i dr. te se iz toga može zaključiti kako prikupljaju i neke druge podatke koji ovdje nisu navedeni;
- Ne navode koje funkcije aplikacije korisnik neće moći koristiti ukoliko odbije ili izbriše kolačiće;
- Vezano za dijeljenje podataka navode kako ih dijele i „s korisnicima Interneta i Njuškala", no to nije pobliže pojašnjeno i samim time nije jasno koji su to korisnici Interneta s kojima Njuškalo dijeli podatke svojih korisnika;
- Vezano za dijeljenje podataka s trećim stranama, navedeno je kako se podaci obrađuju i u svrhe usluga koje netko drugi pruža Njuškalu kao što su računovodstvene i IT usluge i slično, no nije navedeno koji se to podaci dijele s trećim stranama i jesu li anonimizirani;
- Odabir „Slažem se i zatvori" vezano za kolačiće je jače istaknut od odabira „Saznajte više";
- Partneri koji prikupljaju podatke, njih 519, su svi predefinirano označeni da mogu prikupljati podatke.

5.1.3. PBZ mobilno bankarstvo

PBZ mobilno bankarstvo je mobilna aplikacija Privredne banke Zagreb koja nudi razne mogućnosti kao što su (PBZ mobilno bankarstvo, Google Play):

- Uvid u stanje financija
- *Push* notifikacije za praćenje transakcija
- Ugovaranje štednje
- Ugovaranje proizvoda i usluga online
- Pronalazak najbližeg bankomata i poslovnice
- Autorizacija transakcija otiskom prsta
- Prebacivanje financijskih sredstava osobama čiji se kontakt podaci nalaze u mobilnom uređaju i dr.

Razvojni programer je Privredna banka Zagreb, a aplikaciju je do sada preuzelo preko 100 000 ljudi (PBZ mobilno bankarstvo, Google Play,). Naziv izjave o privatnosti je *Informacija o obradi osobnih podataka Privredne banke Zagreb d.d. (sukladno člancima 13. i 14. Opće uredbe o zaštiti podataka)* i sastoji se od 10 189 riječi što se u prosjeku može pročitati za oko 85 minuta. Poveznica na istu u trgovini Google Play korisnika vodi na praznu mrežnu stranicu Privredne banke Zagreb[31]. Međutim, na početnoj stranici nalazi se poveznica na *Zaštitu privatnosti* gdje možemo pronaći izjavu o privatnosti u pdf formatu[32].

Od šest analiziranih aplikacija, PBZ mobilno bankarstvo ima najviše zahtijevanih informacija, čak 19 od 22, što je bilo i za pretpostaviti s obzirom da se radi o aplikaciji banke. Nedostaju informacije o zaštitnim mjerama prilikom prijenosa podataka kao i kako je moguće dobiti kopiju istih, a osim toga nije navedeno koji su ostali izvori osobnih podataka (Privredna banka Zagreb, d.d.). Međutim, za sve te informacije navedeno je kako ispitanici mogu zatražiti informacije o prijenosu podataka, a informacije o prikupljanju podataka iz nekih drugih izvora bit će korisniku dostavljene najkasnije u roku od mjesec dana (Privredna banka Zagreb, d.d.: str. 3, 14).

Odmah pri pokretanju preuzete aplikacije, pojavljuje se skočni prozor (za ovu aplikaciju nije moguće snimiti snimku zaslona) u kojem aplikacija traži dozvolu za

[31] https://www.pbz.hr/sites/default/files/dokumenti/2017/zastita_privatnosti.pdf
[32] https://www.pbz.hr/gradjani/zastita-privatnosti.html

uspostavu poziva, a nakon što korisnik odbije dati dozvolu, pojavljuje se obavijest kako se to traži iz sigurnosnih razloga, no ne traži se ponovno dozvola. Zatim se pojavljuje skočni prozor gdje aplikacija traži dozvolu za pristup lokaciji te korisnik može prihvatiti ili odbiti pri čemu može i dalje koristiti aplikaciju (ukoliko odbije, neće moći iskoristiti funkcionalnost koja omogućuje pronalazak bankomata i poslovnica u njegovoj blizini). Ukoliko se korisnik odluči registrirati kako bi mogao iskoristiti sve funkcionalnosti aplikacije, pojavljuje se i skočni prozor vezan za pristup fotoaparatu u trenutku kada korisnik može ručno unijeti QR kod ili ga skenirati.

5.1.3.1. Privola i potvrda o čitanju izjave o privatnosti

U Informaciji o obradi osobnih podataka Privredne banke Zagreb d.d. navedeno je kako ispitanici imaju pravo povući privolu (Privredna banka Zagreb, d.d.: str. 12), no za korisnike aplikacije (s obzirom da se izjava o privatnosti odnosi na sve usluge Privredne banke Zagreb d.d.) nije jasno kada su dali privolu. Niti ova aplikacija ne traži potvrdnu radnju o tome da je pročitana izjava o privatnosti koja se nigdje ne pojavljuje prilikom pokretanja aplikacije. Osim toga, nigdje se ne traži privola kojom korisnik potvrđuje svoju suglasnost s prikupljanjem i obradom navedenih podataka u izjavi. Ukoliko korisnik želi pročitati navedeni dokument, mora se odabirom prozora #withPBZ povezati na mrežnu stranicu Privredne banke Zagreb d.d. gdje će pri dnu stranice pronaći dio o Zaštiti korisnika i poveznicu na Politiku o zaštiti osobnih podataka.

Osim toga, na stranici 12 (Privredna banka Zagreb, d.d.) navedeno je kako privola u slučaju prestanka ugovornog odnosa i dalje vrijedi te ju korisnik može povući kontaktiranjem Banke ili službenika za obradu podataka. Pojašnjenje ove rečenice nije dano.

5.1.3.2. Transparentnost predočenih informacija

S obzirom na navedeno, Informacija o obradi osobnih podataka Privredne banke Zagreb d.d. (sukladno člancima 13. i 14. Opće uredbe o zaštiti podataka) je zadovoljavajuće, ali ne u potpunosti transparentna iz sljedećih razloga:

- Nisu definirali što se smatra osobnim podacima. Ovo nije zahtijevana informacija, no s obzirom da često navode izraz „osobni podaci“ bilo bi ih poželjno definirati;

- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „itd.“, „određene osobne podatke“, „uključivo“ i dr. te se iz toga može zaključiti kako prikupljaju i neke druge podatke koji ovdje nisu navedeni.

5.1.4. Moj A1

Moj A1 je aplikacija A1 Hrvatska d.o.o. telekoma pomoću koje privatni pretplatnici i korisnici bonova mogu provjeriti stanje na računu, trenutnu potrošnju, datum isteka bona, obnoviti račun A1 na bonove i drugo. Razvojni programer je A1, a aplikaciju je do sada preuzelo preko 500 000 ljudi (Moj A1, Google Play). Naziv izjave o privatnosti je *Izjava o zaštiti osobnih podataka za A1 d.o.o.* i sastoji se od 3 221 riječi te se može pročitati za oko 27 minuta.

Odabirom poveznice za izjavu o privatnosti u trgovini Google Play, korisnik se preusmjerava na mrežnu stranicu A1 Hrvatska gdje se nalazi preko 40 uvjeta korištenja za razne njihove usluge[33] te zbog toga korisnik Izjavu mora sam aktivno tražiti, a za što je u Smjernicama o transparentnosti navedeno kako ne bi smio biti slučaj. *Izjava o zaštiti osobnih podataka* u pdf formatu može se pronaći pod „Podrška“ na dnu glavne mrežne stranice A1 Hrvatska[34] i to u dva „dodira“.

Izjava o zaštiti osobnih podataka sadrži 16 od 22 zahtijevane informacije. Nedostaju sljedeće informacije (A1 d.o.o.):

- Koji su izvori podataka ukoliko ne dolaze od ispitanika te dolaze li iz javno dostupnih izvora? Moguće je da ne prikupljaju takve podatke pa iz toga razloga nisu naveli izvore.
- Hoće li informacije o tim podacima biti dostavljene u roku propisanom Člankom 14. GDPR-a?
- Koje su zaštitne mjere prilikom prijenosa podataka i kako je moguće dobiti kopiju istih s obzirom da su naveli kako dolazi do takvog prijenosa podataka?
- Informacije o daljnjoj obradi u neke svrhe i koje su to svrhe.

[33] https://www.a1.hr/uvjeti-koristenja
[34] https://www.a1.hr/podrska

5.1.4.1. Privola i potvrda o čitanju izjave o privatnosti

U tekstu se spominje mogućnost povlačenja privole (A1 d.o.o.: str. 3), no u slučaju aplikacije ona nigdje nije niti zatražena, a nije zatražena niti potvrda o čitanju Izjave o zaštiti osobnih podataka. Jednako tako, ukoliko unutar aplikacije korisnik ode na Postavke pa zatim Uvjete korištenja, poveznica ga vodi na mrežnu stranicu A1 Hrvatska gdje se pojavljuje sljedeći skočni prozor vezan za kolačiće (Slika 5.5):

Slika 5.5 Obavijest o kolačićima nakon povezivanja na mrežnu stranicu A1 Hrvatska iz mobilne aplikacije. Napomena autorice: zelene strelice su naknadno dodane. Izvor: aplikacija Moj A1.

Kao i kod Njuškala, odabir „Pristajem na korištenje kolačića“ je istaknut, dok se poveznice za više informacija i neke druge postavke kolačića niti ne vide. „Više informacija možeš saznati ovdje“ vodi korisnika na mrežnu stranicu gdje se nalazi „Izjava o kolačićima“[35], a ukoliko odabere „Pristajem na korištenje kolačića“, nema dodatnih opcija i korisnik može nastaviti pregledavati mrežnu stranicu.

Osim toga, u Izjavi je navedeno kako postoji „osnovno“ i „bolje“ profiliranje te da je za „osnovno“ profiliranje moguće u svakom trenutku uputiti prigovor. Ovdje je svakako potrebno napomenuti stavku 6.e u kojoj je navedeno sljedeće:

> *Privola koju ste nam dali ili opoziv privole uvijek vrijedi za sve proizvode i usluge koje ste ugovorili. Molimo da ostale korisnike koji se koriste Vašim priključkom ili našim uslugama (npr. zaposlenici ili članovi kućanstva) obavijestite o obradi i prosljeđivanju osobnih podataka u opsegu suglasnosti koju ste nam dali i zatražite i njihovu izričitu suglasnost. Na naš zahtjev dužni ste nam predočiti takvu pismenu suglasnost ostalih korisnika.* (A1 d.o.o.: str. 6).

[35] https://www.a1.hr/uvjeti-koristenja-kolacica

Recital 32 GDPR-a zahtijeva višestruke privole za višestruke svrhe. Osim toga, zahtjev za predočavanjem suglasnosti ukućana ili drugih zaposlenika je jedini takav zahtjev među odabranim aplikacijama, a ta mogućnost nije spomenuta u GDPR-u.

5.1.4.2. Transparentnost predočenih informacija

S obzirom na navedeno, Izjava o zaštiti osobnih podataka je srednje transparentna iz sljedećih razloga:

- Nisu predočene sve potrebne informacije prema Člancima 13. i 14. GDPR-a;
- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „primjerice“, „uključujući“ , „npr.“ i „i slično“ te se iz toga može zaključiti kako prikupljaju i neke druge podatke koji ovdje nisu navedeni;
- Nisu transparentni o tome tko su izvršitelji obrade podataka;
- Nisu u potpunosti transparentni o tome kome prosljeđuju podatke korisnika;
- Odabir „Pristajem na korištenje kolačića“ se čini kao jedini mogući odabir jer se poveznice na riječi „ovdje“ ne vide.

5.1.5. Facebook

Facebook je aplikacija društvene mreže Facebook pomoću koje se korisnici mogu povezati s prijateljima i obitelji koji su također korisnici Facebooka, mogu razmjenjivati poruke, fotografije, audio i video zapise, mogu igrati igrice, kupovati i prodavati na Facebook Marketplace, pratiti razne tvrtke i njihove mrežne stranice, označavati što im se sviđa (popularni „Like“ ili gumbić „Sviđa mi se“) i drugo. Razvojni programer je tvrtka Facebook, a aplikaciju je u cijelom svijetu preuzelo preko milijardu ljudi (Facebook, Google Play).

Naziv izjave o privatnosti je Pravila o upotrebi podataka (engl. *Data Policy*). Hrvatska verzija tih Pravila sadrži 4 296 riječi i u prosjeku ju se može pročitati za oko 36 minuta. Međutim, s obzirom na opseg prikupljanja podataka i necjelovitost informacija u Pravilima o upotrebi podataka (Facebook, Pravila o upotrebi podataka), za bolji uvid u podatke koji se prikupljaju, s kojom svrhom i ostalo poželjno je pročitati i Uvjete pružanja usluge (Facebook, Uvjeti pružanja usluge) i Pravila o upotrebi kolačića (Facebook, Pravila o upotrebi kolačića). Uvjeti pružanja usluge imaju 3 803 riječi i mogu se pročitati za oko 32

minute dok Pravila o upotrebi kolačića imaju 1 541 riječ i mogu se pročitati za oko 13 minuta što bi značilo da je vrijeme čitanja za sva tri dokumenta oko 81 minutu. Nažalost, u slučaju Facebooka brojne potrebne informacije nalaze se na raznim mjestima na njihovim mrežnim stranicama te time niti ova tri dokumenta nisu dovoljna da bi se stekao uvid u sve što bi jedna izjava o privatnosti trebala sadržavati.

Također, potrebno je imati na umu kako se Facebookova Pravila o upotrebi podataka odnose i na ostale njihove proizvode kao što su Facebook Messenger i Instagram, još dvije vrlo popularne aplikacije u svijetu i u Republici Hrvatskoj (Facebook, Pravila o upotrebi podataka). WhatsApp je također jedna od Facebookovih tvrtki, ali ima zasebna Pravila o privatnosti.

Poveznica za pravila o privatnosti u trgovini Google play (bez obzira je li trgovina na hrvatskom ili engleskom jeziku) korisnika vodi na englesku verziju[36] izjave o privatnosti pod nazivom *Data Policy*. Hrvatska verzija može se pronaći putem tražilice ili na glavnoj stranici hrvatske verzije Facebooka[37] pod poveznicom „Privatnost".

Facebookova Pravila o upotrebi podataka sadrže 14 od zahtijevane 22 informacije. Informacije o razdoblju na koje će se podaci čuvati se djelomično nalaze u Uvjetima pružanja usluge gdje se također nalaze i informacije o tome što se događa nakon brisanja korisničkog računa (Facebook, Uvjeti pružanja usluge). Nedostaju sljedeće informacije:

- Hoće li informacije o podacima prikupljenim iz drugih izvora dostaviti korisnicima u propisanom roku u skladu s Člankom 14. GDPR-a?
- Koje su zaštitne mjere prilikom prijenosa podataka te kako je moguće dobiti kopiju istih? i
- Postoji li automatizirano donošenje odluka i kojom se logikom služe kao i kakve su posljedice takve obrade za pojedinca?

Osim toga, nije izrijekom navedeno da voditelj obrade izrađuje profil ispitanika, no to je jasno iz više rečenica u samim Pravilima, kao i u Uvjetima pružanja usluge i Pravilima o upotrebi kolačića. Tako je npr. u Pravilima o upotrebi kolačića navedeno kako pomoću kolačića stječu uvid u to koje osobe upotrebljavaju Facebookove proizvode kao i da na taj način pomažu poduzećima razumjeti skupine ljudi koje koriste njihove aplikacije ili koji su

[36] Facebook, Data Policy, https://www.facebook.com/about/privacy/
[37] https://hr-hr.facebook.com/

stisnuli gumb „Sviđa mi se“ na njihovoj stranici, a kako bi mogli „pružiti relevantniji sadržaj“ (Facebook, Pravila o upotrebi kolačića) što bi značilo personalizirane oglase. Dakle, kolačiće postavljaju na računalo ili uređaj svih osoba koje koriste Facebook ili mrežne stranice Facebookovih partnera i ostalih koji upotrebljavaju Facebookove tehnologije, dakle korisnika i nekorisnika Facebooka. Tako kolačiće koriste kada osoba upotrebljava Facebookove proizvode, proizvode drugih tvrtki u vlasništvu Facebooka ili posjećuje mrežne stranice ili aplikacije gore navedenih, a pri tome prikupljaju podatke o uređaju i aktivnostima na stranici ili u aplikaciji (Facebook, Pravila o upotrebi kolačića).

5.1.5.1. Privola i potvrda o čitanju izjave o privatnosti

U Uvjetima pružanja usluge navedeno je sljedeće:

> *Ne naplaćujemo vam upotrebu Facebooka ili drugih proizvoda i usluga obuhvaćenih ovim Uvjetima. Umjesto toga, poduzeća i organizacije plaćaju nam da vam prikazujemo oglase za njihove proizvode i usluge. Upotrebom naših proizvoda pristajete na to da vam prikazujemo oglase koje smatramo relevantnima za vas i vaše interese. Na temelju vaših osobnih podataka određujemo koje ćemo vam oglase prikazivati… oglašivači nam mogu priopćiti primjerice vrstu publike za koju žele da vidi njihove oglase, a mi prikazujemo te oglase ljudima koje bi oni mogli zanimati.* (Facebook, Uvjeti pružanja usluge)

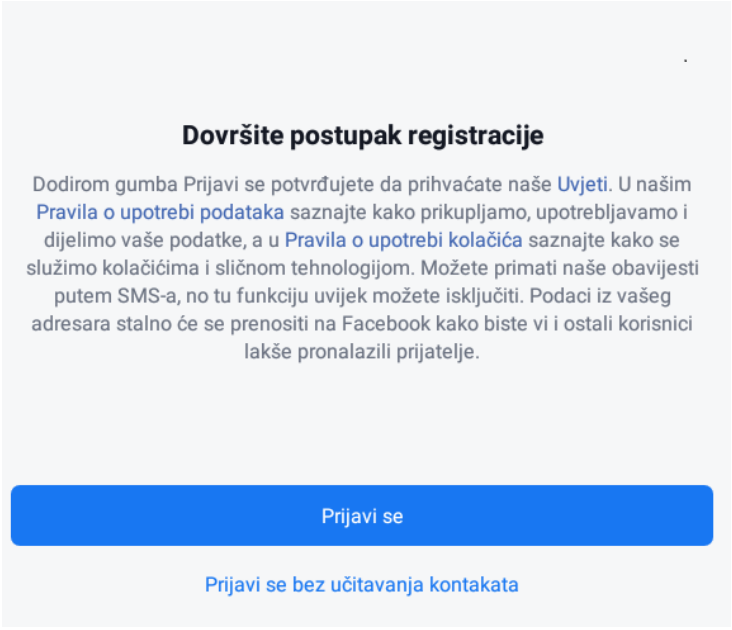
Iz navedenog odlomka vidljivo je kako je Facebook zauzeo pristup „Uzmi ili ostavi“ iako se u postavkama može isključiti prikaz oglasa temeljenih na aktivnostima unutar Facebookovih tvrtki i poduzeća, u vezi s drugim poduzećima i dr. S obzirom da je Facebookov poslovni model takav da ostvaruju prihode na temelju omogućavanja prikaza personaliziranih oglasa od strane oglašivača Facebookovim korisnicima, neka vrsta oglasa će uvijek biti prisutna.

Odmah po preuzimanju, aplikacija traži pristup kontaktima i uspostavljanju i upravljanju telefonskim pozivima. Nakon davanja potrebnih osobnih podataka (ime i prezime, datum rođenja, spol i e-mail adresa ili telefonski broj), korisnik se može registrirati na dva načina, jedan s učitavanjem kontakata iz mobilnog uređaja i jedan bez učitavanja kontakata (Slika 5.6). Kao i u aplikacijama Njuškalo i Moj A1, odabir koji aplikaciji omogućuje veći pristup podacima je jače istaknut.

Facebook kao ni prethodne analizirane aplikacije ne traži potvrdnu radnju o tome da je pročitana izjava o privatnosti i nema mogućnosti davanja privole za prikupljanje i obradu

podataka, već odabirom gumba „Prijavi se“ korisnik u biti prihvaća Uvjete korištenja Facebooka. Pravila o upotrebi podataka i Pravila o upotrebi kolačića spominju se samo kao izvor informacija. Ovakva vrsta formularnog ugovora u elektroničkom obliku naziva se *click wrap* ugovor.[38] Korisnike se traži da pristanu na prikupljanje podataka bez da doista razumiju kakvi se podaci prikupljaju i u kakve svrhe.

Također, već na tom ekranu prilikom registracije problematična je rečenica gdje navode kako će se podaci iz adresara korisnika kontinuirano prenositi na Facebook zbog lakšeg pronalaženja prijatelja. Ovdje se radi o podacima svih kontakata korisnika koji se, dakako, ubrajaju u osobne podatke, a za što bi, ukoliko doslovno čitamo GDPR, Facebooku pak trebala privola svakog od tih korisnika.



Slika 5.6 Prikaz ekrana prilikom registracije aplikacije Facebook. Izvor: aplikacija Facebook.

5.1.5.2. Transparentnost predočenih informacija

U Pravilima o upotrebi podataka navode se brojni podaci koje Facebook prikuplja, no kako bi korisnik shvatio koji su to podaci i kako to utječe na njihovu privatnost, poželjno je poznavati određene termine i tehnologije kao što su pikseli, pratilice i dr. (Facebook, Pravila o upotrebi podataka). Međutim, ni tada nije potpuno jasno što se sve prikuplja i na

[38] *Click wrap* ugovor je vrsta ugovora koja se sklapa na mrežnim stranicama u elektroničkom obliku gdje korisnik, tj. ponuđeni u potpunosti prihvaća ponudu ponuditelja, u ovom slučaju Facebooka, uz uvjet da je kupac pregledao tekst ugovora, iako ga ne mora pročitati da bi ga prihvatio (Matić, 2008: str. 1).

koji način, a shvaćanje istog je otežano zbog brojnih poveznica na kojima se nalaze razne informacije, ali i zbog toga što često poveznice ne vode tamo gdje bi trebale. Teško je pratiti dane informacije i snaći se u raznim postavkama i skrivenim lokacijama informacija. Facebookova Pravila o upotrebi podataka sadrže preko 70 poveznica koje vode na različite lokacije informacija kao što je stranica Centra za pomoć[39], definicije pojmova iz Pravila i drugo. Na primjer, odlaskom na poveznicu koja se tiče softvera za prepoznavanje lica[40] (Facebook Help Center, What is the face recognition setting on Facebook and how does it work?) nailazite na poveznicu[41] (Facebook Help Center, How does automatic alt text work?) koja se tiče davanja glasovnih objašnjenja za razne sadržaje koje kreirate, a koja služe slabovidnim i slijepim osobama kako bi znale što se na nekoj fotografiji ili video zapisu nalazi i za to se upotrebljava strojno učenje. Međutim, na toj poveznici saznajete da se ne radi samo o prepoznavanju lica, već i raznih objekata.

Osim mnogih navedenih podataka, jasno je kako prikupljaju i brojne druge podatke koji nisu navedeni. Jednako tako, spominju osobne podatke i podatke pomoću kojih je moguće nekoga identificirati gdje za primjer navode samo ime i e-mail adresu, no brojni drugi navedeni podaci prema GDPR-u također se ubrajaju u osobne podatke. Osim toga, spominju da postoje posebne kategorije podataka koje korisnik može odabrati pružiti te da podliježu posebnoj zaštiti temeljem prava Europske unije, no u profilu Facebook otvoreno traži te podatke i ondje ne naglašava kako se radi o podacima koji zahtijevaju posebnu zaštitu.

Među ostalim, spominju se i partneri za mjerenja s kojima Facebook dijeli podatke u svrhu pružanja analitičkih i mjernih izvješća Facebookovim partnerima, no ne pružaju nikakvo objašnjenje (Facebook, Pravila o upotrebi podataka).

Nakon brojnih kritika tijekom godina, Facebook je odlučio poboljšati i pojačati kontrole vezane za privatnost i sigurnost te se time daje privid kako korisnik doista ima kontrolu nad svojim osobnim podacima i svim sadržajem koji kreira i dijeli na Facebooku, no ta kontrola odnosi se samo na to tko će podatke s nečijeg korisničkog računa moći vidjeti, ali ne i hoće li ih Facebook prikupljati.

---

[39] https://en-gb.facebook.com/help/
[40] https://www.facebook.com/help/122175507864081
[41] https://www.facebook.com/help/216219865403298?helpref=faq_content

Osim što sadrži preko 5 000 riječi, sadrži i puno poveznica na kojima možete pronaći dodatna objašnjenja, no koja ponekad nisu dovoljno jasna te nemate cjelokupnu i jasnu sliku o tome koji se podaci prikupljaju, na koji način i kako se točno koriste. Moguće je da je razlog poveznicama taj da izjava o privatnosti odnosno Pravila o upotrebi podataka ne budu preduga i još kompliciranija, no moguće je i kako je razlog taj da zbuni i umori korisnika kako ne bi ulazio u razne postavke na Facebooku i regulirao dopuštenja koja može regulirati, odnosno za što svojim postupcima daje privolu (Facebook, Pravna osnova):

- dopuštenje za korištenje tehnologije prepoznavanja lica pomoću strojnog učenja;
- dopuštenje za obradu posebnih kategorija osobnih podataka, a koje korisnik navodi u svom profilu ukoliko to želi i time daje privolu;
- dopuštenje za korištenje podataka koje oglašivači i drugi partneri pružaju Facebooku;
- dopuštenje za dijeljenje podataka koji mogu identificirati osobu;
- dopuštenje za prikupljanje podataka putem raznih uređaja kao što su GPS za određivanje lokacije, kamera, fotografije i dr.; i
- dopuštenje za korištenje lokacije i pozadinske lokacije na razne načine (Facebook Help Center, How do Facebook's Location Settings Work?).

Slijedom navedenoga, Facebookova Pravila o upotrebi podataka su srednje transparentna iz sljedećih razloga:

- Nisu predočene sve potrebne informacije prema Člancima 13. i 14. GDPR-a;
- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „može uključivati“, „npr.“, primjerice“, „može“ i dr. te se iz toga može zaključiti kako prikupljaju i mnoge druge podatke koji ovdje nisu navedeni;
- Pravila o upotrebi podataka i Uvjeti pružanja usluge čitatelja pogrešno navode na zaključak kako su podaci koji ga osobno identificiraju samo podaci kao što su ime, adresa elekroničke pošte ili drugi kontakt podaci.

5.1.6. Gmail

Gmail je aplikacija istoimene usluge Googleove elektroničke pošte. Funkcionira jednako kao i online verzija Gmaila. Razvojni programer je Google, a aplikacija je do sada preuzeta preko pet milijardi puta (Gmail, Google Play). Naziv izjave o privatnosti je Googleova Pravila o privatnosti. Kao i kod Facebookovih proizvoda, s obzirom da je Gmail

Googleov proizvod, na njega se primjenjuju Googleova Pravila o privatnosti koja se primjenjuju i na web preglednik Google Chrome[42], YouTube i druge Googleove proizvode, ali i na sve Android uređaje.

Googleova Pravila o privatnosti sadrže 4 316 riječi te se mogu pročitati za oko 36 minuta. Ukoliko pročitate i sve skočne prozore kada kliknete na određene poveznice, broj riječi penje se na preko 6 800 riječi što zahtijeva oko 57 minuta čitanja. Međutim, kako bi se stvorila bolja slika, poželjno je pročitati i Uvjete pružanja usluge (Googleovi uvjeti pružanja usluge) kao i dio koji se odnosi na tehnologije koje Google koristi pod nazivom Tehnologije (Google, Tehnologije), a sve zajedno može se naći pod Privatnost i uvjeti (Google, Privatnost i uvjeti). Uvjeti pružanja usluge imaju 1 912 riječi, dok Tehnologije imaju 6 816 riječi. Ta dva dokumenta mogu se pročitati za oko 73 minute što znači da je za čitanje svih dokumenata potrebno preko dva sata.

Poveznica na izjavu o privatnosti za Gmail iz trgovine Google Play korisnika vodi do Googleovih pravila o privatnosti. Pravila o privatnosti sadržavaju 12 od zahtijevane 22 informacije. Za dvije informacije postoji izravna poveznica (zaštitne mjere prilikom prijenosa podataka i razdoblje na koje će se podaci čuvati) dok će kontakt podatke voditelja obrade i službenika za zaštitu podataka korisnik morati potražiti putem poveznice koja za početak vodi na obrazac za različite upite te se tek u trećem koraku dolazi do poveznice za službenika za zaštitu podataka i za voditelja obrade, Google Ireland Limited.[43]

Osim navedenoga, prava ispitanika prema GDPR-u su u Pravilima o privatnosti (Googleova pravila o privatnosti) samo spomenuta, dok je njihovo ostvarivanje moguće putem Google korisničkog računa. Iako se ovdje radi analiza aplikacije koju vlasnik Androida već posjeduje i morao je izraditi Gmail korisnički račun kako bi koristio svoj Android uređaj, postavlja se pitanje kako ta prava mogu ostvariti ispitanici koji koriste Googleove proizvode, a nemaju Gmail korisnički račun s obzirom da Google kao i Facebook prikuplja podatke o korisnicima svih stranica koje koriste Googleove tehnologije i alate. U Pravilima o privatnosti ta informacija nije navedena.

Jednako tako, profiliranje nije izrijekom navedeno, ali je na temelju svega navedenog lako zaključiti kako profiliraju sve korisnike imali oni korisnički račun ili ne jer se i njihov

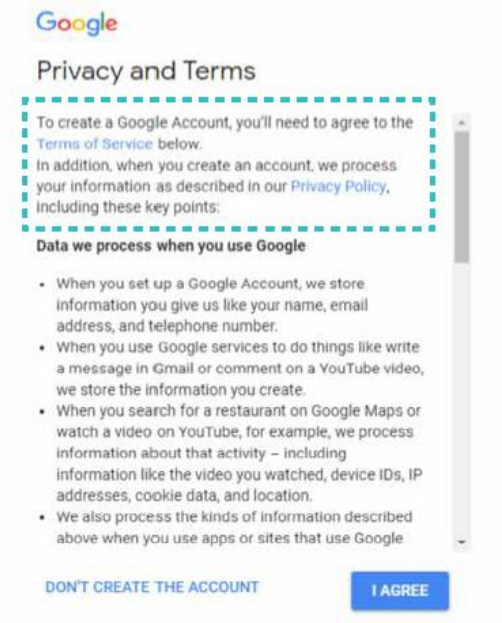
---

[42] Za Google Chrome postoje još dodatna pravila koja se mogu pronaći na sljedećoj poveznici: https://www.google.com/chrome/intl/hr/privacy.html.
[43] https://support.google.com/policies/troubleshooter/7575787#ts=7588508%2C9007816

poslovni model kao i kod Facebooka temelji na pružanju prostora oglašivačima koji će uz Googleovu pomoć korisnicima moći pružati personalizirane oglase (Google Safety Center).

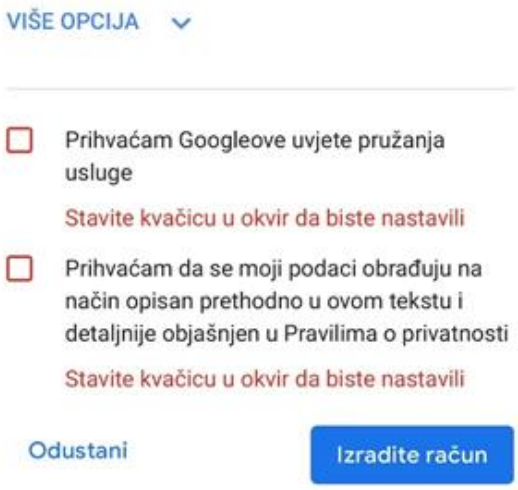
5.2.6.1. Privola i potvrda o čitanju izjave o privatnosti

S obzirom da se radi o aplikaciji koja dolazi s Android uređajima te ju nije moguće izbrisati, nije bilo moguće iznova preuzeti aplikaciju iz trgovine Google Play. No postupak je gotovo jednak kreiranju novog korisničkog računa za Gmail. Gmail je od odabranih aplikacija jedini koji traži svjesnu privolu za obradu podataka kako je navedeno u Pravilima o privatnosti, a sažetak kojih se pojavljuje prilikom izrade korisničkog računa. Opcije koje korisnik ima su odabrati prihvaća li Googleove uvjete pružanja usluge te odabrati prihvaća li obradu podataka kako je objašnjeno u Pravilima o privatnosti (Slika 5.8). Ukoliko odabere „Izradi račun“ bez označavanja ta dva prazna polja kvačicom, dobit će upozorbu (Slika 5.9) kako mora prihvatiti Uvjete pružanja usluge i pristati na obradu podataka. Prilikom kreiranja korisničkog računa nije zatražena potvrda o čitanju Pravila o privatnosti, već samo potvrda da korisnik prihvaća da se njegovi podaci obrađuju na način kako je opisano u Pravilima o privatnosti i kako je sažeto u skočnom prozoru (Slika 5.7). Google kao i Facebook ovdje koristi *click wrap* ugovor.



Slika 5.7 Prikaz sažetka Googleovih pravila o privatnosti koji se pojavljuje prilikom kreiranja korisničkog računa. Izvor: Gmail – Izradite račun

Slika 5.8 Ponuđene opcije prilikom kreiranja Gmail korisničkog računa. Izvor: Gmail – Izradite račun



Slika 5.9 Nije moguće izraditi račun bez prihvaćanja uvjeta pružanja usluge i pristanka na obradu podataka. Izvor: Gmail – Izradite račun

Nakon označavanja polja kvačicom, pojavi se skočni prozor u kojem Google želi potvrditi da korisnik pristaje na sve navedeno i nudi mu mogućnost „Više opcija“. Ukoliko korisnik odabere te opcije, dolazi na stranicu gdje su ponuđene sljedeće mogućnosti davanja ili uskraćivanja privole:

- Spremanje korisnikove aktivnosti na webu i u aplikacijama – označeno potvrdno, korisnik može isključiti;
- Prilagodba oglasa – označeno potvrdno, korisnik može isključiti;
- Povijest pretraživanja na YouTubeu – označeno potvrdno, korisnik može isključiti;
- Povijest gledanja na YouTubeu - označeno potvrdno, korisnik može isključiti;

- Povijest lokacija – isključeno, korisnik može uključiti;
- Glasovne i audioaktivnosti – isključeno, korisnik može uključiti.

Pretpostavka je kako Google smatra da korisnici praćenje lokacija i snimanje glasovnih i audioaktivnosti smatraju previše invazivnim za svoju privatnost pa su te dvije opcije predefinirano isključene za razliku od ostale tri opcije.

Nakon odabira opcija potrebno je ponovno označiti da korisnik prihvaća uvjete pružanja usluge i obradu podataka. Na ovaj način Google se osigurao da je korisnik svjesno dao svoju privolu iako nije zatražio potvrdnu radnju kojom bi korisnik potvrdio kako je pročitao Pravila o privatnosti gdje bi saznao kakvi se sve podaci prikupljaju i u koje svrhe.

5.2.6.2. Transparentnost predočenih informacija

Kako je navedeno u dokumentu o tehnologijama (Google, Tehnologije), čak i kada je prilagodba oglasa isključena, oglasi će biti prilagođeni prema IP adresi (općenitoj lokaciji), modelu uređaja, senzorima uređaja, temama mrežnih stranica ili aplikacija koje korisnik gleda ili pojmovima koje korisnik pretražuje u web tražilici. Navode kako se u tom slučaju oglasi neće temeljiti na interesima, povijesti pretraživanja ili pregledavanja što je nejasno jer se prema pojmovima, lokaciji i temama mrežnih stranica koje korisnik pregledava također može dobiti uvid u interese korisnika. Samim time nije jasno što je korisnik postigao isključivanjem prilagodbe oglasa.

Za razliku od Facebooka, barem načelno, Googleove postavke privatnosti se odnose na sam Google i korisnik određuje koje podatke Google može prikupljati i kako ih može upotrebljavati. Jednako tako, iako znatno dulja od Facebookovih Pravila o upotrebi podataka, Googleova Pravila o privatnosti puno su bolje posložena jer poveznice vode na skočne prozore i izravno na mrežne stranice gdje se korisniku dodatno pojašnjavaju određeni pojmovi te je puno lakše steći uvid u sve potrebne informacije.

S obzirom na navedeno, Googleova pravila o privatnosti su srednje transparentna iz sljedećih razloga:

- Nisu predočene sve potrebne informacije prema Člancima 13. i 14. GDPR-a;
- Nejasno je što smatraju osobnim podacima jer napominju kako s oglašivačima ne dijele podatke koji bi ih mogli identificirati gdje za primjer navode ime i adresu elekroničke pošte;

- Prilikom navođenja podataka koje prikupljaju koriste izraze kao što su „uključujući“ i „kao što su“ te se iz toga može zaključiti kako prikupljaju i neke druge podatke koji ovdje nisu navedeni;
- Nejasno je iz kojih javno dostupnih izvora prikupljaju podatke;
- Nejasno je kakve podatke primaju od oglašivača za usluge istraživanja.

U Tablica 5.3 predočen je rezultat analize odabranih aplikacija po pitanju transparentnosti, a prema ljestvici transparentnosti iz Tablica 5.1 na str. 43.

Tablica 5.3 Ocjena transparentnosti izjava o privatnosti odabranih aplikacija

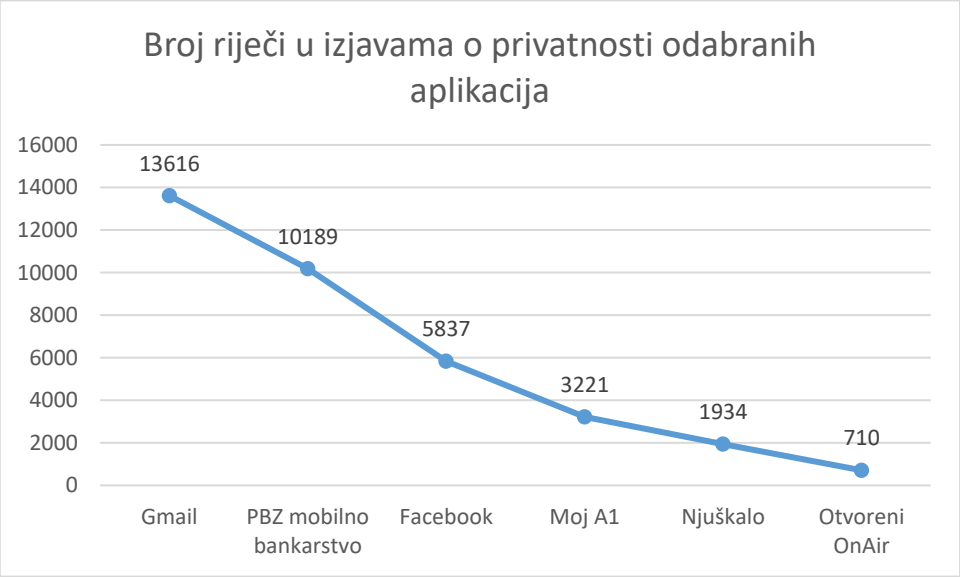
Naziv aplikacije	**Broj sadržanih informacija (od ukupno 22)**	**Ocjena transparentnosti**
Otvoreni	4	Nedovoljno transparentna
Njuškalo	16	Srednje transparentna
PBZ mobilno bankarstvo	19	Zadovoljavajuće transparentna
Moj A1	16	Srednje transparentna
Facebook	14	Srednje transparentna
Gmail	12	Srednje transparentna

Vezano za dodatne kriterije koji se tiču privole i izjave o privatnosti, u Tablica 5.4 prikazano je u kojoj su mjeri odabrane aplikacije zadovoljile tražene kriterije. Niti jedna aplikacija nije prilikom preuzimanja odnosno prvog korištenja zatražila potvrdu o čitanju izjave o privatnosti, a samo je Gmail zatražio izričitu privolu za obradu korisnikovih podataka. Osim toga, kriterij da se izjava o privatnosti unutar aplikacije treba nalaziti unutar dva „dodira“ zadovoljile su aplikacije Otvoreni, Njuškalo i Gmail dok je za ostale aplikacije trebalo tri do pet „dodira“.

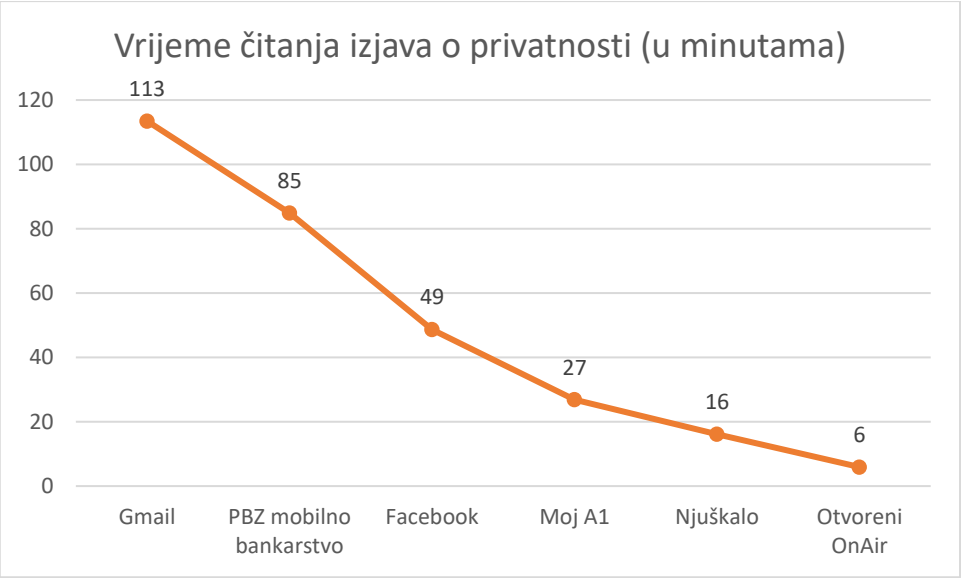
Tablica 5.4 Pregled zadovoljenja dodatnih kriterija transparentnosti

Kriterij	Otvoreni	Njuškalo	PBZ mobilno bankarstvo	Moj A1	Facebook	Gmail
Traži li aplikacija potvrdnu radnju o čitanju izjave o privatnosti?	NE	NE	NE	NE	NE	NE
Traži li aplikacija privolu za prikupljanje i obradu podataka?	NE	NE	NE	NE	NE	DA
Nalazi li se izjava o privatnosti u aplikaciji unutar dva „dodira“?	DA	DA	NE (3)	NE (5)	NE(4)	DA

Slika 5.10 i Slika 5.11 prikazuju broj riječi i potrebno vrijeme čitanja izjava o privatnosti odabranih aplikacija.



Slika 5.10 Duljina izjava o privatnosti odabranih aplikacija. Napomena: Za Facebook i Google uključena su i Pravila o upotrebi kolačića (Facebook) i Tehnologije (Google).



Slika 5.11 Potrebno vrijeme čitanja izjava o privatnosti odabranih aplikacija. Napomena: Za Facebook i Google uključena su i Pravila o upotrebi kolačića (Facebook) i Tehnologije (Google).

5.2. Uvid u transparentnost po pitanju prikupljanja osobnih podataka temeljem usporedbe izjava o privatnosti i dozvola aplikacija

U ovom podpoglavlju bit će dan pregled svih dozvola odabranih aplikacija kako je bilo navedeno u trgovini Google Play početkom srpnja 2019. godine, a zatim i popis podataka koje voditelji obrade prikupljaju, a koji su navedeni u dokumentima vezanim za privatnost kao što su izjave o privatnosti, pravila o upotrebi kolačića, uvjeti pružanja usluge i dokumenti o korištenim tehnologijama. Na ovaj način dobit će se uvid u količinu i raznovrsnost prikupljanih podataka.

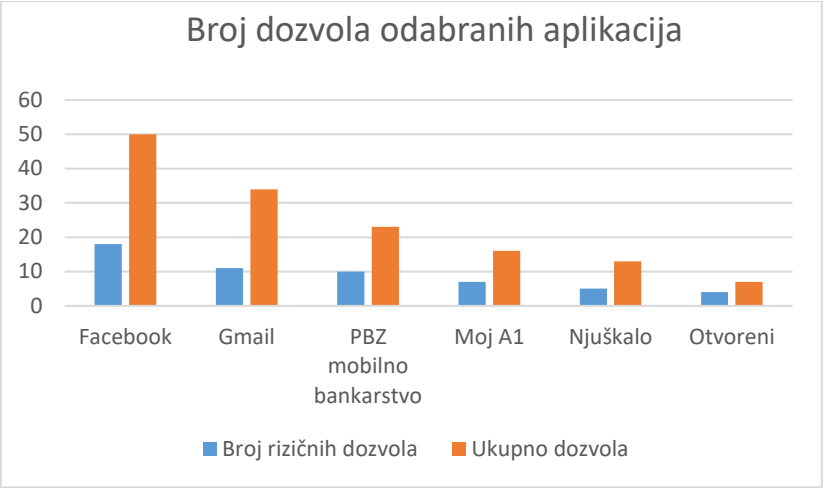
Prema Tablica 5.5, najviše „rizičnih“ dozvola traži aplikacija Facebook, njih čak 18 od ovdje mogućih 20 i to u devet kategorija. Jedina rizična kategorija koja ovdje nije navedena jest ona koja se odnosi na tjelesne senzore, a tu kategoriju u srpnju 2019. godine u trgovini Google Play nije imala niti jedna od odabranih aplikacija. Tablica 5.6 prikazuje sve ostale dozvole odabranih aplikacija, a na Slika 5.12 može se vidjeti odnos „rizičnih“ i svih ostalih dozvola za odabrane aplikacije.

Tablica 5.5 Pregled „rizičnih“ dozvola u odabranim aplikacijama.

RIZIČNE DOZVOLE		Otvoreni	Njuškalo	PBZ mobilno bankarstvo	Moj A1	Facebook	Gmail
SKUPINA DOZVOLA	POJEDINAČNE DOZVOLE						
Kontakti							
	čitanje kontakata			X	X	X	X
	pronalaženje računa na uređaju					X	X
	izmjena kontakata					X	X
Fotografije/mediji/datoteke							
	mijenja ili briše sadržaj vaše USB memorije	X	X	X	X	X	X
	čita sadržaj vaše USB memorije	X	X	X	X	X	X
Kalendar							
	dodaje ili mijenja kalendarske događaje i šalje e-poštu gostima bez znanja vlasnika					X	X
	čita kalendarske događaje i povjerljive informacije					X	X
Pohrana							
	mijenja ili briše sadržaj vaše USB memorije	X	X	X	X	X	X
	čita sadržaj vaše USB memorije	X	X	X	X	X	X
Telefon							
	čita zapis poziva					X	X
	piše zapis poziva					X	X
	čita status telefona i identitet			X		X	
	izravno pozivanje telefonskih brojeva					X	
Lokacija							
	približna lokacija (na temelju mreže)			X		X	
	precizna lokacija (na temelju GPS-a i mreže)			X	X	X	
Fotoaparat							
	snima fotografije i video zapise		X	X	X	X	
Mikrofon							
	snimanje zvuka			X		X	
SMS							
	čita SMS ili MMS poruke					X	
	prima SMS poruke						
	šalje SMS poruke						
UKUPNO SKUPINA DOZVOLA		**2**	**3**	**7**	**5**	**9**	**5**
UKUPNO POJEDINAČNIH DOZVOLA		4	5	10	7	18	11

Tablica 5.6 Pregled dozvola odabranih aplikacija koje se u Androidu 9 ne ubrajaju u „rizične“ dozvole

OSTALE DOZVOLE		Otvoreni	Njuškalo	PBZ mobilno bankarstvo	Moj A1	Facebook	Gmail
Identitet							
	čita vašu kontakt karticu					X	X
	traži korisničke račune na uređaju					X	X
	dodaje ili briše korisničke račune					X	X
Informacije o Wi-Fi vezi							
	uvid u Wi-Fi mreže		X	X	X	X	
Povijest uređaja i aplikacije						1	
	uvid u aplikacije pokrenute na uređaju					X	
ID uređaja i informacije o pozivu							
	čita status telefona i identitet			X		X	
Ostalo							
	preuzmi datoteke bez obavijesti					X	X
	čita statistiku sinkronizacije						X
	čita pretplaćene sadržaje						X
	piše pretplaćene sadržaje						X
	uvid u konfigurirane račune						X
	Google mail						X
	sprječava uređaj da ode u stanje mirovanja		X	X	X	X	X
	izvršavanje pri pokretanju					X	X
	mjeri prostor za pohranu za aplikaciju						X
	instaliranje prečaca					X	X
	čitanje postavki sinkronizacije						X
	potpuni pristup mreži	X	X	X	X	X	X
	uključivanje/isključivanje sinkronizacije		X			X	X
	koristi račune na uređaju						X
	uvid u mrežne veze	X	X	X	X	X	X
	čita konfiguracije Googleove usluge			X	X	X	X
	kreira račune i postavlja lozinke					X	X
	upravljaj beskontaktnom (NFC) komunikacijom						X
	kontrolira vibriranje		X	X		X	X
	prima podatke s Interneta		X	X	X	X	
	reorganizira pokrenute aplikacije					X	
	pristup postavkama Bluetootha					X	
	promjena postavki zvuka			X		X	
	uparivanje s Bluetoothh uređajima			X		X	
	prilagođava veličinu wallpapera					X	
	mijenja postavke sustava					X	
	slanje privlačnih prijenosa					X	
	postavljanje wallpapera					X	
	čitanje statistike baterije					X	
	uspostava i prekidanje veza s Wi-Fi mrežama				X	X	
	proširi/suzi statusnu traku					X	
	promjena mrežne povezivosti					X	
	crtanje preko drugih aplikacja			X		X	
	kontrolira svjetiljku			X	X		
UKUPNO DOZVOLA		3	8	13	9	32	23



Slika 5.12 Prikaz broja dozvola odabranih aplikacija

S obzirom na izjave o privatnosti odabranih aplikacija i količinu podataka koju prikupljaju od svojih korisnika, bilo je za očekivati kako će u broju dozvola aplikacija prednjačiti Facebook i Google. Međutim, i aplikacija Privredne banke Zagreb zahtijeva velik broj „rizičnih“ dozvola, njih čak 10.

5.3. Prikupljanje podataka od strane voditelja obrade odabranih aplikacija

Slijedi popis podataka koje odabrane aplikacije, odnosno voditelji obrade s obzirom da se izjave o privatnosti odnose na sve usluge koje voditelj obrade pruža, prikupljaju od svojih korisnika, a kako je navedeno u izjavama o privatnosti.

5.3.1. Otvoreni

U Općim uvjetima Otvorenog ne spominju se dozvole koje zahtijeva sama aplikacija. Prema Općim uvjetima prikupljaju se sljedeći podaci (Otvoreni, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir):

- „primjerice“ podaci o načinu korištenja aplikacije
- podaci o mobilnom uređaju
- podaci o pružatelju mrežnih usluga/Internetskih usluga
- preferencije
- hobiji

- interesi
- aktivnosti i
- tehnički podaci “uključujući i” IP adresa.

Usporedbom dozvola aplikacije Otvoreni s Općim uvjetima zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir uviđa se kako dozvole aplikacija nisu spomenute u Općim uvjetima, odnosno kako u Općim uvjetima nisu navedeni svi podaci koji se prikupljaju (npr. pristup fotografijama) te time izjava o privatnosti aplikacije Otvoreni nije u potpunosti transparentna po pitanju podataka koje prikuplja.

5.3.2. Njuškalo

Kao i kod aplikacije Otvoreni, u Politici privatnosti Njuškala ne spominju se dozvole i za što im služe, no navedeno je kako prikupljaju sljedeće podatke (Njuškalo – Politika privatnosti):

- Ime i prezime
- Adresu
- Podatke za kontakt
- OIB
- Ostale podatke koje korisnik upisuje
- Geolokaciju
- Informacije o uređaju – model, identifikator uređaja, mobilna mreža i slično
- IP adresu
- Vrijeme i trajanje pristupa
- Vrstu preglednika
- Način pristupa Njuškalovim stranicama
- Pregledane stranice
- Korištene funkcionalnosti u mobilnoj aplikaciji
- Greške tijekom korištenja i slično
- Sadržaj, vrijeme i trajanje telefonskog razgovora s Njuškalom
- Telefonski broj
- Usluge koje koriste, kada i na koji način
- Iz ostalih izvora – podatke od drugih korisnika – npr. komentari, ocjene, prijave zloupotreba, adresa kupca za dostavu i slično

- Podatke od vanjskih partnera - npr. kod SMS uplate broj s kojeg je napravljena uplata i slično
- Podatke s društvenih mreža ako je Njuškalov račun s njima povezan – npr. ime korisničkog profila, broj telefona, adresa e-pošte, ostali podaci za koje korisnik da dozvolu.

Posebno dopuštenje će biti zatraženo za posebne kategorije osobnih podataka.

Njuškalo prikuplja veliku količinu informacija od kojih su samo neke navedene u Politici o privatnosti što je očito po konstrukciji rečenica gdje prilikom nabrajanja često imaju „i slično“, „npr“ i ostalo. Tako u odjeljku „Koje kolačiće i alate koristim?“ stoji sljedeća rečenica koju bi trebalo dodatno pojasniti u svrhu transparentnosti: „Koristim alate pomoću kojih analiziram korištenje Njuškala i prikupljam informacije o tvojim navikama i aktivnostima čime bolje prepoznajem tvoje potrebe u svrhu poboljšanja kvalitete ponude.“ (Njuškalo, Politika privatnosti).

Usporedbom dozvola aplikacije Njuškalo s Politikom privatnosti uviđa se kako dozvole aplikacija nisu spomenute u Politici privatnosti, odnosno kako u njoj nisu navedeni svi podaci koji se prikupljaju (npr. pristup pohrani) te time izjava o privatnosti aplikacije Njuškalo nije u potpunosti transparentna po pitanju podataka koje prikuplja.

5.3.3. PBZ mobilno bankarstvo

U Informaciji o obradi osobnih podataka Privredne banke Zagreb, a koja se odnosi i na aplikaciju PBZ mobilno bankarstvo, dozvole koje aplikacija zahtijeva nisu spomenute niti objašnjene. PBZ također prikuplja veliku količinu informacija (Privredna banka Zagreb, d.d.):

- „određene podatke“ iz uputa za plaćanje;
- „podatke koji proizlaze iz korištenja različitih aplikacija“ povezanih s nekom njihovom uslugom („uključivo“ geolokacija, podaci nastali korištenjem web usluga „itd.“);
- Ime i prezime, datum, mjesto i država rođenja, OIB, adresa prebivališta/boravišta;
- Podatke o identifikacijskoj ispravi, državljanstvu, državi porezne obveze, porezni identifikacijski broj;
- Podatke za kontakt – broj telefona, broj mobilnog uređaja, e-mail adresu;
- Podatke o spolu;
- Moguće i posebne kategorije osobnih podataka;

- Presliku identifikacijskog dokumenta;
- Snimanje telefonskih razgovora;
- „neke druge Vaše podatke nužne za izvršenje ugovora ili ...“;
- „podatke drugih sudionika u kreditu“;
- Podatke o bračnom statusu, osobama s kojima je korisnik povezan (npr. članovi obitelji, podaci o suprugu/zi, osobama s kojima su korisnici poslovno povezani);
- Podatke o stručnoj spremi, zaduženjima u raznim financijskim institucijama, podatke o stanovanju, vrsti kreditne kartice, broju članova obitelji, uzdržavanih članova i slično, „primjerice“ djevojačko prezime majke;
- Podatke o statusu zaposlenja, visini primanja, potrošnji i dr.;
- Podatke o IP adresi i geolokaciji;
- Tehničke podatke sustava – npr. operativni sustav, vrsta mobilnog uređaja, tip i verzija preglednika, veličina zaslona, koje su postavke jezika za preglednik i mobilni uređaj, koji su naziv i verzija mobilne aplikacije, „drugi podaci ove vrste“;
- Podatke o pokretima miša, kretanje po tipkovnici ili kretanje prstiju; i
- Fizička obilježja kao što su otisak prsta i obilježja za identifikaciju lica.

Usporedbom dozvola aplikacije PBZ mobilno bankarstvo s Informacijom o obradi osobnih podataka Privredne banke Zagreb d.d. uviđa se kako dozvole aplikacija nisu spomenute u Informaciji o obradi, odnosno kako u njoj nisu navedeni svi podaci koji se prikupljaju (npr. pristup pohrani) te time izjava o privatnosti aplikacije PBZ mobilno bankarstvo nije u potpunosti transparentna po pitanju podataka koje prikuplja.

5.3.4. Moj A1

A1 Hrvatska d.o.o. u svojoj Izjavi o zaštiti osobnih podataka spominje samo lokaciju od ranije navedenih dozvola unutar aplikacije. U Izjavi su naveli kako prikupljaju sljedeće podatke (A1 d.o.o.):

- Ime i prezime
- Adresu
- Datum rođenja
- Spol
- Broj mobitela
- Adresu e-pošte
- Broj telefona

- Informacije o vrsti ugovornog odnosa i sadržaju
- Informacije o bonitetu
- Podatke s osobne iskaznice
- Bankovni račun
- Ovlasti potpisivanja ili zastupanja
- OIB
- „Npr.“ broj minuta razgovora
- Broj SMS poruka
- Broj međunarodnih poziva
- Trajanje poziva
- Količinu podatkovnog prometa
- „Npr.“ vrijeme aktiviranja i deaktiviranja usluga
- Način korištenja u izbornicima
- Vrijeme promjene TV kanala, naziv TV kanala na koji je prebačen program i prosječno trajanje zadržavanja na pojedinom TV kanalu
- Mjerne podatke prikupljene s korisnikove terminalne opreme, npr. mobilnog uređaja ili routera
- Podatke o telekomunikacijskom prometu, „uključujući“ podatke koje obrađuju radi prosljeđivanja poruke u neku elektroničku komunikacijsku mrežu ili obračuna
- Podatke o lokaciji
- Ispise poziva i „ostale prometne podatke prema važećem Zakonu o elektroničkim komunikacijama“
- „podatke o navikama“ korištenja, „npr.“ korištenje usluga trećih strana putem mreže A1
- Podatke koje prikupljaju putem kolačića, „primjerice“ IP adresa, vrijeme pristupanja „i slično“
- Podatke o načinu korištenja njihovih proizvoda i usluga
- Preferirani način komunikacije
- Demografske podatke („dob, spol...“)
- Kod provjere boniteta još i „učestalost neplaćanja duljeg od 60 dana i podatke o pokrenutom postupku prisilne naplate zbog nepodmirenih dugovanja za elektroničke komunikacijske usluge“ (A1 d.o.o.).

U stavku 4. g pod „Bolje profiliranje“ navode kako neće pratiti sadržaj komunikacije i identifikaciju kontakata dok npr. njihova aplikacija traži pristup kontaktima korisnika na njegovom uređaju.

Usporedbom dozvola aplikacije Moj A1 s Izjavom o zaštiti osobnih podataka za A1 d.o.o. uviđa se kako dozvole aplikacija nisu spomenute u Izjavi, odnosno kako u njoj nisu navedeni svi podaci koji se prikupljaju (npr. fotografije) te time izjava o privatnosti aplikacije Moj A1 nije u potpunosti transparentna po pitanju podataka koje prikuplja.

5.3.5. Facebook

Facebookova Pravila o upotrebi podataka također ne sadrže pojašnjenje zahtijevanih dozvola aplikacije. Osim ranije navedenih dozvola koje traži Facebookova aplikacija, prema važećim dokumentima vezano za privatnost (Facebook - Pravila o upotrebi podataka, Facebook – Pravila o upotrebi kolačića, Facebook – Uvjeti pružanja usluge) Facebook prikuplja i sljedeće podatke:

- Podatke koje korisnik unosi prilikom registracije;
- Svu komunikaciju i sadržaj koji korisnici kreiraju na Facebooku, Instagramu, WhatsAppu i drugim Facebookovim proizvodima (Facebook Help Center - What are the Facebook products), a koji se kombiniraju;
- Metapodatke iz sadržaja kao npr. lokacija fotografije ili datum izrade nekog dokumenta;
- „Može uključivati“ ono što korisnik vidi prilikom korištenja značajki koje Facebook pruža, a jedna od njih je i njihova kamera;
- „Podatke s posebnim zaštitama“ – ukoliko u svom profilu korisnik navede svoja vjerska i politička opredjeljenja, podatke o zdravlju i za koga se „zanimaju“;
- Podatke o osobama, mrežnim stranicama, korisničkim računima, znakovima # i grupama s kojima su korisnici povezani;
- Podatke o interakcijama s ranije navedenim u svim Facebookovim proizvodima;
- Podatke za kontakt ukoliko ih korisnik odluči prenijeti, sinkronizirati ili uvesti s uređaja bilo to iz adresara, popisa poziva ili na temelju brojeva korištenih u SMS porukama;
- Podatke o tome kako korisnici upotrebljavaju Facebookove proizvode, kakve sadržaje (objave, video zapise i dr.) pregledavaju, na koje sadržaje reagiraju, kakve

su aktivnosti korisnika, kao i podatke o tome koliko se korisnik zadržava na Facebookovim proizvodima, koliko često i kada koristi te proizvode;

- Podatke o transakcijama u slučaju bilo kakvih plaćanja ili donacija unutar Facebookovih proizvoda – npr. broj kreditne kartice i ostale podatke o kartici i računu, podatke za kontakt i podatke za slanje računa i pošiljke;
- Podatke o aktivnostima drugih osoba i podatke koje te druge osobe pružaju o korisniku – tu se spominju npr. komentari na objavljene sadržaje i fotografije, kao i kada te druge osobe sinkroniziraju ili uvezu podatke za kontakt tog korisnika;
- Podatke o uređaju (računalu, telefonu, povezanom televizoru i drugim uređajima) koji se integriraju s Facebookom, a koje zatim kombiniraju na različitim uređajima:
    - Svojstva uređaja „kao što su“ operativni sustav, razina baterije, snaga signala, popunjenost prostora za pohranu, preuzete aplikacije, datoteke, dodaci, vrsta preglednika, verzija hardvera i softvera;
    - Radnje na uređaju – npr. položaj prozora i pokreti miša, moguće i prsta;
    - Identifikatori – jedinstveni identifikatori, identifikatori uređaja, identifikatori iz igrica i aplikacija, „obiteljski identifikatori uređaja“ ili „drugi identifikatori koji su jedinstveni za proizvode Facebookovih tvrtki povezane s istim uređajem ili korisničkim računom“;
    - Signali uređaja – Bluetooth i Wi-Fi pristupne točke, odašiljači mobilne mreže;
    - Podaci iz postavki uređaja – npr. dozvole aplikacije – GPS lokacija, kamera, fotografije;
    - Mreže i veze – broj mobilnog telefona, IP adresa, brzina veze, podaci o drugim uređajima koji se nalaze u blizini ili na toj mreži, podaci o davatelju usluge mobilne mreže ili Interneta, vremenska zona, jezik;
    - Podaci iz kolačića pohranjenih na uređaju.
- Podatke od partnera – dakle svih onih koji koriste Facebookove poslovne alate, odnosno svih onih koji na svojoj mrežnoj stranici koriste dodatke za tu društvenu mrežu, npr. gumb „Sviđa mi se“, svih koji koriste prijavu putem Facebooka i dr.;
    - To su podaci o npr. uređaju korisnika, web stranicama koje pregledava, podaci o izvršenim kupnjama, podaci o pregledanim oglasima i sve to bez obzira ima li taj korisnik Facebookov korisnički račun te je li prijavljen na Facebook;

- Podaci o aktivnostima i kupnjama na Internetu i izvan njega „od trećih strana davatelja podataka koji imaju pravo pružiti“ Facebooku te podatke.

- Podatke o korisnikovim vezama, preferencijama, interesima i aktivnostima;
- Podatke o ljudima, mjestima i stvarima s kojima je korisnik povezan i za koje se zanima;
- Podatke o lokaciji – trenutačna lokacija, mjesto gdje korisnik živi, radi, mjesta na koja voli ići, tvrtke i ljudi u blizini kojih se korisnik nalazi:
    - Te podatke temelji na preciznoj lokaciji uređaja (ako korisnik da dozvolu to na svom uređaju), IP adresama, podacima koje prikupe prilikom korištenja Facebookovih proizvoda od strane tog, ali i drugih korisnika – npr. prijave ili događaji kojima korisnik prisustvuje.

Usporedbom dozvola aplikacije Facebook s ranije navedenim dokumentima uviđa se kako dozvole aplikacija nisu poimence spomenute u dokumentima, no podaci koji se putem tih dozvola prikupljaju većinom jesu spomenuti (mikrofon npr. nije spomenut) te time Facebookova Pravila o upotrebi podataka nisu u potpunosti transparentna po pitanju podataka koje aplikacija prikuplja.

5.3.6. Gmail

Neke od dozvola aplikacije spominju se u Googleovim Pravilima o privatnosti[44] kao npr. uvid u pozivane brojeve i slično (dozvola za telefon), lokacija i mikrofon, ali ne na način da navode dozvole aplikacije, već samo govore o podacima koje prikupljaju. Osim toga, u Pravilima o privatnosti navedeno je kako prikupljaju sljedeće podatke:

- Ime – pri izradi korisničkog računa
- Model uređaja
- Zaporku – pri izradi korisničkog računa
- Telefonski broj – ukoliko ga korisnik unese
- Podatke o plaćanju – ukoliko ih korisnik unese
- Adresu elektroničke pošte
- IP adresu
- Sadržaj elektroničke pošte

[44] Googleova pravila o privatnosti, https://policies.google.com/privacy, preuzeto 2. 7. 2019.

- Kontakte iz elektroničke pošte
- Fotografije i videozapise „koje spremite“
- „dokumente i tablice koje izradite“
- „komentare koje objavite uz videozapise na YouTubeu“
- Jedinstvene identifikatore – koji identificiraju web preglednik, aplikaciju ili uređaje, npr. oglašivački identifikator (engl. *Advertising* ID), UUID[45], IMEI broj
- Jezik kojim korisnik govori
- Pretraživanja na Google Play trgovini
- Pretraživanja u web tražilici
- Podatke o aplikacijama, preglednicima i uređajima koje korisnik koristi za pristup Googleovim uslugama:
    - Vrsta i postavke preglednika – npr. jezik, vrsta preglednika
    - Vrsta i postavke uređaja
    - Operativni sustav
    - Podaci o mobilnoj mreži koji „uključuju naziv operatera i telefonski broj te broj verzije aplikacije“
    - Podatke o interakciji aplikacija, preglednika i uređaja s njihovim uslugama, „uključujući IP adresu, izvješća o rušenju, aktivnost sustava, datum, vrijeme i URL preporuke“
    - MAC adrese uređaja u blizini, jačinu signala
    - Podatke iz trgovine Google Play o instaliranim aplikacijama
    - Podatke s YouTubea o videozapisima koje korisnik pregledava.
- Također spominju vlasnike Android uređaja, a u pop-up prozoru spominju se aplikacije koje dolaze s Android uređajima kao što su Gmail, Karte, fotoaparat uređaja, birač poziva, konverzija teksta u govor, tipkovnica i sigurnosne značajke;
- „mogu uključivati“ videozapise koje korisnik gleda, sadržaj oglasa i interakciju s njima, „podatke o glasovnoj i audioaktivnosti prilikom upotrebe audioznačajki“ što bi značilo snimanje korisnikovog glasa, podatke o izvršenim kupnjama, o osobama s kojima korisnici komuniciraju kao i aktivnosti na mrežnim stranicama i aplikacijama trećih strana koje koriste Googleove usluge kao što su AdSense i Google Analytics;

[45] *Universally Unique Identifier*

- Također se spominju i usluge za pozive i poruke, tada „mogu prikupljati“ korisnikov telefonski broj, broj koji je pozvan, broj na koji je poziv možda preusmjeren, vrijeme i datum poziva i poruka, trajanje poziva, podatke o usmjeravanju i vrste poziva;
- Podatke o lokaciji putem GPS-a, IP adrese, podataka senzora na uređaju (mjerač ubrzanja za mjerenje brzine i žiroskop za određivanje smjera kretanja), putem Wi-Fi pristupnih točki, mobilnih odašiljača ili uređaja koji imaju omogućen Bluetooth;
- Podatke iz javno dostupnih izvora – npr. lokalnih novina, od partnera uključujući i marketinške partnere i partnere za sigurnost, a zatim i od oglašivača (kao što su podaci iz programa vjernosti koje su oni odlučili dati na uvid Googleu). U pop-up prozoru stoji kako mogu prikupljati informacije koje su javno dostupne online ili iz „drugih javnih izvora“.
- Podatke iz e-pošte o npr. potvrdi rezervacije
- Fotografije i video zapise koje korisnik stavi na Google Photos
- Adresu iz podataka o kupnji za dostavu
- Podatke iz kolačića na web stranicama koje korisnici posjećuju.

Usporedbom dozvola aplikacije Gmail s Googleovim pravilima o privatnosti uviđa se kako dozvole aplikacija nisu poimence spomenute u dokumentima, no podaci koji se putem tih dozvola prikupljaju većinom jesu spomenuti (npr. pristup pohrani nije) te time Googleova pravila o privatnosti nisu u potpunosti transparentna po pitanju podataka koje aplikacija prikuplja.

Tablica 5.7 daje pregled usklađenosti dozvola aplikacija s podacima navedenima u izjavama o privatnosti odabranih aplikacija.

Tablica 5.7 Pregled usklađenosti dozvola aplikacija s izjavama o privatnosti odabranih aplikacija

	Otvoreni	**Njuškalo**	**PBZ mobilno bankarstvo**	**Moj A1**	**Facebook**	**Gmail**
Spominju li se u izjavi o privatnosti poimence dozvole aplikacija?	NE	NE	NE	NE	NE	NE
Spominju li se u izjavi o privatnosti svi podaci koji se mogu prikupljati putem dozvola?	NE	NE	NE	NE	VEĆINA	VEĆINA

5.4. Zaključak analize

Provedenom analizom utvrđeno je kako je jedino izjava o privatnosti aplikacije PBZ mobilno bankarstvo (koja se odnosi na sve usluge Privredne banke Zagreb d.d., a ne samo na aplikaciju) zadovoljavajuće transparentna s obzirom da sadrži 19 od ukupno 22 zahtijevane informacije. Aplikacija Otvoreni sa samo četiri informacije je ocijenjena kao nedovoljno transparentna dok su ostale aplikacije ocijenjene kao srednje transparentne iako je Gmail na granici sa samo 12 danih informacija. Dodatni kriterij potvrdne radnje vezano za privolu, odnosno jasnog davanja privole za obradu podataka ispunila je samo aplikacija Gmail, a izjava o privatnosti mogla se unutar dva „dodira“ naći samo u aplikacijama Otvoreni, Njuškalo i Gmail. S obzirom na navedeno, u svrhu bolje transparentnosti izjava o privatnosti prema smjernicama iz GDPR-a i popratnih dokumenata, voditelji obrade odabranih aplikacija (osim aplikacije PBZ mobilno bankarstvo) trebali bi navesti dodatne informacije iz Članaka 13. i 14., a što se posebno odnosi na aplikaciju Otvoreni.

Uvidom u dozvole aplikacija i njihovom usporedbom s podacima koji su navedeni u izjavama o privatnosti, a koje voditelji obrade prikupljaju i obrađuju, utvrđeno je kako izjave o privatnosti ne sadrže poimence navedene dozvole aplikacija s pojašnjenjima koji se podaci putem koje dozvole prikupljaju i u koje svrhe. Temeljem te usporedbe može se zaključiti kako izjave o privatnosti po ovom kriteriju također nisu u potpunosti transparentne. Međutim, Facebook i Gmail, aplikacije koje među odabranim aplikacijama prikupljaju

najveću količinu podataka, u izjavama o privatnosti navele su većinu podataka iz dozvola aplikacija.

6. Istraživanje o privatnosti i fenomen „paradoksa privatnosti“

U drugom dijelu praktičnog dijela cilj je bio istražiti koliko su građani Republike Hrvatske svjesni činjenice kako velike tehnološke tvrtke, ali i aplikacije općenito prikupljaju velike količine informacija, koliko cijene svoju privatnost kao i ponašaju li se u skladu s proklamiranom brigom za privatnost. Jedan od ciljeva je bio utvrditi može li se na ovom uzorku potvrditi postojanje paradoksa privatnosti, fenomena gdje ljudi koji visoko cijene svoju privatnost u zamjenu za određene usluge tehnoloških tvrtki tu brigu za privatnost zanemaruju i preuzimaju aplikacije koje im narušavaju privatnost. Pojam *paradoks privatnosti* prva je upotrijebila Susan Barnes opisujući njime pojavu kada tinejdžeri na društvenim mrežama objavljuju razne intimne podatke, ali su zgroženi ukoliko njihovi roditelji te podatke pronađu (Pavuna, 2019: str. 142; prema Barnes, 2006).

Istraživanje je provedeno na 148 ispitanika u Republici Hrvatskoj putem internetskog servisa Google Forms u srpnju 2019. godine. U istraživanju su sudjelovale 92 ženske osobe i 56 muških osoba u rasponu od 16 do 69 godina s najvećim postotkom onih od 36 do 50 godina. Udio ispitanika s visokom stručnom spremom ili diplomskim/dodiplomskim studijem bio je 39,2 % dok je drugi najveći broj ispitanika imao srednju stručnu spremu, njih 29,1 %. Čak 27 % ispitanika radi u sektoru informacijskih i komunikacijskih tehnologija (IT) ili studira na studijima vezanim za IT. Anketa se sastojala od 38 pitanja. Udio korisnika Androida u uzorku prati svjetsku statistiku (prema Gartner, Inc., podaci s kraja 2017. godine govore kako 85,9 % korisnika mobilnih uređaja u svijetu koristi Android uređaje) pa tako čak 86,5 % ispitanika posjeduje Android uređaj, njih 12,8 % posjeduje iPhone, dok jedna osoba posjeduje Windows Phone. Popis anketnih pitanja nalazi se u Prilogu 1.

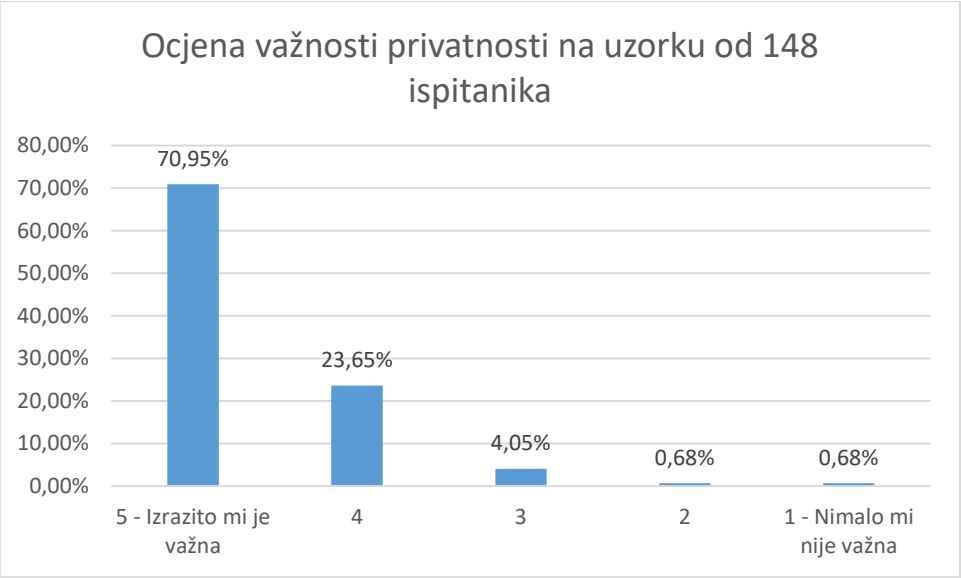
6.1. Svijest o privatnosti

Ne postoji univerzalna definicija privatnosti. Taj pojam označava različite stvari kao što su vrijednosti, prava, oblik kontrole i dr., a povezuje ga se s pojmovima sigurnosti, informacijama o sebi, autonomijom, vlastitim identitetom i dr. Zbog navedenoga, definicije su grupirane u četiri, pet ili ponekad šest kategorija (Pavuna, 2019: str. 13; prema Rössler, 2004b i Solove, 2002.). Jedan od značajnijih autora po pitanju privatnosti, Alan Westin,

opisao je privatnost kao "mogućnost svakog pojedinca (…) da za sebe odredi na koji će način, kada, kome i do koje mjere biti prezentirani podaci o njemu" (Pavuna, 2019; str. 14; prema Westin, 1967). Burgoon je pak privatnost podijelila u četiri dimenzije koje se teoretski i preklapaju (Pavuna, 2019; str. 17; prema Burgoon, 1982; Burgoon et al., 1989):

- Fizička privatnost – odnosi se na vlastito tijelo i osobni prostor, a definira se kao sloboda u kojoj nema nadzora ili neželjenog pristupa istima;
- Društvena ili interakcijska – ova dimenzija odnosi se na mogućnost pojedinca da sam odabere što će, kada i s kim dijeliti;
- Psihološka – odnosi se na misli, osjećaje, vrijednosti i stavove i na njihovu zaštitu, ali i slobodu od manipulacije drugih, vrijeđanja ili uvjeravanja; te
- Informacijska – „kao mogućnost kontrole tko, i pod kojim okolnostima, može prikupljati i širiti podatke o osobi".

S obzirom na postojanje ovih različitosti u pojmovima, ispitanicima je prvo pitanje postavljeno na način da je dana definicija informacijske privatnosti koja uključuje intimne informacije, podatke o obitelji, podatke o zdravstvenom stanju, fotografije, visinu plaće i slično. Ispitanici su zamoljeni da na ljestvici od 1 do 5 (od „Nimalo mi nije važna" do „Izrazito mi je važna") navedu koliko važnom smatraju svoju privatnost. Čak 70,9 % ispitanika ocijenilo je svoju privatnost izrazito važnom dok ju važnom (ocjena 4) smatra 23,6 % ispitanika. 4,1 % ispitanika ju smatra srednje važnom dok je samo po jedan ispitanik naveo kako ju smatra nimalo ili malo važnom (Slika 6.1). Prema ovome gotovo 95 % ispitanika svoju privatnost smatra izrazito važnom ili važnom.



Slika 6.1 Ocjena važnosti privatnosti među 148 sudionika istraživanja. Pri tome je ispitanicima navedeno kako definicija privatnosti obuhvaća njihove intimne informacije, podatke o njima i njihovoj obitelji kao što su podaci o zdravstvenom stanju, njihovi stavovi, politička i vjerska opredijeljenost i dr.

Osim toga, gotovo svi sudionici istraživanja, njih 98 %, naveli su kako podacima sadržanima na njihovim mobilnim uređajima i njihovoj privatnoj komunikaciji nitko ne bi smio pristupiti bez njihovog dopuštenja, što znači da čak i oni koji svoju privatnost smatraju srednje važnom, ove podatke smatraju privatnima i ne žele da im netko pristupa bez dozvole. U istraživanju Eurobarometra o e-privatnosti provedenom u Europskoj uniji, 78 % građana navelo je kako im je vrlo važno da se njihovim informacijama na raznim uređajima može pristupiti samo ukoliko oni to odobre (Prijedlog Uredbe o privatnosti i elektroničkim komunikacijama, 2017: str. 6).

Jednako tako, 96,6 % ispitanika smatra kako ima pravo na privatnost na svom mobilnom uređaju i prilikom posjećivanja raznih web stranica bez obzira čine li to na računalu ili na mobilnom uređaju. Međutim, čak 83,1 % ispitanika vjeruje kako nemaju kontrolu nad svojim osobnim podacima na mobilnom uređaju temeljem čega možemo zaključiti kako je većina ispitanika svjesna količine prikupljanja podataka i mogućnosti postojanja zlonamjernih aplikacija s obzirom da se zadnjih godina sve češće pojavljuju vijesti o skandalima, napadima *malwarea* i sl. U skladu s tim, čak 87,8 % ispitanika smatra kako na pametnim telefonima i Internetu općenito nije moguće zadržati svoju privatnost.

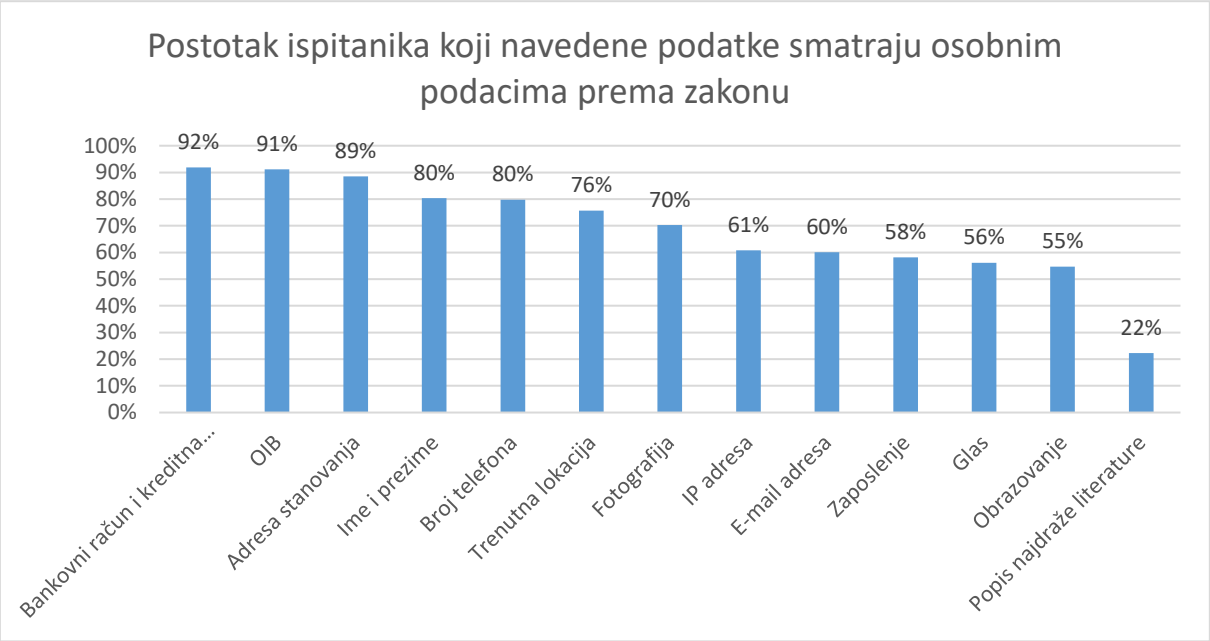
Zanimljivo je kako je čak 52 % ispitanika izjavilo kako smatraju da nemaju ništa za sakriti što također može biti jedno od potencijalnih objašnjenja zašto neki ljudi olako dijele svoje osobne i druge privatne podatke na Internetu i zašto ne prezaju od preuzimanja aplikacija koje traže prekomjerne dozvole kako bi prikupljale podatke. Solove takav stav smatra pogrešnim zbog raznih potencijalnih posljedica s obzirom da ljudi niti ne znaju koji se sve podaci prikupljaju pa ne mogu reći kako tvrtke, odnosno algoritmi koje koriste, neće iz mnoštva podataka putem rudarenja podataka otkriti upravo one informacije koje korisnik želi sakriti (Obar i Oeldorf-Hirsch, 2018: str. 25; prema Solove, 2007). Jednako tako, Solove smatra kako se na temelju ponašanja pomoću raznih programa mogu otkriti budući postupci te da niti zbog toga ne stoji njihova tvrdnja kako nemaju ništa za sakriti jer ne znaju što će se dogoditi i hoće li to nešto ipak željeti sakriti (Obar i Oeldorf-Hirsch, 2018: str. 25; prema Solove, 2007).

6.2. Dijeljenje osobnih podataka od strane ispitanika

Kada govorimo o davanju stvarnih tj. istinitih podataka prilikom kreiranja Gmail računa ili Apple ID-a nakon kupnje novog pametnog telefona, vidimo da je unatoč proklamiranoj zabrinutosti za privatnost čak 71,6 % ispitanika koristilo istinite podatke, dok je 26,4 % njih dalo samo dio stvarnih podataka, a druge su lažirali. Samo 2 % ispitanika odgovorilo je kako uopće nisu koristili stvarne podatke. Na društvenim mrežama koje koriste u privatne svrhe stvarno ime dalo je 76,4 %, a prezime i fotografiju njih 70,9 % i 71,6 %. Ostale podatke ispitanici nisu bili toliko voljni dijeliti te je samo njih 45,9 % podijelilo svoju e-mail adresu, a 41,9 % je dalo svoje podatke o školovanju. 5,4 % izjavilo je kako uopće ne daje stvarne podatke na društvenim mrežama dok je čak 14,2 % izjavilo kako ne koristi društvene mreže. Bilo bi zanimljivo istražiti koji su razlozi nekorištenja društvenih mreža ili činjenice da na društvenim mrežama neki korisnici nikada ne dijele svoje stvarne podatke kao i u kolikoj je to mjeri povezano s razinom zabrinutosti za privatnost.

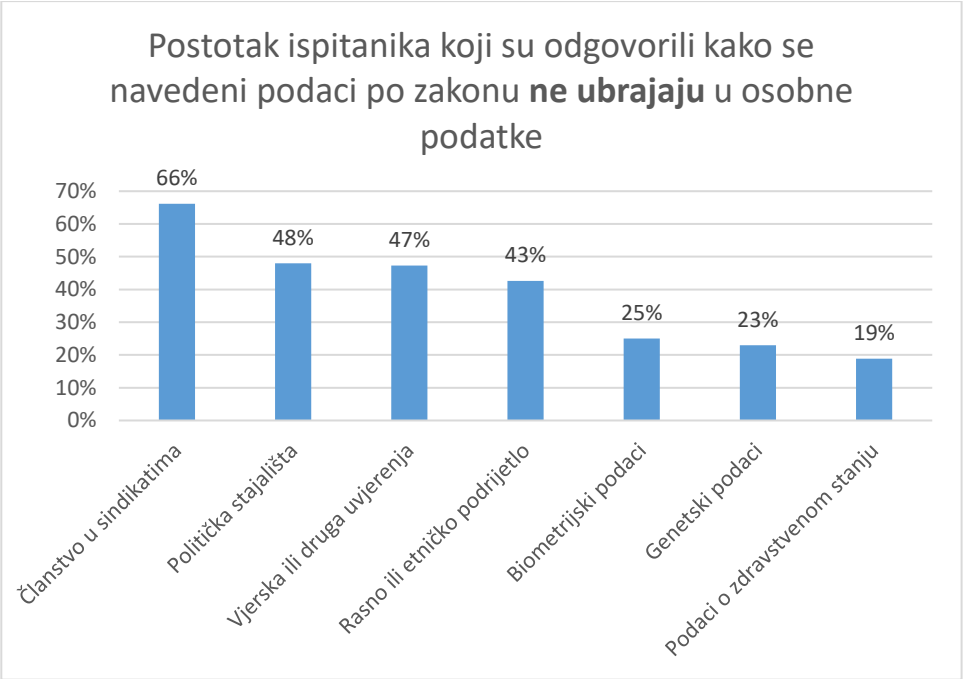
Bilo bi potrebno provesti daljnja istraživanja kako bi se uvidjelo koji su razlozi odavanja osobnih podataka, radi li se o povjerenju u voditelja obrade podataka, o jednostavnosti korištenja umjesto smišljanja lažnih informacija i vođenja evidencije o istima, ili se možda radi o tome da ljudima nije niti palo na pamet davati lažne podatke za uređaj koji će stalno koristiti i to u brojne svrhe. Međutim, postoji još jedan potencijalni razlog, a taj je da određene osobne podatke neki ljudi ne smatraju osobnim podacima i ne znaju kako imaju pravo na zaštitu istih. Naime, u jednom od pitanja sudionicima istraživanja predočeno

je 20 vrsta osobnih podataka prema GDPR-u te su zamoljeni da označe sve one za koje smatraju da se prema zakonu ubrajaju u osobne podatke. Kako je bilo i za očekivati, većina je odgovorila kako su ime i prezime, OIB, adresa stanovanja, broj telefona, podaci o zdravstvenom stanju, bankovnom računu, biometrijski i genetski podaci sve osobni podaci prema zakonu. Međutim, iznenađujuće je kako nisu svi ispitanici smatrali da se ime, prezime, OIB i podaci o bankovnom računu i kreditnoj zaduženosti prema zakonu ubrajaju u osobne podatke. Čak 19,6 % sudionika ne smatra ime i prezime osobnim podatkom, OIB 8,8 % ispitanika, a podatke o bankovnom računu i kreditnoj zaduženosti osobnim podatkom ne smatra 8 % ispitanika. Grafikon na Slika 6.2 prikazuje koliki postotak ispitanika za navedene osobne podatke smatra kako se prema zakonu ubrajaju u osobne podatke.



Slika 6.2 Postotak ispitanika koji znaju kako se navedeni podaci prema zakonu ubrajaju u osobne podatke

Od 20 navedenih osobnih podataka u pitanju, sedam ih se ubraja u posebne kategorije osobnih podataka koja zaslužuju dodatnu zaštitu prema Općoj uredbi o zaštiti podataka. Nažalost, veliki postotak ispitanika niti ne zna kako su politička stajališta, vjerska uvjerenja, etničko podrijetlo i ostalo osobni podaci što se može vidjeti na grafikonu na Slika 6.3.



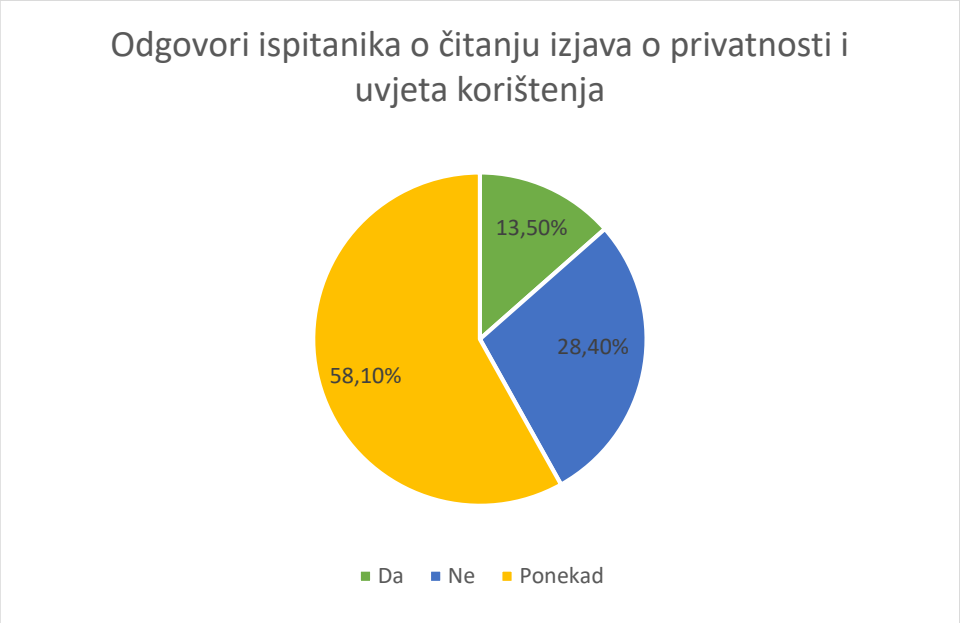
Slika 6.3 Postotak ispitanika koji za navedene podatke iz posebne kategorije podataka nisu znali da se ubrajaju u osobne podatke

S obzirom da tako veliki broj ljudi ove podatke ne smatra osobnim podacima, moguće je da će ih biti spremniji i dijeliti. Na to moguće računa i Facebook kada od korisnika traži da unesu svoje osobne podatke u profil i pri tome traži i podatke iz posebnih kategorija osobnih podataka.

6.3. Navike čitanja izjava o privatnosti

Pozitivno je što čak 81,8 % ispitanika zna da na razini EU postoji Opća uredba o zaštiti podataka. Međutim, poražavajuća je činjenica kako izjave o privatnosti i uvjete korištenja prije preuzimanja aplikacija redovito čita samo 13,5 % sudionika istraživanja, a 58,1 % izjavilo je kako ih ponekad čita. Preostalih 28,4 % nikada ne čita izjave o privatnosti i uvjete korištenja (grafikon na Slika 6.4). Za usporedbu, prema empirijskom istraživanju Andre Pavune provedenom 2017. godine na uzorku od 966 sudionika, 30,3 % sudionika istraživanja u prethodnih šest mjeseci nije niti jednom pročitalo izjavu o privatnosti prije preuzimanja mobilne aplikacije ili registracije na neku web stranicu, a 22,8 % je to činilo rijetko (Pavuna, 2019: str. 191-192).

Situacija je nešto bolja s dozvolama aplikacija koje prilikom preuzimanja aplikacija provjerava čak 43,9 % dok ih ponekad provjerava njih 45,3 %. Samo 10,8 % ispitanika izjasnilo se kako nikada ne čitaju dozvole. Ujedno i 10,1 % ispitanika ne smatra kako aplikacije traže previše dozvola (grafikon na Slika 6.5).



Slika 6.4 Prikaz odgovora ispitanika o čitanju izjava o privatnosti i uvjeta korištenja prije preuzimanja mobilnih aplikacija

Slika 6.5 Prikaz odgovora ispitanika o provjeravanju dozvola aplikacija prije preuzimanja

U prethodnom poglavlju napravljena je analiza transparentnosti izjava o privatnosti šest popularnih aplikacija u Republici Hrvatskoj i niti jedna od izjava nije imala poimence navedene sve dozvole koje ta aplikacija zahtijeva pa samim time niti pojašnjenje za što su one potrebne. Pojedinačno su neke od dozvola bile spomenute, ali ne na način da se pojašnjava kako aplikacija traži pristup određenim dozvolama na uređaju i za što su te dozvole potrebne, među ostalim i jer se izjave o privatnosti nisu odnosile samo na aplikaciju, već na sve usluge koje taj voditelj obrade pruža. Od 148 ispitanika, njih 133, odnosno 89,9 % smatra kako bi izjave o privatnosti trebale sadržavati pojašnjenje dozvola aplikacije na koju se odnose.

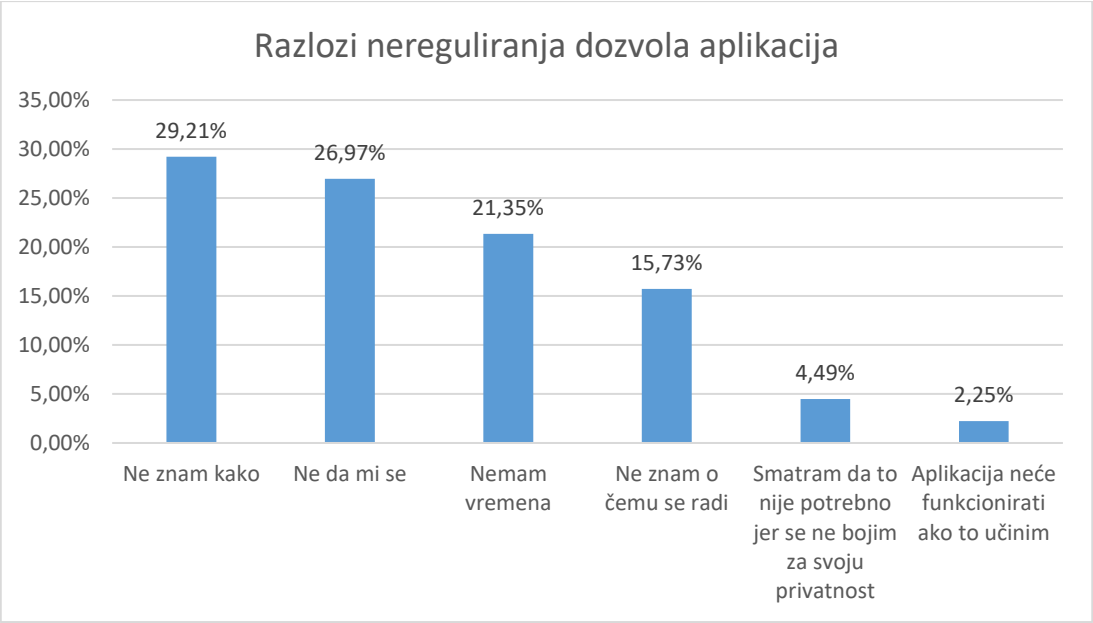
U znanstvenom istraživanju koje su proveli Obar i Oeldorf-Hirsch (Obar, Oeldorf-Hirsch, 2018) o navikama korisnika[46] vezanim za čitanje izjava o privatnosti i uvjeta korištenja istraživači su došli do zaključka kako ispitanici izjave o privatnosti i uvjete korištenja smatraju smetnjom i ignoriraju ih kako bi što prije mogli vidjeti sadržaj zbog kojeg su se na toj mrežnoj stranici i našli. Za potrebe istraživanja kreirana je fiktivna društvena mreža *NameDrop*. Čak 74 % ispitanika preskočilo je čitanje izjave o privatnosti i odmah ju je prihvatilo, a 23 % ispitanika izjavu o privatnosti čitalo je samo oko 73 sekunde (za cijelu je bilo potrebno oko 30 minuta) i nakon toga ju prihvatilo. Dakle, ukupno 97 % ispitanika prihvatilo je izjavu o privatnosti i pri tome je čak 98 % njih previdjelo klauzule o tome da pristaju na davanje svojih osobnih podataka američkoj Nacionalnoj agenciji za sigurnost (*National Security Agency* - NSA) i svojim poslodavcima kao i da će sredstvo plaćanja za korištenje društvene mreže biti njihovo prvorođeno dijete (Obar, Oeldorf-Hirsch, 2018: str. 11-12). Ovo je drastičan primjer mogućih posljedica pukog prihvaćanja izjava o privatnosti, no s obzirom na ranije provedenu analizu i dobivanje uvida u vrste i količinu podataka koje razne aplikacije prikupljaju, ljudi se doista odriču velike količine privatnih informacija korištenjem raznih usluga, a da to niti ne znaju. U istraživanju Obar i Oeldorf-Hirsch glavni prediktor za nečitanje je bio strah od preopterećenosti informacijama (Obar, Oeldorf-Hirsch, 2018: str. 23).

[46] Radilo se o studentima komunikacija koji posjeduju neka znanja o privatnosti, nadzoru i velikim skupovima podataka (engl. *Big Data*).

6.4. Reguliranje dozvola aplikacija

S obzirom na 95 % ispitanika koji svoju privatnost smatraju važnom ili izrazito važnom kao i na činjenicu kako bi njihovim podacima na mobilnom uređaju netko drugi smio pristupiti samo uz njihovu dozvolu, zanimljivo je kako njih samo 25 % uvijek regulira dozvole aplikacija nakon preuzimanja aplikacije, dok ponekad to čini 56,8 % ispitanika. Dozvole nikada ne regulira čak 18,2 %. Ovdje je bitno ponovno napomenuti kako čak oko 25 % korisnika Android uređaja u svijetu i dalje koristi uređaje s Android operativnim sustavom 5.1.1 ili starijim (Android Developers, Distribution Dashboard) što znači da niti nemaju mogućnost upravljanja dozvolama, a što je pojašnjeno u četvrtom poglavlju. Od onih koji su odgovorili kako ponekad ili uvijek reguliraju dozvole aplikacija, samo 12,28 % vjeruje kako su aplikaciji doista i onemogućili pristup. Njih 42,11 % ne vjeruje da aplikacije neće imati pristup njihovim podacima, a čak 45,61 % odgovorilo je kako ne zna jesu li im onemogućili pristup. S obzirom na istraživanje Reardon et al. navedeno u četvrtom poglavlju o prikupljanju podataka na Android uređajima čak i kada su dozvole onemogućene, ovih 12,28 % ispitanika je u potpunosti u pravu.

Ispitanici u provedenom istraživanju za potrebe ovoga rada upitani o tome zašto ne reguliraju dozvole aplikacija, odgovorili su na način kako je prikazano grafikonom na Slika 6.6 gdje je čak 29,21 % odgovorilo da ne znaju kako, njih 15,73 % kako ne zna o čemu se radi, dok oni kojima se ne da ili nemaju vremena čine 48,32 % od onih koji su odgovorili da ne reguliraju dozvole aplikacija.



Slika 6.6 Prikaz razloga neregulianja dozvola aplikacija nakon preuzimanja istih na mobilni uređaj

S obzirom da je 45 % ispitanika odgovorilo da ne zna kako ili ne zna o čemu se radi, postoji mogućnost da neki od njih posjeduju mobilni uređaj s operativnim sustavom Android starije generacije (ispod 6.0) pa niti nemaju mogućnost reguliranja dozvola. Druga mogućnost je da ljudi jednostavno ne znaju kako to učiniti te bi ovakvi rezultati istraživanja mogli potaknuti interes za edukacijom o privatnosti i sigurnosti na mobilnim uređajima.

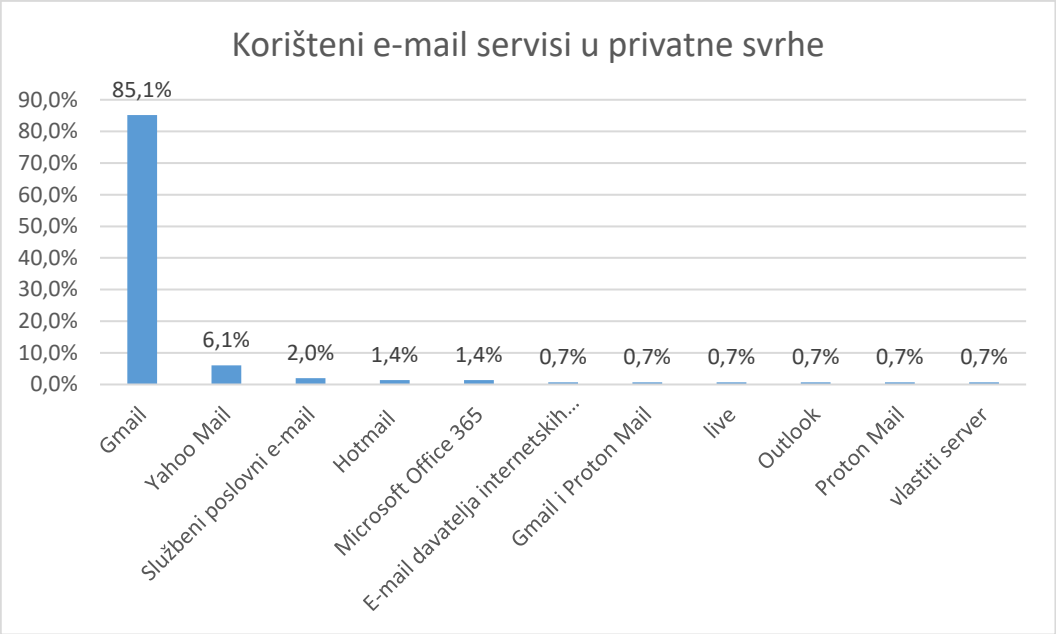
6.5. Paradoks privatnosti

Provedena su brojna istraživanja na temu paradoksa privatnosti od kojih su mnoga pokazala kako paradoks privatnosti doista postoji (Barth and De Jong, 2017; Joinson et al., 2010) te da varijabla zabrinutosti za privatnost i vjerojatnost objavljivanja osobnih podataka uopće nisu povezani (Pavuna, 2019: str. 143; prema Tufekci, 2008). Taddei i Contena (Pavuna, 2019: str. 143; prema Taddei i Contena, 2013) također nisu pronašli povezanost tih varijabli, kao ni Acquisti i Gross kojima je predmet istraživanja bilo korištenje Facebooka. Oni su uvidjeli da stavovi o privatnosti i zabrinutost za privatnost igraju ulogu pri odluci o pristupanju Facebooku, no nakon izrade korisničkog računa te stavke se gotovo zanemaruju (Pavuna, 2019: str. 143; prema Acquisti i Gross, 2006).

Prema definiciji paradoksa privatnosti ljudi unatoč zabrinutosti za svoju privatnost poduzimaju radnje na Internetu/mobilnim uređajima koje im narušavaju privatnost. U

istraživanju provedenom za potrebe ovoga rada, upitani jesu li ikada odustali od preuzimanja aplikacije jer su smatrali da traži prevelik pristup podacima na njihovom mobilnom uređaju, čak 81,8 % ispitanika odgovorilo je kako su to učinili više puta, dok je njih 6,8 % navelo kako su to učinili samo jednom. 5,4 % odgovorilo je kako ih to ne brine, dok je 6,1 % odgovorilo da ne čitaju izjave o privatnosti i dopuštenja aplikacija. U istraživanju iz 2012. godine u sklopu projekta Pew Internet i American Life, 54 % korisnika aplikacija odustalo je od preuzimanja aplikacije nakon što su uvidjeli kako traži prekomjerne dozvole. U istom istraživanju njih 30 % izbrisalo je već korištenu aplikaciju kada su uvidjeli kako prikuplja određene osobne podatke za čije prikupljanje korisnici nisu htjeli dati svoj pristanak (Boyles, Smith i Madden, 2012).

U autoričinom istraživanju, od 148 ispitanika njih čak 85,1 % koristi Gmail kao glavni e-mail servis u privatne svrhe. Drugi po redu je Yahoo Mail s 6,1 % dok preostalih 8,8 % koristi neke druge e-mail servise (grafikon na Slika 6.7).



Slika 6.7 Prikaz e-mail servisa koje sudionici istraživanja koriste u privatne svrhe

U sljedećem pitanju navedeno je 19 vrsta podataka koje Google prikuplja s web stranica, uređaja, aplikacija i svih svojih usluga te su ispitanici upitani jesu li znali da ih Google prikuplja. Velika većina ispitanika znala je kako Google prikuplja sadržaj web stranica, preuzete aplikacije, povijest kupnje, povijest gledanja zapisa na YouTubeu i slično. Za čitanje elektroničke pošte i njezinih privitaka znalo je 54,7 % ispitanika. Za podatke o

pozivima znalo je 43,2 %, dok je za prikupljanje jezika i izričaja kojim se korisnik služi kao i za glas korisnika i osoba u blizini znala oko trećina ispitanika, njih 34,5 % za jezik i 30,4 % za glas. 58,1 % ispitanika izjavilo je kako su znali da Google na temelju prikupljenih podataka izrađuje profile korisnika i dijeli ih s oglašivačima (Tablica 6.1).

S obzirom na ranije navedene podatke o tome da velika većina ispitanika svoju privatnost smatra važnom ili izrazito važnom te da je potrebno njihovo dopuštenje za prikupljanje određenih podataka, postavlja se pitanje zašto njih čak 85,1 % koristi Gmail kao preferirani e-mail servis za privatne svrhe ukoliko znaju za opseg prikupljanja podataka od strane Googlea i to smatraju narušavanjem vlastite privatnosti (njih čak 93,9 %). Osim Gmaila, Yahoo Mail također prikuplja mnoge od navedenih podataka. Ovakav rezultat ide u prilog postojanju fenomena paradoksa privatnosti, no potrebno je istražiti koji je razlog što je Gmail tako raširen, radi li se samo o lakoći korištenja, navici, kombinaciji tih dviju stvari ili nečem drugom.

Tablica 6.1 Pregled nekih od podataka koje Google prikuplja i postotak ispitanika koji su znali za prikupljanje navedenih podataka

Podaci koje Google prikuplja	Postotak ispitanika koji tvrde da su znali za prikupljanje navedenih podataka
Web stranice koje posjećujete	98,0%
Pojmovi pretraživanja	89,9%
Sadržaj web stranica	85,1%
Preuzete aplikacije	81,1%
Povijest kupnje	80,4%
Video zapisi na YouTubeu	75,0%
Oglasi koje ste pregledali	73,0%
Geografski podaci	70,3%
Podaci o uređajjima	62,2%
Kontakti	60,8%
Wi-Fi mreže i mobilni odašiljači	59,5%
e-mail i privici	54,7%
Fotografije i ostali sadržaj	49,3%
Demografski podaci	48,6%
Podaci iz javno dostupnih izvora i od oglašivača	43,9%
Podaci o pozivima (bez sadržaja poziva)	43,2%
Psihografski podaci	38,5%
Jezik i izričaj	34,5%
Glas korisnika i osoba u blizini	30,4%

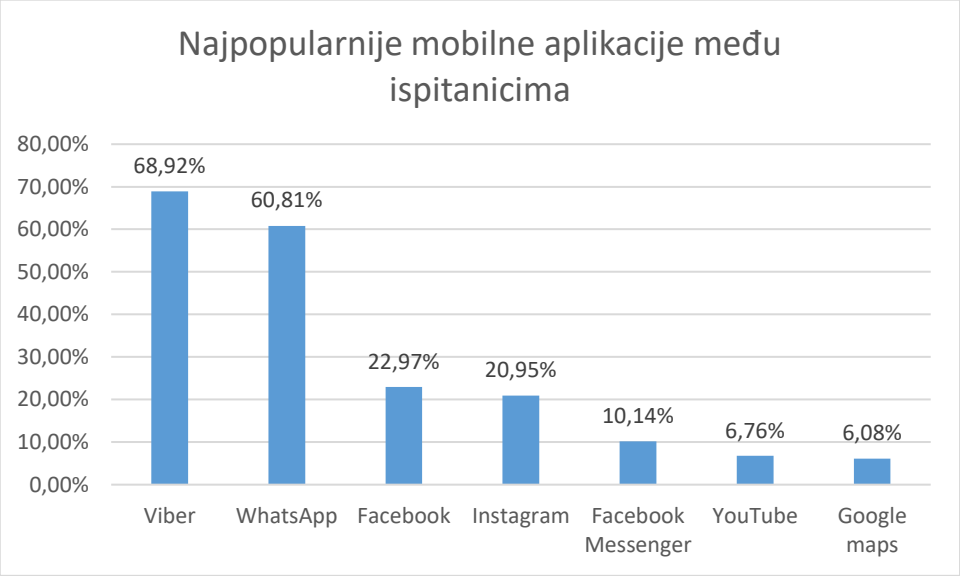
Također je zanimljiv i podatak da se ukupno 4,8 % ispitanika izjasnilo kako ih nimalo ili malo smeta da neka privatna tvrtka posjeduje toliku količinu podataka o njima, dok je 10,1 % negdje u sredini. 23,6 % ispitanika izjasnilo se kako ih to smeta, dok se 61,5 % ispitanika izjasnilo kako ih to izrazito smeta. Za one koji su odgovorili da ih to nimalo ne smeta ili ih malo smeta, razlozi koje su za to dali su sljedeći (postojala je mogućnost višestrukih odgovora):

- Od 16 osoba koje su odlučile odgovoriti zašto ih to ne smeta, njih 10 (62,5 %) izjavilo je kako ne znaju što bi koristili ako ne Google;
- Sedmero (43,75 %) je izjavilo da će tako dobiti bolju uslugu;

- Njih šest (37,5 %) se izjasnilo da će tako dobiti personalizirane oglase koji odgovaraju njihovim interesima; dok je
- Jedna osoba (6,25 %) je izjavila kako joj je to „potpuno nebitno“.

Osim toga, jedan od ispitanika je ispravno primijetio da se „većina tih usluga temelji na tome da što više korisnika daje povratnu informaciju“ te da navedene usluge ne bi bez toga tako dobro radile onako kako su ljudi navikli da one rade i za primjer je dala uslugu gdje joj aplikacija prikazuje lokaciju prometne gužve i na koji način ju zaobići. Jedna osoba je komentirala kako ne vjeruje da tvrtke na taj način prikupljaju i čuvaju njezine podatke.

Za Facebookovo prikupljanje podataka nekorisnika na stranicama s gumbom „*Like*“ znalo je 51,4 % ispitanika. Unatoč svijesti o privatnosti i izraženoj zabrinutosti, zanimljivi su rezultati pitanja o njima najdražim aplikacijama. Među ispitanicima je svakako najpopularnija aplikacija Viber koju koristi čak 102 ispitanika (njih gotovo 70 %) (grafikon na Slika 6.8), a koja prema njezinoj politici privatnosti također prikuplja brojne osobne podatke (Viber Privacy Policy). Sljedeće četiri najpopularnije aplikacije pripadaju Facebookovoj skupini proizvoda, o čijem prikupljanju podataka je bilo govora u prethodnom poglavlju.



Slika 6.8 Najpopularnije mobilne aplikacije među ispitanicima. Grafikon prikazuje aplikacije za koje je devet ili više ispitanika izjavilo da su im najdraže, a prikazan je postotak ispitanika koji ih koriste.

Prema podacima dobivenim ovim istraživanjem, a koji se odnose na čitanje izjava o privatnosti te korištenje Gmaila kao preferiranog e-mail servisa, kao i na popularnost aplikacija poznatih po svom prikupljanju velikih količina osobnih podataka, može se zaključiti kako je u ovom slučaju potvrđen paradoks privatnosti. Unatoč proklamiranoj brizi za privatnost i svijesti o tome da im je privatnost važna ili izrazito važna za gotovo 95 % ispitanika, njihovo stvarno ponašanje, odnosno korištenje navedenih usluga (Gmail, Viber, WhatsApp, Facebook, Instagram i Facebook Messenger) pokazuje kako ih svijest o važnosti privatnosti ne sprječava u korištenju brojnih usluga koje im tu privatnost uvelike narušavaju. Prema tome, većina ispitanika zanemaruje svoju privatnost kako bi koristila neku uslugu.

6.5.1. Istraživanja o paradoksu privatnosti

Provedeno je više istraživanja o paradoksu privatnosti, no ona vezana za mobilne aplikacije su rijetka. Barth et al. su pokušali pronaći objašnjenje za to paradoksalno ponašanje te su došli do saznanja kako na odluku o preuzimanju aplikacije ne utječu svijest o privatnosti, postojanje tehničkih znanja i financija kojima si mogu priuštiti aplikaciju, već će glavni aspekti na koje će korisnici obratiti pažnju biti funkcionalnost aplikacije, njezin dizajn i trošak (Barth et al., 2019: str. 55). Dakle, iako imaju potrebna sredstva, opet će radije odabrati aplikacije koje su besplatne, a koje zahtijevaju više dozvola zbog poslovnog modela koji koriste za ostvarivanje prihoda (Barth et al., 2019: str. 57, prema Chia et al., 2012). Liccardi et al. su također dokazali kako korisnici preferiraju potpuno besplatne aplikacije, čak i kada su druge aplikacije gotovo besplatne (Barth et al., 2019: str. 57, prema Liccardi et al., 2014).

Razlozi preuzimanja aplikacija koje narušavaju privatnost su različiti, od druženja, zabave, personaliziranih usluga pa do nekih financijskih prednosti (Barth et al., str. 57, prema Shklovski et al., 2014.). Tako je Bergström zaključio kako s porastom razine privatnosti podataka raste i svijest o privatnosti, no ona i dalje ne utječe na korisnikovo korištenje određenih usluga (Barth et al., str. 58, prema Bergström, 2015). Svijest o privatnosti postoji i korisnici su sve više svjesni kako aplikacije narušavaju privatnost, no dijeljenje informacija putem Interneta i raznih usluga i dalje raste (Barth et al., str. 57, prema Zafeiropoulou et al., 2013.) Barth i De Jong takvo paradoksalno ponašanje pojašnjavaju raznim psihološkim procesima koji se odvijaju tijekom procesa donošenja odluke (Barth et al., str. 57, prema Barth i De Jong, 2017):

- korisnici racionalno kalkuliraju odnos između rizika i prednosti;

- korisnici su svjesni rizika, no daju prednost čimbenicima kao što su nekakvo obećano zadovoljstvo ili zadovoljština, privlačnost aplikacije ili ograničeno vrijeme;
- korisnici intuitivno djeluju i ne procjenjuju rizik dijeljenja informacija.

S obzirom na rezultate istraživanja autorice ovoga rada vezano za znanje o tome što se prema zakonu ubraja u osobne podatke, postoji mogućnost kako je i to neznanje djelomično odgovorno za široko rasprostranjenu praksu dijeljenja osobnih podataka na Internetu. Međutim, pitanje je bi li svijest o tome što se sve ubraja u osobne podatke utjecala na dijeljenje podataka i preuzimanje aplikacija ukoliko korisnici aplikacija nisu svjesni rizika koji mogu proizaći iz njihovog korištenja mobilnih aplikacija koje prikupljaju velike količine podataka. Osim toga, Liccardi et al. navode kako tehnička znanja kao što je preuzimanje aplikacije nisu jednaka tehničkoj pismenosti gdje bi korisnik razumio procese koji se odvijaju unutar aplikacije pa korisnici koji jesu zabrinuti za svoju privatnost i dalje koriste online usluge (Barth et al., 2019: str. 57, prema Liccardi et al., 2014). Također, Acquisti et al. za paradoksalno ponašanje razlog pronalaze u neznanju i nerazumijevanju procesa jer korisnici u biti ne razumiju kako se njihovi podaci prikupljaju i koriste (Barth et al., 2019: str. 58, prema Acquisti et al., 2015), dok Barth et al. navode kako prosječnom čovjeku nije moguće utvrditi/provjeriti tehničke procese unutar aplikacija vezano za dopuštenja aplikacija čak i kada korisnici pročitaju dokumente kojima vlasnici aplikacija pojašnjavaju korištenje tih dopuštenja (Barth et al., 2019: str. 58.). S njima se slažu i Felt et al. koji smatraju kako je razumijevanje dozvola koje aplikacija traži ključna stavka jer korisnici ne mogu donijeti ispravne odluke vezane za svoju privatnost ukoliko ne razumiju što točno te dozvole znače (Barth et al., 2019: str. 65; prema Felt et al., 2012). Benton et al. su zaključili kako su dozvole nerazumljive i stoga neučinkovite (Barth et al., 2019: str. 64-65; prema Benton et al., 2013).

Zafeiropoulou et al. su proveli istraživanje vezano za aplikacije temeljene na lokaciji gdje su korisnici aplikacija privatnost stavljali u drugi plan jer im je korist koju dobivaju važnija (Barth et al., 2019., str. 65, prema Zafeiropoulou et al., 2013) što je također važan čimbenik za uzeti u obzir prilikom pronalaženja razloga za paradoksalno ponašanje.

Spyros Kokolakis pak smatra kako se paradoks privatnosti može dobro objasniti te da se više ne bi niti trebao smatrati paradoksom, već dilemom vezanom za privatnost. Navodi

kako bi ljudi voljeli zadržati svoju privatnost, ali u isto vrijeme žele koristiti usluge koje se temelje na dijeljenju osobnih podataka (Burkhardt, 2018).

Postoje dakako i istraživanja koja nisu potvrdila postojanje paradoksa privatnosti kao što je to istraživanje Krasnove et al. gdje je uočena negativna korelacija varijable percipiranog rizika privatnosti i varijable objavljivanja podataka na društvenim mrežama (Pavuna, 2019., str. 144; prema Krasnova et al. 2010). Prema Kokolakisu, rezultati istraživanja su različiti zbog različitih istraživačkih metoda, različitih konteksta u kojima su provedena, ali i različitih predodžbi što ustvari paradoks privatnosti jest. On predlaže daljnja istraživanja koja bi uzela u obzir stvarno ponašanje ispitanika, a ne samo samoprijavljeno ponašanje (Kokolakis, 2015: str. 2). Potvrda da paradoks privatnosti postoji ide u prilog onim tvrtkama koje prikupljaju velike količine osobnih podataka koje na taj način dobivaju poticaj za daljnje korištenje, ali i dovodi do povećavanja količine prikupljanja podataka (Kokolakis 2015: str. 3).

Zaključak

Pametni telefoni kao i drugi pametni uređaji donose sa sobom brojne prednosti, no i određeni rizik za privatnost korisnika s obzirom na količinu podataka koji su sadržani na samom uređaju kao i dozvole aplikacija koje korisnici na njih preuzimaju. Uvidom u literaturu i pojašnjenja različitih dozvola aplikacija za mobilne uređaje s Android operativnim sustavom, uočeno je kako rizici na istima proizlaze iz „rizičnih“ dozvola koje su inače aplikacijama potrebne kako bi pravilno funkcionirale (fotoaparat, pristup pohrani, slanje SMS poruka i dr.), a koje zlonamjerne aplikacije mogu iskoristiti za prikupljanje osobnih i drugih privatnih podataka. Osim „rizičnih“ dozvola, uvidom u podatke koji se mogu prikupiti putem „normalnih“ dozvola, može se zaključiti kako i one predstavljaju određeni rizik za privatnost jer se i putem njih mogu prikupljati podaci koje GDPR definira kao osobne podatke (npr. MAC adresa i jedinstveni identifikator uređaja). Zlonamjerne aplikacije prikupljene podatke mogu dalje prodavati zainteresiranim stranama koje će kombiniranjem prikupljenih podataka moći identificirati korisnike i izrađivati sveobuhvatne profile, a koji se zatim mogu iskoristiti za personalizirano oglašavanje. Osim navedenog, zlonamjerne aplikacije mogu uzrokovati i sigurnosni rizik za korisnika (npr. iskoristiti pristup SMS porukama i kontaktima kako bi s tog uređaja slali neželjene SMS poruke).

U praktičnom dijelu rada je temeljem Članaka 13. i 14. Opće uredbe o zaštiti podataka provedena analiza transparentnosti izjava o privatnosti šest odabranih mobilnih aplikacija po pitanju zahtijevanih informacija. Temeljem ljestvice koja je kreirana za potrebe ovoga rada, utvrđeno je kako je jedino izjava o privatnosti odabrane financijske aplikacije ocijenjena kao Zadovoljavajuće transparentna s obzirom da sadrži 19 od ukupno 22 zahtijevane informacije. Aplikacija iz kategorije zabave pokazala se kao Nedovoljno transparentna jer sadrži samo četiri od 22 zahtijevane informacije. Preostale četiri aplikacije iz kategorija oglasi/prodaja i kupnja, korisnička služba, društvene mreže i komunikacija ocijenjene su kao Srednje transparentne. Najčešće su nedostajale informacije o tome kako je moguće dobiti kopiju prenesenih podataka (u svih šest aplikacija), zatim hoće li informacije o podacima prikupljenim iz drugih izvora biti dostavljene ispitaniku u propisanom roku (u pet aplikacija), kao i koje su zaštitne mjere prilikom prijenosa podataka (u četiri od šest aplikacija). Osim toga, u četiri aplikacije nedostajale su i informacije o tome postoji li automatizirano donošenje odluka nakon izrade profila kao i kakve su posljedice takve obrade podataka za ispitanika, no moguće je kako je razlog tome nepostojanje automatiziranog

donošenja odluka (s obzirom da niti priroda usluge koju aplikacija pruža nije takva) pa stoga nije niti navedeno.

Možemo pretpostaviti kako je financijska aplikacija sadržavala najviše informacija upravo zbog toga što se radi o banci, a kojoj su za pružanje usluga potrebni razni osobni podaci čija je zaštita i inače na visokoj razini. Međutim, s obzirom na mali broj analiziranih aplikacija bez usporedbe iz jednakih kategorija, nije moguće utvrditi što je tome razlog te bi navedeno trebalo dodatno istražiti. Dodatni kriterij potvrdne radnje vezano za privolu, odnosno jasnog davanja privole za obradu podataka ispunila je samo aplikacija iz kategorije komunikacija, a izjava o privatnosti mogla se unutar dva „dodira" naći samo u aplikacijama iz kategorija zabava, oglasi/prodaja i kupnja i komunikacija. Osim toga, temeljem usporedbe dozvola aplikacija i popisa podataka sadržanih u izjavama o privatnosti, utvrđeno je kako izjave o privatnosti nemaju poimence na jednom mjestu navedene sve dozvole aplikacija s pojašnjenjima u koju svrhu se navedeni podaci prikupljaju, no aplikacije iz kategorija društvenih mreža i komunikacija u svojim izjavama o privatnosti sadrže većinu podataka iz dozvola aplikacija.

U posljednjem dijelu rada provedeno je istraživanje na 148 ispitanika u Republici Hrvatskoj kojemu je cilj bio ustanoviti koliko su građani RH svjesni narušavanja svoje privatnosti putem mobilnih aplikacija te sprječava li ih to saznanje u preuzimanju istih. Dakle, ovim istraživanjem pokušalo se ustanoviti postoji li i ovdje paradoks privatnosti odnosno ponašaju li se ispitanici paradoksalno kada se radi o njihovoj privatnosti. U tu svrhu pojašnjen je i sam paradoks te je dan pregled rezultata nekih od istraživanja, ali su navedena i moguća objašnjenja paradoksalnog ponašanja ispitanika što bi značilo da, prema Kokolakisu (Burkhardt, 2018), paradoks privatnosti ne postoji, već samo dilema privatnosti.

U provedenom istraživanju potvrđeno je paradoksalno ponašanje ispitanika jer su s obzirom na važnost koju pridaju svojoj privatnosti (njih gotovo 95 % izjasnilo se kako svoju privatnost smatra važnom ili izrazito važnom) naveli kako koriste usluge i aplikacije koje narušavaju njihovu privatnost, pri čemu njih samo 13,5 % redovito čita izjave o privatnosti i uvjete korištenja, a dozvole aplikacija uvijek regulira samo 25 %. Pokušaj objašnjavanja paradoksalnog ponašanja prelazi okvire ovoga rada, no s obzirom na rezultate pitanja vezanog za pojam osobnih podataka u kojem čak 19,6 % ispitanika ne zna kako se ime i prezime prema zakonu ubrajaju u osobne podatke, jedan od potencijalnih razloga pružanja osobnih podataka raznim aplikacijama mogao bi biti needuciranost ispitanika o tome što se ubraja u osobne podatke i koji to podaci zaslužuju posebnu zaštitu kao i kakvi rizici proizlaze

iz davanja prekomjernih osobnih podataka. Osim toga, na temelju odgovora nekih od ispitanika koji su izjavili kako ne znaju što bi koristili ako ne Google, otvara se mogućnost za još jedno potencijalno objašnjenje paradoksalnog ponašanja, a to je navika, kao i činjenica da i mnogi drugi koriste iste usluge te je povezivanje s njima na taj način lakše i jednostavnije. S obzirom na navedeno, postoji mogućnost kako doista postoji objašnjenje za paradoksalno ponašanje ispitanika te da se ipak radi o dilemi privatnosti, a ne paradoksu privatnosti.

Popis kratica

ACCC	Australian Competition & Consumer Commission	Australska komisija za tržišno natjecanje i potrošače
AZOP	Agencija za zaštitu osobnih Podataka	
CERT	Computer Emergency Response Team	organizacijski entitet za odgovor na računalno-sigurnosne incidente
ENISA	European Union Agency for Network and Information Security	Agencija Europske unije za mrežnu i informacijsku sigurnost
EU	European Union	Europska unija
FTC	Federal Trade Commission	Savezna trgovinska komisija
GDPR	General Data Protection Regulation	Opća uredba o zaštiti podataka
GPS	Global Positioning System	Globalni položajni sustav
ICO	Information Commissioner's Office	Ured povjerenika za informacije
IMEI	International Mobile Equipment Identity	Međunarodni identifikacijski kod uređaja
IP	Internet Protocol	Internet protokol
IT	Information Technology	Informacijske tehnologije
ISDN	*Integrated Services Digital Network*	digitalna mreža integriranih usluga
JMBG	Jedinstveni matični broj građana	
MAC	Media Access Control (MAC adresa)	Kontrola pristupa medijima
MIT	Massachussets Institute of Technology	
NSA	National Security Agency	Nacionalna sigurnosna agencija
OECD	The Organisation for Economic Co-operation ad Development	Organizacija za ekonomsku suradnju i razvoj
OIB	Osobni identifikacijski broj	
OS	Operativni sustav	
PBZ	Privredna banka Zagreb d.d.	
RFID	Radio Frequency Identification	Radiofrekventna identifikacija
RH	Republika Hrvatska	
SAD	Sjedinjene Američke Države	

SD	Secure Digital	
SMS	Short Message Service	usluga slanja kratkih tekstualnih poruka
SSID	Service Set Identifier	Identifikator postavljenog servisa
MMS	Multimedia Messaging Service	usluga slanja multimedijskih poruka
UK	United Kingdom	Ujedinjeno Kraljevstvo Velike Britanije i Sjeverne Irske
URL	Uniform Resource Locator	Usklađeni lokator sadržaja
UUID	Universally unique Identifier	Univerzalni jedinstveni identifikator
WAP	Wireless Application Protocol	Standard za bežični prijenos informacija do mobilnih telefona

Popis slika

Popis tablica

Literatura

[1] A1 d.o.o., Izjava o zaštiti osobnih podataka za A1 d.o.o., https://ssc.a1.hr/documents/10307706/46596980/A1+Izjava_o_zastiti_osobnih_podataka_TD_20092018.pdf/97948daf-ea8e-ec92-61ee-cec47d6ee62d, preuzeto 2. 7. 2019.

[2] ACHARA, J.P., CUNCHE, M., ROCA, V., FRANCILLON, A., Short Paper: WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission, 2014., http://s3.eurecom.fr/docs/wisec14_Achara.pdf, preuzeto 13. 8. 2019.

[3] ACHARA, J., ACS, G., CASTELLUCCIA, C., On the Unicity of Smartphone Applications, in 14th ACM CCS Workshop on Privacy in Electronic Society (ACM WPES), 2015.

[4] ACHARA, J., ROCA, V., CASTELLUCCIA, C., FRANCILLON, A., MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs, 2016.

[5] ACQUISTI, A., GROSS, R., Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. U *G. Danezis & P. Golle (Eds.), Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science* (Vol. 4258, (2006), str. 36–58). Berlin, Heidelberg: Springer. https://doi.org/10.1007/11957454_3

[6] ACQUISTI, A., BRANDIMARTE, L., LOEWENSTEIN, G., 2015. Privacy and human behavior in the age of information. Science 347 (6221), (2015), 509–514.

[7] AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA (AZOP), Pravo na zaštitu osobnih podataka, https://azop.hr/prava-ispitanika/detaljnije/pravo-na-zastitu-osobnih-podataka, preuzeto 5. 7. 2019.

[8] AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA (AZOP), Vodič kroz opću uredbu o zaštiti podataka, https://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka, preuzeto 5. 7. 2019.

[9] ALAWAJY, A.M., An overview of privacy in mobile applications from an HCI perspective, 2018., https://pdfs.semanticscholar.org/dbd8/51bf6fe0590673b107b3fe6fcd2b36628a62.pdf , preuzeto 29. 7. 2019.

[10] ANDROID DEVELOPERS, Distribution dashboard, https://developer.android.com/about/dashboards/, preuzeto 6. 8. 2019.

[11] ANDROID DEVELOPERS, Permissions overview, https://developer.android.com/guide/topics/permissions/overview#permissions_for_optional_hardware_features, preuzeto 6. 8. 2019.

[12] ANDROIDPERMISSIONS, How permissions can be abused by malicious apps, 1. 4. 2018., http://androidpermissions.org/How-permissions-can-be-abused-by-malicious-apps/, preuzeto 20. 8. 2019.

[13] AUSTRALIAN COMPETITION & CONSUMER COMMISSION (ACCC), Digital Platforms Inquiry - Final Report, lipanj 2019.,

https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf, preuzeto 22. 7. 2019.

[14] BARNES, S. B., A privacy paradox: Social networking in the United States. First Monday, 11(9), (2006) 1–12. http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

[15] BARTH, S., DE JONG, M.D.T., The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telematics and Informatics, 34 (2017) 1038–1058.

[16] BARTH, S., DE JONG, M. D. T., JUNGER, M., HARTEL, P. H., & ROPPELT, J. C., Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and Informatics, 41 (2019), 55-69. https://pure.tudelft.nl/portal/files/54640951/1_s2.0_S0736585317307724_main.pdf, preuzeto 1. 8. 2019.

[17] BATEMAN, R., GDPR and Mobile Apps, 18. 2. 2019., https://www.termsfeed.com/blog/gdpr-mobile-apps/, preuzeto 1. 7. 2019.

[18] BBC NEWS, Facebook „to be fined $5bn over Cambridge Analytica scandal“, 13. 7. 2019., https://www.bbc.com/news/world-us-canada-48972327, preuzeto 4. 9. 2019.

[19] BERGSTRÖM, A., Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. Computers in Human Behavior 53, (2015), 419–426.

[20] BENTON, K., JEAN CAMP, L., GARG, V., Studying the effectiveness of Android application permissions requests. San Diego, USA In: Fifth International Workshop on SECurity and SOCial Networking, (2013), str. 291–296.

[21] BINNS, R., LYNGS, U., VAN KLEEK, M., ZHAO, J., LIBERT, T., SHADBOLT, N., Third Party Tracking in the Mobile Ecosystem, 2018, https://arxiv.org/pdf/1804.03603.pdf, preuzeto 14. 8. 2019.

[22] BLUMBERG, A., ECKERSLEY, P., On locational privacy and how to avoid losing it forever, 2009, https://www.eff.org/files/eff-locational-privacy.pdf, preuzeto 14. 8. 2019.

[23] BOOK, T., PRIDGEN, A., WALLACH, D. S. Longitudinal analysis of android ad library permissions, 18. 4. 2013., https://arxiv.org/pdf/1303.0857.pdf, preuzeto 14. 8. 2019.

[24] BOYLES, J.L., SMITH, A., MADDEN, M., Privacy and Data Management on Mobile Devices, Pew Research Center, 5. 9. 2012, http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx., preuzeto 2. 8. 2019.

[25] BROOKMAN, J., ROUGE, P., ALVA, A.E.A., Cross-Device Tracking: Measurement and Disclosures, in Proceedings on Privacy Enhancing Technologies (PETS2017), 2017.

[26] BURGOON, J. K., Privacy and Communication. Annals of the International Communication Association, 6(1), (1982), 206–249. https://doi.org/10.1080/23808985.1982.11678499
BURGOON, J. K., PARROTT, R., LE POIRE, B. A., KELLEY, D. L., WALTHER,

J. B., PERRY, D. Maintaining and Restoring Privacy through Communication in different types of
Relationships. Journal of Social and Personal Relationships, 6, (1989), 131–158.

[27] BURKHARDT, K., The privacy paradox is a privacy dilemma, 24. 8. 2018., https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/, preuzeto 29. 8. 2019.

[28] BURNS, H. How To Protect Your Users With The Privacy By Design Framework, 27. 7. 2017., https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/, preuzeto 10. 7. 2019.

[29] BURNS, H., How GDPR Will Change The Way You Develop, 27. 2. 2018., https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/, preuzeto 5. 7. 2019.

[30] BUSINESSDICTIONARY, Terms and Conditions, http://www.businessdictionary.com/definition/terms-and-conditions.html, preuzeto 12. 7. 2019.

[31] CADWALLADR, C., "I made Steve Bannon's psychological warfare tool": meet the data war whistleblower, 18. 3. 2018., https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump, preuzeto 15. 9. 2019.

[32] CARNet, Usporedba "sandbox" programskih alata, 2009, https://www.cert.hr/wp-content/uploads/2009/03/CCERT-PUBDOC-2009-03-259.pdf, preuzeto 16. 9. 2019.

[33] CAVOUKIAN, A., Privacy by Design, The 7 Foundational Principles, 2009., https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf, preuzeto 10. 7. 2019.

[34] CHIA, P.H., YAMAMOTO, Y., ASOKAN, N., Is this app safe? A large scale study on application permissions and risk signals. Proceedings of the 21st International Conference on World Wide Web 2012, (2012), str. 311–320.

[35] CIMPANU, C., Google restricts which Android apps can request Call Log and SMS permissions, 9. 10. 2018., www.zdnet.com/article/google-restricts-which-android-apps-can-request-call-log-and-sms-permissions, preuzeto 6. 9. 2019.

[36] CLEARY, G., Mobile Privacy: What Do Your Apps Know About you?, 16. 8. 2018. https://www.symantec.com/blogs/threat-intelligence/mobile-privacy-apps, preuzeto 1. 8. 2019.

[37] COOPER, S., How to secure your Android app permissions, 22. 8. 2018., https://www.comparitech.com/blog/vpn-privacy/secure-android-app-permissions/, preuzeto 20. 8. 2019.

[38] CUNCHE, M.-A. KAAFAR, AND R. BORELI. Linking wireless devices using information contained in Wi-Fi probe requests. Pervasive and Mobile Computing, 2013.

[39] DATTA, AMIT, TSCHANTZ, M.C., DATTA, ANUPAM. 2015. Automated experiments on ad privacy settings. Proceedings on Privacy Enhancing Technologies 2015, 1 (2015), 92–112.

[40] DROZHZHIN, A., App permissions in Android 8: The complete guide, 24. 9. 2018., https://www.kaspersky.com/blog/android-8-permissions-guide/23981/, preuzeto 19. 8. 2019.

[41] EGELMAN, S., Ad IDs behaving badly, 14. 2. 2019., https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly/, preuzeto 16. 8. 2019.

[42] E-PRIVACY FACTSHEET, svibanj 2018., https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53969, preuzeto 10. 8. 2019. godine

[43] EUROPEAN COMMISSION, COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications, 10.1.2017., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0003, preuzeto 10. 8. 2019.

[44] ENISA - EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Privacy and data protection in mobile applications. A study on the app development ecosystem and the technical implementation of GDPR. Technical report, studeni 2017., https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications, preuzeto 15. 7. 2019.

[45] EUROPSKA KOMISIJA, Preuzmite kontrolu nad svojim identitetom, lipanj 2019, https://ec.europa.eu/commission/sites/beta-political/files/virtual_identity_hr.pdf, preuzeto 7. 8. 2019.

[46] FACEBOOK, Google Play, https://play.google.com/store/apps/details?id=com.facebook.katana, preuzeto 2. 7. 2019.

[47] FACEBOOK HELP CENTER, How does automatic alt text work?, https://www.facebook.com/help/216219865403298?helpref=faq_content, preuzeto 7. 8. 2019.

[48] FACEBOOK HELP CENTER, How does Facebook's face recognition work?, https://www.facebook.com/help/218540514842030?ref=dp, preuzeto 1. 8. 2019.

[49] FACEBOOK HELP CENTER, How do Facebook's Location Settings work?, https://www.facebook.com/help/278928889350358?helpref=search&sr=2&query=location%20services, preuzeto 1. 8. 2019.

[50] FACEBOOK HELP CENTER, What are the Facebook Products?, https://www.facebook.com/help/1561485474074139?ref=dp, preuzeto 5. 8. 2019.

[51] FACEBOOK HELP CENTER, What is the face recognition setting on Facebook and how does it work?, https://www.facebook.com/help/122175507864081, preuzeto 7. 8. 2019.

[52] FACEBOOK, Pravila o upotrebi podataka, https://hr-hr.facebook.com/privacy/explanation, preuzeto 2. 7. 2019.

[53] FACEBOOK, Pravna osnova, https://www.facebook.com/about/privacy/legal_bases, preuzeto 1. 8. 2019.

[54] FACEBOOK REPORTS FOURTH QUARTER AND FULL YEAR 2018 RESULTS. https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q4/Q4-2018-Earnings-Release.pdf, preuzeto 10. 9. 2019.

[55] FACEBOOK, Uvjeti pružanja usluge, https://hr-hr.facebook.com/legal/terms, preuzeto 2. 7. 2019.

[56] FACEBOOK, Pravila o upotrebi kolačića, https://hr-hr.facebook.com/policies/cookies/, preuzeto 2. 7. 2019.

[57] F-DROID, https://f-droid.org/en/packages/de.wikilab.android.ldapsync/, preuzeto 1. 8. 2019.

[58] FEDERAL TRADE COMMISSION, Mobile privacy disclosures, Buildign Trust Through Transparency, 2013., https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf, preuzeto 13. 8. 2019.

[59] FEINER, L., Alphabet rises after earnings beat, announces $25 billion share repurchase, 25. 7. 2019., https://www.cnbc.com/2019/07/25/alphabet-q2-2019-earnings.html, preuzeto 10. 9. 2019.

[60] FELT, A.P., HA, E., EGELMAN, S., HANEY, A., CHIN, E., WAGNER, D., Android permissions: user attention, comprehension, and behavior. Symposium on Usable
Privacy and Security (SOUPS), July, 11–13, 2012. Washington DC USA.

[61] FREEPRIVACYPOLICY, „Privacy Policies versus Terms and Conditions“, 11. 3. 2019., https://www.freeprivacypolicy.com/blog/privacy-policy-vs-terms-conditions/, preuzeto 12. 7. 2019.

[62] GADALETA, M., AND ROSSI, M., IDNET: Smartphone-based Gait Recognition with Convolutional Neural Networks, 2016.

[63] GARTNER, INC., Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017, 22. 2. 2018., https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017, preuzeto 6. 9. 2019.

[64] GMAIL, Google Play, https://play.google.com/store/apps/details?id=com.google.android.gm&hl=hr, preuzeto 2. 7. 2019.

[65] GMAIL – Izradite račun, https://accounts.google.com/signup/v2/webcreateaccount?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fpc%3Dtopnav-about-n-en&flowName=GlifWebSignIn&flowEntry=SignUp

[66] GOOGLEOVA PRAVILA O PRIVATNOSTI, https://policies.google.com/privacy, preuzeto 2. 7. 2019.

[67] GOOGLE, Privatnost i uvjeti, https://policies.google.com/?hl=hr

[68] GOOGLE SAFETY CENTER, Understanding how Google ads work, https://safety.google/privacy/ads-and-data/, preuzeto 2. 7. 2019.

[69] GOOGLE, Tehnologije, https://policies.google.com/technologies, preuzeto 2. 7. 2019.

[70] GOOGLEOVI UVJETI PRUŽANJA USLUGE, https://policies.google.com/terms, preuzeto 2. 7. 2019.

[71] HANNAK, A., SOELLER, G., LAZER, D., MISLOVE, A., WILSON, C., 2014. Measuring price discrimination and steering on e-commerce web sites. In Proceedings of the 2014 conference on internet measurement conference. ACM, (2014), 305–318.

[72] HARCOURT, B. E., Exposed: desire and disobedience in the digital age. Cambridge, Massachusetts: Harvard University Press, 2015.

[73] HBO GO, Pravila o kolačićima, https://hbogo.hr/pravila-o-kolacicima, preuzeto 16. 8. 2019.

[74] HILDENBRAND, J., What those scary app permissions mean, 26. 1. 2017. https://www.androidcentral.com/look-application-permissions, preuzeto 20. 8. 2019.

[75] HILTS, A., PARSONS, C., KNOCKEL, J., Every Step You Fake. A Comparative Analysis of Fitness Tracker Privacy and Security," 2016., https://citizenlab.org/2016/04/every-step-you-fake-finalreport/.

[76] JOINSON, A.N., REIPS, U.D., BUCHANAN, T., PAINE SCHOFIELD, C.B., Privacy, trust, and self- disclosure online. Human-Computer Interaction 25(1) (2010), 1–24

[77] KEACH, S., Data Danger – Cambridge Analytica closure – how was it involved with the Facebook data scandal and who is whistleblower Christopher Wylie?, 3. 5. 2018., www.thesun.co.uk/news/5844734/cambridge-analytica-closure-facebook-data-scandal-christopher-wylie/, preuzeto 4. 8. 2019.

[78] KOKOLAKIS, S., Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security, July 2015, DOI:10.1016/J.COSE.2015.07.002, https://www.researchgate.net/publication/280244291_Privacy_attitudes_and_privacy_behaviour_A_review_of_current_research_on_the_privacy_paradox_phenomenon, preuzeto 13. 8. 2019.

[79] KRASNOVA, H., SPIEKERMANN, S., KOROLEVA, K., & HILDEBRAND, T. Online social networks: Why we disclose. Journal of Information Technology, 25(2) (2010) 109–125. https://doi.org/10.1057/jit.2010.6, preuzeto 10. 7. 2019.

[80] KURTZ, A., GASCON, H., BECKER, T., FREILING, G., RIECK, K., Fingerprinting Mobile Devices Using Personalized Configurations, in Proceedings on Privacy Enhancing Technologies, 2016, https://petsymposium.org/2016/files/papers/Fingerprinting_Mobile_Devices_Using_Personalized_Configurations.pdf, preuzeto 15. 7. 2019.

[81] LAMARCA, A., Y. CHAWATHE, S. CONSOLVO, J. HIGHTOWER, I. SMITH, J. SCOTT, T. SOHN, J. HOWARD, J. HUGHES, F. POTTER, Tabert, J., Powledge, P. Borriello, G., Schilit, B. Place lab: Device positioning using radio beacons in the wild. In Pervasive computing. Springer, 2005.

[82] LICCARDI, I., PATO, J., WEITZNER, D.J., ABELSON, H., DE ROURE, D., No technical understanding required: Helping users make informed choices about access

to their
personal data. MOBIQUITOUS, 2014, London, Great Britain, 140-150.

[83] LINDQVIST, J., AURA, T., DANEZIS, G., KOPONEN, T., MYLLYNIEMI, A., MÄKI, J., ROE, M.
Privacy-preserving 802.11 access-point discovery, ACM WiSec, 2009.

[84] MANGSET, P.L. Analysis of Mobile Application's Compliance with the General Data Protection Regulation (GDPR) https://www.nodesagency.com/services-old/gdpr-mobile-apps/, 2018. preuzeto 3. 7. 2019.

[85] MARCO, Automatska identifikacija: RFID, http://marco.hr/tehnologije/tehnologije-RFID.htm, preuzeto 20. 7. 2019.

[86] MASLOW, A.H. A Theory of human Motivation. Psychological Review, 50(4) (1943), 370–396

[87] MATIĆ, T., Formularni ugovori u elektroničkom obliku, veljača 2008., pregledni znanstveni rad, https://hrcak.srce.hr/file/34600, preuzeto 10. 9. 2019.

[88] MAVROUDIS, V., S. HAO, S., Y. FRATANTONIO, Y., On the Privacy and Security of the Ultrasound Ecosystem., in Proceedings on Privacy Enhancing Technologies, 2017.

[89] MELICHER, W., MAZUREK, M.L., KURILOVA, D., SEGRETI, S.M., KALVANI, P., SHAY, R., UR, B., BAUER, L., CHRISTIN, N., CRANOR, L., Usability and security of text passwords on mobile devices, in 34th Annual ACM Conference on Human Factors in Computing Systems, 2016.

[90] MICHALEVSKY, Y. BONEH, D., AND NAKIBLY, G., Gyrophone: Recognizing speech from gyroscope signals. In USENIX Security Symposium (2014), 1053–1067.

[91] MIHALIĆ, A., Platform mediated business networks, 1. 4. i 5. 4. 2017. godine, kolegij Disruptivne tehnologije, Visoko učilište Algebra

[92] MIKIANS, J., GYARMATI, L, ERRAMILLI, V., AND LAOUTARIS, N. Detecting price and search discrimination on the Internet. In Proceedings of the11th ACM Workshop on Hot Topics in Networks, ACM (2012), 79–84.

[93] MOJ A1, Google Play, https://play.google.com/store/apps/details?id=hr.infinum.mojvip, preuzeto 2. 7. 2019.

[94] MONTJOYE, Y.A. DE, HIDALGO, C., VERLEYSEN, M., AND BLONDEL, V., Unique in the Crowd: The Privacy Bounds of Human Mobility, 2013., https://www.nature.com/articles/srep01376, preuzeto 16. 8. 2019.

[95] NACIONALNI CERT, Phishing, www.cert.hr/phishing, preuzeto 1. 8. 2019.

[96] NACIONALNI CERT, Sigurnosni pregled Android operacijskog sustava, CERT.hr-PUBDOC-2018-8-365, 21. 8. 2018., https://www.cert.hr/wp-content/uploads/2018/08/android.pdf, preuzeto 19. 7. 2019.

[97] NG, A. More than 1,000 Android apps harvest data even after you deny permissions, 8. 7. 2019., https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/, preuzeto 20. 8. 2019.

[98] NJUŠKALO, Google Play, https://play.google.com/store/apps/details?id=com.undabot.android.njuskalo, preuzeto 2. 7. 2019.

[99] NJUŠKALO, Politika privatnosti, https://www.njuskalo.hr/3d/static/lgl/index.html, preuzeto 2. 7. 2019.

[100] NJUŠKALO, Undabot, https://undabot.com/projects/njuskalo/, preuzeto 3. 7. 2019.

[101] OBAR, J.A., OELDORF-HIRSCH; A., The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, lipanj 2018. godine, https://www.ftc.gov/system/files/documents/public_comments/2016/10/00067-129185.pdf, preuzeto 10. 7. 2019.

[102] OECD, The App Economy, 16. 12. 2013. OECD DigitalEconomy Papers, No. 230, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3ttftlv95k-en, preuzeto 13. 8. 2019.

[103] O'NEIL, F., Analyzing Privacy Policies using the Privacy by Design Framework, 2016., https://www.ftc.gov/system/files/documents/public_comments/2016/10/00025-129036.pdf, preuzeto 19. 7. 2019.

[104] OPĆA UREDBA O ZAŠTITI PODATAKA (GDPR), Europski parlament i Vijeće Europske unije, 27. 4. 2016., https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=HR, preuzeto 2. 7 2019.

[105] OTVORENI, Opći uvjeti zaštite osobnih podataka unutar mobilne aplikacije OtvoreniOnAir, https://www.globaldizajn.hr/GooglePlay/GooglePlayPrivacyPolicy.aspx?id=174, preuzeto 2. 7. 2019.

[106] OTVORENI, Google Play, https://play.google.com/store/apps/details?id=com.globaldizajn.otvoreni.onair, preuzeto 2. 7. 2019.

[107] PAVUNA, A. Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova. Doktorski rad. Fakultet političkih znanosti, Sveučilište u Zagrebu, 2019. https://hrcak.srce.hr/219878, preuzeto 14. 7. 2019.

[108] PBZ MOBILNO BANKARSTVO, Google Play, https://play.google.com/store/apps/details?id=hr.asseco.android.intesa.isbd.pbz, preuzeto 2. 7. 2019.

[109] PONTIUS, N., What are RFID Tags? Learn How RFID Tags Work, What They're Used for, and Some of the Disadvantages of RFID Technology, 7. 4. 2017., https://www.camcode.com/asset-tags/what-are-rfid-tags, preuzeto 25. 7. 2019.

[110] PRIVREDNA BANKA ZAGREB, d.d., Informacija o obradi osobnih podataka Privredne banke Zagreb d.d.(sukladno člancima 13. i 14. Opće uredbe o zaštiti podataka), https://www.pbz.hr/document/documents/PBZ/ostalo/Informacija-o-obradi-osobnih-podataka-Privredne-banke-Zagreb.pdf, preuzeto 2. 7. 2019.

[111] PRIJEDLOG UREDBE O PRIVATNOSTI I ELEKTRONIČKIM KOMUNIKACIJAMA, 2017., Europski parlament i Vijeće, https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52017PC0010&from=EN, preuzeto 21. 8. 2019.

[112] PRIVACY INTERNATIONAL, How Apps on Android Share Data with Facebook – Report, 29. 12. 2018a. https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report, preuzeto 14. 8. 2019.

[113] PRIVACY INTERNATIONAL, How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), prosinac 2018b., https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf, preuzeto 14. 8. 2019.

[114] RADNA SKUPINA ZA ZAŠTITU PODATAKA IZ ČLANKA 29., Opinion 2/2013: Apps on smart devices, 2013., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, preuzeto 2. 8. 2019.

[115] RADNA SKUPINA ZA ZAŠTITU PODATAKA IZ ČLANKA 29., Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9. 4. 2014., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, preuzeto 15. 7. 2019.

[116] RADNA SKUPINA ZA ZAŠTITU PODATAKA IZ ČLANKA 29., Smjernice o transparentnosti na temelju Uredbe 2016/679, 11. 4. 2018., https://azop.hr/images/dokumenti/217/smjernice-o-transparentnosti.pdf, preuzeto 5. 7. 2019.

[117] REARDON, J., FEAL, Á., WIJESEKERA, P., ELAZARI BAR ON, A., VALLINA-RODRIGUEZ, N., EGELMAN, S., 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, 28th USENIS Security Symposium, 14-16.8.2019., https://www.usenix.org/system/files/sec19-reardon.pdf, preuzeto 20. 8. 2019.

[118] REDDY, S., Android Runtime Permissions, Recent Policy Changes and Security Vulnerabilities, 7. 12. 2018., https://medium.com/finbox/android-runtime-permissions-recent-policy-changes-and-security-vulnerabilities-935c5fc88f3d, preuzeto 13. 8. 2019.

[119] RÖSSLER, B., Privacies. U B. Rössler (Ed.), Privacies: Philosophical Evaluations (str. 1–19). Stanford: Stanford University Press, 2004.

[120] RUHENSTROTH, M., Mobilsicher.de, How Facebook knows which apps you use – and why this matters, 20. 12. 2018. , https://mobilsicher.de/hintergrund/how-facebook-knows-which-apps-you-use-and-why-this-matters, preuzeto 16. 8. 2019.

[121] RUHENSTROTH, M., Auch iOS-Apps senden unbemerkt Daten an Facebook, 6. 1. 2019., https://mobilsicher.de/aktuelles/auch-ios-apps-senden-unbemerkt-daten-an-facebook, preuzeto 26. 7. 2019.

[122] SAISH K., (57) Detailed Android App Permissions List and What Do They Mean, 24. 2. 2019., https://www.techk47.com/android-app-permissions-list/, preuzeto 19. 8. 2019.

[123] SENEVIRATNE, S., SENEVIRATNE, A., MOHAPATRA, P., MAHANTI, A., Predicting user traits from a snapshot of apps installed on a smartphone, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 18, no. 2, (2014), p. 1–8.

[124] SHKLOVSKI, I., MAINWARING, S.D., SKÚLADÓTTIR, H.H., BORGTHORSSON, H., Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. Chi,
Toronto, ON, Canada, 2347-2356, 2014.

[125] SIMON, L., XU, W., ANDERSON, R., Don't interrupt me while i type: Inferring text entered through gesture typing on android keyboards. Proceedings on Privacy Enhancing Technologies, 2016(3):136–154, 2016.

[126] SOLOVE, D. J., Conceptualizing privacy. California Law Review, 90(4), (2002), 1087–1155.
https://doi.org/10.1145/1929609.1929610

[127] SOLOVE, D. J., 'I've got nothing to hide' and other misunderstandings of privacy. San Diego Law Review, 44: (2007), 745-772.

[128] SOLOVE, D. J., Introduction: Privacy self-management and the consent dilemma. Harvard Law Review, 126 (2012), 1880-1903.

[129] STATISTA.COM, Number of apps available in leading app stores as of 2nd quarter 2019, 6. 8. 2019., https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, preuzeto 14. 8. 2019.

[130] STEGNER, B., 5 Smartphone App Permissions You Need to Check Today, 15. 1. 2018., https://www.makeuseof.com/tag/important-smartphone-app-permissions/, preuzeto 19. 8. 2019.

[131] TADDEI, S., CONTENA, B. (2013). Privacy, trust and control: Which relationships with online
self-disclosure? Computers in Human Behavior, 29(3), (2013), 21–826.
https://doi.org/10.1016/j.chb.2012.11.022

[132] TERMSFEED, „5 reasons why you need Terms and Conditions";
https://www.termsfeed.com/blog/5-reasons-need-terms-conditions/, preuzeto 12. 7. 2019.

[133] TREND MICRO, 12 Most abused Android app permissions, http://about-threats.trendmicro.com/us/library/image-gallery/12-most-abused-android-app-permissions, preuzeto 29. 7. 2019.

[134] TUFEKCI, Z., Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), (2008), 20–36. https://doi.org/10.1177/0270467607311484

[135] UK INFORMATION COMMISSIONER'S OFFICE, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information, 25. 10. 2018., https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/, preuzeto 1. 11. 2018.

[136] VAN DIGGELEN, F., WANT, R. WANG, W., How to achieve 1-meter accuracy in Android, 3. 7. 2018., https://www.gpsworld.com/how-to-achieve-1-meter-accuracy-in-android/, preuzeto 21. 8. 2019.

[137] VAUGHAN-NICHOLS, S.J., COTANA: The spy in Windows 10, 15. 8. 2016., https://www.computerworld.com/article/3106863/cortana-the-spy-in-windows-10.html, preuzeto 7. 9. 2019.

[138] VIBER PRIVACY POLICY, https://www.viber.com/terms/viber-privacy-policy/, preuzeto 11. 9. 2019.

[139] WEEKS, C., Guide to Android App Permissions & How to Use Them Smartly, 29. 1. 2018., https://www.avg.com/en/signal/guide-to-android-app-permissions-how-to-use-them-smartly, preuzeto 19. 8. 2019.

[140] WESTIN, A. F. Privacy and freedom. New York: Atheneum Press, 1967.

[141] WHITTAKER, Z., Many popular iPhone apps secretly record your screen without asking, 7. 2. 2019., https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=djS5oy86t1v95E2VqeZAQA, preuzeto 16. 8. 2019.

[142] YERUKHIMOVICH, A., BALEBAKO, R., BOUSTEAD, A. E., CUNNINGHAM, R. K., WELSER, W. I HOUSLEY, R. Can Smartphones and Privacy Coexist?, RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1393.html, preuzeto 1. 8. 2019.

[143] ZAFEIROPOULOU, A.M., MILLARD, D.E., WEBBER, C., O'HARA, K., Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decision? New Your, USA U: *WebSci '13 Proceeding of the 5th Annual ACM Web Science Conference*, str. 463–472 (2013).

[144] ZOU, Y., ZHU, J., HANZO, L., A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Proceedings of the IEEE, 104/9 (2016), 1727-1765, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467419, preuzeto 15. 8. 2019.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristila sam tuđe materijale navedene u popisu literature, ali nisam kopirala niti jedan njihov dio, osim citata za koje sam navela autora i izvor te ih jasno označila znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spremna sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, 15. 10. 2019.,

Prilog

Pitanja za anketu

SVIJEST O PRIVATNOSTI

1. Definiramo li privatnost kao nešto što je samo Vaše, Vaše intimne informacije, podatke o Vama i Vašoj obitelji kao što su podaci o zdravstvenom stanju, Vaši stavovi, politička i vjerska opredijeljenost, Vaše fotografije, visina plaće, navike kupovanja, Vaš dom i dr., koliko važnom smatrate svoju privatnost?
    a. 1 – Nimalo mi nije važna
    b. 2
    c. 3
    d. 4
    e. 5 – Izrazito mi je važna
2. Smatrate li podatke sadržane na Vašim mobilnim uređajima i Vašu komunikaciju privatnim stvarima kojima nitko ne bi trebao imati pristup osim ako im Vi te informacije svjesno i svojevoljno pružite?
    a. Da
    b. Ne
3. Smatrate li da imate pravo na privatnost na svom mobilnom uređaju i prilikom posjećivanja raznih web stranica putem mobilnog uređaja ili računala?
    a. Da
    b. Ne
4. Smatrate li da nemate ništa za sakriti?
    a. Da
    b. Ne
5. Vjerujete li da imate kontrolu nad svojim osobnim podacima koji se nalaze na Vašem mobilnom uređaju?
    a. Da
    b. Ne
6. Smatrate li da je u današnje vrijeme moguće koristiti Internet, društvene mreže, pametne telefone i slično, a u isto vrijeme zadržati svoju privatnost?
    a. Da
    b. Ne

UREĐAJ OPĆENITO

7. Koju vrstu uređaja koristite u privatne svrhe?
    a. iPhone
    b. Android
    c. Windows Phone
    d. Ne koristim pametni telefon

8. Jeste li prilikom kreiranja Gmail računa ili Apple ID-a na svom novom pametnom telefonu koristili stvarne osobne podatke (ime i prezime, datum rođenja, spol i dr.)?
    a. Da
    b. Ne
    c. Jedan dio da, drugi ne
9. Navedite barem tri Vama najdraže mobilne aplikacije (npr. Viber, WhatsApp, neka igrica...)

GDPR

10. Znate li da na razini Europske unije (EU) odnosno za sve građane EU-a postoji Opća uredba o zaštiti podataka (engl. General Data Protection Regulation - GDPR) kojoj je svrha zaštita prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka?
    a. Da
    b. Ne
11. Molim Vas označite ono što smatrate da se prema zakonu ubraja u osobne podatke.
    a. Ime i prezime
    b. OIB
    c. Adresa stanovanja
    d. E-mail adresa
    e. Broj telefona
    f. Podaci o obrazovanju
    g. Podaci o zaposlenju
    h. Podaci o zdravstvenom stanju
    i. Podaci o bankovnom računu i kreditnoj zaduženosti
    j. Podaci o lokaciji (gdje se nalazite u danom trenutku)
    k. Popis najdraže literature/pjesama/filmova
    l. IP adresa
    m. Biometrijski podaci – mrežnica i šarenica oka, raspored crta lica, otisak prsta i dr.
    n. Genetski podaci
    o. Etničko i rasno podrijetlo
    p. Vaša fotografija
    q. Vaš glas
    r. Vaša politička mišljenja
    s. Vjerska ili filozofska uvjerenja
    t. Sindikalno članstvo
12. Čitate li Izjave o privatnosti i Uvjete korištenja prije preuzimanja i korištenja neke mobilne aplikacije?
    a. Da
    b. Ne
    c. Ponekad
13. Čitate li koja dopuštenja traže aplikacije koje preuzimate (fotoaparat, fotografije, kontakti, Vaša lokacija, kalendar, mikrofon i dr.)?
    a. Da
    b. Ne

c. Ponekad

14. Smatrate li da aplikacije traže previše dopuštenja, čak i ona koja im nisu prijeko potrebna za funkcioniranje aplikacije (npr. treba li jednoj aplikaciji za popis za kupnju pristup Vašim kontaktima)?
    a. Da
    b. Ne
15. Smatrate li da bi Izjave o privatnosti mobilnih aplikacija trebale poimence navoditi za što im je svaka dozvola potrebna (pristup fotografijama, telefonu, Vašim kontaktima, podacima o uređaju, lokaciji, mikrofonu i dr.)?
    a. Da
    b. Ne
    c. Ne znam
16. Jeste li zabrinuti za svoju privatnost pri korištenju mobilnih uređaja i mobilnih aplikacija?
    a. 1 – Uopće nisam zabrinut/a
    b. 2
    c. 3
    d. 4
    e. 5 – Izrazito sam zabrinut/a
17. Smeta li Vas kada mobilne aplikacije traže pristup Vašim osobnim podacima?
    a. 1 – Uopće me ne smeta
    b. 2
    c. 3
    d. 4
    e. 5 – Jako me smeta
18. Regulirate li dozvole aplikacija nakon preuzimanja kako biste onemogućili pristup nekim ili svim navedenim dozvolama?
    a. Nikada
    b. Ponekad
    c. Uvijek
19. Ukoliko ste na prethodno pitanje odgovorili potvrdno, vjerujete li da ste toj aplikaciji doista onemogućili pristup podacima?
    a. Da
    b. Ne
    c. Ne znam
20. Ukoliko ne regulirate dozvole aplikacija, možete li navesti razlog?
    a. Ne znam o čemu se radi
    b. Ne znam kako
    c. Smatram da to nije potrebno jer se ne bojim za svoju privatnost
    d. Nemam vremena
    e. Ne da mi se
    f. Ostalo ---------
21. Jeste li ikada namjeravali preuzeti aplikaciju pa ste odustali zato što ste smatrali da ima prevelik pristup podacima na Vašem mobilnom uređaju?
    a. Da, jednom
    b. Da, više puta
    c. Ne, ne čitam Izjave o privatnosti i dopuštenja aplikacija

d. Ne, to me ne brine
e. Ostalo

GOOGLE STUFF

22. Koji e-mail servis najčešće koristite u privatne svrhe?
    a. Gmail
    b. Yahoo mail
    c. Microsoft Office 365
    d. E-mail Vašeg davatelja internetskih usluga (T-Com, CARnet, A1 i dr.)
    e. Proton mail
    f. Službeni poslovni e-mail
    g. Proton Mail
    h. Nešto drugo_____
23. Jeste li znali da Google prikuplja sljedeće podatke? Označite sve prikladne odgovore.
    a. Koje web stranice posjećujete
    b. Kakav je sadržaj stranica koje posjećujete
    c. Ključne riječi koje pretražujete
    d. Sadržaj Vaše elektroničke pošte i privitke
    e. Vaše demografske podatke kao što su dob, razina obrazovanja, bračni status, podatke o djeci, o plaći i slično
    f. Geografske podatke kao što su država, adresa, poštanski broj i dr.
    g. Psihografske podatke kao što su društvena pripadnost, životni stil, osobine ličnosti i dr.
    h. Povijest kupnje
    i. Zvuk Vašeg glasa i ljudi u Vašoj neposrednoj blizini
    j. Jezik odnosno izričaj kakvim se služite
    k. Podatke o uređaju kojim se služite – model, operativni sustav, jedinstvene identifkatore uređaja (npr. IMEI broj), mobilna mreža i Vaš telefonski broj
    l. Koje ste aplikacije preuzeli na svoj mobilni uređaj
    m. Vaše kontakte
    n. Popis poziva, vrijeme i trajanje poziva
    o. Vaše fotografije i sav sadržaj koji Vi izradite
    p. Povijest gledanja video zapisa na YouTubeu
    q. Podatke o Wi-Fi pristupnim točkama i mobilnim odašiljačima
    r. Podatke o Vama iz javno dostupnih izvora (npr. lokalnih novina), marketinških partnera i oglašivača
    s. Podatke o oglasima koje ste pregledali
24. Jeste li znali da Google na temelju prikupljenih podataka izrađuje sveobuhvatne profile pojedinaca i te podatke dijeli s trećim stranama (oglašivačima)?
    a. Da
    b. Ne
25. Smatrate li takvo prikupljanje podataka narušavanjem Vaše privatnosti?
    a. Da
    b. Ne

26. Smeta li Vas činjenica da jedna privatna tvrtka posjeduje toliku količinu podataka o Vama?
    a. 1 – Nimalo me ne smeta.
    b. 2
    c. 3
    d. 4
    e. 5 – Izrazito me smeta
27. Ukoliko ste na prethodno pitanje odgovorili s 1 ili 2, možete li odgovoriti zašto Vas to ne smeta? Možete zaokružiti više ponuđenih odgovora
    a. Nisam odgovorio/la s 1 ili 2
    b. Zato što ću tako dobiti bolju uslugu
    c. Zato što ću dobiti personalizirane oglase koji odgovaraju mojim interesima
    d. Ne znam što bih koristio/la ako ne Google
    e. Ne vjerujem da na taj način prikupljaju i čuvaju moje podatke
    f. Ostalo____
28. Znate li da Facebook radi to isto pa čak i ako nemate korisnički račun/account na Facebooku (dovoljno je da ste posjetili stranicu na kojoj se nalazi Facebookova oznaka „Sviđa mi se“ ili popularni „Like“)?
    a. Da
    b. Ne
29. Da znate da postoje web tražilice (npr. DuckDuckGo) i servisi za elektroničku poštu (npr. Proton Mail) koji ne prikupljaju Vaše osobne podatke, biste li radije njih koristili?
    a. Da, ali samo ako je besplatno
    b. Da, pa čak i ako moram nešto platiti
    c. Ne
30. Ukoliko ste na prethodno pitanje odgovorili s „Ne“, možete li navesti razlog?

31. Molim Vas da označite stvarne podatke koje ste stavili na društvene mreže (u privatne svrhe):
    a. ime
    b. prezime
    c. fotografija
    d. podaci o školovanju
    e. podaci o zaposlenju
    f. omiljene knjige, filmovi, glazba i dr.
    g. broj telefona ili mobitela
    h. adresa
    i. religijski ili politički stavovi
    j. e-mail adresa
    k. ne dajem stvarne podatke
    l. ne koristim društvene mreže

32. Ukoliko imate maloljetnu djecu, služe li se pametnim telefonima ili drugim mobilnim uređajima?
    a. Da
    b. Ne
    c. Nemam maloljetnu djecu
33. Regulirate li dozvole aplikacija na mobilnim uređajima Vaše djece nakon preuzimanja kako biste onemogućili pristup nekim ili svim navedenim dozvolama?
    a. Da
    b. Ne
    c. Nemam maloljetnu djecu
34. Ukoliko ste na prethodno pitanje odgovorili „Ne“, možete li dati razlog?
    a. Smatram da to nije potrebno
    b. Ne znam kako se to radi
    c. Ostalo_____

Demografski podaci

35. Koliko imate godina?
    a. 13-15
    b. 16-18
    c. 19-35
    d. 36-50
    e. 51-69
    f. Iznad 70
    g. Ispod 13
36. Kojeg ste spola?
    a. Muško
    b. Žensko
37. Koji je stupanj Vašeg obrazovanja
    a. Osnovna škola
    b. Srednja škola
    c. Preddiplomski studij (viša škola)
    d. Diplomski ili dodiplomski studij (VSS)
    e. Poslijediplomski specijalistički studij ili znanstveni magisterij
    f. Poslijediplomski sveučilišni ili doktorski studij
38. Ukoliko studirate ili radite, je li vaš studij ili posao vezan za sektor informacijske i komunikacijske tehnologije?
    a. Da
    b. Ne
    c. Ne studiram i ne radim