FILOZOFSKI FAKULTET U ZAGREBU

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

AKADEMSKA GODINA 2017. /2018.

Ivan Boban

Odnos sigurnosti i zaštite podataka

Završni rad

Mentor: Dr. sc. Vjera Lopina

Zagreb, 2018.

Sadržaj

1. Uvod

U današnjem vremenu gdje nam je privatnost pod konstantnom opasnošću, potreba da ju zaštitimo je sve veća, a načini napada postaju sve više raznovrsniji. U ranim danima Interneta svi smo bili upozoravani kako ne bismo smjeli osobne podatke ostavljati na Internetu, no s evolucijom društva i napretkom tehnologije, pogotovo Interneta i mobilnih telefona, ti podatci su veoma lako dostupni. Suvremeni život se veoma bazira na konstantom interakcijom sa svijetom, te radi toga različiti podatci su dostupni svima koji će uložiti trud da ih pronađu. Upravo iz tog razloga web-stranice, različite aplikacije i usluge su morale povećati mjere sigurnosti u sklopu svojih usluga. Razvojem enkripcije naša privatnost na Internetu je višestruko povećana, a naši podatci sve više i više zaštićeni. No unatoč tome pristup tim podatcima je još uvijek veoma velika rasprava između samih pružatelja usluga i državnih ustanova koje žele imati posebna prava pristupu našim podatcima. Najkontroverzniji slučaj gdje su državne institucije zahtijevale posebna prava je spor između FBI-a (eng. FederalBureauofInvestigation) i Apple-a.

2. FBI–Apple spor oko enkripcije

U periodu od kraja 2015. pa do sredine 2016. godine FBI i Apple su bili u sporu oko Apple-ovog načina enkripcije i zaštite podataka svojih korisnika. Naime, u San Bernardinu u Kaliforniji dvojica muškaraca su ubili 14 ljudi i ranili još 22 osobe u Inland regionalnome centru, oba napadača su bila ubijena u pucnjavi s policijom. Razlog spora između FBI-a i Apple-a je bila činjenica što je jedan od napadača u poslovne svrhe koristio Apple-ov iPhone 5C, te je FBI htio pristup njegovome uređaju, no radi načina enkripcije tog uređaja to nije bilo lako izvodivo. Razlog tome je činjenica da je Apple u Rujnu 2015. izdao novu inačicu operativnog sustava za svoje uređaje, iOS 9, koji je u sebi sadržavao novi način zaštite podataka.[1]

Svaki pametni mobitel posjeduje mogućnost zadavanja lozinke kako neovlaštene osobe ne bi mogle pristupiti tome uređaju, a lozinku zadaje sam vlasnik uređaja. Lozinka se može sastojati od nekakvog uzorka, riječi ili četveroznamenkasti broj (*eng. PIN)*, sličan onima na karticama bankovnih računa. U slučaju spornog iPhone-a, lozinka je bila četveroznamenkasti broj, što znači da lozinka može biti jedna od 10,000 mogućih kombinacija, no tu nije kraj

[1] https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

problemima s kojim se FBI morao suočiti. Spomenuta inačica iOS-a je dodala inovaciju kako će nakon deset neuspjelih pokušaja unošenja lozinke svi podatci s uređaja biti uništeni. Strah od uništenja svih podataka na uređaju je razlog zašto je FBI od Apple-a zatražio da stvore način kako bi FBI s lakoćom mogao pretražiti napadačev mobitel. FBI-jev točni zahtjev bio je da Apple stvori novu inačicu iOS-a, nazvanu „*GovtOS"(eng. Goverment OS)* koji bi se mogao instalirati koristeći *RAM* (*eng. Randomaccessmemory*, memorija s nasumičnim pristupom). Apple je odbio FBI-ev zahtjev, navodeći kako bi kreiranje takvoga operativnog sustava kršilo njihova stajališta oko ugrožavanja sigurnosti njihovih proizvoda, te je Tim Cook, direktor Apple-a, naveo kako bi kreiranje takvog operativnog sustava učinilo *bruteforce*napade na uređaje trivijalnim. Iako je FBI-ev zahtjev bio odbijen, oni nisu odustajali te su odlučili stvar staviti u ruke pravosuđa.

U S.A.D.-u postoji zakon pod nazivom *All WritsAct*, putem kojega se mogu odobriti nalozi koji nisu svrstani pod uobičajene naloge. Zakon glasi:

a) Vrhovni sud i svi sudovi osnovani aktom kongresa mogu izdati sve potrebne ili prikladne isprave u korist svojih nadležnosti i prihvatljive za primjenu i načela zakona.
b) Alternativni nalog ili *rule nisi* može biti izdan od suda ili sudca koji posjeduje nadležnosti[2]

No kako bi se zakon mogao pozvati moraju se ispuniti četiri preduvjeta:

- Nepostojanje alternativnih pravnih lijekova – zakon se primjenjuje samo kad druga pravosudna sredstva nisu dostupna.
- Neovisna osnova za nadležnost – zakonom se ovlašćuju sudski nalozi u korist nadležnosti, ali sam po sebi ne stvara stvarnu nadležnost.
- Potrebno ili prikladno u korist nadležnosti – sudski nalog mora biti potreban ili prikladan za pojedini slučaj.
- Pravni običaji i načela – statutom se od sudova zahtijeva izdavanje sudskih naloga koji su „u skladu s pravnim običajima i načelima".[3]

Na osnovi ovoga zakona FBI je podnio tužbu kojom bi Apple bio prisiljen izraditi tako zvani „*GovtOS"*.

U sudskoj odluci navodi se da Apple pruža pomoć radi postizanja sljedećeg:

[2] https://www.law.cornell.edu/uscode/text/28/1651
[3] http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-83-1-Portnoi.pdf

1. „zaobići će ili onemogućiti funkciju automatskog brisanja bez obzira na to je li ona bila omogućena“ (ovom značajkom operacijskog sustava iOS 8 koju korisnik može konfigurirati automatski se brišu ključevi potrebni za čitanje kriptiranih podataka nakon deset uzastopnih neuspješnih pokušaja)

2. „omogućit će FBI-u slanje pristupnih šifri za PREDMETNI UREĐAJ radi elektroničkog testiranja preko priključka fizičkog uređaja, Bluetootha, Wi-Fi-a ili drugog dostupnog protokola“

3. „osigurat će da kad FBI pošalje pristupne šifre za PREDMETNI UREĐAJ, softver koji se izvodi na uređaju ne dovede namjerno do dodatnog kašnjenja između pokušaja pristupnih šifri osim onog koje proizlazi iz Apple-ova hardvera“[4]

U odluci se također navodi da Apple-ova pomoć može uključivati pružanje softvera FBI-u „koji će Apple kodirati s pomoću jedinstvenog identifikatora za telefon tako da bi se [softver] učitavao i izvršavao samo na PREDMETNOM UREĐAJU“[5]

Apple je tužbu odbio, te je ponovno naveo kako kreiranje takvoga operativnog sustava narušava sigurnosti njihovih uređaja i u konačnosti njihovih korisnika.

Tužba je u konačnosti bila povučena od strane FBI-a, razlog povlačenju je bila činjenica što je nezavisna kompanija pokazala mogućnost otključavanja iPhone-a koristeći vlastitu tehnologiju. Ime kompanije nikada nije izašlo u javnost, no spomenuto je kako su alati koji su bili korišteni koštali 1,3 milijuna američkih dolara. U konačnosti na spornom uređaju FBI nije pronašao ništa vrijedno spomena, uređaj je bio korišten samo u poslovne svrhe.

Spor između FBI-a i Apple-a prouzrokovao je veliku medijsku pažnju i bio veoma kontroverzna tema upravo zbog mjera do kojih je FBI bio spreman ići kako bi dobili ono što su zahtijevali. Ovo zapravo nije bio prvi pokušaj da američka vlada traži narušavanje privatnosti svojih građana, pod isprikom poboljšanja nacionalne sigurnosti.

3. Clipper čip

Za vrijeme Clintonove administracije, Nacionalna Sigurnosna Agencija (*eng. NSA- National SecurityAgency*) kreirala je Clipper čip[6]. Čip je bio namijenjen za telekomunikacijske uređaje, te bi kriptirao glasovne i tekstualne poruke slane uređajem koji bi u sebi sadržavao čip.

[4] https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf
[5] https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf
[6] http://www.cryptomuseum.com/crypto/usa/clipper.htm

Algoritam za enkripciju čipa je također bio razvijen od strane NSA-a, te je bio nazvan *Skipjack*[7]. Prva od mnogih mana ovog čipa je činjenica da je algoritam bio klasificiran kao strogo povjerljiv, te ga je stoga bilo nemoguće podlegnuti evaluaciji od strane susrtučnjaka u enkripcijskoj znanstvenoj zajednici. Državni vrh je izjasnio da algoritam koriti 80 bitni ključ, da je algoritam simetričan, te da je veoma sličan DES algoritmu. Mnogi stručnjaci iz područja enkripcije su nakon kreiranja čipa naveli mnoge mane i kritične slabosti u načinu enkripcije, no činjenica koja je širu populaciju zabrinula je ta što je čip u sebi sadržavao *backdoor*.*Backdoor* je način pristupa uređajima ili informacijama na ne uobičajen način. U većini slučajeva se upotrebljavaju za udaljen pristup uređajima. Ideja Clintonove administracije je bila da svi proizvođači telefonskih uređaja u svoje uređaje ugrade Clipper čip, ponovno pod izlikom nacionalne sigurnosti. Svaki uređaj imao bi poseban ključ koji bi državnim tijelima omogućavao pristup uređaju za koji je taj ključ napravljen.[8] U teoriji bi svi proizvođači morali za svaki stvoreni mobitel, američkoj vladi slati baze sa svim ključevima za svaki uređaj koji je proizveden.

Osim narušavanja privatnosti svojih građana, implementacija Clipper čipova kreirala bi mnoge dalekosežne probleme. Teoretski američka vlada može natjerati sve američke proizvođače da u svoje uređaje moraju implementirati Clipper čip, no ne postoji način da natjeraju strane proizvođače da ga također implementiraju. Takav teoretski scenarij doveo bi do velikih gubitaka američkih proizvođača, pošto bi građani počeli kupovati uređaje stranih proizvođača kako im privatnost ne bi bila pod napadom u svakom trenutku. Zbog svih svojih mana Clipper čip je 1996., nakon samo tri godine postojanja bio povučen. Usprkos povlačenja Clipper čipa, američka vlada je i dalje inzistirala da proizvođači sami kreiraju vlastite načine enkripcije putem kojih bi oni regulirali ključeve slične onima potrebnima na Clipper čipu. Razvojem novih i boljih načina enkripcije, velikim dijelom zbog kreiranja PGP-a (*eng. PrettyGoodPrivacy*), njihovi novi zahtjevi su također bili neuspješni. Propast Clipper čipa usporio je želje američke vlade da stvore načine „zaštite“ svojih građana u tehnološkom dobu, no nisu odustajali. Zbog njihove upornosti i želje za što boljom „sigurnošću“ kreirali su jedan od najvećih sustava nadzora u povijesti.

[7] http://www.cryptomuseum.com/crypto/usa/skipjack.htm
[8] https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

4. PRISM program

1978. godine u američki savezni zakon usvojen je Zakon o Nadzoru stranih obavještajnih službi (*eng. ForeignIntelligenceSurveillanceAct*)[9]. Ključna točka zakona je ustanovljene procedura za fizičko i elektroničko prikupljanje informacija od stranih obavještajnih službi, stranih snaga i agenata stranih snaga koji su pod sumnjom špijunaže ili terorizma. Usvajanje zakona ustanovljen je i Sud za nadzor stranih obavještajnih službi (*eng. ForeignIntelligenceSurveillance Court*) čija je služba nadgledati i odobravati naloge za nadzor od strane državnih i nadzornih agencija. Radi svoje starosti i ne prikladnosti u modernome informacijskome dobu zakon je kroz 21. stoljeće morao više puta biti izmijenjen i proširen. Zakon je prvi puta bio izložen kritikama 2005. nakon što je *The New York Times*[10] izdao članak o tome kako je Busheva administracija dopustila NSA-u da prisluškuje razgovore građana. U svoju obranu su, ponovno, naveli kako su prisluškivali razgovore samo onih građana koji su bili „sumnjivi“ i potencijalna „prijetnja“ nacionalnoj sigurnosti. Nakon što je njihov plan prisluškivanja bio razotkriven Busheva administracija je 2007. Kongresu uručila amandman pod nazivom Zakon za zaštitu Amerike (*eng. Protect America Act*)[11]. Nova verzija zakona omogućila bi da državne i nadzorne agencije mogu nadgledati i prisluškivati pojedince, putem izmjene zakona pojedinac može biti pravna ili fizička osoba, bez nadzora pod uvjetom da se jedna od strana u komunikaciji ne nalazi na teritoriju S.A.D.-a. Način na koji je amandman napisan ne navodi da pojedinac koji je na meti za prisluškivanje mora nužno biti izvan teritorija S.A.D.-a, već da je dovoljna sumnja da se on ne nalazi u S.A.D.-u kako bi prisluškivanje i nadzor bili odobreni. Amandman je bio predložen 28. Srpnja 2007. te je, zbog Bushevog inzistiranja i požurivanja bio usvojen 5. Kolovoza 2007., samo 11 dana nakon njegovog predlaganja. Usvajanje zakona prouzročilo veliku pobunu protiv njegove legitimnosti pošto su zbog već navedenih razloga državne agencije imale nespriječen pristup informacijama svojih građana. Pružatelji komunikacijskih usluga su također bili pod velikim pritiskom usvajanjem ovoga zakona, pošto se u njemu navodi kako državne i nadzorne agencije imaju pravo od njih tražiti informacije o njihovim korisnicima koje oni smatraju „sumnjivima“. Odbijanje suradnje prouzrokovalo bi tužbom prema FISC-u, te odbijanje odredbi FISC-a bi uzrokovalo daljnje kazne određene prema sudu. Tijekom narednih godinu dana doneseno je još par izmjena prema zakonu, najbitnija od kojih bi bila

[9] https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf
[10] https://web.archive.org/web/20060206162614/http://www.commondreams.org:80/headlines05/1216-01.htm (arhivirana verzija članka)
[11] https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg552.pdf

izmjena o imunitetu pružatelja usluga.[12] Ovom promjenom pružatelji usluga nisu bili podložni nikakvim sudskim sporovima koji se zasnivaju na njihovom pomaganju državnih ili nadzornih agencija.

Procedura o izmjeni zakona je, kao što je već navedeno, bila pod isprikom „zaštite građana“ i „sprječavanje terorizma“, no u stvarnosti sve ove izmjene zakona su zapravo bile način da S.A.D. i NSA legaliziraju i legitimiziraju najveći globalni sustav nadzora i prisluškivanja PRISM. Izmjena o ostvarivanju imuniteta pružateljima usluga koji su surađivali s NSA-om pružila je veoma primamljivu priliku. Razvojem Interneta u 21. stoljeću većina ljudske komunikacije bila je prebačena na Internet. Usluge poput Facebook-a, Yahoo!-a, Skype-a i sličnih pružale su besplatne načine komunikacije koje je moderno društvo s lakoćom implementiralo u svoj svakodnevni život. Jedna od najbitnijih stvari u svemu tome je činjenica da se sve navedene kompanije nalaze u S.A.D.-u, što znači da se gotovo sav način komuniciranja na Internetu odvija na teritoriju S.A.D.-a. Upravo je to razlog zašto je program PRISM bio toliko profitabilan za agencije i za kompanije. PRISM je program putem kojega su internetske kompanije sakupljale komunikacije koje su se odvijale putem njihovih usluga, te ih predavale NSA-u. Cijeli program počeo je 2007. nakon usvajanja prvog amandmana, te se iste godine pridružila i prva kompanija Microsoft. Nedugo nakon Microsofta programu su se pridružili Yahoo! 2008. , Google, Facebook i Paltalk 2009. , YouTube 2010. , AOL i Skype 2011., te Apple 2012. . Program je bio vođen u tajnosti sve od svog osnutka pa do 2013. kada je „zviždač“ Edward Snowden razotkrio cijeli projekt novinarima iz *TheGuardian*[13]i *The Washington Post*[14]. Članci koji razotkrivaju cijeli program prikazuju prezentaciju na kojoj je objašnjen način na koji program radi, koje kompanije surađuju s programom i koje informacije koja kompanija pruža, koje su države pod najvećim nadzorom i razlozi iza toga, te još mnogo dodatnih informacija o cijelome projektu. Tri države koje se spominju u razotkrivenoj prezentaciji su:

- Venezuela – pod nadzorom su bile informacije o vojsci i informacije o nafti
- Meksiko – informacije o narkoticima, energiji, unutarnjoj sigurnosti i informacije o političkim aferama

[12] https://www.gpo.gov/fdsys/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf
[13] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[14] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

- Kolumbija – radi trgovine narkoticima i ljudima, te informacije o revolucionarnoj vojsci (*eng. FARC*)[15]

Bitno je ponovno obratiti pažnju na činjenicu kako su sve internetske kompanije koje su sudjelovale u programu smještene u Americi. Prema podatcima navedenim u prezentaciji gotovo 80% svjetske komunikacije odvija se preko infrastrukture koja se nalazi na teritoriju Amerike. Razlog tome je činjenica da se komuniciranje odvija putem najjeftinijeg puta, ne nužno putem najkraćeg puta, što je povećavalo mogućnost da se komunikacija odvija putem infrastrukture u S.A.D.-u[16].

Nakon razotkrivanja projekta PRISM američka vlada je potvrdila postojanje programa, no upravo radi prijašnje navedenih izmjena u zakonu smatrali su da su njihove radnje opravdane postojanjem tog zakona i da njime nisu kršili nikakva prava svojih građana[17]. S druge strane sve kompanije koje su bile navedene da su surađivale s programom negirale su postojanje ikakve suradnje i negirali da su posjedovali znanje o postojanju takvoga programa. Sve kompanije su navele kako su jedino predavali podatke svojih korisnika u slučaju da im je bilo naređeno od strane suda.

Američka vlada nikada nije iznijela planove o prestanku rada programa PRISM, te je veoma vjerojatno da se njime i dalje služe u svrhu nadziranja komunikacija. PRISM dakako nije bio prvi, a nesumnjivo neće biti ni zadnji, program nadzora građana.

5. ECHELON

Jedan od glavnih razloga osnivanja programa PRISM je zastarjelost njegova pretka, programa ECHELON. Tragovi o osnutku ECHELON-a mogu se naći još za vrijeme Drugog svjetskog rata kada su S.A.D. i Ujedinjeno Kraljevstvo potpisale Atlantsku povelju. Nedugo nakon potpisivanja povelje donesen je još jedan dogovor (*eng. BRUSA- Britain-United Statesof America agreement*), no ovaj put dogovor se odnosio pretežito na razmijeni informacija oko komunikacijama neprijateljskih snaga. Dogovorom su Britanci otkrili svoje napretke u razbijanju nacističkih načina komunikacije, dok su Amerikanci napravili isto, no za japanske komunikacije. Završetkom Drugog svjetskog rata i početkom Hladnoga rata cilj dogovora

[15] https://commons.wikimedia.org/wiki/Category:PRISM_(surveillance_program) (sačuvane verzije prezentacija)
[16] http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
[17] https://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html

prerastao je u nadzor komunikacija država koje su obje strane smatrale opasnima, pretežito SSSR-a, Kine i mnogih država istočne Europe. Tijekom Hladnoga rata u program su se uključile još i Kanada, Australija, te Novi Zeland tako stvorivši alijansu pod nazivom *FiveEyes*(eng. Pet oči, često skraćeno kao *FVEY*)[18]. Svaka država imala je svoj poseban odjel koji se uz ostale poslove vezane za komunikacije, bavio i presretanjem i prisluškivanjem komunikacija:

- S.A.D. – NSA
- Ujedinjeno Kraljevstvo - GCHQ(*eng. Government Communications Headquarters*)
- Kanada – CSE (*eng. Communications SecurityEstablishmen*)
- Australija –ASD (*eng. AustralianSignalsDirectorate*)
- Novi Zeland – GCSB (*eng. Government Communications SecurityBureau*)

Alijansi su pomagale još par zemalja poput Danske, Nizozemske, Izraela i Francuske[19]. Države su međusobno prisluškivale razgovore ciljanih meta te međusobno izmjenjivale sakupljene informacije putem tajnih i strogo zaštićenih linija, te informacije pohranjivale su se na lokacijama diljem planeta. Jedan od najvećih pomagatelja u tome je bio ECHELON. Kako je ECHELON bio nastavo u sklopu *FiveEyes*alijanse njegova prvobitna namjena je bila očuvanje sigurnosti, no ubrzo se njegova uloga proširila na globalni nadzor. Tijekom 60-ih godina prošloga stoljeća osnovan je INTELSAT (danas Intelsat) organizacija kojoj je bio cilj poboljšati načine komunikacije putem satelita. Sateliti su bili postavljeni u orbitu iznad mnogih mjesta na Zemlji, te su njihovi sateliti bili korišteni u misiji *Appolo 11*. Kreiranje ovakve tehnologije omogućilo je sasvim novi aspekt prisluškivanja pošto su se do tada pretežno koristili radio signali ili zemaljski kablovi. ECHELON je na ciljanim lokacijama na planeti postavio postrojenja za prisluškivanje signala koji su se kretali putem satelita. Postrojenja su signale presreli putem masovnih antena, te su ih potom posebno trenirani stručnjaci interpretirali, nadgledavali i analizirali. Osim što su pratili komunikacije pojedinaca, ECHELON je pratio i komunikacije stranih kompanija, te tako postoji par primjera kako su putem programa bili ukradeni patenti za nove inovacije u različitim industrijama. U svome izvješću prema Europskom Parlamentu iz 2001. Gerhard Schmid navodi kako je putem ECHELONA američka tvrtka Kentech ukrala ideje o patentu oko inovacije u generatorima za vjetrene turbine od njemačkog suparnika Enercon. Schmid u

[18] https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released
[19] https://www.bbc.com/news/technology-25085592

svojem izvješću navodi kako je Kentech uz pomoć NSA-a prisluškivao i identično imitirao patent koji je Enercon imao plan patentirati[20]. Enercon naravno nije jedina kompanija koja je bila oštećena putem prisluškivanja, kompanije poput Air France, Airbus, BASF, te japanski proizvođači automobila su također bili oštećeni te su njihovi strogo čuvani podatci također bili sakupljeni[21].

Velike kompanije nisu jedine koje su bile prisluškivane od strane *FiveEyes*. Značajni političari poput Angele Merkel[22] i Nelsona Mendele[23] su također bili prisluškivani. Veoma je interesantno istaknuti kako je *FiveEyes* također prisluškivao i nadzirao različite političke aktiviste poput princeze Diane[24] i pjevača *The Beatlesa* John Lennona[25]. Jedan od najvećih glumaca nijemoga filma Charlie Chaplin je, zbog svojih navodnih veza s komunizmom, također bio pod nadzorom[26]. U novije vrijeme otkriveno je da je kreator stranice za dijeljenje datoteka Megaupload, Kim Dotcom (rođen Kim Schmitz) bio nadgledan od strane Novo Zelandskog GCSB[27]. Kim je jedan od rijetkih slučajeva gdje su državne agencije izdale službenu ispriku zbog ilegalnog nadziranja pojedinca[28].

6. Zakonske regulative za nadzor građana

S otkrivanjem globalnih programa za nadzor pitanje o njihovoj legalnosti i legitimnosti se često dovodi u upit. Već prije spomenuti amandmani na američki zakon su učinili programe poput PRISM djelomično legalne zbog svojih nedefiniranih granica primjene, no što je s regulativama i zakonima na području Europe i Hrvatske?

6.1. Europska Unija

Unutar Europske Unije dvije su regulative bitne kada je u pitanju zaštita osobnih podataka građana: Data Protection Directive i Opća uredba o zaštiti podataka.

[20] https://fas.org/irp/program/process/rapport_echelon_en.pdf
[21] https://fas.org/irp/program/process/rapport_echelon_en.pdf
[22] https://www.bbc.co.uk/news/world-europe-24690055
[23] https://www.telegraph.co.uk/news/worldnews/nelson-mandela/10169630/British-intelligence-birdwatchers-spied-on-Nelson-Mandelas-hideout.html
[24] https://www.washingtonpost.com/wp-srv/national/daily/dec98/diana12.htm
[25] https://www.nytimes.com/2006/09/21/opinion/21thu4.html
[26] https://www.theguardian.com/uk/2012/feb/17/mi5-spied-on-charlie-chaplin
[27] https://www.bbc.co.uk/news/world-asia-21695978
[28] https://www.telegraph.co.uk/technology/internet/9569986/Kim-Dotcom-NZ-Prime-Minister-apologises-over-unlawful-spy-operation.html

6.1.1. Data Protection Directive

Europska unija je veoma rano uvidjela potrebu za uvođenjem pravila po kojemu su privatni podatci građana zaštićeni u očima zakona. Već sredinom 90-ih godina prošloga stoljeća Europska Komisija predložila je regulativu pod nazivom *Dana Protection Directive*(eng. Direktiva o zaštiti podataka)[29]. Za razliku od američkih amandmana donesenih deset godina nakon, direktiva veoma jasno i sveobuhvatno određuje pojmove i procedure vezane za osobne podatke. Tako direktiva jasno određuje kako su osobni podatci: „bilo kakvi podatci koji su povezani s identificiranom fizičkom osobom ili fizičkom osobom koju se može identificirati“[30]. Pojam namjerno obuhvaća širok spektar upravo radi povećanih mjera sigurnosti te tako obuhvaća razne podatke poput adrese stanovanja, bankovne ispise i slično. Unutar direktive se određuje i što spada pod pojam „obrada osobnih podataka“: „ bilo kakva operacija ili set operacija koje se vrše nad osobnim podatcima, vršeni automatski ili ne, poput sakupljanja, bilježenja, organiziranja, pohranjivanja, adaptacije ili izmjena, vađenja, konzultiranja, korištenja, otkrivanja putem prijenosa, širenja ili na druge načine omogućavanje, svrstavanje ili kombiniranje, brisanje ili uništavanje“[31]. Konačno direktiva određuje pojam voditelja obrade podataka, koji je u pogledu ove direktive pravna ili fizička osoba koja određuje svrhe i sredstva obrade osobnih podataka[32]. Voditelj obrade podataka nije nužno osoba koja će i obrađivati podatke, te je osoba koja je zadužena za obradu definirana kao „izvršitelj obrade“[33]. Iako je direktiva namijenjena za korištenje unutar EU, ona dodatno štiti građane navodeći kako se i strani pružatelji usluga moraju pridržavati pravila u slučaju da se korisnik koristi uređajem koji se nalazi na teritoriju Europske Unije. Navedeno je kako se privatni podatci ne bi uopće smjeli obrađivati, no pod posebnim uvjetima to je dopušteno. Uvjeti o dopuštenju obrade osobnih podataka su podijeljeni u tri kategorije: transparentnost, legitimna namjena i proporcionalnosti. Kategorija transparentnosti navodi kako osoba čiji se podatci obrađuju ima pravo na znanje o tome da mu se podatci obrađuju, te tako ima pravo na znanje o adresi i osobi koja obrađuje podatke, namjeni obrade te krajnjim primateljima podataka i svim informacijama kako bi se osiguralo pravednost obrade podataka. Članak sedam određuje šest kriterija, od kojih barem jedan mora biti zadovoljen, kako bi obrada

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 2, pod točka a
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 2, pod točka b
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 2, pod točka d
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 2, pod točka e

osobnih podataka bila pravedna[34]. Kategorija legitimnosti navodi kako se podatci smiju obrađivati samo za specificirane eksplicitne i legitimne svrhe, te kako se podatci ne smiju obrađivati na druge načine van tih svrha[35]. Zadnja od tri kategorija je proporcionalnost, ona navodi kako se osobni podatci mogu obrađivati utoliko je to prikladno, relevantno i ne pretjerano u odnosu sa svrhom za koju su prikupljani i/ili naknadno obrađivani. Kada su u pitanju veoma osjetljivi podatci, treba primijeniti dodatne restrikcije. Pošto je određeno da svaka fizička osoba mora biti obaviještena o obradi njegovih podataka, točka 14 dopušta pravo protivljenju takvome činu[36]. Putem direktive svaka država članica mora ustanoviti nadzorno tijelo koje će motriti razinu zaštite podataka u državi, savjetovati u izgradnji novih zakona i regulativa oko zaštite osobnih podataka, te pripomoći u sporovima vezanih uz kršenje pravila donesenih regulativom[37]. Nadzorno tijelo također uvijek mora biti obaviješteno od strane potencijalnog voditelja obrade osobnih podataka prethodeći samoj obradi. Obavijest o prikupljanju mora sadržavati sljedeće informacije:

- Naziv i adresu voditelja obrade i predstavnika, ako postoje
- Namjenu ili namjene obrade
- Opis kategorije ili kategorija o subjektu podatakai o podatcima ili kategorijama podataka povezane s njima
- Primatelju ili kategoriji primatelja kojima bi podatci mogli biti otkriveni
- Predloženi transferi podataka u treće zemlje
- Generalni opis o mjerama koje osiguravaju sigurnost obrade

Sve informacije se moraju čuvati u javnome registru, te tako biti dostupne javnosti.

Direktiva je bila predložena 24. Listopada 1995. , te je bila implementirana točno tri godine nakon njenog predlaganja. Veoma je interesantno kako je direktiva bila predložena prije masovne implementacije Interneta u naš svakodnevni život. Usprkos veoma ranoj implementaciji direktive ona kvalitetnije štiti osobne podatke svojih građana od regulativa koje su donesene desetljeće kasnije. No upravo radi implementacije Interneta u naš svakodnevni život direktiva je s vremenom zastarjela, te njene smjernice nisu bile u skladu s

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 7
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 6, pod točka b
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 14
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 Članak 28

modernim načinom života, stoga je 2018. donesena odluka o uvođenju nove regulacije o zaštiti podataka modernog građana Europske Unije.

6.1.2. GDPR – General Data Protection Regulation

Mnogi smatraju kako je Opća uredba o zaštiti podataka (*eng. General Data Protection Regulation*) bila produkt otkrivanja programa PRISM i način kako bi se spriječilo ponavljanje sličnog. Europska komisija je još početkom 2012. započela inicijativu kako bi se pooštrile mjere zaštite osobnih podataka. Kako su društvene mreže postale dio naše svakodnevnice, ono što dijelimo na njima se također smatra osobnim podatcima. Također implementacijom Interneta i povećanim brojem usluga koje su bazirane isključivo na Internetu bitno je zakone prilagoditi modernim načinima poslovanja. Upravo iz tih razloga je 14. Travnja 2016. kreirana Opća uredba o zaštiti podataka koja je sa sobom dovela mnogo nužne regulacije za zaštitu osobnih podataka. Unutar njenih 173 stavaka donesen je mnogi broj novih zakonskih normi, te tako stavak 15 navodi važnost neutralnosti obrade osobnih podataka. Neutralnost obrade odnosi se na činjenicu kako je obrada podataka tehnološki nezavisna, stoga je nebitno vrši li se obrada automatski ili ručno[38]. Interesantno je istaknuti kako stavak 18 uspostavlja granicu između osobne i profesionalne obrade podataka. Odredba se ne odnosi na osobne ili kućne aktivnosti obrade podataka, ali se odnosi na voditelje i izvršitelje obrade koji pružaju usluge za obradu osobnih podataka za osobne ili kućne aktivnosti[39]. Iznenađujuća je činjenica kako osobni podatci preminulih osoba nisu zaštićeni putem Odredbe, no ona dopušta moguće izmijene od strane država članica u tome aspektu[40]. Stavci 28 do 30 bave se pojmompseudonimizacije. Pseudonimizacijaje unutar odredbe 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“[41]. Važnost pseudonimizacije se ističe unutar stavka 30 koji navodi različite faktore koji mogu poslužiti identifikaciji pojedinca poput adrese Internetskog protokola, identifikatori kolačića ili oznaka za radiofrekvencijsku identifikaciju[42]. Radi što veće transparentnosti Odredba jasno navodi

[38] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 15
[39] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 18
[40] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 27
[41] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Članak 4. pod točka 5
[42] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 30

kada je privola na obradu osobnih podataka važeća, a kada ne. Biranje polja s kvačicom ili biranje tehničkih postavki usluge se smatraju ispravnim načinom davanja privole. Unaprijed označena polja s kvačicom ili manjak aktivnosti za regulaciju osobnih podataka se u ovome pogledu ne smatraju kao davanje privole[43]. Zbog povećanja broja djece i njihovog sve većeg korištenja Internetom bitno je odrediti pravila putem kojega će njihovi osobni podatci biti pod mnogo većom sigurnošću. Pošto su djeca najranjiviji dio stanovništva, te se radi toga moraju voditi posebne mjere pri upotrebi osobnih podataka djece, a posebno u svrhu marketinga, prilikom izrade osobnih ili korisničkih profila[44]. Privola roditelja ne bi smjela biti potrebna u kontekstu preventivnih usluga koje su ciljane za djecu. U skladu s Direktivom o Zaštiti Podataka ponovno se ističe važnost transparentnosti od strane voditelja obrade, te se dodatno ističe važnost lakoće komunikacije između osobe čiji se podatci obrađuju i voditelja obrade. Ponovno se napominje kako se podatci ne bi smjeli biti korišteni izvan namjena navedenih od strane voditelja, te kako se čuvanje istih podataka mora svesti na apsolutni minimum. U skladu sa svime navedenim stavak 42 proširuje obaveze voditelja obrade, te tako određuje da prilikom davanja važeće privole ispitanik mora imati uvid u identitet voditelja obrade i svrhu obrade kojom će se njegovi podatci obrađivati. Prema stavku 42 privola ne može biti dana dobrovoljno ako ispitanik nema pravo povući privolu bez posljedica[45]. Kako bi ispitanici bili svjesni o prikupljanju njihovih osobnih podataka Odredba određuje potrebu za korištenjem jednostavnog i lako razumljivog jezika, te da se prema potrebi koristiti vizualizacijom. U slučaju da je obrada podataka namijenjena djeci, svaka informacija i komunikacija mora biti na jasnom i jednostavnom jeziku koje dijete može razumjeti. Regulativa također oštro kažnjava kršenje njenih pravila, te se tako kršenje pravila kažnjava s novčanim kaznama u iznosu od 20 000 000 EUR ili ako je u pitanju poduzetnik do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće[46].

Iako regulativa na svim razinama povećava mjere sigurnosti postoje par točaka koje su u određenoj mjeri kontradiktorne njenoj namjeni. Prethodno spomenut stavak 27 navodi kako osobni podatci preminulih osoba nisu zaštićeni Uredbom, što se može i ne mora dovesti do komplikacija.Prema stavcima 60 i 61[47] voditelj obrade dužan je ispitaniku pružiti sve dodatne informacije kako bi se osigurala poštena i transparentna obrada, te ga obavijestiti o

[43] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 32
[44] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 38
[45] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 42
[46] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Članak 48. pod točka 5
[47] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 60 i 61

mogućnosti legitimnog otkrića osobnih podataka drugome primatelju, no stavak 62 ipak ističe mogućnost uskraćivanja informacija. Stavak 62 ističe iznimke kada pružanja tih informacija nije potrebno:

- Ako ispitanik već posjeduje tu informaciju
- Ako je bilježenje ili otkrivanje osobnih podataka izrijekom propisano zakonom
- Ako je pružanje informacije ispitaniku nemoguće
- Ako pružanje informacije zahtijeva nerazmjeran napor

Primjeri u kojima se takve iznimke mogu primijeniti su:

- U svrhu arhiviranja u javnom interesu
- U svrhe znanstvenih ili povijesnih istraživanja
- U statističke svrhe[48]

Navedeno je kako bi se kako je potrebno razmotriti broj ispitanika, starost podataka i druge zaštitne mjere, unatoč tome takva odluka je kontradiktorna ideji Odredbe po kojoj su svi dužni poduzeti sve mjere kako bi ispitanici što bolje bili informirani i zaštićeni. Osim stavka 62, stavak 85 također ističe zabrinjujuću mogućnost. Prema njoj su voditelji obrade nužni obavijestiti nadležna nadzorna tijela o bilo kakvoj povredi osobnih podataka, pošto one mogu prouzročiti fizičku, materijalnu ili nematerijalnu štetu pojedincima, poput krađe identiteta, prijevare financijskih gubitaka i slično. Od trenutka saznanja o povredi osobnih podataka voditelj ima 72 sata da obavijesti nadležno tijelo o povredi, no postoji iznimka. U slučaju da voditelj obrade može dokazati da povreda osobnih podataka neće prouzrokovati rizik za prava i slobode pojedinaca[49]. Davanjem toliko moći voditeljima obrade podataka može dovesti do neželjenih rezultata. Svaki ispitanik trebao bi biti obaviješten o povredi svojih osobnih podataka, nebitno o magnitudi povrede, no omogućavanje zatajivanja povreda moglo bi dovesti do ne željenih posljedica i zaobilaženja zakona sličnim onima u S.A.D.-u.

Uredba je stupila na snagu 25. Svibnja 2018., no period do njenog stupanja na snagu nije bio lak za kompanije. Zbog pomalo rigoroznih mjera koje je GDPR uveo,kompanije su morale veoma brzo izmijeniti svoje uvjete korištenja njihovih usluga, no unatoč njihovih najboljih upora zabrinjavajući broj kompanija nije uspjelo uvesti sve mjere zaštite za svoje korisnike. Britanski *TheGuardian* je u Srpnju ove godine izdao članak kako i najveće kompanije poput

[48] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 62
[49] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 85

Google-a i Amazon-a nisu pravilo uspjeli implementirati sve potrebne mjere zaštite, te kako su uvjeti korištenja još uvijek relativno nerazumljivi i veoma nejasni[50].

6.2. Zakoni na razini Hrvatske

Kako je hrvatska 2013. postala službena članica Europske Unije dužna je poštivati zakone koji vrijede diljem Unije, uključujući i Opću uredbu o zaštiti podataka. Vodeće tijelo za brigu oko osobnih podataka je Agencija za zaštitu osobnih podataka. Zadaće i ovlasti Agencije propisane su unutar Članaka 57. i 58[51]. Uredbe. Agencija mora konstantno biti u komunikaciji s predstavnicima voditelja ili izvršitelja obrade. Predstavnici su imenovani od strane voditelja ili izvršitelja obrade u slučaju kada voditelj ili izvršitelj obrade nema nastan na području Europske Unije[52]. Uz Uredbu u Hrvatskoj na snazi je i Zakon o tajnosti podataka. Vrhovno tijelo koje se bavi nadzorom provođenja Zakona je Vijeće za nacionalnu sigurnost.

6.2.1. Zakon o tajnosti podataka

Prema Zakonu o tajnosti podataka, podatak je definiran kao „dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika“[53]. Vlasnik podataka „je nadležno tijelo u okviru čijeg djelovanja je klasificirani ili neklasificirani podatak nastao“[54]. Putem Zakona određene su četiri stupnja tajnosti podataka: VRLO TAJNO, TAJNO, POVJERLJIVO i OGRANIČENO[55]. Svi podatci prilikom njihovog klasificiranja se moraju tretirati prema najnižem stupnju tajnosti, no bilo kakvi prilozi uz klasificirane podatke se ne moraju označivati stupnjem klasifikacije[56]. Pristup klasificiranim podatcima moguć je uz dobivanje

[50] https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant
[51] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Članci 57 i 58
[52] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679 Stavak 80
[53] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 2
[54] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 2
[55] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 4
[56] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 12

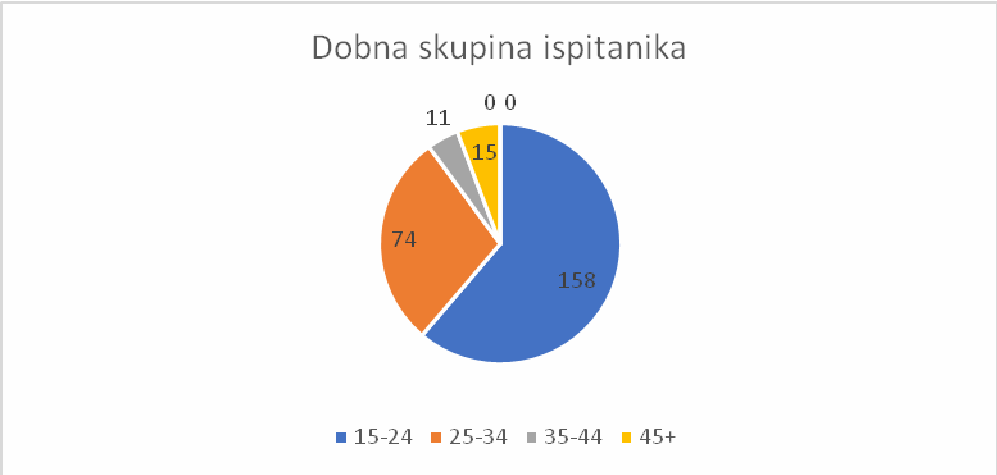
certifikata od strane Vijeća za nacionalnu sigurnost koje prosuđuje valjanost zahtjeva[57]. Certifikat se dodjeljuje na period od pet godina, no ponovno postoje iznimke. Člankom 20. određuju se pojedinci koji pristup klasificiranim podatcima imaju bez certifikata, jedino u slučaju ako je pristup klasificiranim podatcima potreban u sklopu obavljanja poslova iz njihovog djelokruga[58]. Takav pristup odobren je: saborskome zastupniku, ministru, državnom tajniku središnjega državnog ureda, sudcu i Glavnome državnome odvjetniku[59]. Iako nemaju potrebu za dobivanjem certifikata, dužni su potpisati izjavu kojom potvrđuju da su upoznati s odredbama Zakona i poštivati propise navedene u zakonu[60]. Certifikat nije ograničen samo na klasificiranim podatcima unutar Hrvatske, te tako u slučaju da je certifikat odobren može zatražiti proširenje njegovog područja djelotvornosti i time ostvariti pristup klasificiranim podacima drugih država i međunarodnih organizacija[61].

U slučaju pristupa ne klasificiranim podatcima, zakon je veoma pristupačan. Ne klasificiranim podatcima imaju pristup svi kojima je to nužno u službene svrhe radi obavljanja poslova iz njihovog djelokruga, te svi zainteresirani koji su ovlašteni od strane Vijeća za nacionalnu sigurnost[62]. Uzevši u obzir kako se podatci kategoriziraju prema odlukama vlasnika podataka to može dovesti do ne željenih posljedica. Pogotovo u slučaju ako se neki podatak krivo klasificira ili se ne sagleda njegova važnost u cijelosti.

7. Mišljenje građana

Uzevši u obzir sve navedeno bitno je čuti mišljenje građana, te je u svrhu ovoga rada provedena anketa[63]. Anketa se sastoji od 10 pitanja konkretno vezanih uz zaštitu osobnih podataka, te jednoga pitanja kako bi ispitanike mogli podijeliti u skupine prema dobi. Iako je anketa bila namijenjena svim dobnim skupinama, najveći odaziv bio je od građana dobi od15-34 (Graf 1).

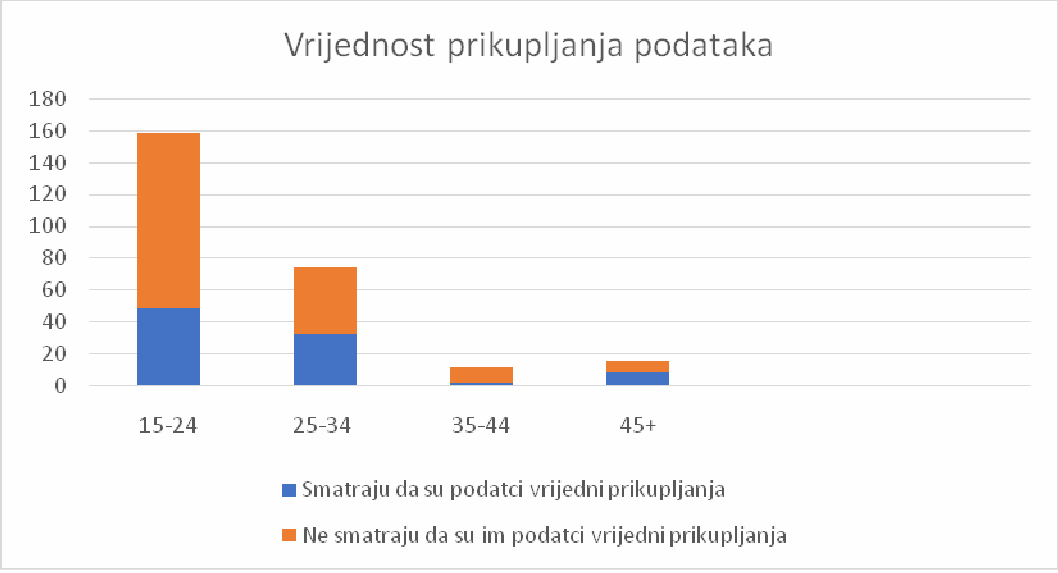
[57] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 18
[58] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 20
[59] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 20 pod točka 1
[60] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 20 pod točka 2
[61] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 22
[62] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf Članak 23
[63] Anketa „Mjere zaštite podataka“ https://docs.google.com/forms/d/e/1FAIpQLSe58sIy4ZnQf05VMjZxD4k65swj9vFxsCagq1lwiGXdxKgZwA/viewform



Graf 1 Dobne skupine ispitanika

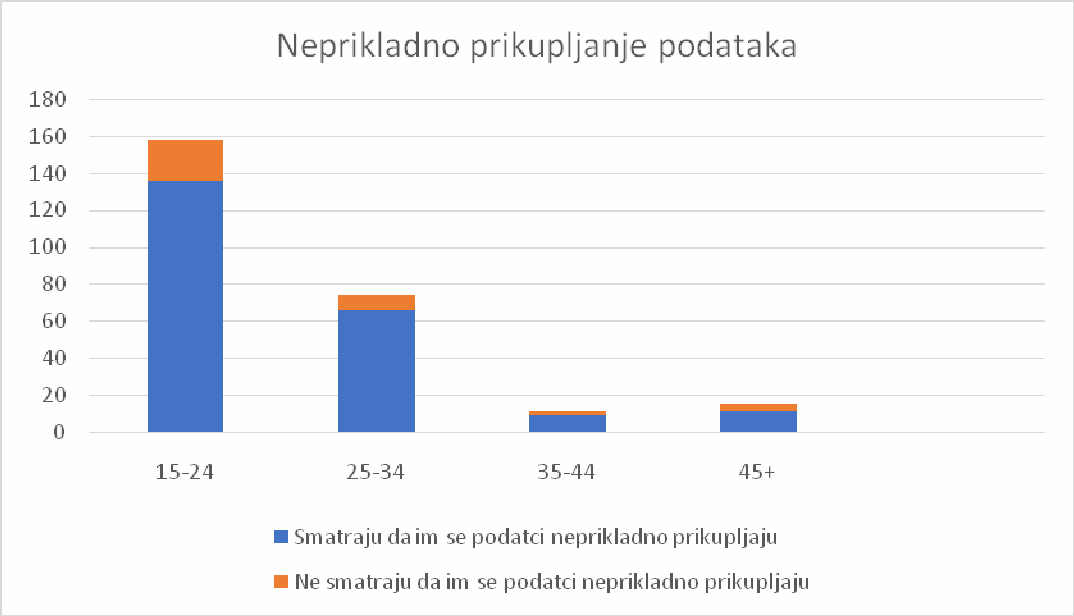
Iako su unutar ankete ponuđene tri skupine za građane starije od 45 godina njihova zastupljenost je veoma mala nasuprot ostalim skupinama te će se oni grupirati u jednu skupinu.

Povećanjem osviještenosti brige oko podataka unazad zadnji par godina dovodi do pitanja što građani misle o svojim podatcima. Uzevši to u obzir ispitanici su bili ispitani kako oni vrednuju svoje podatke, te je prema rezultatima iz ankete moguće zaključiti kako 65.1% ispitanika smatra kako njihovi podatci nisu vrijedni prikupljanja, dok 34.9% ispitanika smatra suprotno(Graf 2).



Graf 2 Vrijednost prikupljanja podataka

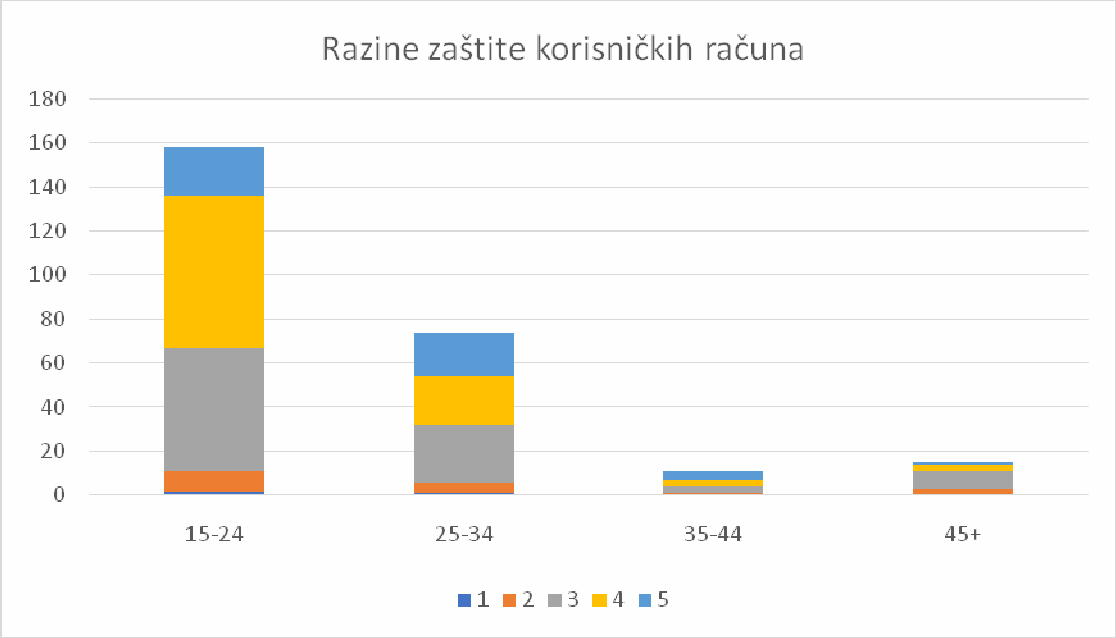
Iako većina ispitanika smatra kako njihovi podatci nisu vrijedni prikupljanja rezultati ankete pokazuju na činjenicu kako većina ispitanika smatra da se njihovi podatci neprikladno prikupljaju (Graf 3). Dok je 34.9% ispitanika smatralo kako su njihovi podatci vrijedni prikupljanja, 86% ispitanika smatra kako se njihovi podatci neprikladno prikupljaju, dok samo 14% njih smatra kako se njihovi podatci neprikladno ne prikupljaju.



Graf 3 Neprikladno prikupljanje podataka

Kako većina ispitanika smatra da se njihovi podatci neprikladno prikupljaju bitno je preispitati koliku brigu oni sami vode o svojim podatcima. Ispitanicima je bila ponuđena skala od 1 do 5, 1 predstavlja najnižu dok 5 predstavlja najvišu vrijednost, na kojoj su mogli odabrati koju razinu zaštite koriste na svojim korisničkim računima. Najveći udio ispitanika navelo je kako se koristivišom razinom zaštite (broj 4) na svojim korisničkim računima i to njih 37,6%. Druga po zastupljenosti je srednja razina zaštite (broj 3) te ju je odabralo 36% ispitanika. Najvišu razinu zaštite (broj 5) koristi 18,2% ispitanika, dok najnižu (broj 1) koristi najmanji udio ispitanika 1,2%. Nižom razinom zaštite koristi se 7% ispitanika. Anketa nije specificirala što podrazumijeva koju razinu, te je to bilo prepušteno ispitanicima da prosude samostalno. Pretpostavka ankete je kako su ispitanicu koji su odabrali broj 3, 4 ili 5 više informatički pismeni te tako snažnu lozinku ne smatraju kao višu razinu zaštite korisničkih računa. Opcije poput tko može vidjeti njihove objave, te oprez pri objavljivanju sadržaja na internetskim uslugama su neke od mjera koje bi se smatrale kao više razine zaštite korisničkih računa. Uočljivo je kako mlađi ispitanici koriste više mjere zaštite svojih korisničkih računa te se takav rezultat može povezati s njihovom većom informatičkom

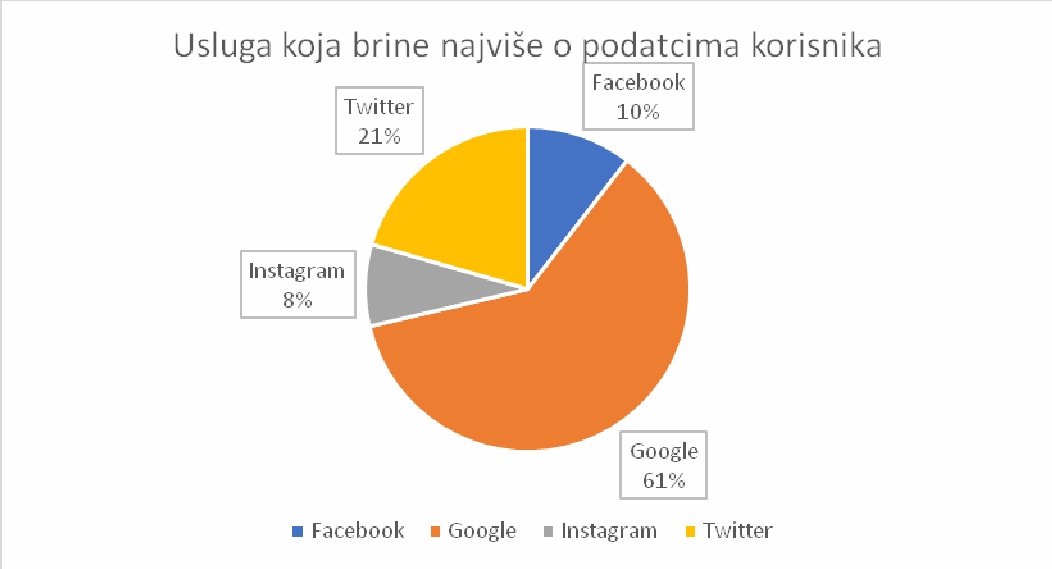
pismenošću i boljom osviještenošću oko mogućih posljedica niske zaštite. Iako mlađi građani čine većinski udio ispitanika, te se radi toga statistika kreće u smjeru veće zaštite korisničkih računa, prosječni ispitanik ipak štiti svoje korisničke račune na srednjoj ili višoj razini. Ovakvi podatci najvjerojatnije su posljedica GDPR-a koji je sa svojim uvođenjem uvelike povećao javno znanje oko zaštite podataka i time potaknuo pojedince da obrate veću brigu svojim korisničkim računima i njihovim mjerama zaštite.



Graf 4 Razine zaštite korisničkih računa

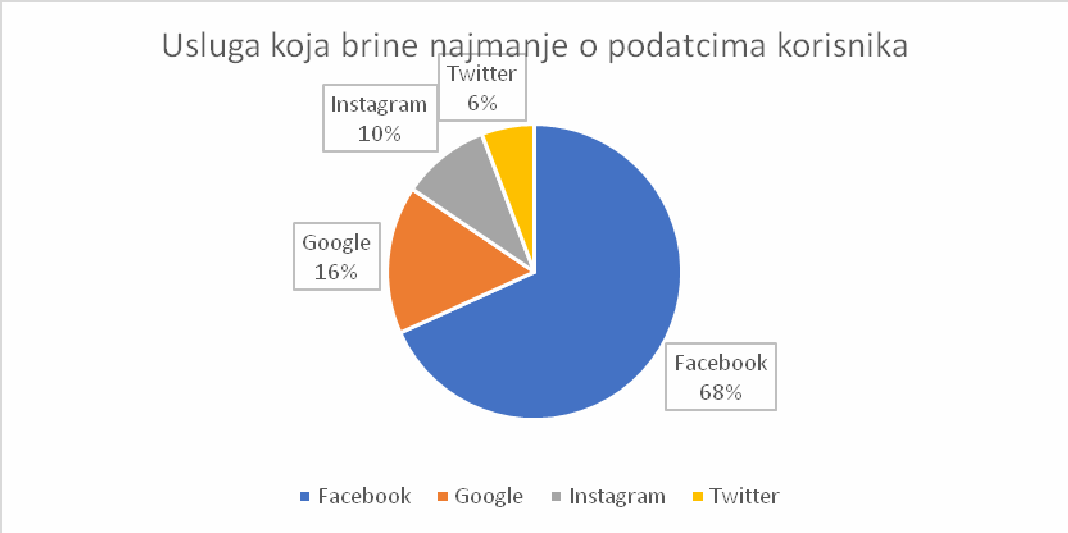
Samostalna briga oko korisničkih računa nije dovoljna za čuvanje svojih podataka, programi poput PRISM su dokazali kako su svakodnevne usluge poput Facebook-a spreme predati podatke svojih korisnika bez da ih obavijeste, te stoga je interesantno sagledati koja usluga prema njihovom mišljenju brine najviše, a koja najmanje o njihovim podatcima (Graf 5). Google je prema mišljenju ispitanika, 61%, usluga koja najviše brine oko podataka svojih korisnika. Takav rezultat nije iznenađujući pošto Google posjeduje većinu usluga s kojima se ljudi koriste na svakodnevnoj razini. Usluge poput Gmail-a, YouTube-a i još mnogih drugih su dio privatne, ali i poslovne svakodnevice, te ispitanici polažu mnogo pouzdanja u njih. Twitter je prema ispitanicima druga po redu usluga, te 21% ispitanika smatra kako oni vode najveću brigu o njihovim podatcima. Facebook (10%) i Instagram (8 %) su dvije usluge za koji najmanji broj ispitanika smatra da vode najveću brigu oko njihovih podataka, što je bilo predvidivo. Facebook je navodno bio u sklopu PRISM programa te se to može smatrati kao

jedan od ključnih razloga zbog kojega je mali broj ispitanika odabrao Facebook. Instagram je jedan od ponuđenih odabira pretežito zbog njegove popularnosti, iako je on od 2012. u vlasništvu Facebook-a, te se odgovori koji su za njega mogu pridodati Facebook-u.



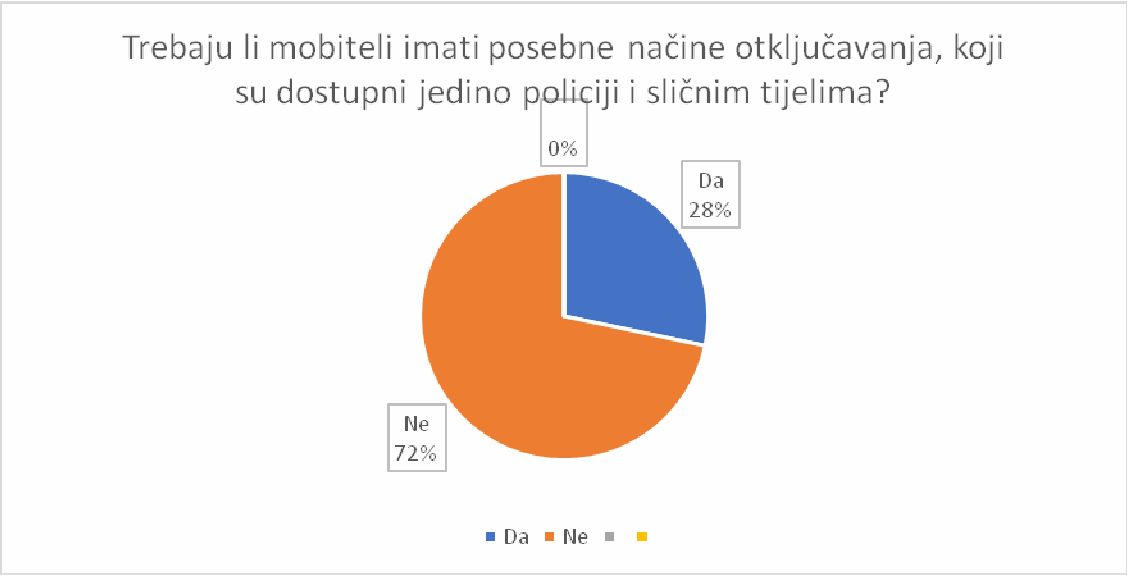
Graf 5 Usluga koja brine najviše o podatcima korisnika

Sukladno s pitanjem koja usluga brine najviše potrebno je i preispitati koja brine najmanje (Graf 6). Rezultati ovoga pitanja sukladni su rezultatima prethodnog pitanja. Facebook je usluga kojoj ispitanici najmanje vjeruju, 68%. Interesantno je kako je Google usluga za koju čak 16% ispitanika smatra da brine najmanje za njihove podatke, iako je u većina ispitanika upravo Google odabrala kaj najpouzdaniju uslugu. Instagram je odabralo 10% ispitanika, te se ponovno taj postotak može pridodati postotku Facebook-a. Twitter ima najmanji broj odabira unutar ovoga pitanja, te je samo 6% ispitanika odabralo tu opciju.



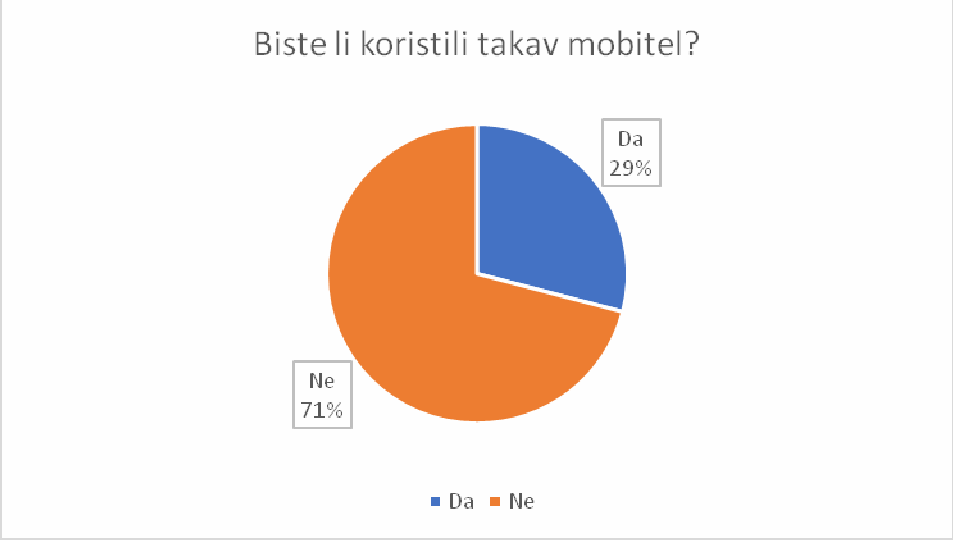
Graf 6 Usluga koja brine najmanje o podatcima korisnika

Clipper čip i spor FBI-a i Apple-a samo su neki od primjera putem kojih zakonodavstvo pokušava prilagođavati zakone za ostvarivanje svojih ciljeva pritom zanemarujući sigurnost podataka građana. Iako su oba slučaja bila neuspješna nesumnjivo je kako će se takve situacije ponavljati, te upravo iz toga razloga anketa je usmjerena prema ispitivanju što pojedinci misle o ideji sličnoj Clipper čipu. Pitanje koje je bilo postavljeno glasi: „ Trebaju li mobiteli imati posebne načine otključavanja, koji su dostupni jedino policiji i sličnim tijelima? “. Pitanje je namjerno postavljeno veoma laičkim jezikom kako se ne bi trebalo ulaziti u točne specifikacije načina otključavanja. 72% ispitanika odgovorilo je kako mobiteli ne bi trebali imati takve mogućnosti, dok se 28% njih izjasnilo kako bi trebali (Graf 7). Sukladno s ovim pitanjem ispitanici su bili upitani bi li oni sami koristili takav uređaj(Graf 8).



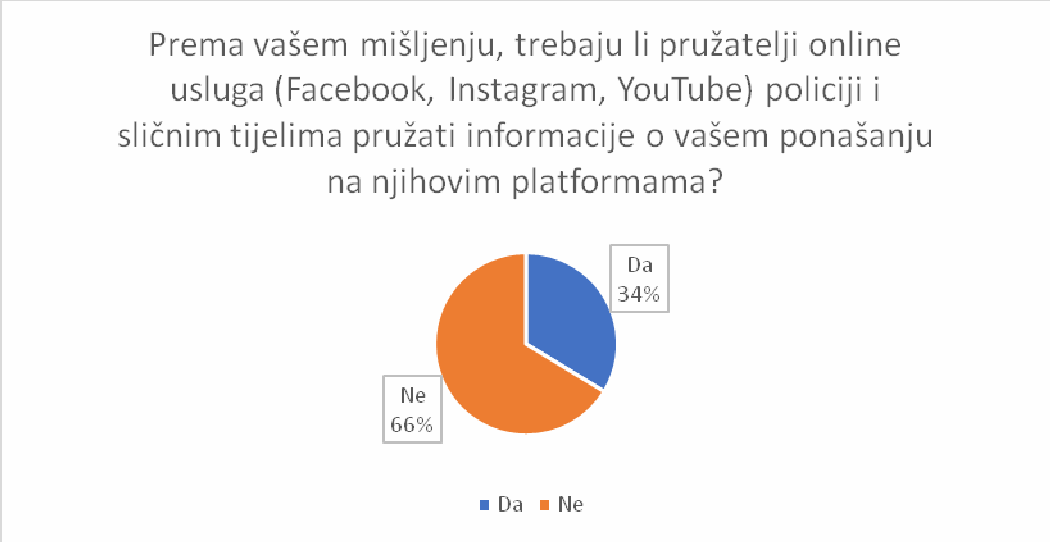
Graf 7Trebaju li mobiteli imati posebne načine otključavanja, koji su dostupni jedino policiji i sličnim tijelima?

Ispitanici su veoma konzistentni kada je u pitanju ideja poput Clipper čipa, te smatraju kako takvi uređaji ne bi smjeli postojati, te kako oni sami ne bi koristili takve uređaje. Razlika u odgovorima je minimalna, pošto je u pitanju razlika od svega 1%. 1% čini 2 do 3 ispitanika koji su protiv ideje mobitela koji bi omogućavali pristup, ali bi ipak koristili takav uređaj.



Graf 8 Korištenje mobitela s posebnim pristupom

Iz podataka je vidljivo kako su ispitanici pretežito protiv ideja poput Clipper čipa i „GovtOS“, no to nisu jedini načini na koji zakonodavstvo pokušava narušiti privatnost građana. PRISM je program koji je ukazao kako su pružatelji usluga poput Facebook-a spremi predati informacije o svojim korisnicima. Iako 72 % ispitanika smatra kako mobiteli s mogućnošću

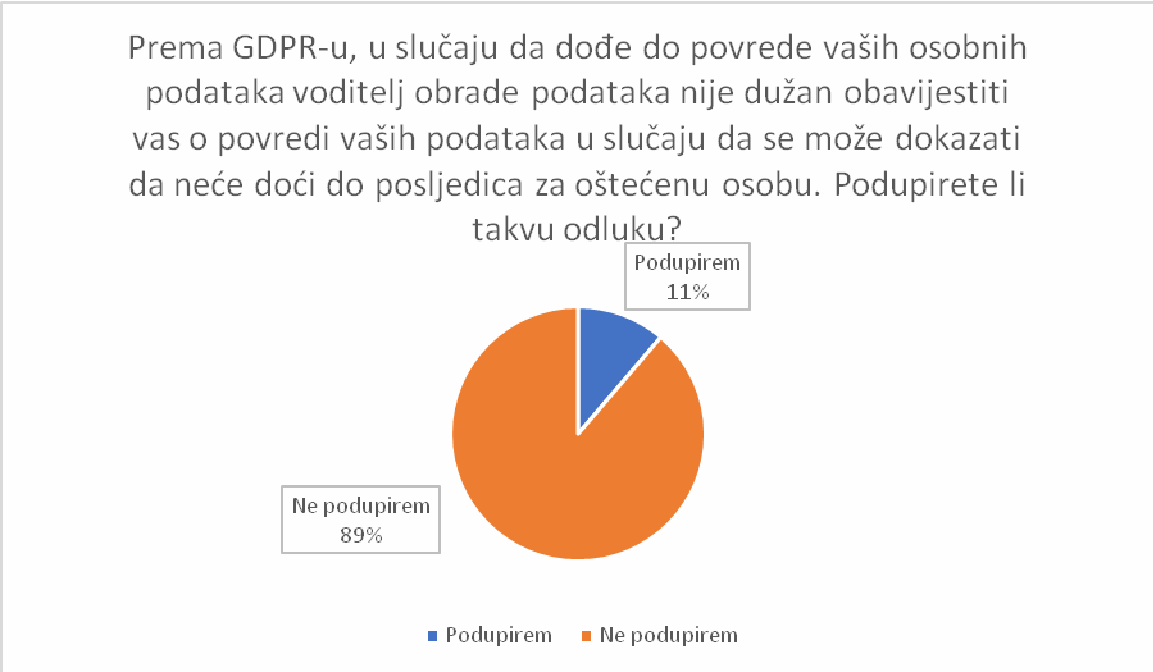


Graf 9Prema vašem mišljenju, trebaju li pružatelji online usluga (Facebook, Instagram, YouTube) policiji i sličnim tijelima pružati informacije o vašem ponašanju na njihovim platformama?

direktnog pristupa ne bi smjeli postojati, 66 % njih smatra kako *online* usluge ne bi smjele predavati podatke svojih korisnika policiji i sličnim tijelima. Scenariji nisu veoma slični, no ipak je vidljivo kako ispitanici više brinu za privatnost na svojim mobitelima nego za privatnost na *online* uslugama.

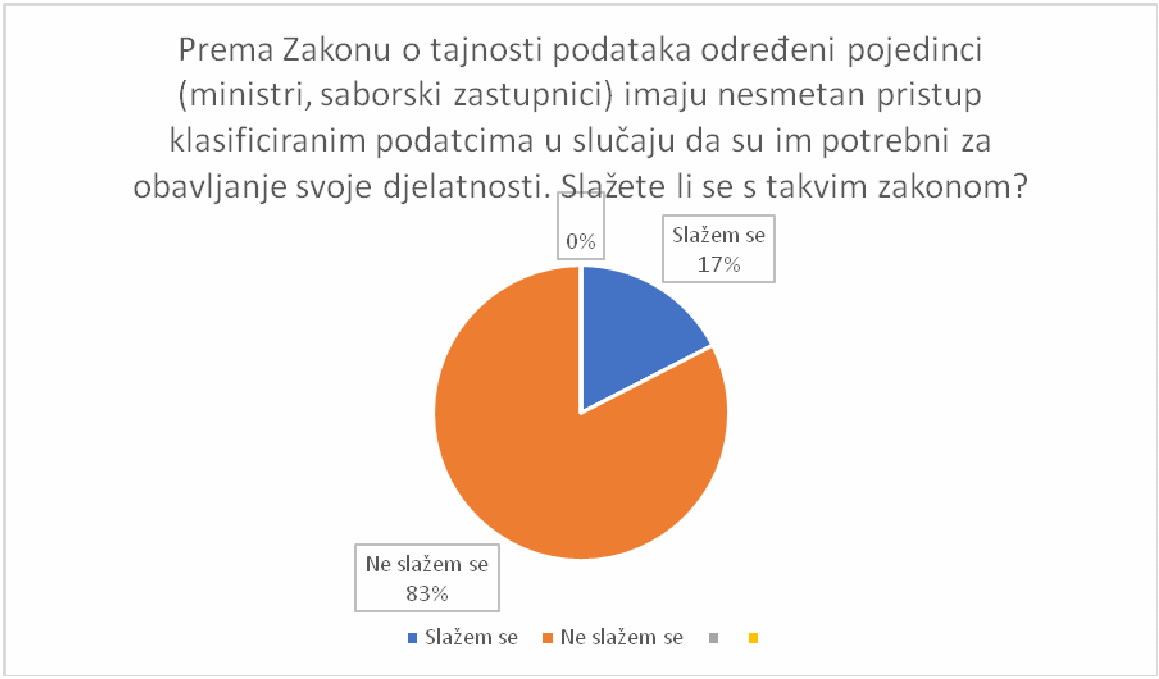
Završno anketa je ispitala mišljenje ispitanika oko prethodno navedenih problematičnih zakona. Prvo takvo pitanje preispitalo je stavak 85 GDPR-a[64] prema kojem, kao prethodno navedeno, voditelj obrade podataka nije dužan obavijestiti o povredi podataka u slučaju da može dokazati kako to neće prouzročiti rizik za pojedinca. Rezultati pokazuju čvrsto protivljenje takvoj odluci, s 89 % odabira protiv takve odluke, te samo 11 % za takvu odluku (Graf 10). Ovakva reakcija je očekivana pošto su pojedinci danas mnogo više oprezniji i mnogo zabrinutiji oko svojih podataka, te bilo kakvo zatajivanje o njihovoj povredi, nebitno o magnitudi povrede, može biti rizično.

[64] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679



Graf 10 Podupiranje stvaka 85 GDPR-a

Zadnje pitanje u anketi odnosi se na Zakon o tajnosti podataka, točnije Članku 20. prema kojemu određeni pojedinci, poput saborskih zastupnika i ministra imaju pristup klasificiranim podatcima bez certifikata u slučaju da im je pristup potreban za obavljanje svoje djelatnosti. Većina ispitanika ponovno ne podupire takav zakon, 83 % njih, dok 17 % ipak podupire takav zakon (Graf 11). Ministri i saborski zastupnici moraju potpisati izjavu oko činjenice kako su upoznati s regulativama Zakona o tajnosti podataka, no za razliku od drugih pojedinaca ne moraju podnijeti zahtjev i dobiti certifikat Vijeća za nacionalnu sigurnost. Manjak uvida u namjere saborskih zastupnika i ministra za pristup klasificiranim podatcima je najvjerojatniji razlog protivljenju ovakvome zakonu. Uvjet da im je pristup omogućen ako im je potrebno za obavljanje svoje djelatnosti također je veoma sveobuhvatan termin jer je , po primjerima američkih zakona, veoma lagano oblikovati svoje namjere kako bi bile u sklopu zakona.



Graf 11 Podupiranje Članka 20. Zakona o tajnosti podatak

8. Zaključak

Pitanje odnosasigurnosti, bila ona nacionalna ili osobna, i zaštite podataka vjerojatno nikada neće biti razriješeno. S jedne strane su država i državne agencije koje smatraju da trebaju poduzeti sve moguće mjere i konstantno kreirati nove mjere kako bi zaštitile svoje građane, dok su s druge strane građani koji žele zaštititi svoju privatnost. Razvojem tehnologije unazad zadnjih pedesetak godina, a pogotovo unazad zadnja dva desetljeća, načini života su se drastično promijenili. Razvojem Interneta i društvenih mreža privatnost je postala relativan pojam, pošto se društvo razvilo u smjeru sveopćeg dijeljenja informacija i podataka. Načini komunikacije nikada nisu bili lakši što je sa sobom dovelo dobre i loše stvari. Unazad dvadeset godina transkontinentalna komunikacija bila je skup i naporan proces, no danas svatko od nas to može izvesti pomoću pametnog uređaja kojeg nosimo sa sobom svakodnevno. Razvoj tehnologije doveo je i do potrebe izmjene zakona, pogotovo u radi sve većega obavljanja poslova putem Interneta. Određene izmjene zakona, poput onih na području Europe unazad dvadeset godina predvidjele su potrebu za zaštitom podataka građana, dok su one na području S.A.D.-a učinile skoro pa upravo suprotno. S.A.D. je svojim izmjenama zakona legitimizirao programe poput PRISM-e pod isprikom nacionalne sigurnosti zanemarivši time sigurnost svojih građana i njihovih podataka. Povjerenje je ključan pojam unutar ovoga razgovora. Kada bi građani imali povjerenja u državu i država u građane programi poput PRISM-e i ECHELON-a, te ideje poput Clipper čipa uopće ne bi bili potrebni, no ipak takvo povjerenje je ideja za savršen svijet. S.A.D. naravno nije jedina država koja je izgubila povjerenje svojih građana, rezultati ankete čvrsto prikazuju kako zakoni i regulative koji su na području Hrvatske također nisu podupirani od strane hrvatskih građana. Problem unutar svega ovoga moguće je uvidjeti i u *online* uslugama u koje su pojedini ipak možda ulagali previše povjerenja, iako je vidljivo kako one također gube povjerenje od strane svojih korisnika. Sveukupno ovoj problematici je teško pronaći rješenje, jer svaka strana nudi svoje idealno rješenje bez pristanka na kompromis, te je potrebno još par godina kako bismo uvidjeli kako će rješenja poput GDPR-a utjecati na odnos sigurnosti i zaštite podataka. Možda će upravo takva regulativa potaknuti sve strane da napokon dođu do kompromisa i postignu savršen odnos između sigurnosti i zaštite podataka.

9. Literatura

28 U.S. Code § 1651 – Writshttps://www.law.cornell.edu/uscode/text/28/1651

BattleoftheClipperChiphttps://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

British intelligence 'birdwatchersspied on Nelson Mandela'shideout' https://www.telegraph.co.uk/news/worldnews/nelson-mandela/10169630/British-intelligence-birdwatchers-spied-on-Nelson-Mandelas-hideout.html

Clipperchiphttp://www.cryptomuseum.com/crypto/usa/clipper.htm

Court says Kim Dotcomcansue New Zealandspyagencyhttps://www.bbc.co.uk/news/world-asia-21695978

Data Protection Directive https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

Foreignintelligencesurveillanceacthttps://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

iOSSecurityhttps://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

Kim Dotcom: NZ Prime Ministerapologisesoverunlawfulspyoperationhttps://www.telegraph.co.uk/technology/internet/9569986/Kim-Dotcom-NZ-Prime-Minister-apologises-over-unlawful-spy-operation.html

MI5 spied on Charlie Chaplin after FBI asked for help to banishhimfrom US https://www.theguardian.com/uk/2012/feb/17/mi5-spied-on-charlie-chaplin

Notsosecret: deal at theheartof UK-US intelligencehttps://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released

NSA-GCHQ Snowdenleaks: A glossaryofthekeytermshttps://www.bbc.com/news/technology-25085592

NSA Admits to Spying on Princess Diana https://www.washingtonpost.com/wp-srv/national/daily/dec98/diana12.htm

NSA Prism program tapsin to user data of Apple, Google andothershttps://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

NSA slidesexplainthe PRISM data-collection program http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Opća uredba o zaštiti podatakahttps://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679

"OrderCompelling Apple, Inc. to AssistAgentsin Search" https://assets.documentcloud.org/documents/2714005/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf

SKIPJACKhttp://www.cryptomuseum.com/crypto/usa/skipjack.htm

Sačuvane verzije prezentacija za PRISM https://commons.wikimedia.org/wiki/Category:PRISM_(surveillance_program)

Privacypoliciesoftechgiants 'stillnot GDPR-compliant' https://www.theguardian.com/technology/2018/jul/05/privacy-policies-facebook-amazon-google-not-gdpr-compliant

REPORT on theexistenceof a global system for theinterceptionofprivateandcommercialcommunications (ECHELON interception system) (2001/2098(INI)) https://fas.org/irp/program/process/rapport_echelon_en.pdf

RESORTING TO EXTRAORDINARY WRITS: HOW THE ALL WRITS ACT RISES TO FILL THE GAPS IN THE RIGHTS OF ENEMY COMBATANTS http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-83-1-Portnoi.pdf

US buggedMerkel'sphonefrom 2002 until 2013, reportclaimshttps://www.bbc.co.uk/news/world-europe-24690055

While Nixon Campaigned, the F.B.I. Watched John Lennon https://www.nytimes.com/2006/09/21/opinion/21thu4.html

Zakon o tajnosti podataka https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/ZAKON-O-TAJNOSTI-PODATAKA-NN-79-2007.pdf

10. Prilozi

Anketa „Mjere zaštite podataka“

https://docs.google.com/forms/d/e/1FAIpQLSe58sIy4ZnQf05VMjZxD4k65swj9vFxsCagq1lwiGXdxKgZwA/viewform