Utjecaj društvenih mreža na privatnost korisnika Interneta

Delonga, Luka

SVEUČILIŠTE U ZAGREBU
CENTAR ZA POSLIJEDIPLOMSKE STUDIJE

SVEUČILIŠNI INTERDISCIPLINARNI SPECIJALISTIČKI STUDIJ
REGULIRANJE TRŽIŠTA ELEKTRONIČKIH KOMUNIKACIJA

Luka Delonga, dipl. ing.

UTJECAJ DRUŠTVENIH MREŽA NA PRIVATNOST KORISNIKA INTERNETA

SPECIJALISTIČKI RAD

Zagreb, 2023.

SVEUČILIŠTE U ZAGREBU
CENTAR ZA POSLIJEDIPLOMSKE STUDIJE

SVEUČILIŠNI INTERDISCIPLINARNI SPECIJALISTIČKI STUDIJ
REGULIRANJE TRŽIŠTA ELEKTRONIČKIH KOMUNIKACIJA

Luka Delonga, dipl. ing.

UTJECAJ DRUŠTVENIH MREŽA NA PRIVATNOST KORISNIKA INTERNETA

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
CENTER FOR POSTGRADUATE STUDIES

UNIVERSITY INTERDISCIPLINARY SPECIALIST STUDY
REGULATION OF THE ELECTRONIC COMMUNICATIONS MARKET

Luka Delonga, dipl. ing.

IMPACT OF SOCIAL NETWORKS ON INTERNET USER PRIVACY

SPECIALIST THESIS

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog interdisciplinarnog studija „Reguliranje tržišta elektroničkih komunikacija“.

Mentor:

Specijalistički rad ima: 94 stranice

Završni rad br.:

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Tihomir Katulić, Sveučilište u Zagrebu Pravni fakultet – predsjednik
2. prof. dr. sc. Gordan Ježić – član
3. izv. prof. dr. sc. Marin Vuković - član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Tihomir Katulić, Sveučilište u Zagrebu Pravni fakultet – predsjednik
2. prof. dr. sc. Gordan Ježić – član
3. izv. prof. dr. sc. Marin Vuković - član

Datum obrane: 4. listopada 2023.

SAŽETAK

Specijalističkim radom obrađena je tema povrede privatnosti korisnika interneta te utjecaja društvenih mreža na nju. Tehnološki napredak i pojava interneta omogućili su nastanak društvenih mreža, a upravo su društvene mreže postavile temelj za nastanak novih usluga utemeljenih na internetskoj platformi koje istiskuju tradicionalne elektroničko-komunikacijske usluge. Nove usluge nude više od tradicionalnih, ali zauzvrat da bi ih se moglo koristiti uglavnom zahtijevaju pristanak korisnika na prikupljanje i obradu osobnih podataka. Mogućnosti novih tehnologija te prikupljanje i obrada osobnih podataka stvorile su okolnosti u kojima su ugrožene nesmetana komunikacija, tajnost dopisivanja, sloboda izražavanja, tj. ugroženo je pravo na privatnost pojedinca zagarantirano zakonskim propisima i međunarodnim ugovorima, a zaštita osobnih podataka postala je primarna mjera kojom se ostvaruje pravo na privatnost korisnika interneta. Rad je podijeljen u četiri dijela. U prvom dijelu analizira se broj korisnika interneta, broj korisnika društvenih mreža, ukazuje se na porast novih komunikacijskih usluga u svijetu koje zamjenjuju tradicionalne poput SMS-a, a koje zakonski gotovo da nisu regulirane, što stvara potrebu interveniranja u regulatorne okvire. U drugom dijelu definira se pojam privatnosti, analizira većina relevantnih dokumenata kojima se štiti privatnost korisnika interneta te konkretnim primjerima povrede privatnosti korisnika, usporedno s analizom, ukazuje na njihove nedostatke u odnosu na izazove koje donose nove tehnologije i nove usluge. U trećem dijelu obrađuje se pojam umrežavanja, dijeljenja podataka, ponašanje korisnika unutar društvenih mreža te ukazuje na nove prijetnje po privatnost korisnika i društva u cjelini, a koje se dijelom ili u cijelosti provode putem društvenih mreža. Nadalje, analiziraju se preporuke radnih skupina i međunarodnih tijela za povećanje sigurnosti privatnosti korisnika društvenih mreža. U četvrtom dijelu analizira se broj korisnika interneta i društvenih mreža u Republici Hrvatskoj, njihove navike i poznavanje zakonskih propisa.

KLJUČNE RIJEČI:

internet, društvene mreže, navike korisnika, zaštita privatnosti, zakonski propisi

SUMMARY

Specialist work deals with the topic of violation of privacy of the Internet users and the impact of social networks on it. Technological progress and the emergence of the Internet enabled the emergence of social networks, and it was social networks that laid the foundation for the emergence of new services based on the Internet platform that displace traditional electronic communication services. New services offer more than traditional electronic communication services, but in return for being able to use them, they generally require the user's consent to the collection and processing of personal data. The possibilities of new technologies and the collection and processing of personal data have created circumstances in which unhindered communication, secrecy of correspondence, and freedom of expression are threatened, i.e. the right to privacy of the individual guaranteed by legal regulations and international agreements is threatened, and the protection of personal data has become the primary measure by which the right to privacy of Internet users is achieved. The content of the paper is diveded in four parts. First part analyses the number of Internet users and the number of social network users, points out on the increase of new communication services in the world that are replacing traditional ones, such as SMS, and which for the most part are not legally regulated and create the need for interventions in the regulatory framework. Second part defines privacy of Internet users, analyses majority of relevant documents that are intended to protect privacy of Internet users, with concrete examples of privacy abuse, parallel to analysis, points out on the disadvantages of that documents in comparison with the challenges that new technologies and new services bring. Third part analyses the concept of networking, data sharing, user behavior which are partly or entirely implemented through social networks and points out on the new threats on user privacy and the privacy of society as a whole. Furthermore, it analyses the recomendations of work groups and international bodies for increasing security of social network user privacy. Four part analyses number of Internet users and social network users in Republic of Croatia, their habits and knowledge of legal regulations.

KEYWORDS: Internet, social networks, user habits, privacy protection, legislation

SADRŽAJ

1. UVOD

Pojava interneta kao novog elektroničkog medija omogućila je velike promjene u društvu na svim razinama te je internet postao sastavni dio života u suvremenom društvu. Upravo je internet pokrenuo mnoge društvene promjene, stvorio nove ekonomske mogućnosti, omogućio nastanak novog svijeta, tzv. virtualnog svijeta, a pojavom društvenih mreža virtualni i stvarni svijet postali su bliži no ikad.

Danas je neosporno da su upravo društvene mreže postavile temelj za nastanak novih usluga utemeljenih na internetskoj platformi, koje istiskuju tradicionalne elektroničko-komunikacijske usluge. Nove usluge otvorile su nove mogućnosti za korisnike interneta kao što su jednostavno predstavljanje pojedinaca i tvrtki javnosti, brz i jednostavan pronalazak pojedinih informacija, korištenje novih komunikacijskih usluga koje za nižu cijenu pružaju više od tradicionalnih. Upravo sve te različite aktivnosti koje se svakodnevno mogu obavljati putem interneta i društvenih mreža kao da su utjecale na svijest korisnika te su oni postali spremni dijeliti osobne podatke, ime i prezime, datum rođenja, OIB, broj kreditne kartice, adresu stanovanja i sl. na društvenim mrežama i drugim uslugama utemeljenim na internetskoj platformi, bez razmišljanja o posljedicama.

Dakle, društvene su mreže donijele mnoge pozitivne mogućnosti za korisnike, ali su isto tako donijele i nove mogućnosti ugroze privatnosti korisnika od strane drugih korisnika društvenih mreža, te od strane samih davatelja usluga. Internet je „mreža nad mrežama“, odnosno globalna svjetska mreža, a zakoni koji uređuju područje privatnosti razlikuju se od države do države. Pojavom društvenih mreža, neusklađenošću i nepripremljenošću zakonodavnih okvira zemalja Europske unije i svijeta za nove načine ugroze privatnosti, problem se produbio te je postalo ugroženo jedno od temeljnih ljudskih prava – pravo na privatnost – koje se u virtualnom okruženju temelji na zaštiti osobnih podataka koje je utemeljeno međunarodnim dokumentima i ugovorima koji su implementirani u zakonodavstva većine zemalja svijeta.

Ovaj rad bavi se povredom privatnosti korisnika interneta i utjecajem društvenih mreža na nju, te ukazuje na nove momente ugroze privatnosti i sigurnosti korisnika kojima je često ishodište upravo na društvenim mrežama. Cilj rada je obraditi zaštitu privatnosti korisnika interneta s posebnim osvrtom na korisnike društvenih mreža. Također, cilj je ukazati na bitnost zaštite osobnih podataka jer njihovom zlouporabom može se nanijeti golema i nepopravljiva šteta pojedincima i društvima u cjelini. Nadalje, cilj je upozoriti na nedostatke u zakonskim

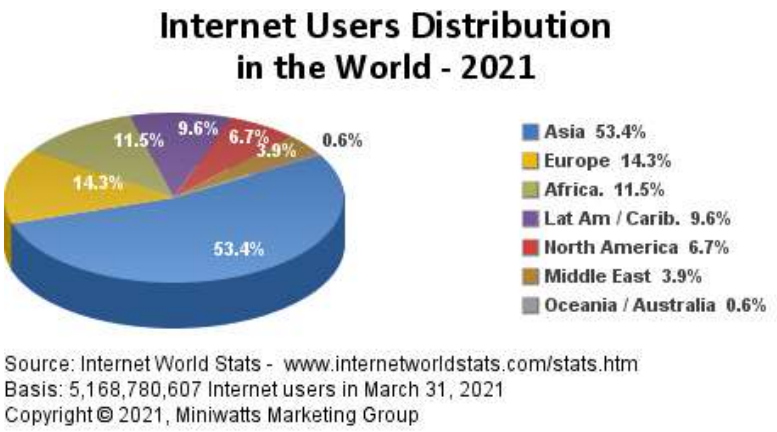
propisima koji se moraju što hitnije mijenjati, kako zbog brzine razvoja novih tehnologija i usluga, tako i zbog neodgovornosti pojedinaca prema vlastitim osobnim podatcima.

2. NOVI IZAZOVI I ZAHTJEVI ZAŠTITE PRIVATNOSTI KORISNIKA INTERNETA

„Povijest nas uči kako veliki pomaci nastaju spontano i iz težnje da se postigne nešto drugo. Često se dogodi da velika postignuća uvelike nadmaše ideje, namjere i očekivanja njihovih tvoraca, ali to ponekad dovodi do neželjenih posljedica. Budući da istovremene koristi i štete nije uvijek lako izbjeći, potrebno je od slučaja do slučaja odmjeravati s koliko se žrtve može ostvariti uspjeh i omogućiti prosperitet. Iako je riječ o suprotstavljenim interesima, to je cijena uspjeha i napretka u svijetu u kojem dobro i zlo idu zajedno u istim pojavama i djelovanjima te ih je nemoguće predvidjeti, isto kao što je nemoguće unaprijed utvrditi koliko će nova tehnologija nekom unaprijediti i olakšati rad, a koliko mu otežati i možda zagorčati život. Internet je zasigurno jedno od takvih postignuća jer je teško vjerovati da je itko od njegovih začetnika i tvoraca mogao naslutiti kako će u samo tri desetljeća od njegova nastanka poprimiti takve razmjere i nuditi sve one usluge koje danas koristimo.“[1]

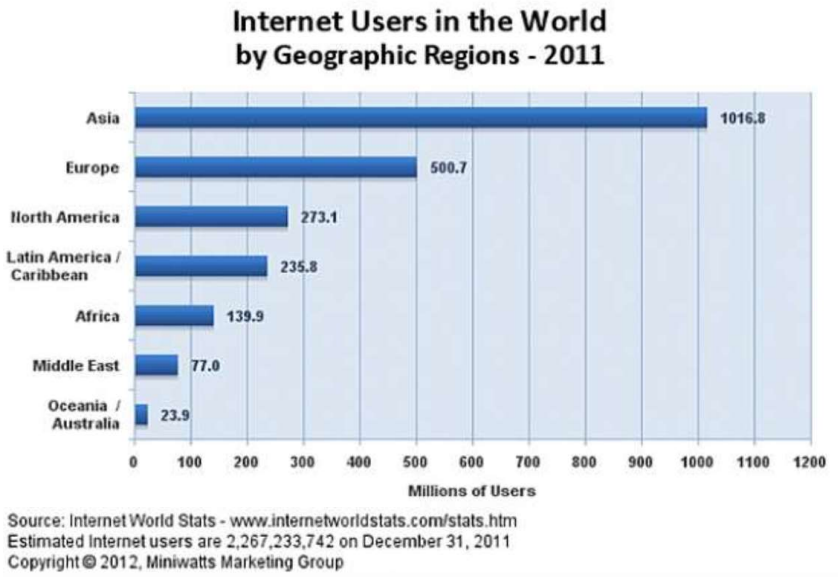
Pojavom interneta i razvojem novih tehnologija omogućena je velika lepeza usluga koja se danas koristi na internetu, a koje olakšavaju, pojednostavljuju, donose financijske i vremenske uštede korisnicima u svakodnevnom životu i poslovnim aktivnostima. Internet omogućuje da korisnici iz udobnosti svog doma ili ureda obavljaju aktivnosti za koje su inače morali utrošiti više vremena i financijskih sredstava. Upravo sve te olakotne okolnosti u svim slojevima društva potaknule su da se internet razvija i raste neslućenom brzinom u svim dijelovima svijeta. U nastavku pregledom Grafa 2.1. možemo vidjeti rasprostranjenost broja korisnika interneta širom svijeta. Tako je broj korisnika interneta sredinom 2021. godine bio veći od 5.17 milijarde, 53,4% korisnika interneta nalazi se u Aziji, 14.3% u Europi, 11,5% u Africi, 9.6% u Latinskoj Americi, 6.7% u Sjevernoj Americi, 3.9% na Srednjem istoku i 0,6% na području Oceanije i Australije.

[1] Dragičević D., Privatnost u virtualnom svijetu, str. 615-616., Zbornik PFZ, 51(34), Zagreb, (Ožujak 2001)



Graf 2.1. *Broj korisnika interneta u regijama svijeta 6. mjesec 2021. prema TitanHQ dostupno na https://www.titanhq.com/safe-browsing-are-your-users-internet-habits-harming-your-corporation/*

Pregledom Grafa 2.2. i usporedbom s Grafom 2.1. možemo utvrditi da je u vremenskom periodu od 10 godina ostvaren rast broja korisnika interneta na razini ukupne svjetske populacije za oko 2,4 milijarde te je gotovo sigurno da će se taj rast nastaviti.[2]



Graf 2.2. *Broj korisnika interneta u regijama svijeta 3 mjesec 2011. prema M. Y. Kasule, B. Consulting, dostupno na https://www.modernghana.com/news/490362/increase-of-internet-usage-in-ghana-and-its-implications.html*

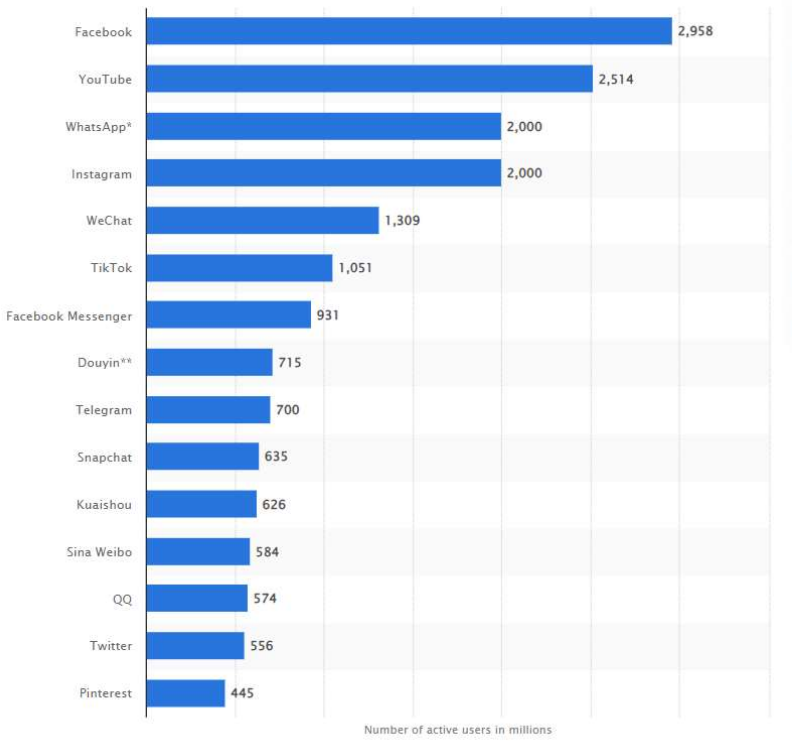
[2] International website that features up to date World Internet Users, dostupno na https://www.internetworldstats.com/stats.htm, stranica posjećena 22.5.2023.

Daljnjom analizom možemo zaključiti da broj korisnika interneta raste u svim regijama svijeta. Afrika je imala rast od 523 milijuna korisnika, Europa je imala rast od oko 200 milijuna korisnika, Sjeverna Amerika od oko 110 milijuna korisnika, Latinska Amerika oko 230 milijuna, a Azija je ostvarila rast od 1,3 milijarde korisnika. Usporedno s rastom broja korisnika interneta dolazi i do pojave i ekspanzije društvenih mreža. Društvene mreže su usluge utemeljene na internetskoj platformi koje omogućuju korisnicima međusobno povezivanje, razmjenu podataka i komuniciranje. Društvene mreže postale su sastavni dio svakodnevnog života svih slojeva društva. Usluge putem društvenih mreže su besplatne, samo što korisnik mora dati privolu na obradu svojih osobnih podataka u određene svrhe. U uvjetima korištenja društvene mreže Facebook navodi se sljedeće: „Ne naplaćujemo vam upotrebu Facebooka ni 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. Upotrebljavamo vaše osobne podatke da bismo odredili koje ćemo vam oglase prikazivati.“[3] Navedeni citat samo je jedan od uvjeta koji se odnosi na obradu osobnih podataka korisnika društvene mreže Facebook te i druge društvene mreže posluju po istom ili sličnom modelu – usluga je besplatna, ali koriste osobne podatke svojih korisnika u određene svrhe kao što su marketinške, poboljšanje kvalitete usluge i slično.

U nastavku Graf 2.3. prikazuje podatke za najpopularnije društvene mreže rangirane prema broju aktivnih računa u Siječnju 2023. godini. Analizom Grafa 2.3. možemo vidjeti da prednjači društvena mreža Facebook koja je na početku 2023. godine imala je dvije milijarde i devetsto pedeset i osam milijuna aktivnih korisnika. Pored društvenih mreža kao vodeće usluge za razmjenu podataka na internetu dolazi do pojave i ubrzanog rasta broja internetskih aplikacija koje omogućavaju komunikaciju i na neki način oponašaju tradicionalne elektroničko-komunikacijske usluge kao što je glasovni poziv i SMS, no one to nisu, a često nude i više, primjerice videopozive.[4]

[3] Terms of Service, Facebook Ireland Limited, dostupno na https://www.facebook.com/legal/terms, stranica posjećena 9.5.2022.

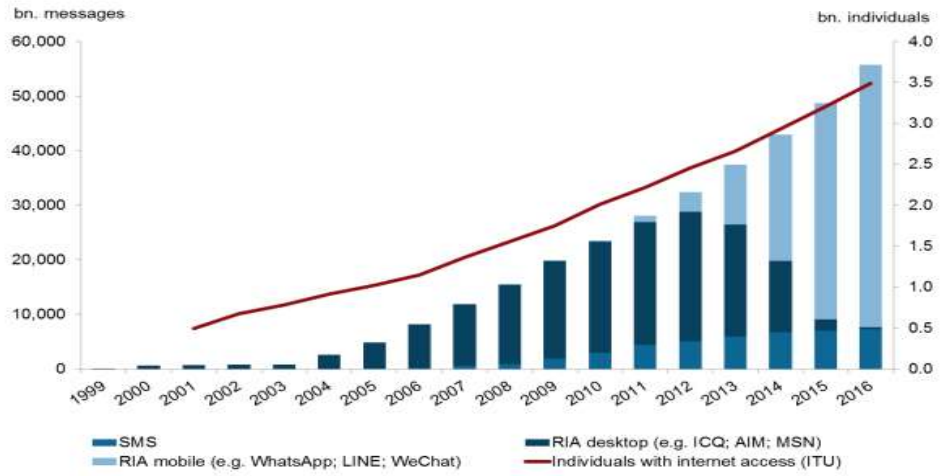
[4] Most popular social networks worldwide as of January 2023, dostupno na https://www.statista.com/statistics/272014/global-social-neusers/, stranica posjećena 24.6.2023.



Graf 2.3. *Društvene mreže poredane prema broju aktivnih računa 1. mjesec 2023. prema Internet World Stats dostupno na: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/*

Navedene usluge su u svijetu poznate pod nazivom Bogate interaktivne aplikacije (engl. *Rich Interaction Applications* – RIA), a pripadaju OTT – uslugama (engl. *Over-the-Top*). Graf 2.4. prikazuje odnos RIA poruka i SMS poruka poslanih u svijetu od 1999. do 2016. godine.[5] Iz grafa možemo vidjeti kako je još 2016. godine upotreba RIA usluga rasla u odnosu naspram SMS usluge, a tijekom narednih godina ta se razlika samo povećava. Većina davatelja OTT-usluge imaju sličan model poslovanja kao i društvene mreže, usluga je besplatna, ali vrši se prikupljanje i obrada osobnih podataka korisnika u određene svrhe te je prilikom preuzimanja i pokretanja aplikacije potrebno dati privolu na prikupljanje i obradu podatka u određene svrhe.

[5]Arnold R, Hildebrandt C., Kroon P., Taş S. The Economic and Societal Value of Rich Interaction Applications (RIAs). str. 11., WIK - Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef (May 2017).



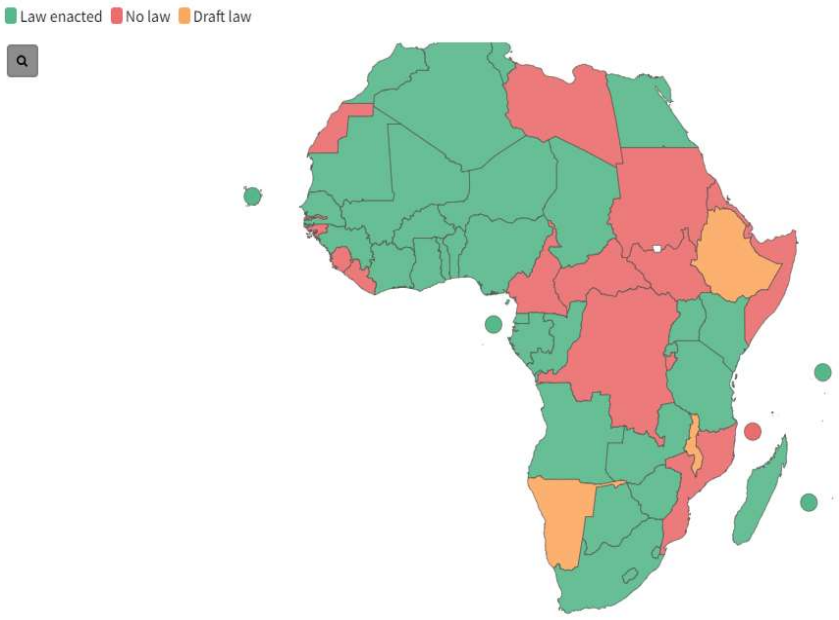
Graf 2.4. *Odnos RIA poruka i SMS poruka poslanih u svijetu od 1999. do 2016. godine, prema Arnold R, Hildebrandt C., Kroon P., Taş S. The Economic and Societal Value of Rich Interaction Applications (RIAs). str. 11., WIK - Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef (May 2017)*

Razvoj interneta omogućio je uzlet društvenih mreža i OTT-usluga koji korisnicima omogućuju usluge u zamjenu za osobne podatke koje pohranjuju prilikom kreiranja računa i korištenja usluga. Nadalje, od korisnika se često traži da davatelju usluge omogući pristup imeniku, kameri, mikrofonu i slikama na uređaju uz uvjeravanje da su ti podatci potpuno sigurni te se neće zlorabiti. Takav pristup od davatelja usluga kod korisnika je stvorio novu paradigmu spram privatnosti, a rezultat je da se osobni podatci dijele gotovo bez razmišljanja. A upravo je to bio i cilj kompanijama koje svoje poslovanje utemeljuju ili unaprjeđuju na prikupljanju i obradi osobnih podataka korisnika te dolazi do prikupljanja i strojne obrade velikih količina podataka pod nazivom „veliki podatci“ (engl. *big data*). Kompanijama koje se bave ciljanim mrežnim marketingom osobni podatci su jako vrijedni te prikupljaju podatke i s korisničkih uređaja poput pametnih telefona, zadiru u privatnost korisnika, a sve u svrhu kvalitetnijeg ciljanog marketinga.[6] Upravo sve veća upotreba Big Data od strane društvenih medija, računalstva u oblaku, interneta i pametnih telefona, javnih tijela, naprednih strojeva koji se sami nadograđuju programiranih u ICT tvrtkama, stvara potrebu za potpuno novim poimanjem privatnosti kod svih dobnih skupina. Premda se na tom polju bilježi napredak, razvoj tehnologije i sve veća

[6] Demetriou S., Merrill W., Yang W., Zhang A., Gunter C.A., Free for All! Assessing User Data Exposure to Advertising Libraries on Android, str. 2., ISOC Network and Distributed System Security 2016, San Diego, (February 2016)

upotreba Big Data zahtijeva da odgovorni za obradu podataka razviju niz mjera u zaštiti privatnosti i podizanju svijesti šire javnosti o privatnosti.[7]

Daljnji problem je u tome što zakonska regulativa u svijetu nije prisutna svugdje na istoj razini i nešto što je kažnjivo u jednoj zemlji nije u drugoj, ali internet je dostupan svugdje. U nastavku možemo vidjeti sliku karte Afrike, zelenom bojom su označene zemlje koje imaju usvojene sveobuhvatne zakone o zaštiti osobnih podataka. Afrika ima 55 zemlja, no samo njih 35 ima usvojene sveobuhvatne zakone o zaštiti privatnosti dok su u 3 zemlje zakoni u izradi. Također, potrebno je naglasiti da pojedine zemlje poput Egipta i Tanzanije, imaju usvojene sveobuhvatne zakone o zaštiti privatnosti, ali nemaju tijela koja bi ih provodila.[8] No, najveći problem Afrike nije neimanje usvojenih zakona o zaštiti privatnosti već kvaliteta provedbe istih. Također zlouporaba raznih alata za nadzor i prikupljanje podataka na afričkom kontinentu od strane vlada afričkih zemalja koje traže informacije o korisnicima od tvrtki kao što su Google, Facebook i Twitter, pritom očito kršeći zakonske norme o privatnosti.[9]



Slika 2.1. *Karta Afrike s označenim zemljama koje imaju zakon o zaštiti osobnih podataka prema Data Protection Africa, ALT Advisory, June 2023 dostupno na:* https://dataprotection.africa

[7] Berbers Y., Hildebrandt M., Vandewalle J., Privacy in an age of the Internet, social networks and Big Dana, str. 48., Royal Flemish Academy of Belgium for Science and the Arts, Brussel, 2018.
[8] Data Protection Africa, ALT Advisory, June 2023 dostupno na: https://dataprotection.africa stranica posjećena 26.07.2023.
[9] Prinsloo P., Kaliisa R., Data privacy on the African continent: Opportunities, challenges and implications for learning analytics, str. 5., British Journal of Educational Technology, 13.4.2022.

Nadalje, društvena mreža Facebook s Free Basics platformom je vodeća mreža za pristup internetu u Africi. Što ukazuje na ta da je Facebook internet za mnoge ljude u Africi.[10] Dakle, društvene mreže koje svoje poslovanje temelje na prikupljanju i obradi osobnih podataka u određenim dijelovima svijeta postaju vodeći davatelj usluge pristupa internetu, a gdje i same vlade tih zemalja traže od njih da krše zakonske propise. A koliko su osobni podatci korisnika nekad u opasnosti, govori nam i to da je nezakonito osobne podatke korisnika u cijelom svijeta prikupljala i NSA *(National Security Agency)* kroz program PRISMA koji je razotkrio Edward Snowden još 2013. godine. Slika 2.2. prikazuje od kojih je davatelja usluga i koje podatke prikupljala NSA.

Slika 2.2. *Detalji o prikupljanju osobnih podataka program PRISMA, E. Snowden, Prezentacija PRISM/US-984XN Overview, str. 3.(travnja 2013.) dostupno na: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-055.pdf*

Pregledom Slike 2. možemo vidjeti da je NSA od Googlea, Skypea, Facebooka, Yahooa i drugih davatelja usluga prikupljala gotovo sve osobne podatke korisnika, a to su: video, razgovor, fotografije, korisničke detalje na društvenim mrežama, pohranjene podatke i dr.

[10] Maggie Fick, Alexis Akwagyiram, In Africa, scant data protection leaves internet users exposed. Reuters. (April 4. 2018), dostupno na https://www.reuters.com/article/us-facebook-africa-idUSKCN1HB1SZ, stranica posjećena 24.5.2023.

Upravo postupak NSA ukazuje nam na to koliko su osobni podatci korisnika tražena roba, ali istovremeno koliko su i ugroženi.

Možemo zaključiti da broj korisnika interneta u svim dijelovima svijeta raste sve više te dolazi do dominacije usluga putem interneta poput društvenih mreže i OTT-usluga. Davatelji tih usluga svoje poslovanje temelje na prikupljanju i obradi osobnih podataka te u pojedinim dijelovima svijeta imaju toliki utjecaj da su i glavni davatelji usluge pristupa internetu. Upravo su davatelji usluga koji svoje poslovanje temelje na osobnim podatcima zaslužni za ideju stvaranja velikih baza osobnih podataka korisnika i strojnu obradu, što povećava rizik povrede privatnosti korisnika. Nadalje, neujednačena zakonska regulativa u pojedinim dijelovima svijeta, nezakonito prikupljanje osobnih podataka korisnika, čak i od vladinih agencija, ukazuje da je pravo na privatnost korisnika interneta ugroženije no ikada te da se nešto mora poduzeti što brže jer je ugroženo jedno od temeljnih ljudskih prava – pravo na privatnost. U radu se dalje bavimo analizom zakonskog okvira i usluga društvenih mreža jer su upravo društvene mreže donijele novi moment u područje internetskih usluga i svoje poslovanje utemeljile na prikupljanju i obradi osobnih podataka korisnika.

3. PRIVATNOST NA INTERNETU I PRAVNA REGULATIVA

3.1. Privatnost kroz povijest i shvaćanje pojma privatnosti

„Pojam *privatnost* dolazi od latinske riječi *privatus*, koja znači lični, osobni, neslužbeni, tajni, skroviti, povjerljivi, zatvoreni...“[11] Privatnost se spominje već od davnina u većini starih kultura. „Tako npr. Biblija ima brojna upućivanja na privatnost, a zaštita privatnosti u različitim aspektima postojala je i u hebrejskoj kulturi, staroj Grčkoj i drevnoj Kini. U početku se najčešće radilo o pravu pojedinca na nepovredivost doma.“[12]

Termin *privatnost* (engl. *privacy*), kako ga danas promatramo, po prvi su put odredili sudac Louis Brandeis i odvjetnik Samuel Warren 1890. godine u eseju *Pravo na privatnost* (engl. *The Right to Privacy*) objavljenom u časopisu *Harvard Law Review* (god. 4, br. 5) kao *Individual's right to be let alone*, tj. „Pravo pojedinca da bude pušten na miru“. Brandeis i Warren navode da je zaštita privatnog okruženja temelj individualne slobode u modernom dobu. S obzirom na razvoj tehnologije te sve veće mogućnosti vlade, tiska, drugih agencija i institucija da napadnu prethodno nedostupne osobne aktivnosti pojedinca. Ustvrdili su da se zakoni moraju razvijati usporedno s tehnološkim promjenama kao odgovor na njih. Smatrali su da su tradicionalne zakonske zabrane protiv prijestupa kao što su napadi, klevete i druge radnje, davale dovoljnu zaštitu u ranijim razdobljima, ali ta uspostavljena načela ne mogu zaštititi pojedince od previše poduzetnog tiska, fotografa ili posjednika bilo kojih drugih modernih uređaja za preoblikovanje ili reprodukciju slike ili zvukova. Slijedom toga, zaključili su da se trebaju razviti pravni lijekovi kako bi se provele određene granice između javnog i privatnog života, kako bi se održalo *pravo na nečiju osobnost* u sučeljavanju s modernom poslovnom praksom i invazivnim izumima.[13]

Pravo na privatnost pojedinca jedno je od temeljnih ljudskih prava i bilo je bitno kroz prošlost čovječanstva, a pojedinci poput Brandeisa i Warrena su još 1890. godine upozoravali na probleme u području privatnosti čiju povredu omogućuju nove tehnologije i općenito novi društveni koncept. Danas, više od 120 godina nakon eseja Brandeisa i Warrena, uslijed

[11] Bratoljub Klaić, Rječnik stranih riječi, str. 1090., Nakladni zavod Matice hrvatske, (Zagreb, 2004)
[12] Dragičević, D., Gumzej, N., Jurić M., Katulić, T., Lisičar, H., Pravna informatika i pravo informacijskih tehnologijastr, str. 102. Narodne novine, (Zagreb, 2015)
[13] Brandeis L. D., Warren, Jr. S. D., THE RIGHT TO PRIVACY, Harvard Law Review, V. IV, No. 5, (December 1890). dostupno na https://faculty.uml.edu//sgallagher/Brandeisprivacy.htm, stranica posjećena 16.3.2023.

nevjerojatnog napretka tehnologije, erupcije društvenih mreža i razvoja usluga utemeljenih na internetskoj platformi, esej postaje aktualniji no ikada. Osobni podatci postali su traženiji no ikada. Upravo na temelju zahtjeva za osobnim podatcima koje omogućuju nove usluge i tehnologije Andro Pavuna u doktorskom radu navodi sljedeće: "…privatnost je suočena s opsegom i razinom eksternih i internih ugroza privatnosti, a pojam privatnosti radikalno je transformiran iz temeljnog ljudskog prava u robu kojom se trguje."[14] Ako uzmemo u obzir da je preduvjet za korištenje usluga društvenih mreža i drugih usluga utemeljenih na internetskoj platformi poput OTT-usluga, pristanak na prikupljanje i obradu osobnih podataka, slobodno možemo zaključiti da su osobni podatci svakako postali sredstvo plaćanja i roba kojom se trguje te su samim time postali ugroženiji no ikada. Dakle u novonastalim okolnostima pravo na privatnost usko se povezuje s pravom na zaštitu osobnih podataka, premda su to prema Europskoj povelji o temeljnim ljudskim pravima dva odvojena temeljna prava. „Zaštita podataka odnosi se na zaštitu svih informacija koje se odnose na identificiranu ili prepoznatljivu fizičku (živuću) osobu, uključujući imena, datume rođenja, fotografije, videosnimke, adrese e-pošte i telefonske brojeve. Ostale informacije, kao što su IP adrese i komunikacijski sadržaj, koje su povezane s krajnjim korisnicima komunikacijskih usluga ili ih pružaju krajnji korisnici komunikacijskih usluga, također se smatraju osobnim podatcima. Pojam zaštite podataka proizlazi iz prava na privatnost i oba su ključna za očuvanje i promicanje temeljnih vrijednosti i prava;…."[15] Pravom na zaštitu podataka osigurava se pravo na privatnost korisnika jer upravo obradom osobnih podataka može se povrijediti pravo na privatnost korisnika. „Na primjer, ako poslodavac bilježi informacije o imenima i naknadama zaposlenika, samo bilježenje tih informacija ne može se smatrati miješanjem u privatni život. To bi se, međutim, moglo smatrati miješanjem ako bi poslodavac te osobne podatke zaposlenika prenosio trećim stranama."[16] Dalje u ovom poglavlju bavimo se analizom propisa kojima se osigurava zaštita privatnosti korisnika interneta.

[14] Pavuna A., Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova, str. 194., (Zagreb, 2019), dostupno na https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:868, stranica posjećena 17.6.2023.

[15] The European Data Protection Supervisor, Data Protection, dostupno na https://edps.europa.eu/data-protection/data-protection_en, stranica posjećena 05.7.2023.

[16] Priručnik o europskom zakonodavstvu o zaštiti podataka, str. 24., dostupno na https://www.echr.coe.int/documents/d/echr/handbook_data_protection_hrv, 04.7.2023.

3.2. Temeljni dokumenti zaštite privatnosti

Sredinom prošlog stoljeća briga za privatnost pojedinca počinje doživljavati punu afirmaciju i opće priznanje te dovodi do prihvaćanja prvog dokumenta pod nazivom *Opća deklaracija o ljudskim pravima*. Opća deklaracija o ljudskim pravima usvojena je na Općoj skupštini Ujedinjenih naroda Rezolucijom 217 A (III) 10. prosinca 1948. godine. Deklaracija je sveobuhvatni instrument zaštite ljudskih prava, proglašen od strane jedne međunarodne organizacije s ciljem da osigura „zajedničko razumijevanje" ljudskih prava i sloboda. Iako je donesena kao neobvezujući dokument, danas je prihvaćena kao normativni instrument koji stvara, barem neke, pravne obveze za države članice Ujedinjenih naroda. Deklaracija, kao najstariji dokument u području ljudskih prava člankom 12. propisuje da „…nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada."[17] Opća deklaracija o ljudskim pravima je odlukom Vlade Republike Hrvatske i objavom 27. studenoga 2009. godine prihvaćena od strane Republike Hrvatske. Na temeljima Opće deklaracije o ljudskim pravima članice Vijeća Europe 4. studenog 1950. godine potpisuju međunarodni ugovor pod nazivom *Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda,* koja stupa na snagu 1953. godine. Konvencija za zaštitu ljudskih prava i temeljnih sloboda je međunarodni ugovor prema kojemu se države članice Vijeća Europe obvezuju osigurati zaštitu temeljnih građanskih i političkih prava i sloboda. Konvencija djeluje kao opći pravni okvir u kojemu su definirana temeljna ljudska prava i slobode te način njihove zaštite. Države potpisnice Konvencije su se obvezale osigurati primjenu Konvencije u okviru vlastitih pravnih sustava, uvjetima predviđenima Konvencijom. Europski sud za ljudska prava predstavlja supsidijaran mehanizam zaštite te djeluje kao zaštitnik prava iz Konvencije kada njihova zaštita nije osigurana na nacionalnoj razini pojedine države potpisnice Konvencije. Republika Hrvatska je ratificirala Konvenciju 5. studenog 1997. godine, pa stoga Konvencija, sukladno članku 141. Ustava Republike Hrvatske predstavlja dio njezinog unutarnjeg pravnog poretka. Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda je najstariji i najučinkovitiji dokument s pravnom snagom koji je do danas ratificiralo 47 zemalja europskog kontinenta. Članak 8. stavak 1. Konvencije nalaže da: „…svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja", dok stavak 2. istog članaka propisuje da: „…javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u

[17] Odluka o objavi Opće deklaracije o ljudskim pravima NN 12/2009, dostupno na https://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html, stranica posjećena 22.11.2022.

demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih."[18] Pored Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda Republika Hrvatska kao članica Europske unije dužna je pridržavati se i Povelje Europske unije o temeljnim ljudskim pravima (2007/C 303/01) koja je objavljena u službenom listu Europske unije 12. prosinca 2007. godine, a postala je pravno obvezujuća 1. prosinca 2009. godine. Povelja kroz članak 7. i članak 8. uređuje područje privatnosti obrade podataka i komuniciranja. Članak 7. glasi: „…svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja." Članak 8. stavak 1 glasi: „…svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose"; stavak 2 – „takvi podatci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podatcima koji se na njega ili nju odnose i pravo na njihovo ispravljanje"; stavak 3 – „Poštovanje tih pravila podliježe nadzoru neovisnog tijela."[19]

Nadalje, svijet pogođen trećom industrijskom revolucijom *Digitalnom revolucijom*, koju možemo podijeliti u tri razdoblja. Prvo razdoblje sedamdesete godine pojava računala, drugo osamdesete dostupnost računala kompanijama te devedesete kada su računala postala dostupna u većini domova. Za vrijeme tih razdoblja svijet je uvio probleme i u Europi se dogodilo mnoštvo pravnih intervencija s namjerom reguliranja računalne obrade osobnih podataka. „Prvi slučaj pravne intervencije dogodio se u Zapadnoj Njemačkoj gdje savezne države Saska (7. listopada 1970.) i Bavarska (12. listopada 1970.) donose Zakon o zaštiti podataka, nakon čega 1971. godine, slijedi savezni Zakon o zaštiti podataka, a do 1981. godine sve njemačke savezne države imaju posebne zakone o zaštiti podataka. Dalje, zakone o zaštiti podataka donose i druge države Švedska (1973.), Francuska (1978.), Luksemburg (1979.), Danska (1979.), Austrija (1980.), Norveška (1980.), Island (1982.), Velika Britanija (1984.), Finska (1988.), Nizozemska (1990.), Portugal (1991.), Španjolska (1993.), Belgija (1993.) i Švicarska (1993.). Pojedine europske zemlje mijenjale su vlastiti Ustav tako da uključuje klauzule o privatnost."[20]

[18] Konvenciju za zaštitu ljudskih prava i temeljnih sloboda; protokoli broj 1, 4, 6 i 7. NN 6/1999
[19] Povelje Europske unije o temeljnim pravima. dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P, stranica posjećena 10.1.2023.
[20] Guarda P., Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, str. 6. (December 2009). dostupno na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517449, stranica posjećena 14.7.2022.

Ali da digitalna revolucija ide dalje, razvija se brže od zakonskih okvira te su prava pojedinca koja jamče Opća deklaracija o ljudskim pravima, Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, Povelje Europske unije o temeljnim ljudskim pravima i druge zakonske odredbe u pojedinim zemljama postala nedostatna možemo iz puno primjera koji su zahvatili internet i društvene mreže. Jedan od primjera ugroze privatnosti korisnika je *Osvetnička pornografija*. Osvetnička pornografija je oblik internetskog uznemiravanja, a njegove su ključne karakteristike sljedeće:

• da sadrži seksualno eksplicitan sadržaj, koji najčešće uključuje slike ili videozapise
• obično je stvara uz pristanak onih koji su prikazani
• dalje se dijeli bez pristanka onih koji su prikazani
• dijeli se elektroničkim putem, što može biti putem e-pošte, društvenih medija ili web-stranica
• obično je počinjeno u kontekstu prekida veze
• obično se smatra da su ga počinili muškarci protiv žena
• motiviran je osvetom.

„Najveći se dio seksualno eksplicitnih fotografija, a čiju objavu možemo smatrati osvetničkom pornografijom, objavljuje na vodećim društvenim mrežama: Facebooku, Twitteru i Tumblru, gdje ih se može dijeliti u sekundi, a velik broj žrtava koje su istom pogođene često razmišlja i o samoubojstvu.“[21]
Uvidjevši da međunarodni dokumenti koji su implementirani u zakonodavstvo Velike Britanije nisu dovoljni te da hitno treba nešto poduzeti, u travnju 2015. godine Velika Britanija promijenila je kazneni zakon te se osvetnička pornografija tretira kao kazneno djelo.

Njemačka je uvidjevši nedostatke u svom zakonodavnomu okviru u lipnju 2014. godine donijela zakon prema kojem bivši partneri moraju izbrisati sve intimne ili golišave fotografije, ako to jedna strana zatraži.

U Sjedinjenim Američkim Državama ne postoji federalni zakon koji sankcionira osvetničku pornografiju, ali 46 saveznih država ima svoja posebna pravila i zakone koji reguliraju kazne i sankcije za slučajeve osvetničke pornografije, a izrečene kazne protiv osoba koje su počinile takva djela na području Sjedinjenih Američkih Država broje se u milijunima dolara.

[21] Davidson J., Livingstone S., Jenkins S., Dr Gekoski A., Dr Choak C., Ike T., Phillips K., Adult Online Hate, Harassment and Abuse: A rapid evidence assessment, str.71. UK Council for Internet Safety (UK, June 2019), dostupno na https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf, stranica posjećena 12.1.2023.

U Republici Hrvatskoj djelo osvetničke pornografije kvalificira se kao kazneno djelo kažnjivo člankom 146. Kaznenog zakona Nedozvoljena uporaba osobnih podataka i člankom 140. Kaznenog zakona Nametljivo ponašanje, temeljem kojih se predviđa zatvorska kazna u trajanju do jedne odnosno do tri godine. Nadalje, za isto djelo postoji mogućnost utvrđivanja kaznene odgovornosti sukladno Glavi petnaest Kaznenog zakona Kaznena djela protiv časti i ugleda.[22] Kazneni zakon Republike Hrvatske prepoznaje osvetničku pornografiju kao kazneno djelo. Ali, donošenjem posebnog zakona o neprimjerenom/nedozvoljenom ponašanju na internetu i društvenim mrežama, kao što su donijele pojedine zemlje svijeta, svakako bi unaprijedilo postojeći zakonodavni okvir Republike Hrvatske.

3.3. Zaštita privatnosti osobnih podataka temeljem Ustava Republike Hrvatske

Pravo pojedinca i grupa na privatnost u Republici Hrvatskoj štite se temeljem Ustava Republike Hrvatske, nekoliko zakona, međunarodnih ugovora i podzakonskih akta koji su implementirani ili proizlaze iz Ustava Republike Hrvatske. Svakako prvi među njima je temeljni dokument države, a to je Ustav Republike Hrvatske, članak 16. Ustava Republike Hrvatske propisuje da se „…slobode i prava mogu ograničiti samo zakonom da bi se zaštitila sloboda i prava drugih ljudi te pravni poredak, javni moral i zdravlje. Svako ograničenje slobode ili prava mora biti razmjerno naravi potrebe za ograničenjem u svakom pojedinom slučaju“,[23] članak 35. „…svakomu se jamči štovanje i pravna zaštita njegova osobnog i obiteljskog života, dostojanstva, ugleda i časti.“[24] Članak 36. Ustava Republike Hrvatske propisuje „…sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Samo se zakonom mogu propisati ograničenja nužna za zaštitu sigurnosti države ili provedbu kaznenog postupka.“[25] Nadalje članak 37. Ustava Republike Hrvatske propisuje „…svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podatci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.“[26]

[22] Kazneni zakon, NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19
[23] Ustav Republike Hrvatske, NN br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/1
[24] ibid.
[25] ibid.
[26] ibid.

Upravo Ustav i zakonski akti koji proizlaze iz njega daju temeljne odrednice zaštite privatnosti, ali pojavom novih usluga utemeljenih na internetskoj platformi koje potiskuju tradicionalne komunikacijske kanale privatnost korisnika postaje ugrožena. Navedene usluge korisniku omogućuju korištenje istih uz prihvaćanje općih uvjeta korištenja davatelja usluga. Što uglavnom omogućuje davatelju prikupljanje podataka o korisniku i dijeljenje s trećom stranom u određenu svrhu. Upravo uvjeti korištenja omogućavaju i čitanje sadržaja poruka navodno u svrhu zaštite samih korisnika. Na tu temu u intervju za *Vox News* 2. travnja 2018. godine Mark Zuckerberg izjavio je sljedeće: „Mijanmarska pitanja su unutar tvrtke dobila dosta pažnje. Sjećam se, jedne subote ujutro primio sam telefonski poziv da smo otkrili kako ljudi pokušavaju širiti senzacionalističke poruke putem Facebook Messengera svakoj strani u sukobu. Dakle, mislim da je jasno da su ljudi pokušavali koristiti naše alate kako bi potaknuli stvarnu štetu. Sada, u tom slučaju, naši sustavi otkrivaju što se događa, zaustavljamo prolazak tih poruka.“[27] Nadalje, u pravilima upotrebe podataka društvene mreže Facebook piše „Prikupljamo sadržaj, komunikaciju i druge podatke koje unosite prilikom upotrebe naših proizvoda, uključujući one koje unesete kada se registrirate za korisnički račun, kreirate ili dijelite sadržaj te kada šaljete poruke ili komunicirate s drugima…“[28] Izjave čelnika Facebooka kazuju da se podatci iz poruka Facebook Messengera obrađuju i čitaju. Nadalje, u više navrata izjave da se podatci iz poruka i poziva ne prikupljaju u marketinške svrhe, u suprotnosti su s pravilima upotrebe podataka društvene mreže Facebook. Facebook je dostupan i koristi se u kako u cijelom svijetu tako i u Republici Hrvatskoj te postaje nejasno u koju se svrhu podatci prikupljaju i možebitno ukazuje na kršenje temeljnih ljudskih prava zaštite privatnosti zagarantiranih međunarodnim dokumentima, ali i samim Ustavom Republike Hrvatske, iz odredbe članka 35., i drugih zakonskih odredbi koje proizlaze iz Ustava.

3.4. Opća uredba o zaštiti podataka

Zbog tehnološkog razvoja i novih načina obrade osobnih podataka, Europska unija donijela je Opću uredbu o zaštiti podataka (engl. *General Data Protection Regulation*). Opća uredba o zaštiti podataka je Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016.

[27] Klein E., Mark Zuckerberg on Facebook's hardest year, and what comes next. Vox. (Apr 2, 2018), dostupno na https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge, stranica posjećena 23.11.2022.

[28] Data usage rules, Facebook Ireland Limited, dostupno na https://www.facebook.com/privacy/explanation/, stranica posjećena 18.1.2023.

o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Direktive 95/46/EZ. Na snazi je u svih 28 država članica Europske unije od 25. 5. 2018. godine.[29] U Republici Hrvatskoj je stupanjem na snagu Opće uredbe donesen i Zakon o provedbi iste kojim se dodatno reguliraju obaveze i kazne.

Općom uredbom o zaštiti podataka osigurava se ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka što osigurava jednostavniju i jednaku zaštitu prava svih pojedinaca u Europskoj uniji. Nadalje, Općom uredbom su se uvele nove i pojednostavnile pojedine već postojeće definicije, odredili biometrijski i genetski podatci, preciznije opisali postojeći pojmovi, povećala prava ispitanika te se smanjile i pojednostavnile pojedine administrativne obveze za voditelje zbirki osobnih podataka, povećale nadzorne ovlasti te je omogućeno izricanja kazni od strane tijela za zaštitu osobnih podataka.[30]

Uredba člankom 4. definira pojmove koji su povezani uz zaštitu i obradu osobnih podataka pa su tako:

- „**osobni podatci** su svi podatci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podatci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;"[31]
- „**obrada** je svaki postupak ili skup postupaka koji se obavljaju na osobnim podatcima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanjem ili kombiniranjem, ograničavanjem, brisanjem ili uništavanjem;"[32]
- „**izrada profila** je svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s

[29] Agencija za zaštitu osobnih podataka, Osnovne informacije za organizacije, (pro 14, 2020) dostupno na https://azop.hr/osnovne-informacije-za-organizacije/, stranica posjećena 10.7.2023.
[30] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka),SL L 119/1, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, stranica posjećena 11.2.2023.
[31] ibid.
[32] ibid.

pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;“[33]

- „**voditelj obrade** je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;“[34]
- „**sustav pohrane** je svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;“[35]
- „**primatelj** je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podatci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade;“[36]
- „**privola** ispitanika je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;“[37]
- „**povreda osobnih podataka** je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podatcima koji su preneseni, pohranjeni ili na drugi način obrađivani.“[38]

Pojedina nova prava u području zaštite osobnih podataka uređena Općom uredbom propisana su člancima 12. – 22., a to su:

• **transparentnost**: pružanje podrazumijeva informacije prilikom prikupljanja osobnih podataka kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o

[33] ibid.
[34] ibid.
[35] ibid.
[36] ibid.
[37] ibid.
[38] ibid.

svojem identitetu i kontaktnim podatcima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole;[39]

• **pristup podatcima**: znači dobiti od voditelja obrade potvrdu obrađuju li se osobni podatci koji se odnose na njega te ako se takvi osobni podatci obrađuju, pristup osobnim podatcima i informacije, među ostalim, o obrađenim osobnim podatcima, o svrsi obrade, roku pohrane, iznošenju u treće zemlje itd.;[40]

• **pravo na ispravak**: znači da ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;[41]

• **brisanje („pravo na zaborav“)**: znači da ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako, među ostalim, osobni podatci više nisu nužni u odnosu na svrhu obrade, ispitanik je povukao privolu za obradu, osobni podatci su nezakonito obrađeni itd., ovo pravo ima ograničenja pa tako na primjer političar ne može zatražiti brisanje informacija o sebi koje su dane u okviru njegova političkog djelovanja;[42]

• **pravo na ograničenje obrade**: u pojedinim situacijama (na primjer, kada je točnost podataka osporavana ili kada ispitanik želi da voditelj obrade zadrži njegove podatke) ispitanik ima pravo zahtijevati da se obrada ograniči uz iznimku pohrane i nekih drugih vrsta obrade;[43]

• **pravo na prenosivost**: ispitanik ima pravo zaprimiti svoje osobne podatke, a koje je prethodno pružio voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podatci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru;[44]

[39] ibid.
[40] ibid.
[41] ibid.
[42] ibid.
[43] ibid.
[44] ibid.

• **pravo na prigovor**: ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ista temelji na zadaći od javnog interesa, na izvršavanju službenih ovlasti voditelja obrade ili na legitimnom interesu voditelja obrade (uključujući i profiliranje), tada voditelj obrade ne smije više obrađivati osobne podatke ispitanika, osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika te radi zaštite pravnih zahtjeva, također ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podatci više se ne smiju obrađivati;[45]

• **automatizirano pojedinačno donošenje odluka, uključujući izradu profila**: ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom EU-a ili nacionalnim pravom kojim se propisuju odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika.[46]

Donošenjem i stupanjem na snagu Uredbe napravljen je pomak u području zaštite privatnosti korisnika interneta i društvenih mreža. Koliko je to bio potreban, pokazuje nam slučaj Cambridge Analytica. Britanska tvrtka Cambridge Analytica je 2014. pomoću aplikacije na društvenoj mreži Facebook putem psihološkog upitnika prikupila privatne podatke od 87 milijuna korisnika te ih upotrijebila u političke svrhe premda je na upitnik odgovorilo 270.000 osoba. „Cambridge Analytici je uspjelo prikupiti tako veliku količinu podataka jer je na temelju pristanka osobe koja bi popunila ponuđeni upitnik omogućen pristup osobnim podatcima svih njenih prijatelja unutar društvene mreže.“[47] To im je omogućilo da stvore bazu podataka koju je iskoristila kada je angažirana od strane tima koji je vodio izbornu kampanju za predsjednika Sjedinjenih Američki Država, Donalda Trumpa. Nakon što je slučaj otkriven, tvrtki Cambridge Analytica naloženo je da izbriše prikupljene podatke, ali analize koje su napravljene temeljim prikupljenih podatka već su korištene i vjerojatno se mogu i dalje koristiti u određene svrhe. Čelnik Facebooka Mark Zuckerberg bio je pozvan na svjedočenje pred Senatom Sjedinjenih Američkih Država, te je drugog dana svog svjedočenja izjavio: “Nisam tip osobe koja misli da regulacije ne bi trebalo biti, pogotovo zato što internet postaje sve važniji u životima ljudi diljem

[45] ibid.
[46] ibid.
[47] Cadwalladr C., Graham-Harrison E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Guardian. (17. Mar 2018) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, stranica posjećena 18.4.2020. i 30.04.2023.

svijeta…."[48]No, u nekim je ranijim vremenima upravo Mark Zuckerberg izjavljivao da je privatnost kao društvena norma izumrla. Koliko je stvar ozbiljna, potkrepljuje se i nekim sumnjama da je Cambridge Analytica sudjelovala u napetim izborima u Keniji 2017. godine za što postoje i dokazi. Kada pogledamo Poglavlje 2. i prisjetimo se stanja Zaštite privatnosti korisnika interneta u Africi, situacija ne samo da je ozbiljna već i opasna. Slučaj Cambridge Analytica završio je tako što je Facebooku u Velikoj Britaniji izrečena kazna od 500 000 funti, ali da je u tom trenutku bila na snazi Opća uredba o zaštiti podataka, Facebooku je ta kazna mogla biti i veća do 4% ukupnih godišnjih prihoda.[49] Nadalje, u Sjedinjenim Američkim Državama nakon podignute tužbe protiv Facebooka, on se 2019. godine nagodio i pristao platiti kaznu od 5 milijardi dolara, što je najveća kazna u povijesti.[50] Stupanjem na snagu Uredbe napravljeni su pomaci u zaštiti privatnosti korisnika koja je do sada bila nejasna, kao što je ne informiranje korisnika o njihovim pravima kada su u pitanju njihovi osobni podatci te zanemarivanje prava pojedinca prilikom dijeljenja njegovih privatnih podataka s trećom stranom. Nadalje, Uredba uređuje područje prijenosa podataka u treće zemlje koje nisu članice Europske unije; članak 44. Uredbe: „Svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju odvija se jedino ako voditelj obrade i izvršitelj obrade djeluju u skladu s propisanim uvjetima iz Uredbe."[51] Dakle, osobni podatci korisnika se ne mogu iznijeti i obrađivati ni u koje svrhe izvan granica Europske unije ako ta država ili tvrtka ne djeluje s odredbama koje proizlaze iz Uredbe. Uz mnoge pozitivne pomake spram zaštite privatnosti Uredba donosi i određene nejasnoće u odnosu s drugim regulatornim propisima koji uređuju područje privatnosti u elektroničkim komunikacijama, što ćemo obrađivati dalje u radu.

[48] House of Representatives, Committee on Energy and Commerce, FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DANA. D.C., str. 191., (Washington D.C. APRIL 11, 2018), dostupno na https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Transcript-20180411.pdf, stranica posjećena 12.6.2023.

[49] Lomas N., Cambridge Analytica's parent pleads guilty to breaking UK data law, TechCrunch, (January 9, 2019), dostupno na https://techcrunch.com/2019/01/09/cambridge-analyticas-parent-pleads-guilty-to-breaking-uk-data-law/, stranica posjećena 17.6.2023

[50] UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA, Case No. 19-cv-2184; COMPLAINT FOR CIVIL PENALTIES, INJUNCTION, AND OTHER RELIEF. UNITED STATES OF AMERICA v. FACEBOOK, Inc., (Washington D.C. July 24, 2019), dostupno na https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf, stranica posjećena 25.5.2023.

[51] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka),SL L 119/1, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, stranica posjećena 11.2.2023.

3.5. Zakon o provedbi Opće uredbe o zaštiti podataka

Opća uredba o zaštiti podataka u cijelosti je obvezujuća i izravno se primjenjuje u Republici Hrvatskoj od 25. svibnja 2018. godine. Uredbom se predviđaju specifikacije ili ograničenja njezinih pravila pravom države članice, te države članice mogu, u mjeri u kojoj je to potrebno radi usklađenosti i kako bi nacionalne odredbe bile razumljive osobama na koje se primjenjuju, elemente Uredbe uključiti u svoje nacionalno pravo. „Tako je Opća uredba, sukladno njenom članku 8., stavku 1. dozvolila državama članicama da zakonom predvide najnižu dobnu granicu djeteta radi davanja privole u pogledu nuđenja usluga informacijskog društva izravno djetetu.“[52] Republika Hrvatska je sukladno mogućnostima koje joj dozvoljava Opća uredba donijela Zakon o provedbi Opće uredbe o zaštiti podataka koji je stupio na snagu 25. svibnja 2018., te pojedinim člancima dodatno uredila određena područja Uredbe, a u svrhu dodatne zaštite privatnosti.

Zakon o provedbi Opće uredbe o zaštiti podataka propisuje dobnu granicu davanja privole djeteta u odnosu na usluge informacijskog društva u Republici Hrvatskoj.[53] Dalje: članak 19,

„Kod primjene članka 6. stavka 1. točke (a) Opće uredbe o zaštiti podataka, u vezi s nuđenjem usluga informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina.

Odredba stavka 1. ovoga članka primjenjuje se na dijete čije je prebivalište u Republici Hrvatskoj.

Postupanje suprotno odredbama ovoga članka smatra se kršenjem članka 8. Opće uredbe o zaštiti podataka i podliježe sankcioniranju sukladno članku 83. Opće Uredbe o zaštiti podataka.“[54]

Donošenje Opće uredbe i Zakona o provedbi Opće uredbe unaprijedilo je zaštitu osobnih podataka kod svih korisnika pa tako i kod najosjetljivijih skupina – djece i maloljetnika.

[52] Mišljenja Agencije za zaštitu osobnih podataka, Obrada osobnih podataka učenika sukladno Općoj uredbi. dostupno na https://azop.hr/obrada-osobnih-podataka-u-odgojno-obrazovnom-sektoru/, stranica posjećena 12.1.2023.

[53] Zakon o provedbi opće uredbe o zaštiti podataka, NN br. 42/18

[54] ibid.

3.6. Zakon o elektroničkim komunikacijama

Zakonom o elektroničkim komunikacijama (dalje: ZEK) glavom 4. propisuje se zaštita podataka i sigurnost elektroničkih komunikacija, članak 41. ZEK-a nalaže što operatori javnih komunikacijskih usluga moraju poduzeti kako bi se ostvarila sigurnost i cjelovitost elektroničko-komunikacijske mreže, a samim time i sigurnost korisnika i njihovih privatnih podataka.[55] Članak 42. nalaže što su operatori dužni učiniti ukoliko dođe do povreda osobnih podataka korisnika u elektroničkim komunikacijama, te stavak 1. članka 42. „U slučaju povrede osobnih podataka operator javno dostupnih elektroničkih komunikacijskih usluga mora bez odgode obavijestiti tijelo nadležno za zaštitu osobnih podataka o nastaloj povredi, u skladu s propisima o zaštiti osobnih podataka. Ako je vjerojatno da će nastala povreda osobnih podataka štetno utjecati na osobne podatke ili privatnost korisnika ili druge fizičke osobe, operator javno dostupnih elektroničkih komunikacijskih usluga mora o nastaloj povredi bez odgode obavijestiti i korisnika ili drugu fizičku osobu.“[56] Do sada je jedan operator javno dostupnih elektroničkih komunikacijskih usluga obavijestio nadležna tijela o povredi članka 42. ZEK-a. Nadalje, članak 43., stavak 1., ZEK-a propisuje da je u svrhu osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama, zabranjeno slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 52. ovoga Zakona te u slučajevima utvrđenima posebnim zakonima. Stavak 4. članka 43. ZEK-a nalaže da je korištenje elektroničko-komunikacijskih mreža za pohranu podataka ili za pristup već pohranjenim podatcima u terminalnoj opremi pretplatnika ili korisnika usluga dopušteno samo u slučaju kada je taj pretplatnik ili korisnik usluga dao svoju privolu, nakon što je dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade podataka. Time se ne može spriječiti tehnička pohrana podataka ili pristup podatcima isključivo u svrhu obavljanja prijenosa komunikacija putem elektroničke komunikacijske mreže, ili, ako je to nužno, radi pružanja usluga informacijskog društva na izričit zahtjev pretplatnika ili korisnika usluga.[57]

ZEK-om je propisana i obveza zadržavanja podataka te se člankom 53. ZEK-a nalaže da su operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga obvezni zadržati podatke o elektroničkim komunikacijama u svrhu omogućivanja

[55] Zakona o elektroničkim komunikacijama, NN br. 76/08
[56] ibid.
[57] ibid.

provedbe istrage, otkrivanja i kaznenog progona kaznenih djela u skladu s posebnim zakonom iz područja kaznenog postupka te u svrhu zaštite obrane i nacionalne sigurnosti u skladu s posebnim zakonima iz područja obrane i nacionalne sigurnosti. Podatci koji se zadržavaju definirani su člankom 54. ZEK-a i oni obuhvaćaju sljedeće:

- „podatke potrebne za praćenje i utvrđivanje izvora komunikacije,
- podatke potrebne za utvrđivanje odredišta komunikacije,
- podatke potrebne za utvrđivanje nadnevka, vremena i trajanja komunikacije,
- podatke potrebne za utvrđivanje vrste komunikacije,
- podatke potrebne za utvrđivanje korisničke komunikacijske opreme ili opreme koja se smatra korisničkom komunikacijskom opremom, podatke potrebne za utvrđivanje lokacije pokretne komunikacijske opreme.“[58]

Analizom ZEK-a od članka 42. do članka 54. možemo utvrditi da je područje privatnosti i sigurnosti korisnika elektroničko-komunikacijskih usluga kvalitetno uređeno, ako su u pitanju tradicionalne elektroničko-komunikacijske SMS poruke i telefonski razgovori. No ako promatramo iz perspektive nadolaženja novih usluga OTT-usluga utemeljenih na internetskoj platformi koje zamjenjuju tradicionalne usluge, situacija nije više tako bezazlena.
Nadalje, Članak 50. ZEK-a uređuje područje neželjene elektroničke pošte drugog naziva SPAM. Pod SPAM-om obično podrazumijevamo poruke promotivnog karaktera kad nepoznati pošiljatelj nudi svoje usluge primatelju elektroničke pošte. Nažalost, velik broj takvih poruka nije samo problem zatrpavanja primateljeva sandučića neželjenom poštom, nego je i potencijalna opasnost jer poruka može biti zaražena računalnim virusom ili nekim drugim malicioznim kodom te može ugroziti sigurnost podataka na primateljevu računalu, a samim time i privatnost istoga. Stavkom 1. članka 50. propisuje da je „…uporaba automatskih pozivnih i komunikacijskih sustava bez ljudskog posredovanja, telefaks uređaja ili elektroničke pošte, uključujući SMS poruke i MMS poruke, u svrhu izravne promidžbe i prodaje dopuštena samo uz prethodno pribavljenu privolu pretplatnika ili korisnika usluga.“[59] Stavak 2. propisuje da „…fizička ili pravna osoba može upotrebljavati podatke o adresama elektroničke pošte koje je pribavila od svojih potrošača u svrhu prodaje proizvoda i usluga za izravnu promidžbu i prodaju isključivo vlastitih sličnih proizvoda ili usluga, uz uvjet da ti potrošači imaju jasnu i nedvojbenu mogućnost besplatnog i jednostavnog prigovora na takvu uporabu podataka o adresama

[58] ibid.
[59] ibid.

elektroničke pošte prigodom njihova prikupljanja i prigodom zaprimanja svake elektroničke poruke, u slučaju da potrošač nije unaprijed odbio takvu uporabu podataka.“[60]

Zakonska odredba propisana člankom 50., ZEK-a postaje djelotvoran stupanjem na snagu Opće uredbe, do stupanja na snagu Opće uredbe pošiljatelj SPAM-a jednostavno je mogao doći do elektroničkih adresa tvrtki jer su one javne te od istih lako stvoriti bazu podataka i koristiti ih, ali ne slati velike količine elektroničke pošte od jednom, pa ga sustav jednostavno ne bi prepoznao i tretirao kao nekog tko krši zakon. Stupanjem na snagu Opće uredbe korisniku se ne smije slati elektronička pošta ukoliko isti nije dao svoj pristanak. Kada su u pitanju osobni podatci fizičkih osoba, zakon je bio rigorozan i prije stupanja na snagu Opće uredbe. Privatne podatke fizički osoba nije se smjelo obrađivati bez njihovog pristanka, te im se ni u kom slučaju nije smjela slati elektronička poštu ako oni na to nisu pristali. Ali ako uključimo uslugu društvene mreže, od kojih samo Facebook ima više od 2 milijarde korisnika, situacija se znatno mijenja. Društvene mreže dijele podatke o adresi elektroničke pošte s trećom stranom premda ih vrlo malo otkriva tu praksu, podatke uglavnom dijele unutar korporacije s raznim podružnicama koje navode u svojim registracijskim obrascima. Da će dijeliti podatke s trećom stranom najčešće navode u svojim uvjetima i pravilima korištenja, a poznato je da se uvjeti korištenja gotovo i ne čitaju od strane korisnika. Nadalje, ne samo da često nisu jasno ispunjene zakonske norme već se podatci često podijele s kompanijama koje se ne nalaze u registracijskim obrascima. Upravo temu dijeljenja podatka privatnih korisnika od strane društvenih mreža istraživanja su proveli Karel Kubíček, Jakob Merane, i drugi radu navode sljedeće: „Tijekom četrnaest mjeseci našeg istraživanja primijetili smo da je jedna od naših adresa e-pošte primila e-poštu s devet različitih domena. Neke od ovih domena nisu bile navedene u obrascu za registraciju.“[61] Dakle, što se tiče članka 50. ZEK-a, i nakon stupanja na snagu Opće uredbe, situacija se nije znatno promijenila kada su u pitanju osobni podatci privatnih korisnika. Isto se odnosi i na čanak 43. stavak 1 ZEK-a ako uzmemo u obzir internetske usluge koje zamjenjuju tradicionalne poput Facebook Messengera i drugih OTT-usluga. Na temu prisluškuje li nas Facebook Messenger putem mikrofona u marketinške svrhe istraživanje su proveli Zerina Tulek i Louise Arnell 2019. godine za potrebe magistarskog rada, a dobiveni rezultati nisu ukazivali na to da nas Facebook prisluškuje. „No usmjereni oglasi koji su se pojavili u aplikaciji Messenger ukazivali su na to da je Facebook mogao analizirati osobne poruke i prilagoditi

[60] ibid.

[61] Kubiček K., Merane J., Cotrini C., Stremitzer A., Bechtold S., Basin D., Checking Websites' GDPR Consent Compliance for Marketing Emails, str.3., Proceedings on Privacy Enhancing Technologies 2022 (Sydney, July 2022)

oglase prema sadržaju."[62] U pravilima o uporabi podataka stoji sljedeće: „Prikupljamo sadržaj, komunikaciju i druge podatke koje unosite prilikom upotrebe naših proizvoda, uključujući one koje unesete kada se registrirate za korisnički račun, kreirate ili dijelite sadržaj te kada šaljete poruke ili komunicirate s drugima. To može uključivati informacije u sadržaju koji pružate ili povezane s njim (poput metapodataka), kao što je lokacija fotografije ili datum izrade dokumenta. Također može uključivati ono što vidite putem značajki koje pružamo (poput naše kamere)…"[63] „Prikupljamo podatke o osobama, stranicama, korisničkim računima i grupama s kojima ste povezani te o načinu interakcije s njima u svim našim proizvodima. To su npr. osobe s kojima najviše komunicirate ili grupe čiji ste član. Također prikupljamo podatke za kontakt ako ih odlučite prenijeti, sinkronizirati ili uvesti s uređaja (iz adresara, popisa poziva ili povijesti popisa SMS poruka)…"[64] „Također pristali ste i na sljedeće: Ako se promijeni vlasništvo ili nadzor nad svim ili dijelom naših proizvoda ili njihovih značajki, vaše podatke možemo prenijeti na novog vlasnika."[65] Dakle, pristankom na uvjete korištenja pristali ste na prikupljanje i obradu gotovo svih privatnih podataka koji se ne smiju prikupljati temeljem ZEK-a u tradicionalnim komunikacijskim uslugama, davatelj usluge može prodati jedan dio poslovanja i baze podataka milijardu korisnika bez ikakve kontrole, a zakoni su nemoćni.

3.7. Zakonodavstvo Europske Unije

Kada je u pitanju Europsko zakonodavstvo, ono je utemeljeno na Općoj uredbi o zaštiti osobnih podataka i nekoliko direktiva koje su implementirane u zakone zemalja članica pa tako i u zakonodavstvo Republike Hrvatske, a to su:

- Opća uredba o zaštiti osobnih podataka (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 i o stavljanju izvan snage Direktive 95/46 / EZ na snazi je od 25. 5. 2018.[66]

[62] Tulek Z., Arnell L., Facebook Eavesdropping Through the Microphone for Marketing Purpose, str.3. BTH Blekinge Institute of Technology, Karlskrona, Sweden, (Karlskrona, May 2019), dostupno na https://www.diva-portal.org/smash/get/diva2:1332194/FULLTEXT0,1.pdf, stranica posjećena 12.2.2023.
[63] Data usage rules, Facebook Ireland Limited. https://www.facebook.com/about/privacy/update, stranica posjećena 17.6.2022.
[64] ibid.
[65] ibid.
[66] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka),SL L 119/1, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, stranica posjećena 11.2.2023.

- DIREKTIVA 2002/58/EC EUROPSKOGA PARLAMENTA I VIJEĆA *od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti na području* elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama).[67]
- Direktiva 2006/24/EC EUROPSKOGA PARLAMENTA I VIJEĆA od ožujka 2006.[68] (izvan snage, ali ima utjecaj na zakonodavstvo članica EU-a).

Cilj Opće uredbe o zaštiti osobnih podataka je pružiti bolju kontrolu građanima nad njihovim osobnim podatcima i stvoriti, u digitalno doba, visoku i ujednačenu razinu zaštite podataka u EU.[69] Opća uredba je već prethodno analizirana u poglavlju 3.4., ali zbog mogućeg utjecaja na Direktivu 2002/58/EC, potrebno je ponoviti najznačajnija nova pravila u području zaštite osobnih podataka:

- pravo na brisanje / pravo na zaborav
- jasan pristanak na obradu osobnih podataka od strane ispitane osobe
- pravo na prijenos podataka drugom voditelju obrade
- obavještavanje ispitanika o povredi osobnih podataka
- osiguranje da su pravila o privatnosti objašnjena jasnim i razumljivim jezikom
- snažnija provedba odredbi i novčane kazne do 4% ukupnog godišnjeg prometa na svjetskoj razini tvrtkama ako prekrše pravila.[70]

Direktiva 2002/58/EC o privatnosti i elektroničkim komunikacijama je Direktiva EU o zaštiti podataka i privatnosti u digitalnom dobu.[71] Direktiva se bavi regulacijom niza važnih pitanja kao što su povjerljivost informacija, obrada prometnih podataka, neželjena pošta (engl. *SPAM)* i kolačići (engl. *cookies)*. Direktiva 2002/58/EC izmijenjena je i dopunjena Direktivom 2009/136/EC.[72] Najznačajnija izmjena koju je donijela ta promjena je izmijenjeni članak 5. stavak 3. „Države članice osiguravaju da uporaba elektroničkih komunikacijskih mreža za

[67] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća, (12. srpnja 2002), dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058, stranica posjećena 17.1.2023.
[68] Direktiva 2006/24/EZ Europskog parlamenta i Vijeća (15. ožujka 2006). dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024, stranica posjećena 10.8.2023.
[69] Europski parlament. Priopćenje za tisak - Reforma zaštite podataka - EP odobrio nova pravila. (14. ožujka 2016). dostupno na http://www.europarl.europa.eu/news/hr/news-room/20160407IPR21776/reforma-za%C5%A1tite-podataka-ep-odobrio-nova-pravila, stranica posjećena 12.1.2023.
[70] ibid.
[71] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća, (12. srpnja 2002), dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058, stranica posjećena 17.1.2023.
[72] Direktiva 2009/136/EZ Europskog parlamenta i Vijeća. (25. studenoga 2009). dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32009L0136, stranica posjećena 17.1.2023.

pohranu informacija ili za pristup informacijama pohranjenima u terminalnoj opremi pretplatnika ili korisnika bude dopuštena samo pod uvjetom da se pretplatniku ili korisniku pruže jasne i sveobuhvatne informacije u skladu s Direktivom 95/46/EZ, između ostalog, o svrsi obrade te ako mu nadzornik podataka ponudi pravo da odbije takvu obradu. Navedeno ne zabranjuje tehničko pohranjivanje ili pristup isključivo u svrhu provođenja ili olakšavanja prijenosa komunikacija preko elektroničke komunikacijske mreže ili ako je strogo nužno kako bi se pružila neka usluga informacijskog društva koju je pretplatnik ili korisnik izričito zatražio."[73] S obzirom da je Općom uredbom o zaštiti osobnih podataka Direktiva 95/46/EZ, stavljena izvan snage, postavlja se pitanje kakvo će biti međudjelovanje Uredbe s Direktivom 2002/58/EC jer Direktiva 95/46/EC koja je zamijenjena Uredbom direktno se primjenjuje u području elektroničkih komunikacija. Europska komisija provela je javnu raspravu o trenutnom tekstu Direktive 2002/58/EC kao i mogućim promjenama u postojećem pravnom okviru.[74] Izvještaj s provedene javne rasprave promatran detaljno pet određenih tema, pružajući dokaze o tome kako su implementirane i kako se provode u praksi, što ukazuje na nedostatke i na moguće promjene te istražuje kako je Direktiva usklađena s Uredbom analizirali su Elizabeta Upton i Francis Aldhouse, a promatralo se sljedeće:

- opseg primjene direktive
- tajnost komunikacije
- kolačići, špijunski i drugi softveri
- podatci o prometu i lokaciji
- neželjeni izravni marketing.

Nakon provedene analize Upton i Aldhouse zaključuju da se nešto mora učiniti s Direktivom 2002/58/EC, te je potrebno provesti izmjene i urediti područje vezano uz privatnost korisnika. Problemi se mogu uvidjeti u svih pet promatranih područja, a jedan od bitnijih je opseg primjene direktive. Naime, trenutna regulativa ne obuhvaća OTT-usluge jer Direktivom su obuhvaćene elektroničke komunikacijske usluge što OTT-usluge nisu. Nadalje, predlažu da treba razmisliti

[73] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća, (12. srpnja 2002), dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058, stranica posjećena 17.1.2023.
[74] European Commission. Public consultation evaluation and review ePrivacy directive. dostupno na https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive, stranica posjećena 17.1.2017.

o uvođenju Uredbe umjesto direktive jer zbog različitog načina implementacije Direktive u zakone država članica nastaju nejasnoće, što često dovodi do različitih učinaka iste.[75]

A upravo na tragu predloženog Europski parlament i Vijeće su 10. siječnja 2017. objavili prvi nacrt Uredbe o e-privatnosti, dok konačan tekst uredbe još nije usvojen. Uredbom o e-privatnosti će se detaljno regulirati pitanja u vezi s obradom osobnih podataka u javnim imenicima, pitanja digitalnog marketinga te će se postaviti stroža pravila o obradi osobnih podataka. Ključne su točke Komisijinog prijedloga Uredbe o e-privatnosti sljedeće:

- **„Novi igrači**: pravila o privatnosti ubuduće će se primjenjivati i na nove igrače koji pružaju elektroničke komunikacijske usluge kao što su WhatsApp, Facebook Messenger i Skype. To će osigurati da ove popularne usluge garantiraju istu razinu povjerljivosti komunikacija kao i tradicionalni telekomunikacijski operatori.“[76]

- **„Stroža pravila**: svi ljudi i tvrtke u Europskoj uniji putem ove izravno primjenjive uredbe uživat će istu razinu zaštite svojih elektroničkih komunikacija. Tvrtke će dodatno imati koristi od jedinstvenog skupa pravila u cijeloj Europskoj uniji.“[77]

- **„Sadržaj i metapodatci komunikacije**: zajamčena je privatnost komunikacijskog sadržaja i metapodataka. Metapodatci imaju visoku komponentu privatnosti i trebaju se anonimno obrisati ili izbrisati ako korisnici nisu dali svoj pristanak, osim ako su podatci potrebni za naplatu.“[78]

- **„Nove poslovne mogućnosti**: jednom kad se daju suglasnosti za obradu podataka komunikacije – sadržaja i/ili metapodataka – tradicionalni telekomunikacijski operatori imat će više prilika za pružanje dodatnih usluga i razvoj svog poslovanja. Na primjer, mogli bi izraditi toplotne karte koje ukazuju na prisustvo pojedinaca; oni bi mogli

[75] Upton E., The future of the e-privacy directive: now is the time to have your say. (April 2016), dostupno na https://www.twobirds.com/en/insights/2016/uk/the-future-of-the-e-privacy-directive, stranica posjećena 17.1.2023.
[76] European Commission. Proposal for an ePrivacy Regulation. dostupno na https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, stranica posjećena 5.2.2023.
[77] ibid.
[78] ibid.

pomoći javnim vlastima i prijevozničkim kompanijama pri razvoju novih infrastrukturnih projekata.“[79]

- **„Jednostavnija pravila o kolačićima**: odredba o kolačićima, koja je rezultirala preopterećenjem zahtjeva za pristankom za korisnike interneta, pojednostavit će se. Novo će pravilo biti jednostavnije jer će postavke preglednika pružiti jednostavan način prihvaćanja ili odbijanja praćenja kolačića i drugih identifikatora. Prijedlog također pojašnjava da nisu potrebne suglasnosti za nametljive kolačiće koji ne uključuju privatnost i koji poboljšavaju internetsko iskustvo (npr. za pamćenje povijesti košarice) ili kolačiće koje web-stranica koristi za brojanje broja posjetitelja.“[80]

- **„Zaštita od neželjene pošte**: ovaj prijedlog zabranjuje neželjenu elektroničku komunikaciju putem e-pošte, SMS-a i automatiziranih poziva. Ovisno o nacionalnom zakonodavstvu, ljudi će biti zaštićeni zadanim postavkama ili će moći koristiti popis za nepozivanje da ne primaju marketinške telefonske pozive. Marketinški pozivači morat će prikazati svoj telefonski broj ili upotrebljavati poseban predbroj koji ukazuju na marketinški poziv.“[81]

- **„Učinkovitija primjena**: nacionalna tijela koja su nadležna za provedbu Opće uredbe o zaštiti podataka bit će nadležna i za provedbu Uredbe o e-privatnosti.“[82]

Prema Direktivi 2006/24/EC EUROPSKOGA PARLAMENTA I VIJEĆA države članice morale su pohraniti telekomunikacijske podatke građana najmanje 6 mjeseci, a najviše 24 mjeseca.[83] Direktiva je implementirana u zakone Republike Hrvatske i zakone drugih članica Europske unije, ali je presudom C-293/12 i C-594/12 suda Europske unije proglašena nevaljanom zbog nedostatnog reguliranja načina i zaštite podataka te povrede načela proporcionalnosti.[84] Potrebno je naglasiti da presuda ne obvezuje članice Europske unije da

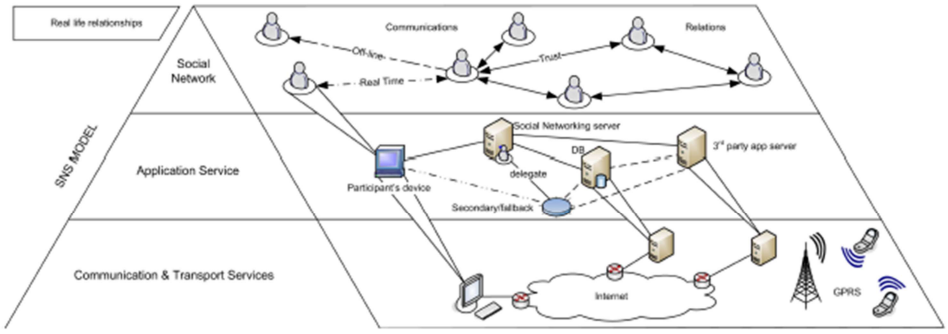
[79] ibid.
[80] ibid.
[81] ibid.
[82] ibid.
[83] Direktiva 2006/24/EZ Europskog parlamenta i Vijeća (15. ožujka 2006). dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024, stranica posjećena, stranica posjećena 10.11.2016.
[84] European Court of Justice. JUDGMENT OF THE COURT (Grand Chamber). In Joined Cases C-293/12 and C-594/12, (8 April 2014), dostupno na https://curia.europa.eu/juris/document/document.jsf?mode=lst&pageIndex=0&docid=150642&part=1&doclang=EN&text=&dir=&occ=first&cid=10349858, stranica posjećena 5.2.2023.

mijenjaju zakone koji su izmijenjeni temeljem Direktive. Tako su mnoge članice Europske unije zadržale odredbe koju su implementirale u svoje zakonodavstvo, a među njima je i Republika Hrvatska. Zadržavanje podataka svih građana najmanje 6 mjeseci, u slučaju Republike Hrvatske 12 mjeseci, što otvara mogućnost zlouporabe istih obzirom na nedostatke trenutnog regulatornog okvira.

4. DRUŠTVENE MREŽE

4.1. Društvene mreže i umrežavanje

Društvene mreže su besplatne usluge utemeljene na internetskoj platformi, a sve što je potrebno kako bi ih korisnici koristili jest registrirati se i dozvoliti u manjoj ili većoj mjeri pristup osobnim podatcima korisnika. Dok samo značenje riječi društvo znači „skup pojedinaca ili skupina ljudi oblikovana suradnjom i komunikacijom, ali i različitostima i sukobima oko raspolaganja materijalnim i simboličkim dobrima, a na osnovi čega se izgrađuju zajednička pravila djelovanja, poduprta minimumom zajedničkih interesa i uvjerenja“.[85] Prema Lee Rainie i Barry Wellmand društvene mreže su omogućile *umreženi individualizam* koji predstavlja pomak naprijed za društvene zajednice te poništava ograničenja koja su uvjetovana povezivanjem uskog kruga ljudi utemeljenih na: geografskim, rodbinskim, nacionalnim, vjerskim i drugim pripadnostima. Rainie i Wellmand tvrde kako *umreženi individualizam* omogućen razvojem tehnologije te integracijom društvenih mreža, interneta i mobilnih telefona što nazivaju *trostruka revolucija*.[86] Upravo ono što tvrde Rainie i Wellmand možemo prepoznati kroz Cjeloviti model društvenih mreža na Slici 4.1.



Slika 4.1. *Cjeloviti model društvene mreže prema Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str.11., Eurecom, (Sophia Antipolis, October 2010)*

[85] Leksikografski zavod Miroslav Krleža, Hrvatska enciklopedija, mrežno izdanje, dostupno na http://www.enciklopedija.hr/natuknica.aspx?id=16328, stranica posjećena 4.12. 2022.
[86] Rainie L., Wellman B., Networked: The New Social Operating System. str. 20., Massachusetts Institute of Technology MIT, (Cambridge, 2012)

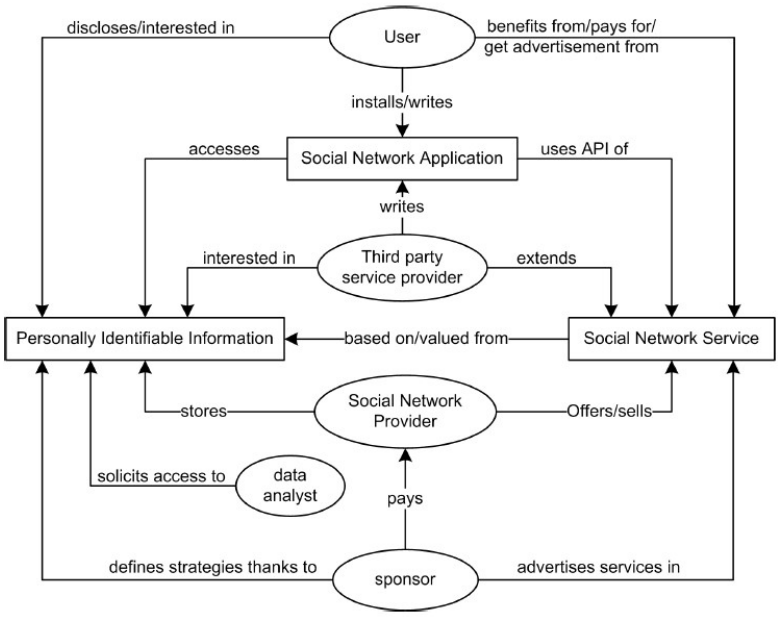
Cjeloviti model društvene mreže model sastoji se od triju razina:

- razina društvene mreže – taj sloj čine umreženi korisnici i njihove veze
- aplikacijska razina – razina koja omogućava korisnicima razmjenu podataka, pohranu podataka te upravlja raznim zahtjevima korisnika razine društvene mreže
- razina komunikacijske mreže – razina koja omogućava komunikaciju i prijenos podataka i usluga[87]

Nove tehnologije bile su podloga za razvoj i uzlet društvenih mreža koje su donijele društvu nove mogućnosti kako navode Rainie i Wellmand te utjecale na društvo u cjelini. Drugi razlog uzletu i utjecaju društvenih mreža na društvo možemo potražiti u definiciji društvenih mreža kako ih definiraju Danah M. Boyd i Nicole B. Ellison. „Društvene mreže su usluge koje su utemeljene na internetu, koje omogućuju pojedincima da osmisle vlastiti potpuno javan ili djelomično javan profil unutar zatvorenog povezanog kruga korisnika, unutar te mreže. Nadalje, omogućuje korisniku da odabere listu drugih korisnika s kojima se želi pokušati povezati i uglavnom omogućuje pregled korisnika koji su povezani s korisnicima s kojima je korisnik povezan unutar iste mreže. Ali ono što društvene mreže čini jedinstvenima nije da one omogućuju pojedincima da upoznaju strance, već da omogući korisnicima da kreiraju i učine vidljivom svoju društvenu mrežu unutar iste mreže, te tako dolazi do veza između pojedinaca koje se inače ne događaju, tj. korisnici pronalaze preko drugih korisnika poveznice i umrežavaju se te tako proširuju vlastitu mrežu.“[88] Definicija društvenih mreža prema Danah M. Boyd i Nicole B. Ellison podudara se s teorijom Rainiea i Wellmanda o utjecaju društvenih mreža na društvo cijelosti koje se mijenja. Premda se definicija Danah M. Boyd i Nicole B. Ellison odnosi samo na umrežavanje i usluge korisnika unutar vlastite mreže te izostavlja druge usluge koje korisnici mogu koristiti poput razmjene poruka, komentiranje objava na profilima korisnika društvene mreža a koji nisu dio korisnikove mreže.[89] Danah M. Boyd i Nicole B. Ellison također izostavljaju druge korisnike, „klijente“ društvenih mreža koji koriste društvene mreže u druge svrhe poput oglašavanja, ili korisnika koji proširuju sadržaj društvenih mreža dodatnim aplikacijama poput kvizova ili igrica, one se implementiraju na platforme društvene mreže, ali

[87] Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str. 8., Eurecom, (Sophia Antipolis, October 2010)
[88] Boyd D.M., Ellison N. B., Social Network Sites: Definition, History, and Scholarship. str. 211., Journal of Computer-Mediated Communication (October 2007), dostupno na https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1083-6101.2007.00393.x, stranica posjećena 3.11.2022.
[89] Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str. 3., Eurecom, (Sophia Antipolis, October 2010)

su pod nadzorom i upravljanjem treće strane.[90] Slika 4.2. prikazuje odnos davatelja usluge društvene mreže i odnos svih korisnika društvene mreže te njihove interese.



***Slika 4.2**. Odnos davatelja usluge društvene mreže i klijenata te njihovi interesi prema Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str. 4., Eurecom, (Sophia Antipolis, October 2010)*

Ako pažljivo promatramo Sliku 4.2., možemo primijetiti da postoji više klijenata društvenih mreža. Prvi su *sponzori* (engl. *sponsors*) koji plaćaju davateljima usluge društvenih mreža za oglašavanje proizvoda na istima, a koje kreiraju na temelju privatnih podataka korisnika. Drugi klijent je *treća strana* (engl. *party service providers*). Oni obogaćuju i proširuju funkcionalnost društvene mreže vlastitim aplikacijama, igricama, kvizovima i sličnim, a zauzvrat imaju pristup osobnim podatcima korisnika. Treći klijent su *analitičar podataka* (engl. *data analyst*), a to su klijenti koji plaćaju za privatne podatke korisnika te analiziraju njihove navike i ponašanja na društvenoj mreži u znanstvene, neznanstvene ili marketinške svrhe.[91]

Upravo zbog prethodno navedenih interesa korisnika i klijenata, a na temelju nove paradigme spram privatnosti gdje korisnici privatne podatke dijele gotovo bez razmišljanja, stvoreno je okružje u kojem privatni podatci naizgled svima donose koristi. Davatelji usluga društvenih mreža koriste privatne podatke korisnika u svrhu novih funkcionalnosti i povećanja kvalitete

[90] ibid. str.4
[91] ibid. str.4.

usluge društvenih mreža, ali za ostvarivanje financijske dobiti dozvoljavajući korisnicima klijentima pristup privatnim podatcima korisnika. Korisnici klijenti društvenih mreža plaćaju za privatne podatke korisnika ili obogaćuju sadržaj na društvenim mrežama u zamjenu za iste. Tako stvoreno okruženje gdje svi imaju korist omogućilo je da društvene mreže u samo 15 godina izađu iz zatvorenih akademskih krugova te postale su neizostavan čimbenik u svim društvenim zajednicama i na svim društvenim razinama. Društvene mreže se javljaju u nekoliko glavnih oblika:

- **„Osobne mreže** – ove društvene mreže omogućuju korisniku stvaranje detaljnog profila i povezivanje s ostalim korisnicima. Primjer ovakvih mreža su Facebook i MySpace. U svojem profilu korisnik objavljuje svoj spol, dob, interese, podatke o obrazovanju i zaposlenju, a može dodavati datoteke i poveznice na glazbu, slike i video. Korisnik može regulirati tko smije vidjeti podatke koje on objavljuje. Tako se pristup nekoj informaciji može dopustiti samo korisnikovim prijateljima ili članovima grupe u kojoj se korisnik nalazi. Ako postavke privatnosti nisu ispravno podešene, korisnikove informacije mogu pregledati i osobe za koje korisnik to ne bi želio.“[92]

- **„Statusne mreže** – kod ovog tipa društvene mreže korisnik na svom profilu objavljuje kratke obavijesti (statuse) i na taj način komunicira s ostalim korisnicima. Praćenjem profila drugih korisnika saznaju se informacije o tom korisniku. Primjer takvih mreža je Twitter. Statusi su javni (može ih pročitati bilo tko), osim ako društvena mreža ne dopušta regulaciju vidljivosti statusa i korisnik podesi da su statusi vidljivi samo određenim osobama (što je rijetko slučaj).“[93]

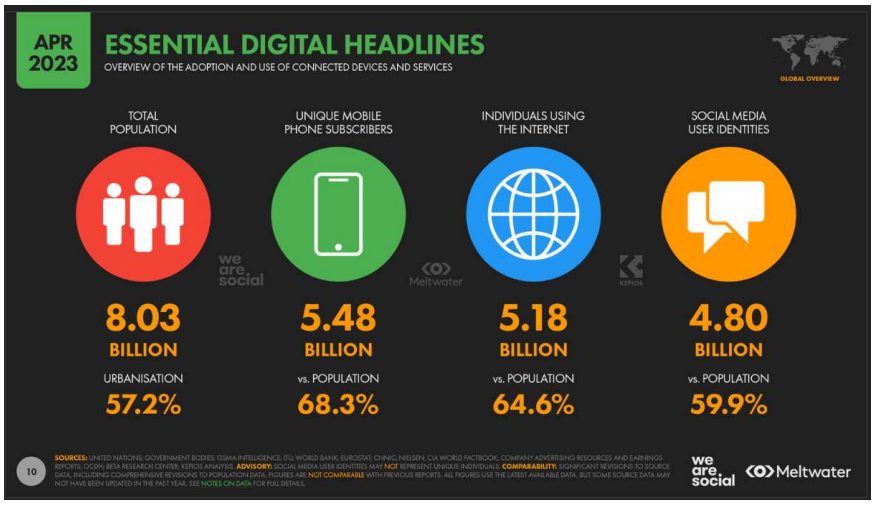
- **„Lokacijske mreže** – ove mreže postaju sve popularnije povećanjem broja mobilnih uređaja s ugrađenim GPS sustavom (engl. – *Global Positioning System*). One objavljuju u realnom vremenu korisnikov položaj ili javno ili samo odabranim korisnicima, ovisno o tome kako korisnik odabere postavke. Većina ovih mreža komunicira s ostalim društvenim mrežama i tako nadopunjava korisnikov profil na nekoj drugoj društvenoj mreži. Neke od ovih mreža su Google Latitude, Foursquare i Loopt.“[94]

[92] Labaratorij za sustave i signale, Informacijska sigurnost. Privatnost na Internetu. str. 12. (Jan 14, 2014), dostupno na https://www.scribd.com/doc/199491060/lss-pubdoc-2010-10-002, stranica posjećena 22.11.2022.
[93] ibid. str. 12.
[94] ibid. str. 12.

- **„Mreže za dijeljenje sadržaja** – glavna namjena ovih mreža je razmjena sadržaja poput glazbe, fotografija i videa. Prije pojave društvenih mreža postojali su servisi koji su se koristili za razmjenu sadržaja. Dodavanjem profila u te servise, oni su postali društvene mreže jer korisnici mogu komentirati sadržaje drugih korisnika i na taj način komunicirati i stvarati nove kontakte. Poznate mreže za dijeljenje sadržaja su YouTube, Picasa i Flickr.“[95]

- **„Mreže sa zajedničkim interesima** – ovo su društvene mreže koje su namijenjene specifičnoj skupini ljudi koji imaju nešto zajedničko. Primjeri ovih mreža su deviantART i LinkedIn.“[96]

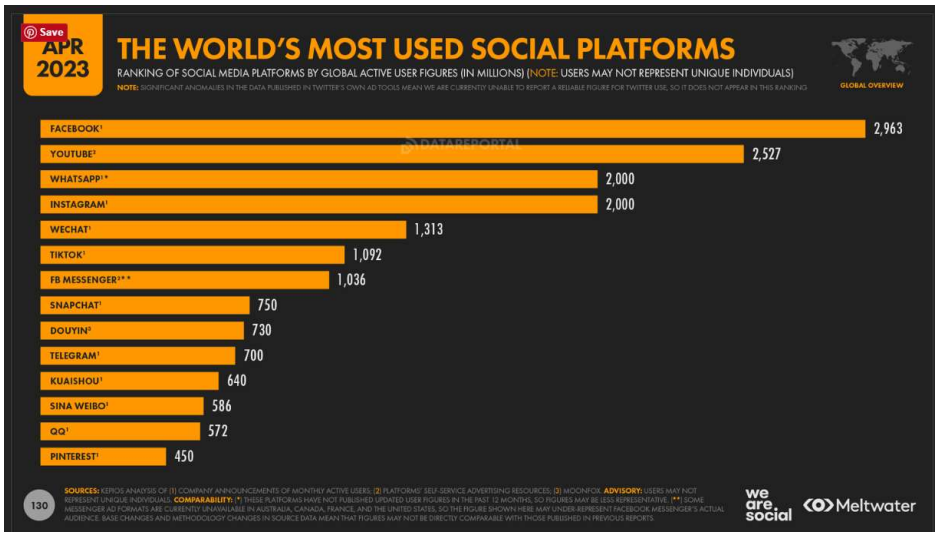
Trenutno u svijetu, po podatcima globalnog istraživanja „Digital In 2023“ koje je provela marketinška agencija We Are Social, koje je obuhvatilo 248 zemlje prikazuje stanje za travanj 2023. godine. Prema tim podatcima u svijetu 64.6% populacije koristi internet, a 59.9% je aktivno na društvenim mrežama.[97] Vidi Sliku 4.3.



Slika 4.3. *Broj korisnika interneta i društvenih mreža u svijetu prema: Digital Global Statshot Report, str. 10, dostupno na https://datareportal.com/reports/digital-2023-april-global-statshot*

[95] ibid. str. 12.
[96] ibid. str. 12.
[97] Digital Global Statshot Report, str.10. dostupno na https://datareportal.com/reports/digital-2023-april-global-statshot, stranica posjećena 10.7.2023.

Nadalje, prema podatcima iste marketinške agencije u svijetu je 2,96 milijardi korisnika društvene mreže Facebook, što je 36% ukupne svjetske populacije. Vidi Graf 4.1.



Graf 4.1. *Broj korisnika društvenih mreža u svijetu prema: Digital Global Statshot Report, str. 130, dostupno na https://datareportal.com/reports/digital-2023-april-global-statshot*

4.2. Dijeljenje podataka i odgovornost korisnika društvenih mreža

Razlozi za velik interes zaštite privatnosti na društvenim mrežama temelje se na činjenicama da je broj korisnika društvenih mreža u stalnom porastu te da sve veći broj korisnika svoje privatne podatke različitog stupnja povjerljivosti dobrovoljno dijeli putem društvenih mreža. Ali i u činjenicama da su privatni podatci korisnika predmet interesa samih davatelja usluga društvenih mreža i drugih korisnika platformi društvenih mreža koji ih žele iskoristiti u različite svrhe. U nastavku Slika 4.4. prikazuje koje podatke korisnici obično pohranjuju na društvenim mrežama, a mogu se podijeliti u pet kategorija:

1. Osobni kontakt-podatci
2. Povezanost
3. Interesi korisnika
4. Životopis korisnika
5. Komunikacija

Osobni kontakt-podatci opisuju tko je korisnik, uz osnovne podatke o korisniku kao što su ime, fotografija, spol, datum i mjesto rođenja te bračni status, generiraju se i drugi korisnički podatci: podatci o članstvu u raznim društvenim mrežama, fizička adresa, adresa elektroničke

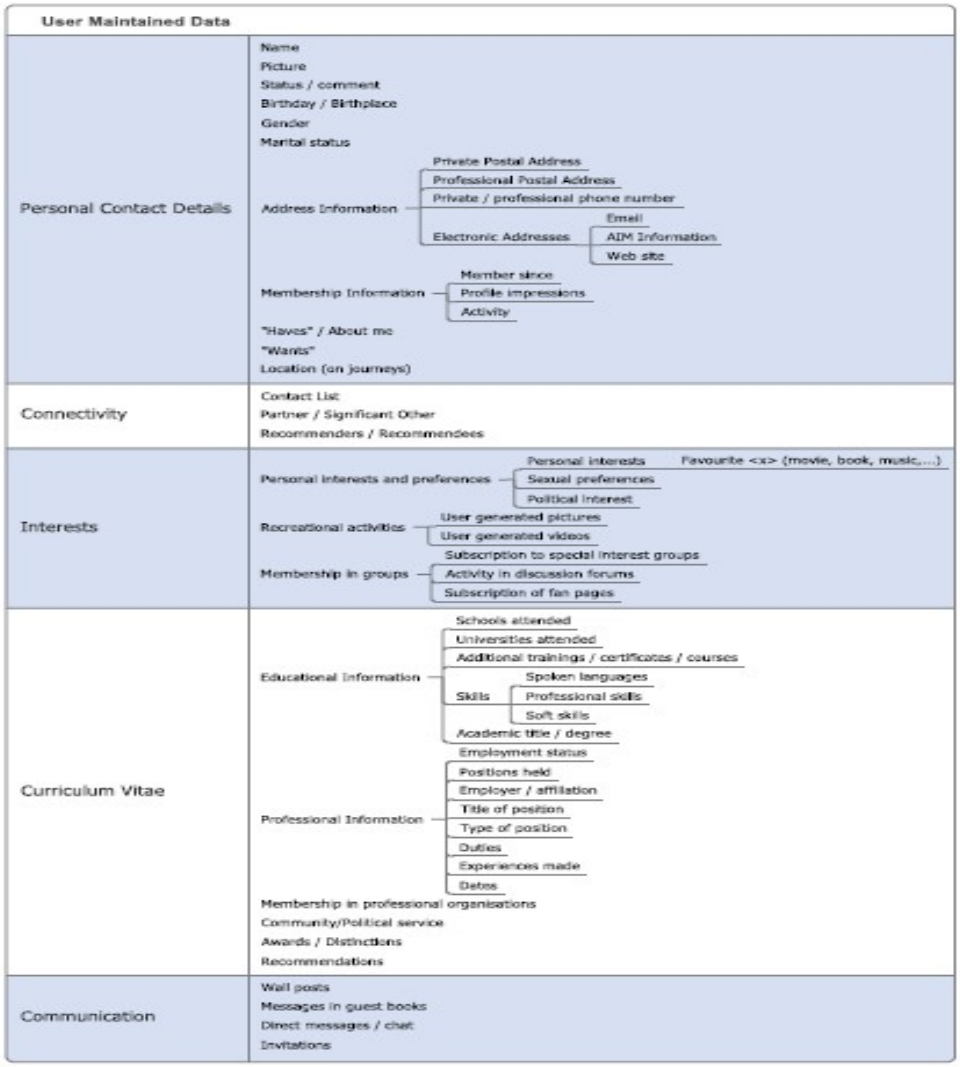
pošte, telefonski broj te podatci o osobnim web-stranicama. Nadalje, opisuju osobni profil korisnika te mogu sadržavati podatke o seksualnim, osobnim, političkim i vjerskim interesima i sklonostima korisnika.[98]

Povezivanje opisuje koga korisnik poznaje, prikazujući korisnikov popis kontakata te upućujući na njihovu prirodu odnosa (npr. obitelj, kolege, najbolji prijatelj, sportski partner). Neke društvene mreže često traže od korisnika i podatak da li je u vezi te posljedično ime i profil partnera. Drugi korisnici, ukoliko ih interesira, mogu od kontakata korisnika tražiti dodatne informacije koje mogu detaljno rasvijetliti prirodu odnosa između osoba koje su navedene kao partneri.[99]

Interesi opisuju što korisnika zanima i što mu se sviđa. Oni sadrže informacije o različitim interesima, hobijima i sklonostima korisnika. Konkretno, mogu sadržavati informacije koji su im omiljeni filmovi, koji stil glazbe slušaju te informacije o seksualnim, vjerskim i političkim stavovima korisnika. Nadalje, mogu sadržavati informacije o rekreacijskoj aktivnosti korisnika koje su prikazane kroz slike ili videozapise iz različitih situacija u života korisnika te informacije o njihovoj pretplati na stranice obožavatelja kao i o članstvu u posebnim interesnim grupama unutar društvene mreže.[100]

Životopis korisnika opisuje obrazovanje i profesionalnu karijeru korisnika, uključujući podatke o završenoj školi, završenom fakultetu i akademskoj tituli koju korisnik posjeduje, također može sadržavati podatke o raznim vještinama i znanjima korisnika poput profesionalnih vještina ili informaciju o tome koje strane jezike korisnik govori. Informacije o profesionalnoj karijeri mogu biti vrlo detaljne i uključivati opis trenutnog i prethodnih radnih mjesta, obično uključujući informacije o trajanju i opisu radnog mjesta (npr. zaposlen na puno radno vrijeme ili na određeni broj sati, slobodnjak, samozaposleni), dužnosti koje korisnik obavlja na trenutnom radnom mjestu te razina odgovornosti. Uz sve navedeno neke društvene mreže od korisnika zatraže da dostave podatke o članstvu u profesionalnim organizacijama u prošlosti i sadašnjosti te informacije o svojoj trenutnoj društvenoj i političkoj ulozi, informacije o članstvu i ulozi u raznim klubovima, udrugama, političkim strankama, stručnim društvima, dodijeljenim nagradama, priznanjima, preporukama i referencama.[101]

[98] Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str.8., Eurecom, (Sophia Antipolis, October 2010)
[99] ibid. str. 8.
[100] ibid. str. 9.
[101] ibid. str. 9.

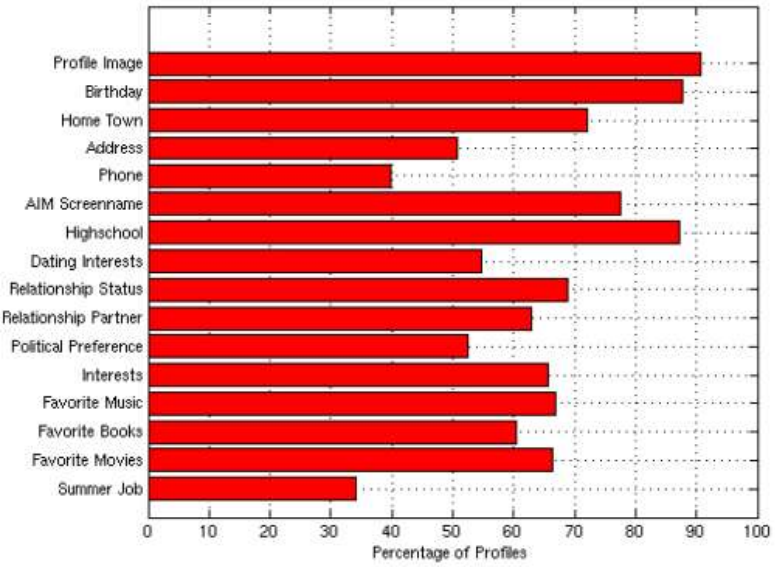


Slika 4.4. *Podatci koje korisnici generiraju na profilima društvenih mreža prema: Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str.8., Eurecom, (Sophia Antipolis, October 2010)*

Komunikacija opisuje koje je poruke korisnik razmijenio i s kim. Društvene mreže uglavnom nude razmjenu osobnih asinkronih poruka putem postova na zidovima profila i unosa u knjige gostiju. To je komunikacija koju vlasnik profila može sakriti ili otkriti drugim korisnicima. Uz njih postoji sinkrona razmjena poruka poput čavrljanja (engl. *chats*), a to su primjeri izravne komunikacije pokrenute od strane korisnika. Također na društvenim mrežama postoji mogućnost manje izravne komunikacije koja je omogućena putem aplikacija (npr. "bockanje", "testovi sličnosti", kvizovi), kao i ciljane ili javne pozivnice za organizirane događaje.[102]

[102] ibid. str. 10.

Kada detaljno pogledamo podatke koje korisnici pohranjuju na društvenim mrežama te se isti mogu detaljnije dopuniti informacijama koje drugi korisnici mogu prikupiti o korisniku od drugih korisnika, sasvim je opravdana zabrinutost za privatnost korisnika. Svi pohranjeni privatni podatci dostupni su davateljima usluga društvenih mreža, dok drugi korisnici imaju uvid ovisno o dopuštenju vlasnika profila. Ali stvarni problem se povećava jer korisnici samoinicijativno daju privatne podatke, a da pri tome jako malo ili gotovo uopće ne razmišljaju o posljedicama. Na tu temu je provedeno više istraživanja, a istraživanje koje su proveli znanstvenici Ralph Gross i Alessandro Acquisti 2005. godine ukazuje na to da 82% korisnika društvene mreže Facebook otkriva povjerljive podatke o sebi kao što su: ime i prezime, broj telefona, seksualna orijentacija, ime partnera.[103] Graf 4.2. prikazuje u kojem postotku korisnici društvenih mreže daju javno svoje privatne podatke.

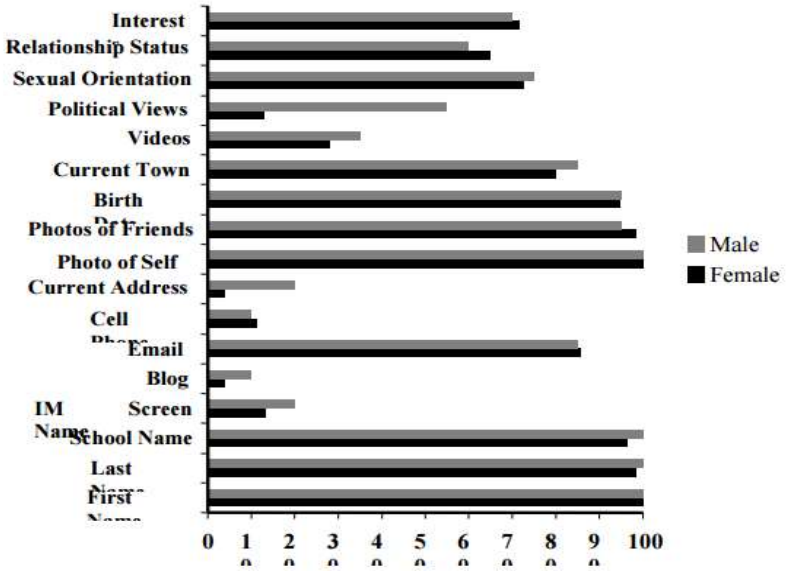


Graf 4.2. *Postotak korisnika društvenih mreža koji javno objavljuju privatne podatke prema* Gross R., *Acquisti A., Information Revelation and Privacy in Online Social Networks, str. 5., Workshop on Privacy in the Electronic Society, WPES 2005, (Alexandria, VA, USA, November 2005)*

Do sličnih podataka dolaze i Alyson L. Young Anabel Quan-Haase u svom istraživanju provedenom među studentima u Kanadi 2009. godine. Podatci pokazuju visoku razinu objavljenih privatnih podataka na društvenoj mreži Facebook pa tako 99,35 % studenata koristi

[103] Gross R., Acquisti A., Information Revelation and Privacy in Online Social Networks, str. 5., Workshop on Privacy in the Electronic Society, WPES 2005, (Alexandria, VA, USA, November 2005)

pravo ime i prezime u svom profilu, a gotovo dvije trećine ispitanika objavilo je svoju seksualnu orijentaciju, trenutni ljubavni status te informacije kao što su najbolja knjiga, najbolji film i fizičke aktivnosti kojima se bave. Dok je 97,4% ispitanika istaknulo ime ustanove koju pohađaju, 83,1 % objavilo je adresu e-pošte, 92,2% objavilo je datum rođenja, 80,5% objavilo je grad ili mjesto u kojem žive, a gotovo svi ispitanici objavili su vlastitu sliku – njih 98,7%, te je 96,1% objavilo sliku prijatelja. Za razliku od visokog postotka objave prethodno navedenih privatnih podataka, razmjerno je mali broj studenata otkrio svoju fizičku adresu i to 7,9% dok je broj mobilnog telefona objavilo 10,5 %. Dodatno zanimljiv podatak je da su muškarci i žene gotovo u istom postotku otkrili svoje privatne podatke na društvenim mrežama, a jedina razlika je u tome da žene više otkrivaju svoje političke stavove u odnosu na muškarce.[104]



Graf 4.3. *Postotak korisnika društvenih mreža koji javno objavljuju privatne podatke Alyson L. Young A.L., Quan-Haase A., Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. str. 5. Conference on Communities and Technologies, C&T 2009 (University Park, PA, USA, June 2009)*

Tako velika sloboda korisnika društvenih mreža u objavi osobnih podataka utemeljena je na novoj paradigmi spram privatnosti te potaknuta i od samih davatelja usluga koji ih uvjeravaju da su njihovi podatci u potpunosti sigurni. No, da situacija nije tako bezazlena, pokazuju mnoge situacije gdje je korisnicima društvenih mreža bila narušena privatnost. Nadalje, u nekim

[104] Alyson L. Young A.L., Quan-Haase A., Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. str. 5. Conference on Communities and Technologies, C&T 2009 (University Park, PA, USA, June 2009)

slučajevima privatnost korisnika bila je ugrožena od samih davatelja usluga društvenih mreža, a sumnju u iskrenost spram privatnosti produbljuje izjava osnivača društvene mreže Facebook, Marka Zuckerberga, „…kako je pojam privatnosti kao prihvatljiva društvena norma mrtav, privatnost kao socijalna norma više ne postoji.“ [105]Izrečena na predavanju održanom u San Franciscu povodom dodjele Crunchie nagrade 2010. Što je pa gotovo suprotno s pojmom privatnosti kako su je definirali Louis Brandeis i odvjetnik Samuel Warren 1890. godine u eseju *Pravo na privatnost* (vidi Poglavlje 2).

A upravo se prva od nekoliko velikih javnih rasprava na temu zlouporabe osobnih podataka korisnika od samih davatelja usluga veže uz društvenu mrežu Facebook. Povod je bilo uvođenje sustava za reklamiranje pod nazivom *Beacon. Beacon* je bila usluga podešena da prati i snima aktivnosti Facebookovih korisnika na internetu i zatim podatke prosljeđuje listi korisnika s profila te osobe. Ideja je bila da se pomoću prikupljenih informacija reklame što više personaliziraju. Ubrzo nakon pokretanja pojavio se problem jer je *Beacon* pratio aktivnosti korisnika i kada nisu bili aktivni na Facebooku te je snimao njihove aktivnosti bez njihova znanja. *Beacon* je pokrenut 6. studenoga 2007. godine i prikupljao podatke do 28. veljače 2008. godine.[106] *Beacon* je možda prvi javni primjer direktne povrede privatnosti korisnika društvenih mreža od samih davatelja usluga koji je ubrzo nakon pokretanja postao predmet tužbi te je ubrzo ugašen. Sljedeća javna rasprava koja se povela bila je najava Facebooka o izmjeni politike vezane uz privatnost podataka. Ono što je posebno pobudilo zanimanje javnosti bila je najava da će Facebook zadržavati prvo na korištenje osobnih podataka korisnika i kada korisnik više nije korisnik Facebook-ovih usluga. A najveća i najozbiljnija tužba spram Facebooka zbog politike privatnosti došla je od Kanadske udruge koja se bavi politikom interneta i javnim interesom (engl. – *Canadian Internet Policy and Public Interest Clinic* – CIPPIC), upućena Uredu povjerenika za privatnost informacija Kanade (engl. – *Office of the Privacy Commissioner* – OPC), iznijeli su optužbe na povredu privatnosti korisnika Facebooka u više slučajeva, od optužbi za neovlašteno prikupljanje podataka do neovlaštenog dijeljenja podataka s trećom stranom u svrhu marketinga. Kao odgovor na tužbe OPC je napravio više analiza tijekom 2009. godine te dao društvenoj mreži Facebook 20 smjernica za uklanjanje uočenih nepravilnosti vezanih uz politiku privatnosti. Kao rezultat tužbe i preporuka od OPC-a

[105] Johnson B., Privacy no longer a social norm, says Facebook founder, The Gurdian. (Jan 2010), dostupno na https://www.theguardian.com/technology/2010/jan/11/facebook-privacy, stranica posjećena 15.11.2016. i 3.5.2023

[106] Jamal, A., Coughlan, J., & Kamal, M. Mining social network data for personalisation and privacy concerns: a case study of Facebook's Beacon, str.180., International Journal of Business Information Systems, 13(2), 173-198. (2013)

Facebook je korigirao dio svoje politike privatnosti, ali veliki dio pritužbi kao što su brisanje profila preminulih osoba, dijeljenje podataka s trećim osobama, zadržavanje osobnih podataka osoba koji više nisu korisnici Facebooka do sada nije riješen.[107] Dalje se pojavljuje slučaj studenta iz Austrije Maximiliana Schremsa koji je, nakon što je Edward Snowden objavio tajne informacije programu „PRISM“, Nacionalne sigurnosne agencije (engl. – *National Security* Agency – NSA) podigao nekoliko tužbi protiv Facebook Ireland Ltd zbog povrede privatnosti. Jedna od tužbi bila je skupna tužba Facebooka zbog povrede privatnosti s više od 25 000 tisuća osoba koje su mu ustupile svoje zahtjeve u tužbi. Slučaj je završio na Europskom sudu pravde koji je ustvrdio da se ne može podignuti kolektivna tužba, ali svaki pojedinac može podignuti tužbu pred nadležnim sudom u zemlji iz koje dolazi.[108] Navedeni primjeri povrede privatnosti direktno su uzrokovani od strane davatelja usluga društvenih mreža, ali privatnost korisnika je ugrožena i od strane drugih korisnika, zlonamjernih napadača koji svoje napade provode putem platformi društvenih mreža. Napadi na privatnost mogu biti sljedeći:

- **Lažno predstavljanje** – prevara je u kojoj prevarant stvori lažni profil s imenom stvarne osobe, tako da stvarna osoba ima lažan profil unutar platforme društvene mrže. Budući da mnoge društvene mreže imaju tendenciju provjere autentičnosti adresa elektroničke pošte, tražeći povratnu potvrdu s navedene adrese elektroničke pošte, uspjeh ovog napada na privatnost ovisi o sustavu autentifikacije koja se koristi prilikom postupka registracije. No, napad se može lako izvesti ukoliko se adresa elektroničke pošte kreira unaprijed te napadač može pristupiti aplikacijama na društvenim mrežama i komunicirati s drugim korisnicima u ime osobe iz stvarnog svijeta, a sve štetne posljedice imaju utjecaj na osobu iz stvarnog svijeta u čije se ime napadač lažno predstavio. Ovakvi napadi mogu se spriječiti jedino implementacijom detaljnijih provjera autentifikacije. Na primjer, bilo bi poželjno zahtijevati od korisnika neki oblik identifikacije iz stvarnog savjeta prije uključivanja računa na društvenoj mreži.[109]

- **Kloniranje profila** – oblik je lažnog predstavljanja unutar platforme iste društvene mreže gdje stvarni korisnik ima aktivan profil. Napad se može izvesti registracijom novog profila koristeći iste parametre poput imena, prezimena, slike i dr., što je izvedivo

[107] The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), Facebook (2008-2010), dostupno na https://cippic.ca/en/Facebook, stranica posjećena 17.12.2022.
[108] Judgment of the Court (Third Chamber). In Case C-498/16, (25 January 2018) dosupno na https://curia.europa.eu/juris/liste.jsf?num=C-498/16&language=HR 242874, stranica posjećena 23.03.2023.
[109] Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks. str.16., Eurecom, (Sophia Antipolis, October 2010)

na većini društvenih mreža budući da se profil veže za adresu elektroničke pošte i jedinstveni ID. No, kako većina korisnika skriva adresu elektroničke pošte, napadač može lako zadobiti povjerenje drugih korisnika i pristupiti njihovim privatnim podatcima jer ga ne razlikuju od stvarne osobe. Danas se pomoću alata iCloner kloniranje profila korisnika društvenih mreža može automatizirati. Rješenje za sprečavanje kloniranja profila moglo bi se realizirati tako da davatelji usluga društvenih mreža implementiraju mehanizme koji mogu otkriti sličnosti između različitih profila te da temeljem podataka koji su im dostupni uklone klonove. Jedan od parametara temeljem kojeg bi se biralo koji profil je klon može biti i vrijeme registracije jer klonovi bi trebali imati noviji datum registracije.[110]

- **Otmica profila –** cilj je ovog napada preuzeti kontrolu nad korisnikom društvene mreže. Kako su pristupi korisničkom profilu najčešće štićeni putem lozinke, napad se može izvesti na više načina, a poznata je činjenica da je većina lozinki slabo kreirana te da većina korisnika upotrebljava istu lozinku za pristup na više mjesta. Kao zaštitu većina društvenih mreža koristi ograničenje broja pokušaja pristupa profilu te, ako je u pitanju ljuska interakcija, napadi će često biti spriječeni. Kada je u pitanju napad u kojem se koriste alati, sigurnosne postavke društvenih mreža lako se mogu zaobići ili napadač može na neki drugi način poput *phishinga* dobiti lozinku korisnika te preuzeti kontrolu nad profilom korisnika. Zaštita od otmice profila može se temeljiti na tome da društvene mreže koje imaju puni pristup svim podatcima korisnika predviđaju koji bi profili bili interesantni za otmicu te sukladno tome, ukoliko se ista dogodi, automatski izvrše promjenu lozinke.[111]
- **Prijenos profila** – cilj je ovog napada lažirati profil s platforme jedne društvene mreže u drugu te se lažno predstavljati. Naime, nemaju svi korisnici otvoren profil na svim društvenim mrežama. Napad je tehnički jednostavno izvediv jer se profil na nekoj od društvenih mreža može otvoriti s nove adrese elektroničke pošte, a svi drugi podatci prenesu se s društvene mreže na kojoj je otvoren stvarni profil te se napadač može lažno predstavljati i zadobiti povjerenje drugih korisnika. Sprečavanje ovog napada je dosta komplicirano, ali svakako bi se mogli upotrebljavati alati za otkrivanje sličnosti, no oni bi trebali biti instalirati na više društvenih mreža te imati uvid u bazu podataka. Suradnju među davateljima usluga društvenih mreža gotovo je nemoguće postići jer su svi oprezni

[110] ibid. str. 16.
[111] ibid. str. 17.

kada daju bilo kakav pristup vlastitoj bazi podataka, a pogotovo kada je u pitanju konkurencija.[112]

- **Krađa identiteta** – oblik je lažnog predstavljanja gdje napadač preuzima fotografiju i druge detalje iz života stvarnog korisnika te stvara novi profil toliko identičan stvarnom profilu, tako da može zavarati bilo koga od drugih korisnika, zadobiti njegovo povjerenje i zloupotrijebiti ga. Krađu identiteta je gotovo nemoguće tehničkim osujetiti programskim rješenjima jer kradljivac uz komunikaciju putem društvene mreže i drugim kanalima prikuplja podatke o stvarnoj sobi. Ukoliko postoji i mala sumnja o mogućoj krađi identiteta, od korisnika profila bi bilo poželjno zatražiti dodatnu potvrdu identiteta dokumentima iz stvarnog svijeta.[113]
- **Profiliranjem** – napad je na bilo kojeg korisnika društvenih mreža, a koji ima za cilj prikupljanje informacija o aktivnostima, navikama i karakteristikama tog korisnika. Davatelji usluga društvenih mreža korisnicima osim održavanja vlastitog profila omogućuju komunikaciju i izražavanje kroz razne aplikacije poput foruma, knjige gostiju, raznih anketa, rasprava, multimedijskog sadržaja itd. Pritom su sve te aktivnosti vidljive i drugim korisnicima unutar platforme društvene mreža. Budući da su sve aktivnosti uglavnom vidljive svim korisnicima društvenih mreža, napad jednostavno može izvesti drugi korisnik društvene mreže i često se izvodi pomoću alata na automatiziran način. Rizik od ovog napada može se smanjiti detaljnijom upotrebom kontrole pristupa i tehnikama anonimizacija. Na primjer, korisnici bi trebali omogućiti pristup određenim dijelovima profila na individualnoj osnovi, a ne da se pristup dobije samo temeljem prihvaćanja prijateljstva, što je dosta davatelja usluga društvenih mreža i omogućilo, no napadači i dalje mogu prikupiti dosta vrijednih informacija iz društvenih aktivnosti korisnika na mreži i javnih informacija o korisniku. Da bi se rizik dodatno umanjio, korisnicima bi trebalo omogućiti da sami odluče hoće li se njihove aktivnosti poput komentara u određenim raspravama direktno povezivati s njihovim profilom. Navedene mjere umanjile bi rizik profiliranja korisnika od strane drugih korisnika, ali umanjivanje i sprečavanje rizika profiliranja od strane društvenih mreža je nemoguće.[114]
- **Sekundarno prikupljanje podataka** – napad je na privatnost korisnika društvenih mreža, a cilj je prikupiti što više podataka o vlasniku profila kako putem platformi

[112] ibid. str. 17.
[113] ibid. str. 17.
[114] ibid. str. 18.

društvenih mreža tako i iz drugih izvora poput internetskih tražilica. Cilj napadača je prikupiti što više podataka o ciljanom korisniku te ih upotrijebiti protiv njega u virtualnom okruženju ili u stvarnom životu. Protiv sekundarnog prikupljanja podataka nema smislene zaštite jer se podatci prikupljaju s različitih platformi, društvenih mreža i drugih internetskih mjesta. U ovom slučaju najveća je odgovornost na korisniku koji bi trebao ograničiti količinu podataka koju pohranjuje na profilu društvene mreže, ali i paziti kome dozvoljava pristup istima kako bi izbjegao povezivanje sa sekundarnim izvorima.[115]

- **Lažni zahtjevi** – ovaj napad je smislen tako da napadač šalje zahtjeve za prijateljstvom drugim korisnicima s ciljem proširivanje vlastite mreže kako bi je mogao iskorištavati u određene svrhe te dobiti pristup privatnim podatcima i aktivnostima što više drugih korisnika, a pristup istima ovisi o prihvaćanju zahtjeva vlasnika profila. Ovaj napad se može lako automatizirati, a gotovo ga je nemoguće spriječiti jer je jedan od osnovnih ciljeva društvenih mreža umrežavanje. Najveća odgovornost je na korisnicima društvenih mreža koji bi trebali opreznije birati koga će prihvatiti za prijatelja. No, nažalost, većina studija ukazuje na to da to ne čine.[116]
- **Puzanje i berba** – automatizirani su napadi gdje napadač prikuplja javno dostupne korisničke podatke na više profila i aplikacija unutar platforme jedne društvene mreže ili više društvenih mreža. Kada to vrši unutar platforme jedne mreže onda to nazivamo *puzanje*, a kada napad vrši na više platformi društvenih mreža to nazivamo *berba*. Za razliku od profiliranja sekundarnog prikupljanja podataka, ovaj napad nije usmjeren na ciljanog korisnika i odvija se samo na platformama društvenih mreža. Da bi se ovaj napad proveo, napadači često provedu i napad lažnih zahtjeva jer je cilj prikupiti što više privatnih podataka korisnika kako bi ih mogli zloupotrijebiti, a jedan od načina je da prikupljene podatke prodaju marketinškim agencijama. Nadalje, analizom prikupljenih podataka mogu stvoriti preduvjete za daljnje ciljane napade. Većina društvenih mreža od ovog napada štiti se tako da uvede određenu razinu zahtjeva za korisničkom autentifikacijom, no napadači pomoću odgovarajućih alata zaobiđu prepreku.[117]
- **Preuzimanje i analiza fotografija** uglavnom je automatizirani napad na profil korisnika s ciljem prikupljanja multimedijskih podataka dostupnih na platformi

[115] ibid. str. 18.
[116] ibid. str. 19.
[117] ibid. str. 20.

društvenih mreža poput fotografija i videozapisa. Kod ovog napada napadač uglavnom pomoću dodatnih alata vrši automatiziranu obradu za prepoznavanje uzoraka te ih koristi za pronalaženje veza s drugim profilima na društvenim mrežama. Objave i pohrana digitalnog sadržaja korisnika svakako potiče društvenu interakciju između korisnika društvenih mreža, ali slobodan pristup istima upravo omogućuje ovaj napad na privatnost korisnika. Kada napadač preuzme te dodatno obradi sadržaj, on može o korisniku otkriti više podataka nego što je sam korisnik spreman dati. Tako, na primjer, analizom fotografija i videozapisa može otkriti tko su korisnikovi prijatelji ili kolege s posla, a koji nisu dio njegove mreže te može otkriti koja mjesta je korisnik posjetio i gdje se trenutno nalazi. A ako napadač uključi i sekundarno prikupljanje podataka iz drugih izvora na internetu, ti podatci o korisniku mogu biti i detaljniji. Obrana od ovog napada može ublažiti se još restriktivnijim pristupom kontrole politika za pristup sadržaju[118]

- **Praćenje komunikacije –** ovaj je napad na neki način napad profiliranjem, a cilj je praćenje i otkrivanje komunikacija ciljanog korisnika. Kako korisnici društvenih mreža međusobno komuniciraju putem različitih aplikacija unutar društvenih mreža, ovim napadom napadač može prikupiti više informacija o korisniku nego što je pohranjeno na samom profilu. Ovaj napad može se izvesti i na automatiziran način tako da se instaliraju alati za pretraživanje komentara koje je ostavio ciljani korisnik na raznim aplikacijama unutar društvene mreže.[119]
- **Dogovoreni napadi –** oblik je napada u kojem se napadači udružuju u svojim zlonamjernim aktivnostima kako bi nanijeli štetu drugim korisnicima društvenih mreža ili izveli napad na aplikacije na društvenim mrežama. Kako je utjecaj gomile uvijek velik, napadači kroz dogovoreni napad mogu pokrenuti kampanje koje mogu imati za cilj narušiti ili popraviti nečiji ugled. Nadalje, pokretanjem ovakvog napada mogu utjecati na pristranost javnog mijenja ili utjecati na javne rasprave koje se provode putem aplikacija, a upravo zbog utjecaja gomile nevini korisnici mogu biti iskorišteni u napadu, a da toga nisu ni svjesni. Takav se napad može izvesti putem lažnih ili stvarnih profila, ali one koji se izvode putem stvarnih profila gotovo je nemoguće otkriti, a čak ni praćenje IP adrese u tim slučajevima ne pomaže.[120]

[118] ibid. str. 20.
[119] ibid. str. 21.
[120] ibid. str. 21.

Na temelju prethodno navedenog možemo zaključiti da korisnici vrlo često prilikom pristupa društvenoj mreži na platformi iste pohranjuju jako detaljne podatke koje s vremenom nadopunjuju, ali i objavljuju i dijele gotovo bez razmišljanja. Istovremeno smo svjedoci da su ti podatci u određenim slučajevima bili ugroženi od samih davatelja usluga društvenih mreža te su izloženi stalnim napadima od strane zlonamjernih napadača. Trenutni zakonodavni okviri nisu dobri i ne štite korisnika u dovoljnoj mjeri. Potrebno ih je mijenjati i utjecati na politike privatnosti davatelja usluga društvenih mreža na način da ih se prisili na razvoj automatiziranih alata koji bi smanjili rizike povrede privatnosti poput kloniranja profila, lažnih zahtjeva za prijateljstvom i spriječili razna neovlaštena prikupljanja privatnih podataka korisnika. Upravo navedeni napadi često su temelji za provođenje dezinformirajuće kampanje i kibernetički kriminal, a koji postaju stvarna prijetnja kako pojedincu tako i cijelom društvu.

4.3. Dezinformiranje putem društvenih mreža

Dezinformiranje postoji stoljećima, internet i društvene mreže su najnovije sredstvo komunikacije koje je omogućilo i unaprijedilo dezinformiranje. Upravo zahvaljujući povezanosti putem interneta i digitalnih platformi koje omogućuju razmjenu i širenje informacija, tradicionalni izazovi poput fizičkih i vremenskih ograničenja više ne postoje. Da bi dezinformiranje uspjelo, trebaju biti omogućena tri uvjeta koja zajedno predstavljaju trokut dezinformiranja. Vidi Sliku 4.5.

Slika 4.5. *Trokut dezinformiranja na internetu prema Gu L., Kropotov V., Yarochkin F., The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public. str. 6. (June 3, 2017), dostupno na https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.247008519.2007575061.1601718271-287436439.1592572077*

Bez jednog od tri navedena uvjeta dezinformacija se ne može proširiti i doseći svoju ciljanu razinu, a to je najčešće manipulacija javnim mnijenjem u različite svrhe.[121]

Prvi zahtjev su alati i usluge – mnogi alati i usluge za širenje dezinformacijskih kampanja kroz platforme relevantnih društvenih medija prodaju se u raznim internetskim zajednicama te su lako dostupni u cijelom svijetu. Neki od tih alata su: kupljeni sljedbenici/obožavatelji, lajkovi, repostovi, komentari, videozapisi, mrežne ankete, brisanje i izmjena sadržaja objava ciljanih korisnika. Navedeni alati i usluge ne moraju nužno biti ilegalni, mogu se nabaviti potpuno legalno, a najčešće se radi o sivom tržištu.[122]

Drugi zahtjev su društvene mreže – da bi alati bili od koristi, moraju postojati društvene mreže kao platforma za provođenje dezinformirajućih kampanja jer upravo korisnici društvenih mreža provode na istima dosta vremena, prikupljaju i dijele najnovije vijesti i informacije, a kako je glavna svrha platformi društvenih mreža umrežavanje i dijeljenje sadržaja, među svim korisnicima geografske i vremenske barijere su uklonjene te se jednostavno provodi. Uz navedene razloge postoji još nekoliko razloga zbog kojih su upravo društvene mreže idealne za provođenje dezinformirajućih kampanja, a to su:

- Cijena – da bi dezinformacijska kampanja uspjela i proizvela ciljane učinke, neusporedivo ju je lakše i jeftinije provesti preko društvenih mreža nego oglašavanje drugim kanalima.
- Anonimnost – puno je lakše sakriti porijeklo lažnih vijesti nego da se provodi kampanja kroz oglašavanje.
- Vjerodostojnost – izvori dezinformirajućih kampanja postaju sami korisnici koji virilno prenose vijest što je učinkovitije od širenja istih putem reklama.[123]

Treći zahtjev je motivacija – provođenje dezinformacijskih kampanja ponekad je jednostavno želja za novčanom dobiti putem oglašavanja. U drugim slučajevima ciljevi mogu varirati od kriminalnih do političkih. U trenutnom okruženju najčešće se smatra da je cilj politički. No bez

[121] Gu L., Kropotov V., Yarochkin F., The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public. str.6. (June 3, 2017), dostupno na https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.247008519.2007575061.1601718271-287436439.1592572077, stranica posjećena 4. i 12.10.2020.
[122] ibid. str.7.
[123] ibid. str.7.

obzira na motiv, uspjeh dezinformirajuće kampanje na kraju će se uvijek mjeriti po tome koliko je utjecala na stvarni svijet.[124]

A koliko su dezinformirajuće kampanje prisutne u današnjem svijetu, govori nam podatak da kriminalne skupine nude usluge provođenja dezinformirajućih kampanja u svim regijama svijeta, kineskoj, ruskoj, bliskoistočnoj i drugim. Ponude su prilagođene regijama te uključuju socijalne, kulturne i regionalne razlike. Dezinformirajuće kampanje ne mora se nužno provoditi preko kriminalnih skupina, no upravo kriminalne skupine nude jedinstvenu prednost, a to je anonimnost i veći uspjeh istih te oslobađaju od bilo kakve odgovornosti naručitelja.[125]

Tako se, na primjer, alati i usluge za provođenje dezinformirajućih kampanja u ruskom podzemlju prodaju za svaku fazu provođenja dezinformirajućih kampanja – od pisanja priopćenja za javnost, njihovog promicanja u vijestima, popratnog podržavanja napisanog pozitivnim ili negativnim komentarima, a neki prihvaćaju da im sam naručitelj dostavi predloške sadržaja. Kampanje se mogu provoditi na ruskom, engleskom ili nekim drugim jezicima što utječe na cijenu provođenja kampanje. Druga tržišta imaju svoje specifičnosti i ponude pa je kinesko orijentirano uglavnom na Kinu što je i razumljivo zbog otežanog pristupa pojedinim stranicama izvan Kine. Bliskoistočno tržište pak ima svoje specifičnosti jer ne promiču pornografiju, vjersku ni rasnu netrpeljivost.[126]

Koliki utjecaj dezinformirajuće kampanje mogu imati na javno mnijenje, govori nam događaj na američkim izborima za predsjednika države kada je pobijedio Donald Trump. Procjenjivalo se da su upravo dezinformirajuće kampanje utjecale na krajnji rezultat izbora i pomogle da ih Trump osvoji. Na temelju tih procjena napravljeno je nekoliko studija na tu temu koje ukazuju da su dezinformirajuće kampanje imale utjecaj, ali se ne može sa sigurnošću tvrditi da su bile presudne. No ono što su dokazale jest da je Facebook imao važnu ulogu u usmjeravanju ljudi na web-mjesta s lažnim vijestima.[127] Kada navedeno povežemo s mogućnosti da se dezinformirajuća kampanja mogla provoditi ciljano, vijesti su se mogle kreirati i usmjeravati prema korisnicima na temelju privatnih podataka korisnika koje je neovlašteno prikupila tvrtka Cambridge Analytica putem društvene mreže Facebook (vidi poglavlje 3). Utjecaj na javno mnijenje je mogao biti velik, a po nekim izvorima i presudan u pobjedi.

[124] ibid. str.8.
[125] ibid. str.9.
[126] ibid. str.9.
[127] Guess A., Nyha B., Reifler J., Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign, str. 1. (January 9, 2018), dostupno na https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf, stranica posjećena 13.10.2022.

Upravo je izborna kampanja Donalda Trumpa proizvela pitanja i strahove zbog utjecaja dezinformirajućih kampanja na demokratske vrijednosti na području Evropske unije. U priopćenju za tisak Europske komisije od 28. travnja 2018. navodi se kako je slučaj Facebook – Cambridge Analytica pokazao kako se osobni podatci mogu iskoristiti u kontekstu političkih izbora i da su otkrića podsjetnik da je potrebno činiti više kako bi se osigurale demokratske vrijednosti i sigurnost demokratskih procesa na području Europske unije. Dalje, u priopćenju se navode statistički podatci ispitivanja provedenog putem Eurobarometra – da dezinformirajuće kampanje ugrožavaju demokraciju izjavilo je 83% ispitanika, a posebna zabrinutost je spram utjecaja dezinformiranja na političke izbore i imigrantske politike. Također, pokazalo se da ispitanici najviše vjeruju tradicionalnim medijima (radio 70%, TV 66%, tisak 63%). Dok internetske izvore i web-mjesta za video hosting smatraju najmanje vjerodostojnijima jer njima vjeruje 26% odnosno 27% ispitanika. Ali istovremeno se dvije trećine ispitanika informira putem platformi upravljanih algoritmima poput tražilica, servisa za prikupljanje vijesti te stranica društvenih medija. Nadalje, studija ukazuje da operatori navedenih platformi sada imaju veću tržišnu snagu i izvore prihoda od novinskih izdavača.[128] Uvidjevši probleme i nove trendove, Europska komisija reagirala je prijedlogom niza mjera za borbu protiv dezinformiranja na internetu, a te mjere uključuju:

- **„kodeks prakse za borbu protiv dezinformiranja**: kao prvi korak internetske platforme trebale bi izraditi i poštivati zajednički kodeks prakse kako bi se:
  - osigurala transparentnost u pogledu sponzoriranog sadržaja, posebno oglašavanja političkog karaktera, ograničile opcije usmjeravanja takvog oglašavanja i smanjili prihodi promicatelja dezinformacija
  - bolje objasnilo funkcioniranje algoritama i omogućavanje provjere trećih osoba
  - korisnicima olakšalo otkrivanje različitih izvora vijesti s drukčijim stajalištem i pristup njima
  - uvele mjere za prepoznavanje i zatvaranje lažnih računa i rješavanje problema automatiziranih botova
  - provjeravateljima činjenica, istraživačima i javnim tijelima omogućilo da stalno prate internetske dezinformacije;“[129]

[128] Europska komisija (priopćenje za tisak), Borba protiv dezinformiranja na internetu: Komisija predlaže uvođenje kodeksa prakse na razini EU-a, dostupno na https://ec.europa.eu/commission/presscorner/detail/hr/IP_18_3370, stranica posjećena 16.10.2022.
[129] ibid.

- **„stvaranje neovisne europske mreže provjeravatelja činjenica** koja će utvrditi zajedničke radne metode, razmjenjivati najbolju praksu i raditi na ostvarivanju što veće zastupljenosti činjeničnih ispravaka u EU-u;“ [130]
- **„sigurnu europsku internetsku platformu o dezinformiranju** pomoću koje će se mreži provjeravatelja činjenica i relevantnim akademskim znanstvenicima osigurati prekogranično prikupljanje i analiza podataka te pristup podatcima iz cijelog EU-a;“ [131]
- **„poboljšanje medijske pismenosti:** viša razina medijske pismenosti europskim će građanima omogućiti da prepoznaju internetske dezinformacije i kritički pristupaju internetskom sadržaju. Komisija će u tu svrhu poticati provjeravatelje činjenica i organizacije civilnog društva da škole i nastavnike opskrbe obrazovnim materijalom i organiziraju Europski tjedan medijske pismenosti;“ [132]
- **„pružanje podrške državama članicama u osiguravanju otpornosti izbora** na sve složenije kibernetičke prijetnje, uključujući dezinformiranje na internetu i kibernetičke napade;“ [133]
- „promicanje dobrovoljnih sustava internetske identifikacije radi boljeg praćenja i identificiranja davatelja informacija i povećanja povjerenja i pouzdanosti u interakcijama na internetu te informacija i izvora informacija;“ [134]
- **promicanje kvalitete i raznolikosti informacija:** komisija poziva države članice da pojačaju svoju potporu kvalitetnom novinarstvu kako bi osigurale pluralističko, raznoliko i održivo medijsko okruženje.[135]

Slijedom zahtjeva Europske komisije sve društvene mreža i internetske tražilice Google, Facebook, Twitter, Mozilla potpisale su kodeks prakse za borbu protiv dezinformiranja.

U Republici Hrvatskoj pojedince i skupine od provođenja dezinformirajućih kampanja prema njima štiti članak 325. Kaznenog zakonom koji glasi:

„(1) Tko putem tiska, radija, televizije, računalnog sustava ili mreže, na javnom skupu ili na drugi način javno potiče ili javnosti učini dostupnim letke, slike ili druge materijale kojima se poziva na nasilje ili mržnju usmjerenu prema skupini ljudi ili pripadniku skupine zbog njihove

[130] ibid.
[131] ibid.
[132] ibid.
[133] ibid.
[134] ibid.
[135] ibid.

rasne, vjerske, nacionalne ili etničke pripadnosti, jezika, podrijetla, boje kože, spola, spolnog opredjeljenja, rodnog identiteta, invaliditeta ili kakvih drugih osobina, kaznit će se kaznom zatvora do tri godine. (2) Tko organizira ili vodi grupu od tri ili više osoba radi počinjenja djela iz stavka 1 ovoga članka, kaznit će se kaznom zatvora od šest mjeseci do pet godina. (3) Tko sudjeluje u udruženju iz stavka 2. ovoga članka, kaznit će se kaznom zatvora do jedne godine. (4) Kaznom iz stavka 1. ovoga članka kaznit će se tko javno odobrava, poriče ili znatno umanjuje kazneno djelo genocida, zločina agresije, zločina protiv čovječnosti ili ratnog zločina, usmjereno prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla ili boje kože, na način koji je prikladan potaknuti nasilje ili mržnju protiv takve skupine ili pripadnika te skupine."[136]

Uz Kazneni zakon RH i Zakon o elektroničkim medijima definira što je zabranjeno u medijskom prostoru te članak 12. Zakon o elektroničkim medijima glasi: „(1) Nisu dopuštene audio i/ili audiovizualne medijske usluge koje ugrožavaju ustavni poredak i nacionalnu sigurnost. (2) U audio i/ili audiovizualnim medijskim uslugama nije dopušteno poticati, pogodovati poticanju i širiti mržnju ili diskriminaciju na osnovi rase ili etničke pripadnosti ili boje kože, spola, jezika, vjere, političkog ili drugog uvjerenja, nacionalnog ili socijalnog podrijetla, imovnog stanja, članstva u sindikatu, obrazovanja, društvenog položaja, bračnog ili obiteljskog statusa, dobi, zdravstvenog stanja, invaliditeta, genetskog naslijeđa, rodnog identiteta, izražavanja ili spolne orijentacije, te antisemitizam i ksenofobiju, ideje fašističkih, nacionalističkih, komunističkih i drugih totalitarnih režima.[137]

Uz članak 12. i članak 1. stavak 4. Zakon o elektroničkim medijima nalaže da: „Audiovizualne komercijalne komunikacije ne smiju: dovoditi u pitanje poštivanje ljudskog dostojanstva, uključivati ili promicati bilo kakvu diskriminaciju na temelju spola, rase, etničke pripadnosti, nacionalnosti, vjere ili uvjerenja, invalidnosti, dobi ili spolne orijentacije, poticati ponašanje koje je štetno za zdravlje ili sigurnost."[138]

Utjecaj Europske unije na područje Republike Hrvatske donosi rezultate u borbi protiv dezinformirajućih kampanja, ali uglavnom se odnose na govor mržnje, rasnu ili neku drugu diskriminaciju koja je definirana Ustavom i drugim zakonima. No stječe se dojam bi se svakako moglo i moralo učiniti više. Prvenstveno je potrebno početi raditi na medijskoj pismenosti

[136] Kazneni zakon, NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19
[137] Zakon o elektroničkim medijima, NN br. 153/2009
[138] ibid.

korisnika interneta, ali i izmijeniti neke zakonodavne odredbe te u budućnosti možemo očekivati pozitivne rezultate.

4.4. Kibernetički kriminalitet i društvene mreže

„Računalni, odnosno kibernetički kriminalitet obuhvaća kaznena djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom komunikacijskih i informacijskih tehnologija i predstavlja prijetnju ostvarenju sigurnijeg informacijskog društva. Uspostava učinkovitih preventivnih mjera, ali i odgovori kaznenog prava na ovu vrstu kriminaliteta ključni su element za postizanje odgovarajuće razine zaštite, nesmetanog djelovanja i sigurnosti računalnih sustava.“[139]

Kriminalni potencijal kibernetičkog prostora proizlazi iz njegove dostupnosti, masovne i sve veće ovisnosti suvremenog društva o korištenju i nesmetanom radu informacijsko-komunikacijskih sustava. „Kako je riječ o globalnom fenomenu, domašaj nacionalnog zakonodavstva i aktivnosti njihovih redarstvenih vlasti da učinkovito odgovore na te izazove uvelike je ograničen. Istovremeno, takvo stanje prate neki opći trendovi koji borbu protiv kibernetičkog kriminala još više otežavaju poput: konvergencija različitih tehnologija, dostupnosti i rasprostranjenosti alata (uređaja i programa) i uputa čija je namjena da olakšaju i omoguće različite zlouporabe, zatim sve je manje znanja potrebno da bi se takva djela činila, nastajanje i širenje crnog tržišta kiberkriminala, te sve veća šteta koje pojedinci i društvo trpe od takvih djela.“[140] Upravo lako dostupni alati za provođenje kibernetičkog kriminala kako na površinskom webu tako i na dubinskom webu (engl. *Deep Web*). Na površinskom webu su dostupni putem različitih hakerskih stranica i drugih web mjesta. „Pri Deep Webu treba razlikovati onaj njegov dio koji je anoniman, ali se ne koristi u nezakonite svrhe od onog koji pogoduje širenju kriminalnih dijela u kiberprostoru ili fizičkom svijetu (*Darkweb* ili *Darknet*). Darknet čine privatne mreže za razmjenu datoteka kojima se pristupa putem nestandardnih pretraživača i protokola. Korisnici mogu sačuvati svoju anonimnost na internetu i učiniti svoj sadržaj nedostupnim web-pretraživačima. Mogućnost anonimnosti komunikacije ubrzo su uvidjeli hakeri i organizirani kriminalci koristeći ih za razmjenu i prodaju alata za činjenje kaznenih djela, razmjenu i prodaju ilegalne robe poput oružja, malvera (engl. *malware*), droge,

[139] NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI, NN br. 108/2015

[140] Dragičević D., Gumzej N., Jurić M., Katulić T., Lisičar, H., Pravna informatika i pravo informacijskih tehnologijastr, str. 167. Narodne novine, Zagreb 2015.

ukradenih brojeva kreditnih kartica i ponude hakerskih usluga."[141] Većina javnosti se prvi put upoznala s *Darknetom* 2013. godine tada je FBI zatvorio stranicu pod nazivom Silk Road na kojoj su se razne usluge poput kupnje ilegalne droge, pranja novca i činjenja drugih kaznenih djela plaćale virtualnom valutom. „Slična stranica Silk Road 2.0 zatvorena je iduće godine. Također iste godine zatvorena je i web-stranica koja je nudila dječju pornografiju, tj. seksualno eksplicitne slike više od 240 dječaka i nekoliko djevojčica iz područja SAD-a, a imala je 27.000 pretplatnika."[142] Iz navedenog vidimo koliko su kriminalne skupine organizirane i kako brzo usvoje i iskoriste nove tehnologije za činjenje najtežih kriminalnih djela. Uz društvene mreže pojavile su se nove mogućnosti prilikom izvođenja kriminalnih radnji i unaprijedile već postojeće. Kako su ih prepoznale i iskoristile kriminalne skupine, možemo vidjeti iz sljedećih primjera koje je objavila web-stranica https://study.com u lekciji: *Kako se društvene mreže koriste u internetskom kriminalu*, a navodi se sljedeći primjer: U 2013. godini burza je izgubila na vrijednosti više od 130 milijardi dolara zahvaljujući jednom događaju. „Ne, nije to bila globalna kriza. Rat nije izbio. Nije bilo promjena u fiskalnoj ili monetarnoj politici. Umjesto toga, pad je pripisan jednom izvoru: društvenim mrežama. Hakeri su preuzeli kontrolu nad Twitter računom Associated Pressa i objavili lažnu vijest da je u Bijeloj kući u Washingtonu aktivirana bomba. Zbog lažne poruke naglo je pao i burzovni indeks S&P 500 i Dow Jones Industrial Average. Uz navedeni primjer ima još nekoliko primjera, a jedan je: Prevaranti su iskoristili smrt glumca Robina Williamsa kako bi potaknuli ljude da dijele lažni videozapis te putem njega šire zlonamjerni softver. A upravo na Twitteru kriminalci često objavljuju zlonamjerne internetske poveznice koje izgledaju legitimno u nadi da će korisnike natjerati da ih otvore i nakon toga i zaraze svoje uređaje."[143] Navedeni primjeri ukazuju da su kriminalne skupine vrlo brzo uvidjele mogućnosti društvenih mreža u provođenju svojih kriminalnih radnji. One se putem njih mogu u cijelosti ili djelomično provoditi. Većina kriminalnih radnji temelji se na ilegalno prikupljenim osobnim podatcima korisnika društvenih mreža ili ima za cilj prikupiti iste (vidi poglavlje 4.2.) gdje smo opisali primjere napada na privatnost korisnika društvenih mreža. U nastavku detaljnije objašnjavamo neke alate i metode koje kriminalne skupine koriste u pripremi i provođenju kriminalnih radnji.

„Zlonamjerni softver – kada kliknete na veze koje ne prepoznajete ili otvorite privitke koje su poslali ljudi s vašeg popisa prijatelja, a softver zarazi računalo korisnika, on će ukrasti njegove

[141] ibid. str. 167.
[142] Ibid. str. 168-169
[143] Beth Hendricks, How Social Networks are Used in Cybercrime dostupno na https://study.com/academy/lesson/how-social-networks-are-used-in-cybercrime.html, stranica posjećena 18.14.2022.

lozinke za sve društvene mreže koje korisnik posjećuje. Na tim društvenim mrežama će u ime korisnika, ali bez njegova znanja, slati poruke svim njegovim kontaktima.“[144]

„Izviđanje – izviđanje nije samo za policajce, kriminalci provode vlastiti način izviđanja ili nadzora kako bi tražili ljude na društvenim mrežama koje bi mogli iskoristiti i prikupiti što više podataka o njima ili njihovim prijateljima. Ti podatci se zatim pretvaraju u lažne profile na društvenim mrežama i koriste u raznim situacijama.“[145]

„Socijalni inženjering – to je niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći. Napadači se često služe ovom tehnikom jer im za uspješan napad nije potrebno složeno probijanje korisnikove sigurnosne zaštite, korištenje ranjivosti njegovog softvera i sl. Pojam socijalnog inženjeringa je popularizirao poznati osuđeni haker Kevin Mitnick, koji tvrdi kako je mnogo lakše nekoga prevariti služeći se socijalnim inženjeringom nego probiti njegov informacijski sustav.“[146]

Možemo zaključiti da su se prijetnje i trendovi kibernetičkog kriminala pojavom društvenih mreža unaprijedile te zbog same prirode društvenih mreža, kojima je glavna svrha umrežavanje i dijeljenje sadržaja, lakše se provode zlonamjerne radnje poput dijeljenja zlonamjernog softvera ili prihvaćanja lažnih profila za prijatelja, koje su temelj za prikupljanje privatnih podataka koji mogu dovesti i dovode do krađe identiteta. Upravo krađa identiteta je pojavom i uspjehom društvenih mreža doživjela ogroman porast. Po nekim istraživanjima više od polovice korisnika interneta u svijetu susrelo se s kibernetičkim kriminalom, a šteta prouzrokovana istim za 2017. godinu procjenjuje se na 600 milijardi dolara.[147] „A zbog sve veće stope rasta kibernetičkog kriminala procjenjuje se da će do kraja 2021. ta šteta doseći godišnji trošak od 6 bilijuna dolara.“[148] Kibernetički kriminal je teško bilo kontrolirati i sprečavati i prije pojave društvenih mreža, a naglim rastom broja korisnika i broja raznih usluga na njima sigurno će biti još teže jer uz pomoć društvenih mreža sofisticirani napadi kriminalnih

[144] Nacionalni CERT, dostupno na https://www.cert.hr/socijalni_inzenjering/, stranica posjećena 18.10.2022.
[145] ibid.
[146] ibid.
[147] Bisson D., Global Cost of Cybercrime Exceeded $600 Billion in 2017, Report Estimates, (February 23, 2018), dostupno na https://securityintelligence.com/news/global-cost-of-cybercrime-exceeded-600-billion-in-2017-report-estimates/, stranica posjećena 16.5.2023.
[148] Irshad S., Soomro T.R., Identity Theft and Social Media, str. 7., IJCSNS International Journal of Computer Science and Network Security (February 2018), 43-55.

skupina imaju puno veće izglede za uspjeh. Kada je u pitanju pravni sustav Republike Hrvatske, u njega je implementiran niz zakona i temeljnih akata u svrhu prevencije kibernetičkog kriminala. Republika Hrvatska potpisnik je Konvencije Vijeća Europe o kibernetičkom kriminalu te je u srpnju 2002. godine donesen Zakon o potvrđivanju Konvencije Vijeća Europe o kibernetičkom kriminalu. Nadalje, donesena je Nacionalna strategija kibernetičke sigurnosti 7. listopada 2015. Upravo Nacionalna strategija kibernetičke sigurnosti, sukladno strateškim ciljevima Europske unije, ima sljedeće opće ciljeve:

- sustavni pristup u razvoju kaznenopravnog okvira
- provođenje aktivnosti i mjera za jačanje sigurnosti kibernetičkog prostora
- uspostava sigurnih mehanizama za razmjenu podataka
- jačanje javne svijesti o kibernetičkom prostoru
- obrazovni programi o razvoju e-usluga
- poticanje istraživanja i razvoja o međunarodna suradnja.[149]

U samoj strategiji predviđeni su rokovi provođenja zadataka i ciljeva kroz izvješća koja se podnose vladi RH. Pored Nacionalne strategije kibernetičke sigurnosti, donesen je i „Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga“[150] Članak 1. glasi:

„(1) Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata (u daljnjem tekstu: nadležni CSIRT) i tehničkog tijela za ocjenu sukladnosti, nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe.“[151]

„(2) Cilj je ovog Zakona osigurati provedbu mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta.“[152]

Napori Republike Hrvatske u suzbijanju kibernetičkog kriminala vidljivi su kroz donošenje zakona, zakonskih akata i druge napore. No, rezultati koje možemo iščitati iz izvještaja

[149] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti , NN108/2015
[150] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN br. 64/18
[151] ibid.
[152] ibid.

Ministarstva unutarnjih poslova o osnovnim sigurnosnim pokazateljima u Republici Hrvatskoj za 2019. godinu pokazuju da je kibernetički kriminal u Republici Hrvatskoj narastao za 87% u odnosu na 2018. godinu.

Tablica 4.1. *Osnovni sigurnosni pokazatelji u Republici Hrvatskoj za 2019. prema MUP RH dostupno na https://mup.gov.hr/UserDocsImages/statistika/Statisticki_ pregled_2019_WEB.pdf*

KRATKI PREGLED OSNOVNIH POKAZATELJA KRIMINALITETA

KRIMINALITET - po službenoj dužnosti	PRIJAVLJENA KAZNENA DJELA			KOEFICIJENT RAZRIJEŠENOSTI [1]			POSTOTAK RAZRIJEŠENOSTI[2]		
	2018.	2019.	2019./2018. %	2018.	2019.	+-	2018.	2019.	+-
OPĆI KRIMINALITET	**39.684**	**42.651**	**+7,5**	**53,8**	**57,0**	**+3,2**	**51,5**	**54,8**	**+3,3**
Ubojstva	22	**30**	+36,4	100,0	**96,7**	-3,3	100,0	**96,7**	-3,3
Pokušaji ubojstva	90	**98**	+8,9	92,2	**100,0**	+7,8	90,0	**96,9**	+6,9
Silovanja	56	**73**	+30,4	94,6	**98,6**	+4,0	94,6	**97,3**	+2,6
Pokušaji silovanja	11	**12**	+9,1	90,9	**58,3**	-32,6	90,9	**58,3**	-32,6
Razbojništva	647	**670**	+3,6	53,9	**45,7**	-8,3	46,4	**40,1**	-6,2
Teške krađe	11.615	**11.579**	-0,3	22,6	**24,0**	+1,4	19,1	**20,5**	+1,4
Otuđenja motornih vozila (dovršena)	859	**940**	+9,4	27,7	**30,1**	+2,4	25,0	**27,1**	+2,1
Pronađena otuđena vozila	*556*	***677***	+21,8						
Kaznena djela na štetu djece i obitelji	**5.188**	**6.859**	+32,2	99,4	**99,4**	+0,0	99,3	**99,3**	0,0
Kaznena djela maloljetnih osoba	1.783	**2.035**	+14,1						
TERORIZAM I EKSTREMNO NASILJE	**26**	**33**	**+26,9**	**88,5**	**87,9**	**-0,6**	84,6	**87,9**	**+3,3**
RATNI ZLOČINI	**33**	**20**	**-39,4**	**124,2**	**105,0**	**-19,2**	97,0	**85,0**	**-12,0**
ORGANIZIRANI KRIMINALITET	**1.937**	**2.044**	**+5,5**	**98,5**	**98,9**	**+0,4**	98,2	**98,5**	**0,3**
Protuzakonito ulaženje, kretanje i boravak u Republici Hrvatskoj ili drugoj državi čl. EU i ili potp. Schengenskog sporazuma	619	**946**	+52,8	**98,9**	**100,1**	+1,2	99,8	**99,6**	**-0,3**
GOSPODARSKI KRIMINALITET	**4.292**	**4.137**	**-3,6**	**100,0**	**101,3**	**+1,3**	99,6	**99,5**	**0,0**
Korupcijska kaznena djela*	515	**785**	+52,4	**100,0**	**99,9**	-0,1	99,4	**99,9**	0,5
KRIMINALITET ZLOUPORABE DROGA	**2.274**	**2.871**	**+26,3**	**99,9**	**99,6**	**-0,3**	**99,8**	**99,6**	**-0,2**
KRIMINALITET KIBERNETIČKE SIGURNOSTI	**1.564**	**2.930**	**+87,3**	**90,8**	**94,5**	**+3,7**	**89,5**	**94,0**	**4,5**
UKUPNO K. D. (bez prometa)	**49.810**	**54.686**	**+9,8**	**62,8**	**66,2**	**+3,4**	**60,0**	**64,3**	**+4,3**
KAZNENA DJELA U CESTOVNOM PROMETU	**1.477**	**1.308**	**-11,4**	**99,1**	**99,0**	**-0,0**	**99,0**	**98,9**	**-0,1**
SVEUKUPNO KAZNENIH DJELA	**51.287**	**55.994**	**+9,2**	**63,9**	**67,0**	**+3,1**	**62,1**	**65,1**	**+3,1**
Počinitelji kaznenih djela u prometu	1.406	**1.259**	-10,5						
UKUPNO POČINITELJA (pravne i fizičke osobe)	**17.399**	**18.675**	**+7,3**						
Maloljetni počinitelji	1.070	**1.135**	+6,1						

Na osnovi tablice o osnovnim sigurnosnim pokazateljima u Republici Hrvatskoj za 2019. možemo utvrditi da su potrebni dodatni napori kako bi se više učinilo u području suzbijanja kibernetičkog kriminala. Nažalost, iz izvještaja ne možemo utvrditi koliki je postotak kaznenih djela bio dijelom ili u cijelosti proveden putem društvenih mreža.

4.5. Preporuke međunarodnih tijela i radnih skupina o smanjenju rizika povrede privatnosti na društvenim mrežama

Sigurnosni su rizici na društvenim mrežama veliki kao i osobni podatci koje korisnik objavljuje na njima, a u kombinaciji s podatcima koji opisuju radnje korisnika i interakcije s drugim ljudima mogu stvoriti bogat profil interesa i osobe te osobe i aktivnosti. Osobne podatke objavljene na stranicama društvenih mreža treće strane mogu koristiti za širok raspon, uključujući komercijalne svrhe i mogu predstavljati velike rizike kao što su krađa identiteta, financijski gubitak, gubitak poslovnih ili radnih prilika i fizička šteta. Svi navedeni rizici stvorili su potrebu za postavljanjem određenih standarda kada je u pitanju privatnost korisnika društvenih mreža. Ovom problematikom još se 2007. godine bavila i Agencija Europske unije za mrežnu i informacijsku sigurnost (engl. – *European Network and Information Security Agency* – ENISA) te je u svom izvještaju „Preporuke za online društvene mreže“ iz 2007. godine navela opasnosti koje su podijeljene u nekoliko kategorija, a one su:

Prijetnje vezane uz privatnost korisnika:

- kreiranje digitalnih dosjea od strane trećih osoba
- sekundarno prikupljanje podataka u marketinške svrhe
- programi za prepoznavanje lica na fotografijama korisnika
- CBIR (*Content-based Image Retrieval*), nova tehnologija koja se bazira na istraživanju sadržaja fotografije u cilju kreiranja ogromne baze podataka
- mogućnost povezivanja slike s metapodatcima (profil ili e-mail)
- poteškoće u brisanju profila nakon što prestanete biti korisnik.[153]

[153] Acquisti A., Carrara E., Stutzman F., Callas J., Schimmer K., Nadjm M., Gorge M., Ellison N., King P., Gross R., Mellon C., Hewlett-Packard H., Security Issues and Recommendations for Online Social Networks. ENISA, str. 2. (October 2007), dostupno na https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks, stranica posjećena 17.1.2023.

Tradicionalne opasnosti za mreže i sigurnost informacija:

- neželjene poruke
- XSS (*Cross site scripting*): zaraza korisnika putem virusa i crva
- alati za grupiranje profila više društvenih mreža – takvi alati (npr. *Snag* i *ProfileLinker*) dozvoljavaju korisnicima da dodavanjem novih podataka ažuriraju korisničke profile na više društvenih mreža istovremeno. U alat je potrebno unijeti korisnička imena i lozinke računa kojima se želi pristupati.[154]

Prijetnje identitetu:

- *Phishing* napadi
- otkrivanje podataka
- lažni profili.[155]

Društvene prijetnje:

- proganjanje
- zlostavljanje
- industrijska špijunaža.[156]

U skladu s utvrđenim prijetnjama ENISA daje sljedeće preporuke i protumjere za povećanje razine sigurnosti korisnika i informacija:

Preporuke u području vladinih regulatornih politika:

- ohrabriti podizanje svijesti i provoditi edukativne kampanje
- ocijeniti i analizirati regulativu
- povećati transparentnost u rukovanju podatcima
- ne zabranjivati korištenje društvenih mreža u školama.[157]

Preporuke za davatelje usluga i njihovu poslovnu politiku:

- uvesti strožu identifikaciju i kontrolu pristupa tamo gdje je to moguće
- uvesti mjere protiv industrijske špijunaže

[154] ibid.str.12.
[155] ibid.str.2.
[156] ibid.str.2.
[157] ibid.str.18.

- maksimalno izvještavati korisnike o zlouporabama
- postaviti odgovarajuća početna podešavanja profila koja će zaista štititi privatnost korisnika
- davatelj usluge društvene mreže treba ponuditi jednostavan način za kompletno brisanje podataka.[158]

Tehničke preporuke:

- poticati naviku ocjenjivanja reputacije korisnika
- ugraditi automatizirane filtre
- tražiti suglasnost za označavanje fotografija
- ograničiti slanje neželjenih poruka
- osigurati bolju kontrolu privatnosti kod pretraživanja osobnih podataka
- regulirati problem slanja neželjenih poruka putem društvenih mreža
- regulirati problem *phishinga* na društvenim mrežama.[159]

Preporuke u području istraživanja i standardizacije:

- promovirati i istražiti tehnike za anonimizaciju fotografija korisnika
- promovirati „prijenosne" mreže
- istražiti nove trendove u vezi s društvenim mrežama.[160]

Istom problematikom bavila se i međunarodna radna grupa za zaštitu podataka u telekomunikacijama (engl. *International Working Group on Data Protection in Telecommunications*). Godine 2008. objavila je dokument pod nazivom Rimski memorandum (engl. *Rome Memorandum*)[161] koji se još preciznije bavi problemom povrede privatnosti korisnika društvenih mreža te upozorava na sljedeće prijetnje:

- nema zaborava na internetu: jednom objavljeni podatci tamo ostaju zauvijek
- stvaranje lažne sigurnosti pod pojmom „zajednica": korisnici se navode da dijele privatne podatke i samim nazivima aplikacija kao što je „Moj prostor" (*MySpace*) stvara se lažna slika sigurnosti

[158] ibid.str.20.
[159] ibid.str.22.
[160] ibid.str.24.
[161] International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services, Rome Memorandum, (Rome, 4 March 2008), dostupno na https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/berlin-group/2008/2008-Rome_Memorandum-en.pdf 13.5.2023.

- besplatne usluge koje se nude uglavnom nisu besplatne, davatelji usluga se naplate kroz sekundarnu upotrebu privatnih podataka korisnika u marketinške svrhe
- prikupljanje podataka o prometu korisnika društvenih mreža na internetu od strane davatelja usluge
- rast potrebe za refinanciranjem i ostvarivanjem profita mogu dodatno potaknuti prikupljanje i obradu osobnih podataka korisnika
- korisnici u stvari daju više privatnih podataka nego što misle da daju. Na primjer, slika može postati univerzalni biometrijski identifikator unutar mreže, pa čak i izvan mreže. Softver za prepoznavanje lica je dramatično poboljšan u posljednjih nekoliko godina, a očekuje se da će u budućnosti biti još bolji
- zloupotreba osobnih podataka iz profila korisnika od treće strane
- povećan rizik od krađe identiteta, s obzirom da su podatci iz profila široko dostupni
- postojeći neriješeni sigurnosni problemi internetskih usluga uz korištenje društvenih mreža u nekim se slučajevima povećavaju i postaju karakteristične za društvene mreže kao što je bullying na društvenim mrežama
- upotreba nesigurne infrastrukture: sigurnosni incidenti koji su se dogodili kod davatelja usluga kao što su Facebook, Flickr, MySpace, Orkut i njemačkog davatelja usluga StudiVZ potvrđuju da je infrastruktura nesigurna
- uvođenje standarda interoperabilnosti i sučelja za programiranje aplikacija u cilju tehničkog izjednačavanja različitih društvenih mreža.[162]

Radna grupa je u skladu s utvrđenim rizicima po privatnost korisnika društvenih mreža dala sljedeće preporuke:

Preporuke za regulatorna tijela:

- omogućiti pravo na upotrebu pseudonima umjesto pravog imena
- osigurati da davatelji usluga budu iskreni i jasni u pogledu informacija koje su potrebne za osnovnu uslugu, tako da korisnici mogu procijeniti hoće li te informacije dati te mogućnost da korisnici mogu zabraniti bilo kakvu daljnju upotrebu svojih podataka, posebno za ciljani marketing[163]
- uvesti obavezu obavještavanja o provali u privatne podatke korisnika društvenih mreža
- revidirati postojeći regulatorni okvir u odnosu na upravljanje osobnim podatcima
- poboljšati integraciju pitanja privatnosti u obrazovni sustav.[168]

[162] ibid.
[163] ibid.

Preporuke za davatelje usluga društvenih mreža:

- transparentno i otvoreno informiranje korisnika
- uvesti mogućnost kreiranja i korištenja profila pod pseudonimom
- poboljšati korisničku kontrolu nad korištenjem privatnih podataka iz profila
- početno zadane postavke trebaju biti usmjerene na zaštitu privatnosti
- poboljšati kontrolu korisnika nad upotrebom njegovih podataka iz profila
- osigurati odgovarajuće mehanizme za upravljanje prigovorima korisnika
- poboljšati i održavati sigurnost informacijskih sustava
- osmisliti i/ili dodatno unaprijediti mjere protiv ilegalne aktivnosti kao što su neželjene poruke i krađa identiteta
- ponuditi kriptiranu vezu za održavanje korisničkih profila, uključujući i sigurnost prijave
- davatelji usluga društvenih mreža koji djeluju u različitim zemljama ili čak globalno trebaju poštovati standarde zaštite privatnosti zemalja u kojima pružaju usluge. [164]

Preporuke za korisnike:

- postupati oprezno, razmisliti dvaput prije objavljivanja osobnih podataka (posebno paziti na ime, adresu ili telefon)
- razmisliti dvaput prije no što se upotrijebi pravo ime u profilu
- poštivati privatnost drugih
- biti informiran o davatelju usluga
- koristiti podešavanja koja omogućavaju zaštitu privatnosti
- koristiti različite identifikacijske podatke (korisničko ime i šifra) na različitim internetskim stranicama
- koristiti mogućnost kontroliranja kako davatelj usluga koristi vaše osobne podatke
- obratiti pozornost na ponašanje djece na internetu, a posebno na društvenim mrežama.[165]

[164] ibid.
[165] ibid.

Sukladno utvrđenim prijetnjama i preporukama radna skupina poziva organizacije za zaštitu potrošača i privatnosti da podižu svijest kod regulatora, davatelja usluga, šire javnosti i posebno kod mladih korisnika.[166]

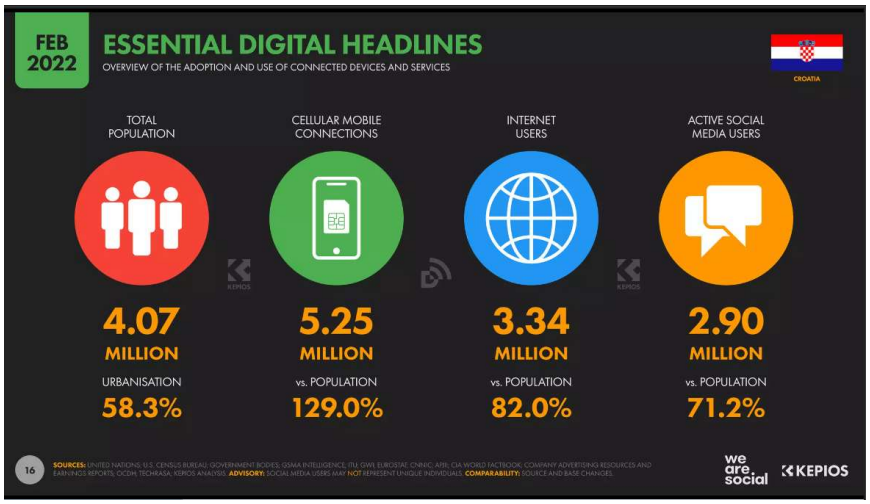
Mogli bismo navesti još neke od radnih grupa koje su se bavile povredom privatnosti korisnika društvenih mreža, ali zaključci svih su slični ili gotovi isti i svi su na tragu preporuka koje su izdane od strane ENISA-e. Nadalje, možemo zaključiti da je većina prijetnji privatnosti korisnika na društvenim mrežama uočena već više od desetljeća, ali te prijetnje nisu se smanjile, nego upravo suprotno.

[166] ibid.

5. KORISNICI INTERNETA U REPUBLICI HRVATSKOJ

5.1. Broj korisnika i njihove navike

Marketinška agencija We Are Social, provela je globalno istraživanje broja korisnika interneta u 248 zemlje svijeta pod nazivom „Digital In 2022“. Prema tim podatcima u Republici Hrvatskoj u 2022. godine bilo je 3,34 milijuna korisnika interneta što čini gotovo 82% ukupne populacije. Kada su u pitanju društvene mreže, po podatcima iz istog istraživanja, u Republici Hrvatskoj je 2.9 milijuna korisnika, što ukazuje na to da je 71% ukupnog stanovništva aktivno na društvenim mrežama. Vidi Sliku. 5.1.

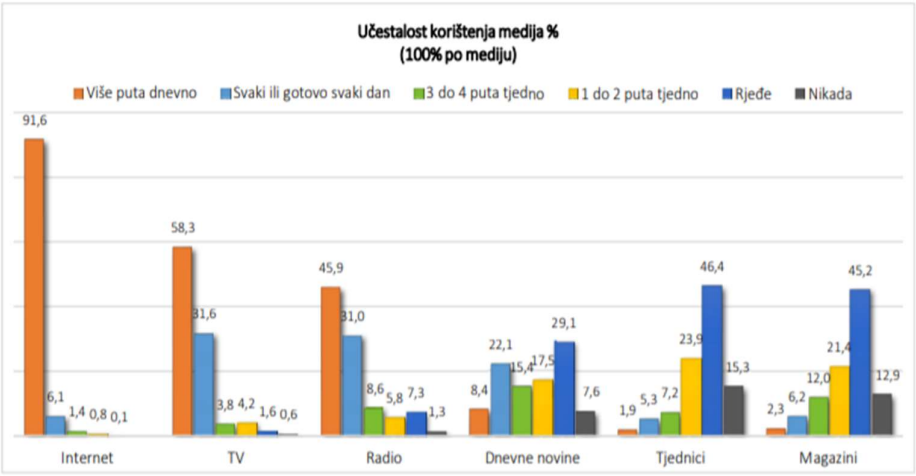


Slika 5.1. *Broj korisnika interneta i društvenih mreža u Republici Hrvatskoj prema: Digital Global Statshot Report, Digital 2022 Croatia, str. 16. (January 2019) dostupno na https://datareportal.com/reports/digital-2022-croatia*

Daljnjom analizom podataka iz izvještaja marketinške agencija We Are Social, možemo utvrditi da u Republici Hrvatskoj društvena mreža Facebook ima 1,75 milijuna korisnika što je gotovo 43 % ukupne populacije, a ako uzmemo u obzir dobno ograničenje od 13 godina u Republici Hrvatskoj 49 % stanovništva koji to zakonski mogu koriste Facebook. Vidi Sliku 5.2.

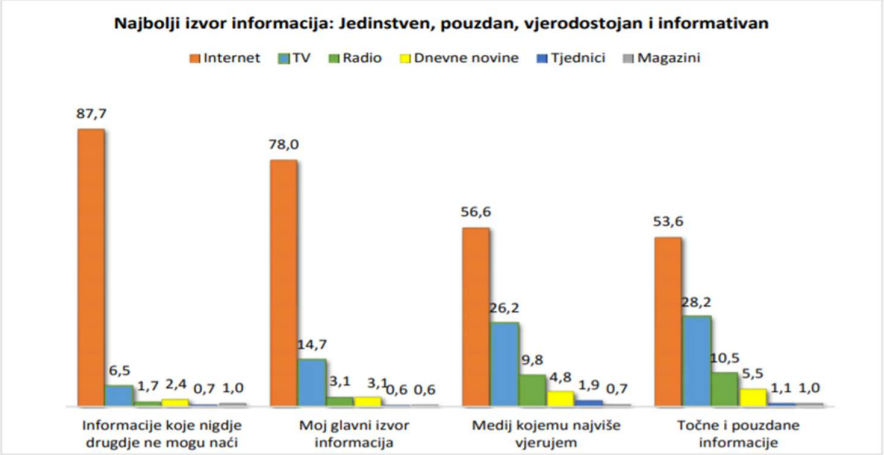
Slika 5.2. *Broj korisnika interneta i društvene mreže Facebook u Republici Hrvatskoj prema: Digital Global Statshot Report, Digital 2022 Croatia, str. 42. (January 2019) dostupno na https://datareportal.com/reports/digital-2022-croatia*

Iz podataka prikupljenih od strane marketinške agencije *We Are Social* možemo zaključiti da većina građana Republike Hrvatske koristi internet te je skoro polovica aktivna na društvenim mrežama. Također, istraživanje koje je nekoliko godina ranije obavila agencija Ipsos Connect o medijskim navikama građana u Republici Hrvatskoj ukazuje na to da je internet najkorišteniji medij prema učestalosti korištenja u odnosu na sve druge medije te 91% ispitanika koji su sudjelovali u istraživanju više puta dnevno koristi internet.



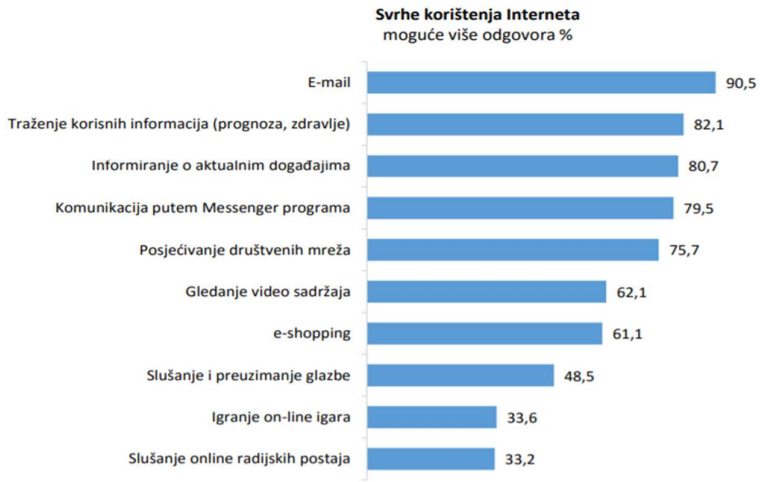
Graf 5.1. *Mediji po učestalosti korištenja u Republici Hrvatskoj prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 6. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Istraživanje također ukazuje na to da građani u Republici Hrvatskoj najviše vjeruju internetu te je internet glavni izvor informiranja (vidi Graf 5.2).



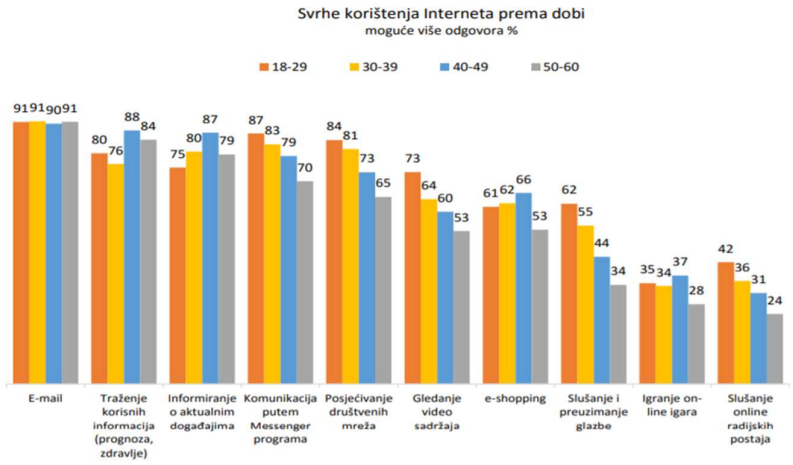
Graf 5.2. *Povjerenje korisnika prema medijima u Republici Hrvatskoj prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 8. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Kada je u pitanju svrha korištenja interneta, preko 90% ispitanika odgovorilo je da se njime koristi u svrhu komuniciranja putem e-maila, slijedi traženje informacija na internetu, komunikacija putem Messengera te posjećivanje društvenih mreža.



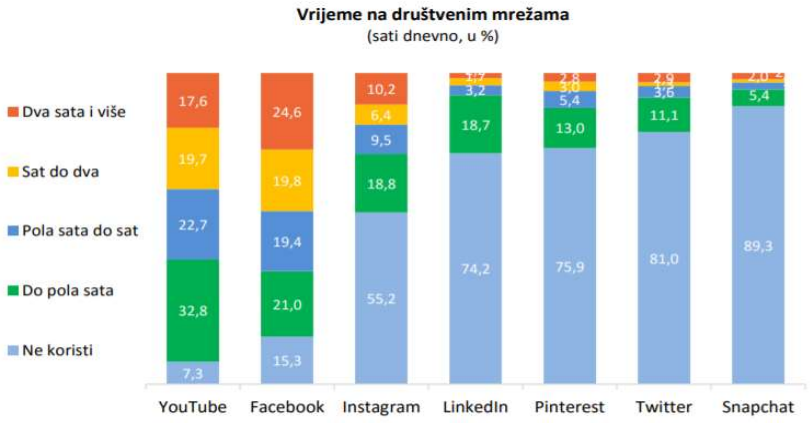
Graf 5.3. *Svrha korištenja interneta u Republici Hrvatskoj prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 16. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Ako promatramo korisnike po dobi i njihovim navikama, stariji češće internet koriste za potrebe kao što su servisne informacije i praćenje aktualnosti, dok mlađi internet više koriste za pristup društvenim mrežama, komunikaciju putem istih, gledanje videa i slušanje glazbe.



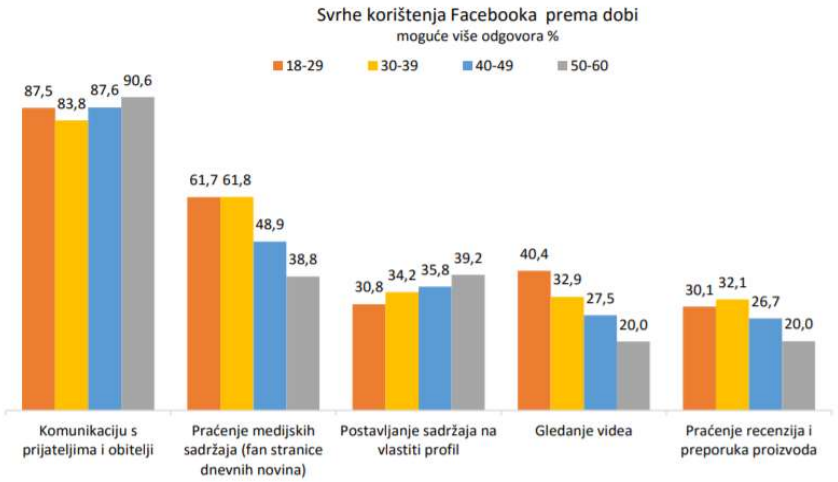
Graf 5.4. *Svrha korištenja interneta po dobnim kategorijama u Republici Hrvatskoj prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 17. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Kod postavljenog pitanja koliko vremena provodite na pojedinoj društvenoj mreži, prvo mjesto zauzima društvena mreža Facebook – 24,6% ispitanika provede više od dva sata na mreži te 19,8% sat do dva. Vidi Graf 5.5.



Graf 5.5. *Provedeno vrijeme na pojedinim društvenim mrežama prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 19. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Daljnje istraživanje otkrilo je svrhu korištenja Facebooka po dobi korisnika, pa tako korisnici stariji od 50 godina najčešće koriste Facebook za komunikaciju s prijateljima i rodbinom – njih 90,6% ispitanih, te postavljaju sadržaj na vlastiti profil – 39,2% ispitanih starijih od 50 postavljaju sadržaj na vlastiti profil. Mlađi ispitanici također najviše koriste Facebook za komunikaciju s prijateljima, ali više prate medije i recenzije proizvoda, u odnosu na starije. Vidi Graf 5.6.



Graf 5.6. *Svrha korištenja društvene mreže Facebook prema dobi prema Ipsos Connect, Medijske navike u Republici Hrvatskoj, str. 20. (ožujak 2019.), dostupno na https://showcase.24sata.hr/2019_hosted_creatives/medijske-navike-hr-2019.pdf*

Na temelju provedenog istraživanja agencije Ipsos Connect možemo zaključiti da je broj korisnika interneta i društvenih mreža u postotku približno sličan prosjeku korisnika u svijetu. Nadalje, neka druga istraživanjima ukazuju na to da su i razlozi korištenja interneta i društvenih mreža slični ili gotovo isti Republici Hrvatskoj kao i u ostatku svijeta. Jedino pitanje koje je u suprotnosti s nekim drugim rezultatima je povjerenje korisnika prema internetu kao mediju kojem se vjeruje. Naime, ovo istraživanje prikazuje internet kao medij kojem se najviše vjeruje kao izvoru informacija što je u suprotnosti s istraživanjem provedenim putem Eurobarometra (vidi poglavlje 4.3.) gdje se internetu kao mediju najmanje vjeruje, ali ga se i najviše koristi u traženju informacija. To nas dovodi do zaključka da korisnici u Republici Hrvatskoj više vjeruju internetu nego korisnici u ostatku EU-a.

5.2. Percepcija zaštite privatnosti korisnika interneta u Republici Hrvatskoj

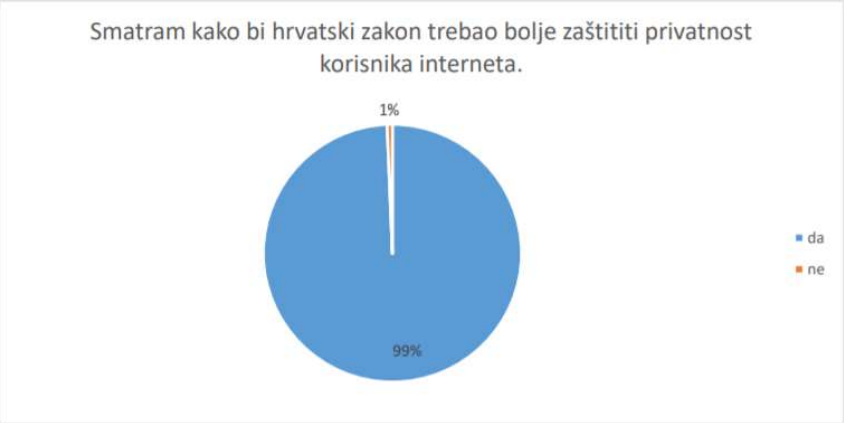
U Republici Hrvatskoj zakonska regulativa koja omogućuje pravo na privatnost korisnicima interneta je na sličnoj ili gotovo istoj razini kao u većini zemalja EU-a. Ona je iskazana kroz Ustav Republike Hrvatske, Zakon o elektroničkim komunikacijama, Opću uredbu o zaštiti podataka te kroz druge zakonske i podzakonske akte. Kakva je percepcija korisnika o zaštiti privatnosti korisnika interneta, poznavanje zakonodavnih akta te određeni stavovi i ponašanja prema zaštiti istih možemo iščitati iz istraživanja koje je proveo student Domagoj Justament za potrebe diplomskog rada.

Kako bi ispitao percepciju zaštite privatnosti korisnika interneta te njihovu svjesnost o razini zaštite privatnosti na internetu, proveo je istraživanje metodom ankete. S obzirom na to da se pojam zaštite privatnosti na internetu može odnositi na izrazito velik broj različitih web-stranica i servisa, odlučio se istražiti društvene mreže te internetske tražilice, odnosno usluge koje te tražilice pružaju. „Istraživanje je provedeno na slučajnom uzorku od 153 ispitanika, raspon godina ispitanika je između 18 i 65 godina od čega je 95 ženskog spola, 58 muškog spola. Kad je u pitanju obrazovanje, 28 ispitanika ima završenu srednju školu ili gimnaziju, 64 ispitanika su prvostupnici ili imaju završenu visoku školu, 27 ispitanika imaju završen diplomski studij, 30 ispitanika su magistri struke ili znanosti, te 4 ispitanika imaju doktorat.“[167] Ako sagledamo strukturu ispitanika po dobi, spolu i obrazovanju, pretpostavka je da rezultati daju realnu sliku koja se može primijeniti na većinu korisnika interneta u Republici Hrvatskoj. Za potrebe ovog rada iskoristit ćemo rezultate odgovora na anketna pitanja koji se odnose na zakonodavni okvir i društvene mreže. Kada je u pitanju zakonodavni okvir jedno od postavljenih pitanja je sljedeće: Smatram kako bi hrvatski zakon trebao bolje zaštititi privatnost korisnika interneta (vidi u nastavku Graf 5.7.).[168] „Rezultati pokazuju kako gotovo svi ispitanici (99%) smatraju da bi zakon Republike Hrvatske trebao kvalitetnije zaštititi njihovu privatnost.“[169] Ako rezultat primijenimo na sve korisnike interneta, možemo zaključiti da velika većina korisnika interneta u Republici Hrvatskoj smatra da zakonodavni okvir nije dobar te da bi se izmjenama i dopunama istoga povećala zaštita njihove privatnosti.

[167] Domagoj J., Zaštita privatnosti na internetu, str. 30. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view, stranica posjećena 16.3.2023

[168] ibid. str. 41.

[169] ibid. str. 41.

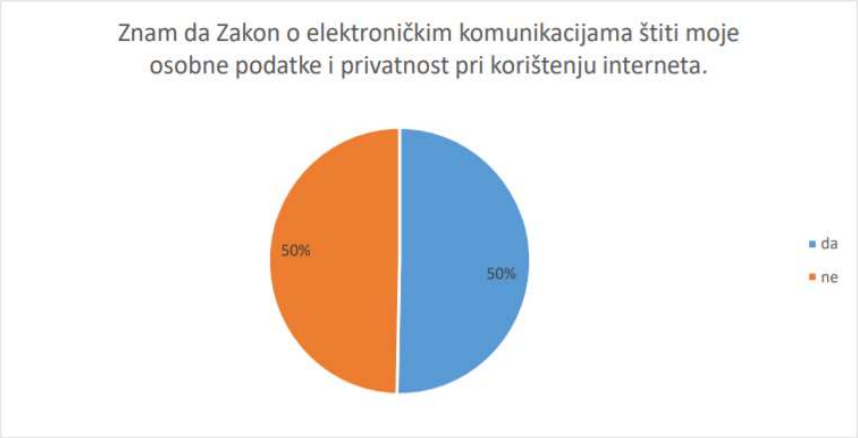


Graf 5.7. *Mišljenje o hrvatskoj zakonskoj regulativi zaštite privatnosti prema Domagoj J.,, Zaštita privatnosti na internetu, str. 41. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view*

Sljedeća postavljena pitanje su: Upoznat sam s postojanjem Agencije za zaštitu osobnih podataka (vidi Graf 5.8). i Znam da Zakon o električnim komunikacijama štiti moje osobne podatke i privatnost pri korištenju interneta (vidi Graf 5.9).[170]

Graf 5.8. *Svjesnost ispitanika o postojanju Agencije za zaštitu osobnih podataka prema Domagoj J., Zaštita privatnosti na internetu, str. 50. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view*

[170] ibid. str. 50.



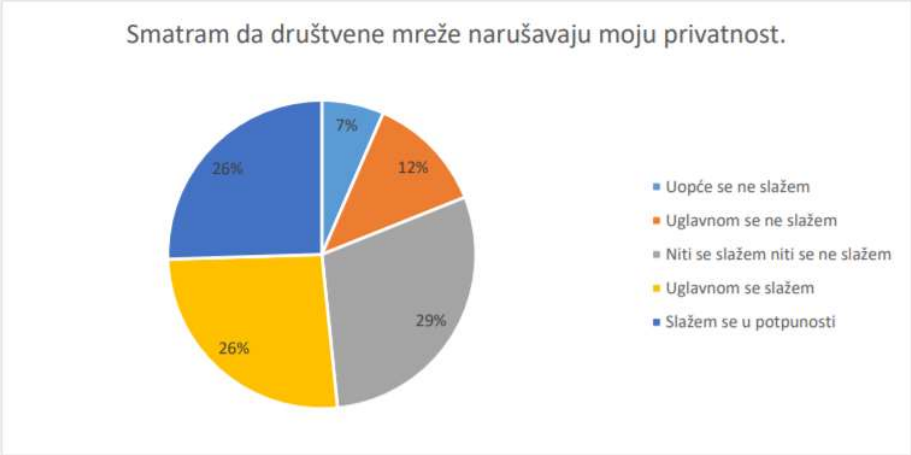
Graf 5.9. *Upoznatost ispitanika sa Zakonom o elektroničkim komunikacijama prema Domagoj J., Zaštita privatnosti na internetu, str. 48. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view*

U oba slučaja, upoznatost s postojanjem Agencije za zaštitu osobnih podataka i poznavanje odredbi Zakona o elektroničkim komunikacijama, 50% ispitanika odgovara potvrdno.[171] Što nam ukazuje na to da rezultati nisu porazni, ali nisu ni dobri ako uzmemo obzir da je u istom ispitivanju velika većina ispitanika – njih 93% – misli za sebe da su medijski pismeni.[172]

Možemo zaključiti, s obzirom na dobiveni rezultat i trendove današnjeg društva prilikom korištenje usluga na internetu te prijetnji spram privatnosti putem istih, da treba više raditi na medijskoj pismenosti korisnika i upoznavanju s mogućnostima samozaštite, zakonima, zakonskim odredbama i instancijama koji nas štite.

Nadalje u anketi je postavljena tvrdnja: Smatram da društvene mreže narušavaju moju privatnost (vidi Graf 5.10.). Većina ispitanika – njih 52% – smatra da je njihova privatnost uglavnom ili u potpunosti narušena od strane društvenih mreže, dok 19% ispitanika smatra da im privatnost uopće ili uglavnom nije narušena od strane društvenih mreža.

[171] ibid. str. 48.
[172] ibid. str. 39.

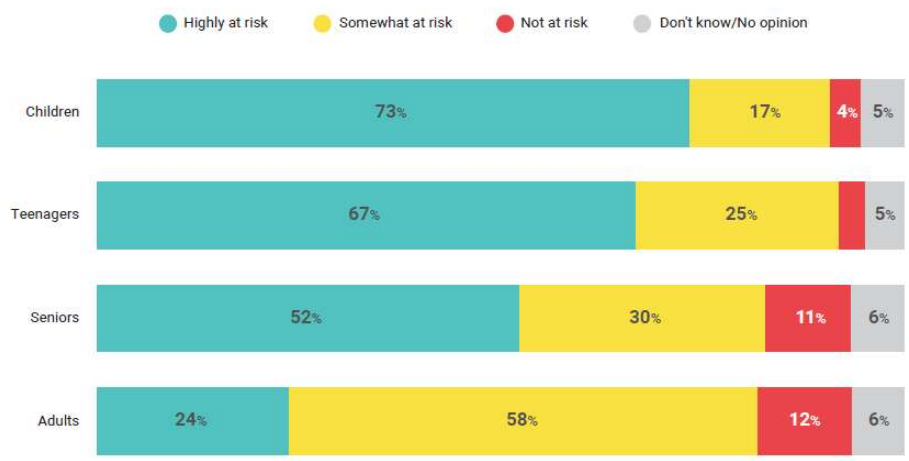


Graf 5.10. *Mišljenje ispitanika o narušavanju privatnosti od strane društvenih mreža prema Domagoj J., Zaštita privatnosti na internetu, str. 31. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view*

Dok na postavljenu tvrdnju o povredi privatnosti od strane usluge internetske tražilice 54% ispitanika smatra da je njihova privatnost ugrožena, a tek 1% smatra da uopće nisu ugroženi.[173] Možemo zaključiti da je većina korisnika svjesna da korištenje usluga društvenih mreža i općenito interneta ugrožava njihovu privatnost.

Do sličnih rezultata dolazi i kompanija Morning Consult koja je provela istraživanja u Sjedinjenim Američkim Državama i objavila studiju pod nazivom *„Studija o zabrinutosti za privatnost i sigurnost na društvenim medijima 2019“* (engl. *2019 Study on Social Media Privacy and Security Concerns*). Istraživanje je provedeno na uzorku od 2200 odraslih osoba.[78] Na pitanje vjeruju li da je njihova privatnost i sigurnost ugrožena na društvenim mrežama većina je odgovorila potvrdno (vidi Graf 5.11.).

[173] ibid. str. 32.



***Graf 5.11**. Mišljenje ispitanika o razini ugroze privatnosti i sigurnost korisnika društvenih mreža po dobnim skupinama prema IDX, 2019 Study on Social Media Privacy and Security Concerns, str. 11, (2019) https://www.idx.us/knowledge-center/2019-study-on-social-media-privacy-and-security-concerns*

Na temelju dobivenih rezultata (vidi Graf 5.11.) vidimo da su građani Sjedinjenih Američkih Država posebno zabrinuti za privatnost i sigurnost djece i tinejdžera, a kada su u pitanju odrasli i starije osobe ta zabrinutost je nešto niža.[174] Postavljeno pitanje u ovoj anketi formulirano je na nešto drugačiji način nego u anketi studenta Domagoja Justamenta pa se ni rezultati ne mogu u potpunosti uspoređivati. No, na temelju dobivenih rezultata možemo zaključiti da je većina korisnika u Republici Hrvatskoj i Sjedinjenim Američkim Državama svjesna da korištenjem usluga društvenih mreža može biti ugrožena njihova privatnost, a samim time i sigurnost. Nadalje, u anketi studenta Domagoja Justamenta postavlja se tvrdnja: Tijekom kreiranja računa na društvenim mrežama uvijek pažljivo pročitam uvjete korištenja (vidi Graf 5.12.).[175]

[174] IDX, 2019 Study on Social Media Privacy and Security Concerns, str.11, (2019) https://www.idx.us/knowledge-center/2019-study-on-social-media-privacy-and-security-concerns, stranica posjećena 20.9.2022

[175] Domagoj J., Zaštita privatnosti na internetu, str. 41. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view, stranica posjećena 16.3.2023

***Graf 5.12**. Navika ispitanika o čitanju uvjeta korištenja prilikom kreiranja računa na društvenim mrežama prema Domagoj J., Zaštita privatnosti na internetu, str. 31. Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view*

Iz rezultata vidimo da samo 14% ispitanika djelomično ili u potpunosti pročita upute za korištenje. Dobiveni rezultati ukazuju da korisnici nisu zainteresirani čitanje uputa ili su im nejasne i kompliciranе za čitanje čime vjerojatno ostaju uskraćeni za određena znanja o zaštiti privatnosti koje im nude davatelji usluga društvenih mreža prilikom kreiranja profila i korištenja usluga, premda je u istom ispitivanju većina ispitanika – njih 93% – odgovorila da je upoznata s mogućnošću uključivanja određenih opcija za zaštitu privatnosti.[176] Iz toga možemo pretpostaviti da, bez obzira na to što većina ispitanika ne čita upute od strane davatelja usluga, ipak je upoznata s mogućnošću zaštite privatnosti temeljem alata koje omogućavaju davatelji usluga te ih vjerojatno jedan dio korisnika i koristi.

Na temelju cjelokupne ankete možemo zaključiti da većina korisnika u Republici Hrvatskoj misli da ih zakoni prilikom korištenja usluga društvenih mreža i interneta općenito trebaju štititi više i bolje te ih treba izmijeniti i dopuniti. Unatoč tome dobar dio ispitanika ne poznaje o kojim se zakonima i institucijama radi te ne pročita ni uvjete korištenja prilikom kreiranja profila na društvenim mrežama. Nadalje, velika većina smatra da je njihova privatnost prilikom korištenja usluga društvenih mreža i općenito interneta ugrožena. Do sličnih zaključaka dolaze i autori *Studije o zabrinutosti za privatnost i sigurnost na društvenim medijima 2019.* Zaključuju da postoji velika zabrinutost među Amerikancima za privatnost i sigurnost korisnika prilikom

[176] ibid. str. 35.

korištenje društvenih mreža. „Mnogi Amerikanci svjesni opasnosti i najčešćih prijetnji koje su moguće putem društvenih mreža te žele da im se omoguće rješenja koja će tu opasnost i njihovu zabrinutost svesti na minimum. Međutim, samo mali dio Amerikanaca je osviješten i koristi mogućnosti koje trenutno imaju na raspolaganju kako bi smanjili vlastitu zabrinutosti za privatnost i sigurnost prilikom korištenja usluga društvenih mreža.“[177]

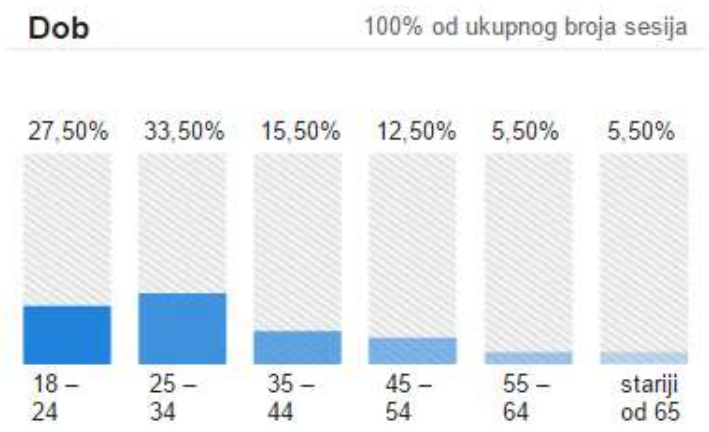
Na temelju iskustava i stavova korisnika u Hrvatskoj i Sjedinjenim Američkim Državama možemo reći da je stav korisnika u Republici Hrvatskoj jako sličan stavovima korisnika u Americi te se vjerojatno može primijeniti na cijeli svijet. Stoga možemo zaključiti da su korisnici usluga društvenih mreža i općenito interneta u Republici Hrvatskoj kao i u cijelom svijetu zabrinuti za svoju privatnost, a samim time i sigurnost. Oni traže izmjene zakonodavnih okvira, ali istovremeno jedan dobar dio njih ne koristi ni trenutne alate i mogućnosti kako bi se bolje zaštitili.

5.3. Najčešće prijetnje privatnosti korisnika interneta

Hrvatska regulatorna agencija za mrežne djelatnosti i Fakultet elektrotehnike i računarstva – FER Sveučilišta u Zagrebu kroz znanstveni su projekt POGLED U BUDUĆNOST – 2020. izradili aplikaciju „Kalkulator privatnosti“ kojoj korisnici mogu pristupiti na http://privatnost.hakom.hr/index.php. Kalkulator privatnosti je informativno-edukativna aplikacija kojoj korisnici mogu pristupiti i unosom određenih parametara u aplikaciju. Kalkulator procjenjuje kolika je vjerojatnost ugroze njihove privatnosti, ukoliko njihovi osobni podatci postanu dostupni zlonamjernom napadaču. Prikazana vrijednost povezuje se sa scenarijem prevare koji se dogodio u stvarnom životu, a koji je prikazan u obliku stripa. Svaki korisnik Kalkulatora nakon pregledanog scenarija ima mogućnost ostaviti informaciju je li mu se takva prevara dogodila.

Rezultati za razdoblje između 12. studenoga i 12. prosinca 2016. godine pokazali su da je aplikaciju posjetilo 518 korisnika od čega su 70% novi korisnici. Kada je u pitanju starosna dob, možemo primijetiti da je najveći broj korisnika između 18 i 24 godine starosti. Graf 5.13. prikazuje postotak posjetitelja Kalkulatora podijeljen po starosnoj dobi.

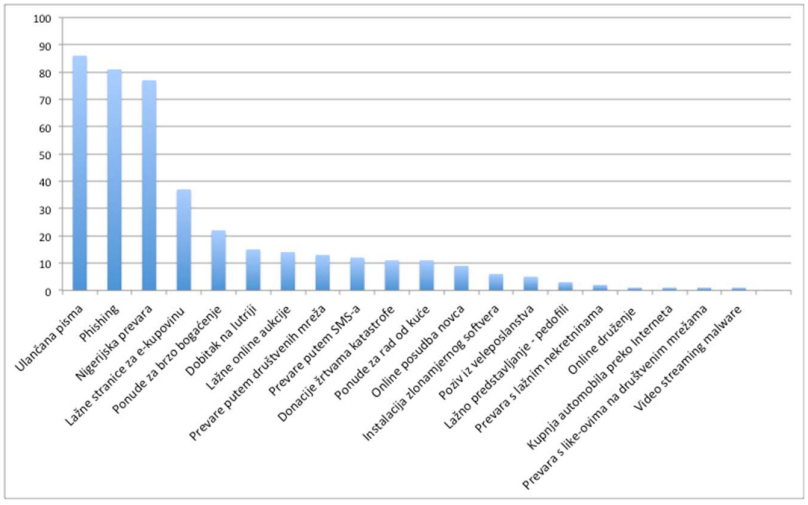
[177] IDX, 2019 Study on Social Media Privacy and Security Concerns, str. 13. (2019) https://www.idx.us/knowledge-center/2019-study-on-social-media-privacy-and-security-concerns, stranica posjećena 17.5.2023



Graf 5.13. *Postotak posjetitelja Kalkulatora privatnosti podijeljen po starosnoj dobi, prema autoru rada podatci prikupljeni na http://privatnost.hakom.hr/index.php*

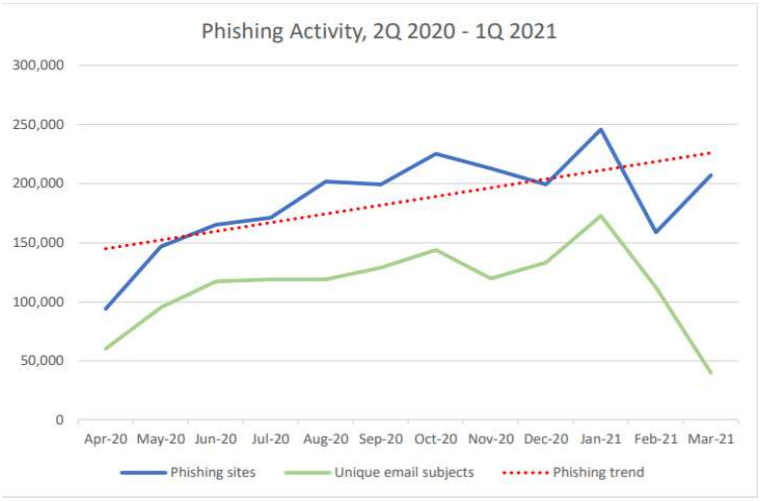
Prikupljeni podatci o prijevarama prikazani su na Grafu 5.14. tri najpopularnije prevare su redom:

- ulančana pisma
- *Phishing* poruke i stranice
- nigerijska prevara



Graf 5.14. *Broj korisnika Kalkulatora koji su se susreli s povredom privatnosti na internetu prema autoru rada podatci prikupljeni na http://privatnost.hakom.hr/index.php*

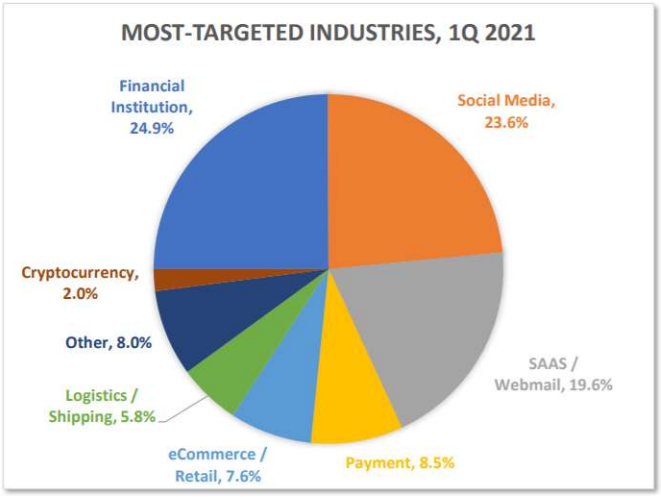
Ulančana pisma i prevare tipa *nigerijska prevara* su uobičajeno najčešće vrste prevara na internetu. Međutim, ovako visok broj prijava *phishing* poruka, odnosno stranica ukazuje na to da ovakve vrste prevara postaju sve popularnije na području Republike Hrvatske, što je i potvrđeno sve češćim lažiranjem stranica javno dostupnih servisa kao što su *PayPal*, *Facebook*, ali i neke banke. Napadi prevarom *phishing* u Republici Hrvatskoj su zabrinjavajući ali ne i iznenađujući s obzirom da trend rasta *phishing* prevara u svijetu (vidi u nastavku Graf 5.15.). Graf 5.15. prikazuje konstantan ukupan rast napada od drugog kvartala 2020. godine i prvi kvartal 2021. godine.[178]



Graf 5.15. *Broj zabilježenih phishing napada u svijetu 2Q 2020. – 1Q 2021. prema APWG, Phishing Activity Trends Report, str. 4. (8 June 2021) dostupno na https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf*

Nadalje, na temelju izvještaja APWG (*Anti-Phishing Working Group*), globalnog udruženja za borbu protiv *phishinga*, možemo vidjeti da su napadi *phishinga* putem lažiranja web-stranica u stalnom porastu kao i sam trend prevare *phishinga* (Graf 5.16.).[179] Koliko su kriminalne skupine napredne te u svakoj novoj poslovnoj aktivnosti na internetu pronađu prostor i za vlastite kriminalne aktivnosti, možemo vidjeti iz Grafa 5.15.

[178] APWG, Phishing Activity Trends Report, str. 4. (8 June 2021) dostupno na https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf, stranica posjećena 13.5.2023
[179] Ibid. str. 5.



Graf 5.16. *Phishing napadi u svijetu putem raznih načina u 1Q 2021. prema APWG, Phishing Activity Trends Report, str. 5. (8 June 2021) dostupno na https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf*

Na temelju Grafa 5.15. možemo vidjeti da su najčešći zabilježeni *phishing* napadi bili vezani za financijske institucije – 24.9%, na drugom mjesto u 1Q 2021. godine nalaze se društvene mreže s udjelom od 23.6%, zatim slijede napadi putem webmaila – 19.6% ali se po prvi put sa značajnim udjelom pojavljuju i napadi *phishinga* uključujući internetske stranice kriptovaluta.[180] Na temelju izvještaja APWG-a i podataka iz kalkulatora privatnosti možemo zaključiti da je *phishing* jedna od najpopularnijih prevara u Republici Hrvatskoj i svijetu koja raste usporedno s brojem korisnika i brojem usluga. Nadalje, *phishing* je najzastupljeniji ali je samo jedna od prevara. Pregledom Grafa 5.14. možemo zaključiti da su i druge prevare, za koje korisnik može odabrati scenarij unutar aplikacije Kalkulator privatnosti, zastupljene na području Republike Hrvatske, a mnoge od njih upravo se događaju na društvenim mrežama i internetu te pokazuju da trenutno stanje nije nimalo bezazleno. Na ozbiljnost trenutnog stanja upozorava nas izvještaj Ministarstva unutarnjih poslova za 2019. godinu, (vidi poglavlje 4.4. tablica 1.) te pregled osnovnih pokazatelja kriminaliteta u Republici Hrvatskoj iz kojeg možemo iščitati da je kibernetički kriminalitet u 2019. odnosu na 2018. godinu porastao za 87%. Svi navedeni podatci, izvještaj iz aplikacije Kalkulator privatnosti, izvještaj APWG-a i tablica osnovnih pokazatelja kriminaliteta u Republici Hrvatskoj ukazuju na to da je potrebna što

[180] ibid. str. 5.

hitnija izmjena zakonodavnih odredbi, ali i edukacija korisnika kako bi se zaštitila njihova privatnost, a samim time i sigurnost na internetu.

6. ZAKLJUČAK

Svjedoci smo sve bržeg razvoja interneta i sve većeg broja njegovih korisnika, kao i usluga koje se na njemu pružaju, što za posljedicu donosi brojne prednosti, ali i sigurnosne rizike. Stoga pitanje zaštite privatnosti na internetu postaje od sve veće važnosti. Podatci o korisniku prikupljaju se već samim njegovim pristupom internetu, traženjem informacija na internetu ili pregledavanjem internetskih sadržaja (prikuplja ih pružatelj usluge, web-preglednik, web-pretraživač, podatci se pohranjuju u kolačićima i sl.). Ti se podatci najčešće koriste u marketinške svrhe, ali ipak postoji mogućnost da dospiju u ruke zlonamjernim korisnicima i da se zloupotrijebe.

Pojavom društvenih mreža dodatno se povećala mogućnost povrede privatnosti korisnika interneta i društvenih mreža, dijelom zbog neopreznosti korisnika koji iz udobnosti svog doma mogu komunicirati, pretraživati, stjecati nova znanja, poslovati, prikazivati sebe kakvima žele u virtualnom svijetu naizgled potpuno sigurni, a dijelom zbog toga što su zlonamjerni napadači jako brzo prepoznali slabosti okruženja društvenih mreža te ih često koriste za prikupljanje podataka koje iskorištavaju za ostvarivanje svojih ciljeva u provođenju svojih namjera koje mogu piti štetne za pojedinca i cjelokupno društvo. Nadalje, neopreznost korisnika na neki je način poticana od samih davatelja usluga društvenih mreža nejasnim i nedovoljnim uputama i upozorenjima za korisnike, dok istodobno zahtijevaju od korisnika da daju privolu za raspolaganje njihovim osobnim podatcima u marketinške i druge svrhe radi ostvarivanja vlastite financijske koristi. Upravo su davatelji usluga društvenih mreža ili druge kompanije na platformi društvenih mreža u nekoliko slučajeva neovlašteno prikupljali i koristili privatne podatke korisnika, što je i potvrđeno sudskim presudama.

Problemi s opasnošću ugroze privatnosti korisnika društvenih mreža prepoznati su gotovo od samih početaka od radnih grupa koje se bave tom problematikom. Tako je ENISA još 2007. godine donijela smjernice i preporuke za davatelje usluga i regulatorna tijela država kako bi se povećala zaštita korisnika društvenih mreža, no nedovoljno je ili malo učinjeno po tom pitanju. Zakonske regulative koje su donesene kako bi zaštitile pravo na privatnost korisnika interneta, samim time i korisnika društvenih mreža gotovo da ne obuhvaćaju društvene mreže, a kada su u pitanju korisnici interneta u širem smislu pokazale su se nedovoljnima i neučinkovitima. Naime, zakoni se donose na razini pojedinih država i bitno se razlikuju od države do države. Nešto što je kažnjivo u jednoj državi, nije u drugoj i obrnuto, a internet je globalna mreža

dostupna svima odsvuda. Nadalje, usluge na internetu i društvenim mrežama puno se brže razvijaju od intervencija u zakonodavne okvire te se često stječe dojam da su zakonodavna tijela troma i nezainteresirana pa imamo situaciju da se naizgled iste usluge, OTT-usluge i SMS, regulatorno potpuno drugačije tretiraju.

A pravo na privatnost je univerzalno, temeljno pravo građana zajamčeno Poveljom o temeljnim pravima i Općom uredbom o zaštiti podataka Europske unije, Ustavom Republike Hrvatske i domaćim zakonodavstvom te relevantnim konvencijama Ujedinjenih naroda i Vijeća Europe koje su postale dijelom našeg nacionalnog zakonodavstva. Istovremeno, nagle i brze društvene, znanstvene i tehnološke promjene zahtijevaju njihovo stalno praćenje, te preispitivanje i prilagođavanje pravnog okvira kako na nacionalnom tako i globalnom planu. Međutim, odgovor na cjelovitu zaštitu privatnosti ne treba tražiti samo u zakonodavstvu, ma koliko ono bilo važno, već je nužno permanentno educirati korisnike društvenih mreža i drugih internetskih servisa o tome kako mogu zaštititi svoju privatnost i postići zadovoljavajući stupanj sigurnosti na internetu.

LITERATURA

[1] Dragičević D., Privatnost u virtualnom svijetu, str. 615-616., Zbornik PFZ, 51(34), Zagreb, (Ožujak 2001)

[2] International website that features up to date World Internet Users, dostupno na https://www.internetworldstats.com/stats.htm, stranica posjećena 22.5.2023.

[3] Terms of Service, Facebook Ireland Limited, dostupno na https://www.facebook.com/legal/terms, stranica posjećena 9.5.2022.

[4] Most popular social networks worldwide as of January 2023, dostupno na https://www.statista.com/statistics/272014/global-social-neusers/, stranica posjećena 24.6.2023.

[5] Arnold R, Hildebrandt C., Kroon P., Taş S. The Economic and Societal Value of Rich Interaction Applications (RIAs)., WIK - Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef (May 2017).

[6] Demetriou S., Merrill W., Yang W., Zhang A., Gunter C.A., Free for All! Assessing User Data Exposure to Advertising Libraries on Android, ISOC Network and Distributed System Security 2016, San Diego, (February 2016)

[7] Berbers Y., Hildebrandt M., Joos Vandewalle J., Privacy in an age of the Internet, social networks and Big Dana, str. 48., Royal Flemish Academy of Belgium for Science and the Arts, Brussel, 2018.

[8] Data Protection Africa, ALT Advisory, June 2023 dostupno na: https://dataprotection.africa stranica posjećena 26.07.2023.

[9] Prinsloo P., Kaliisa R., Data privacy on the African continent: Opportunities, challenges and implications for learning analytics, str. 5., British Journal of Educational Technology, 13.4.2022.

[10] Maggie Fick, Alexis Akwagyiram, In Africa, scant data protection leaves internet users exposed. Reuters. (April 4. 2018), dostupno na https://www.reuters.com/article/us-facebook-africa-idUSKCN1HB1SZ, stranica posjećena 24.5.2023.

[11] Bratoljub Klaić, Rječnik stranih riječi, Nakladni zavod Matice hrvatske, (Zagreb, 2004)

[12] Dragičević, D., Gumzej, N., Jurić M., Katulić, T., Lisičar, H., Pravna informatika i pravo informacijskih tehnologija, Narodne novine, (Zagreb, 2015)

[13] Brandeis L. D., Warren, Jr. S. D., THE RIGHT TO PRIVACY, Harvard Law Review, V. IV, No. 5, (December 1890). dostupno na https://faculty.uml.edu//sgallagher/Brandeisprivacy.htm, stranica posjećena 16.3.2023.

[14] Pavuna A., Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova, (Zagreb, 2019), dostupno na https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:868, stranica posjećena 17.6.2023.

[15] The European Data Protection Supervisor, Data Protection, dostupno na https://edps.europa.eu/data-protection/data-protection_en, stranica posjećena 05.7.2023.

[16] Priručnik o europskom zakonodavstvu o zaštiti podataka, dostupno na https://www.echr.coe.int/documents/d/echr/handbook_data_protection_hrv, 04.7.2023

[17] Odluka o objavi Opće deklaracije o ljudskim pravima NN 12/2009, dostupno na https://narodne-novine.nn.hr/clanci/medunarodni/2009_11_12_143.html, stranica posjećena 22.11.2022.

[18] Konvenciju za zaštitu ljudskih prava i temeljnih sloboda; protokoli broj 1, 4, 6 i 7. NN 6/1999

[19] Povelje Europske unije o temeljnim pravima. dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P, stranica posjećena 10.1.2023.

[20] Guarda P., Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks, (December 2009). dostupno na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517449, stranica posjećena 14.7.2022.

[21] Davidson J., Livingstone S., Jenkins S., Dr Gekoski A., Dr Choak C., Ike T., Phillips K., Adult Online Hate, Harassment and Abuse: A rapid evidence assessment, UK Council for Internet Safety (UK, June 2019), dostupno na https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf, stranica posjećena 12.1.2023

[22] Kazneni zakon, NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19

[23] Ustav Republike Hrvatske, NN br. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/1

[24] Klein E., Mark Zuckerberg on Facebook's hardest year, and what comes next. Vox. (Apr 2, 2018), dostupno na https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge, stranica posjećena 23.11.2022

[25] Data usage rules, Facebook Ireland Limited, dostupno na https://www.facebook.com/privacy/explanation/, stranica posjećena 18.1.2023.

[26] Agencija za zaštitu osobnih podataka, Osnovne informacije za organizacije, (pro 14, 2020) dostupno na https://azop.hr/osnovne-informacije-za-organizacije/, stranica posjećena 10.7.2023

[27] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka),SL L 119/1, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, stranica posjećena 11.2.2023

[28] Cadwalladr C., Graham-Harrison E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Guardian. (17. Mar 2018) https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, stranica posjećena 18.4.2020. i 30.04.2023.

[29] House of Representatives, Committee on Energy and Commerce, FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DANA. D.C., (Washington D.C. APRIL 11, 2018), dostupno na https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Transcript-20180411.pdf, stranica posjećena 12.6.2023

[30] Lomas N., Cambridge Analytica's parent pleads guilty to breaking UK data law, TechCrunch, (January 9, 2019), dostupno na https://techcrunch.com/2019/01/09/cambridge-analyticas-parent-pleads-guilty-to-breaking-uk-data-law/, stranica posjećena 17.6.2023.

[31]] UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA, Case No. 19-cv-2184; COMPLAINT FOR CIVIL PENALTIES, INJUNCTION, AND OTHER RELIEF. UNITED STATES OF AMERICA v. FACEBOOK, Inc., (Washington D.C. July 24, 2019), dostupno na https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf, stranica posjećena 25.5.2023.

[32] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka),SL L 119/1, dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679, stranica posjećena 11.2.2023.

[33] Mišljenja Agencije za zaštitu osobnih podataka, Obrada osobnih podataka učenika sukladno Općoj uredbi. dostupno na https://azop.hr/obrada-osobnih-podataka-u-odgojno-obrazovnom-sektoru/, stranica posjećena 12.1.2023.

[34] Zakon o provedbi opće uredbe o zaštiti podataka, NN br. 42/18

[35] Zakona o elektroničkim komunikacijama, NN br. 76/08.

[36] Kubiček K., Merane J., Cotrini C., Stremitzer A., Bechtold S., Basin D., Checking Websites' GDPR Consent Compliance for Marketing Emails, Proceedings on Privacy Enhancing Technologies 2022 (Sydney, July 2022)

[37] Tulek Z., Arnell L., Facebook Eavesdropping Through the Microphone for Marketing Purpose, BTH Blekinge Institute of Technology, Karlskrona, Sweden, (Karlskrona, May 2019), dostupno na https://www.diva-portal.org/smash/get/diva2:1332194/FULLTEXT0,1.pdf, stranica posjećena 12.2.2023.

[38] Data usage rules, Facebook Ireland Limited. https://www.facebook.com/about/privacy/update, stranica posjećena 17.6.2022.

[39] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća, (12. srpnja 2002), dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058, stranica posjećena 17.1.2023.

[40] Direktiva 2006/24/EZ Europskog parlamenta i Vijeća (15. ožujka 2006). dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024, stranica posjećena 10.8.2023.

[41] Europski parlament. Priopćenje za tisak - Reforma zaštite podataka - EP odobrio nova pravila. (14. ožujka 2016). dostupno na http://www.europarl.europa.eu/news/hr/news-room/20160407IPR21776/reforma-za%C5%A1tite-podataka-ep-odobrio-nova-pravila, stranica posjećena 12.1.2023.

[42] Direktiva 2009/136/EZ Europskog parlamenta i Vijeća. (25.studenoga 2009). dostupno na http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32009L0136, stranica posjećena 17.1.2023

[43] European Commission. Public consultation evaluation and review ePrivacy directive. dostupno na https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive, stranica posjećena 17.1.2017.

[44] Upton E., The future of the e-privacy directive: now is the time to have your say. (April 2016), dostupno na https://www.twobirds.com/en/insights/2016/uk/the-future-of-the-e-privacy-directive, stranica posjećena 17.1.2023

[45] European Commission. Proposal for an ePrivacy Regulation. dostupno na https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, stranica posjećena 5.2.2023.

[46] European Court of Justice. JUDGMENT OF THE COURT (Grand Chamber). In Joined Cases C-293/12 and C-594/12, (8 April 2014), dostupno na https://curia.europa.eu/juris/document/document.jsf?mode=lst&pageIndex=0&docid=150642&part=1&doclang=EN&text=&dir=&occ=first&cid=10349858, stranica posjećena 5.2.2023.

[47] Leksikografski zavod Miroslav Krleža, Hrvatska enciklopedija, mrežno izdanje, dostupno na http://www.enciklopedija.hr/natuknica.aspx?id=16328, stranica posjećena 4.12. 2022.

[48] Rainie L., Wellman B., Networked: The New Social Operating System, Massachusetts Institute of Technology MIT, (Cambridge, 2012)

[49] Cutillo L. A., Mark Manulis M., Strufe T, Security and privacy in online social networks, Eurecom, (Sophia Antipolis, October 2010

[50] Boyd D.M., Ellison N. B., Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication (October 2007), dostupno na https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1083-6101.2007.00393.x, stranica posjećena 3.11.2022.

[51] Labaratorij za sustave i signale, Informacijska sigurnost. Privatnost na Internetu. (Jan 14, 2014), dostupno na https://www.scribd.com/doc/199491060/lss-pubdoc-2010-10-002, stranica posjećena 22.11.2022.

[52] Digital Global Statshot Report, dostupno na Digital Global Statshot Report, dostupno na https://datareportal.com/reports/digital-2023-april-global-statshot, stranica posjećena 10.7.2023.

[53] Gross R., Acquisti A., Information Revelation and Privacy in Online Social Networks, Workshop on Privacy in the Electronic Society, WPES 2005, (Alexandria, VA, USA, November 2005)

[54]. Alyson L. Young A.L., Quan-Haase A., Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook, Conference on Communities and Technologies, C&T 2009 (University Park, PA, USA, June 2009)

[55]. Johnson B., Privacy no longer a social norm, says Facebook founder, The Gurdian. (Jan 2010), dostupno na https://www.theguardian.com/technology/2010/jan/11/facebook-privacy, stranica posjećena 15.11.2016. i 3.5.2023

[56] Jamal, A., Coughlan, J., & Kamal, M. Mining social network data for personalisation and privacy concerns: a case study of Facebook's Beacon, International Journal of Business Information Systems, 13(2), 173-198. (2013)

[57] The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), Facebook (2008-2010), dostupno na https://cippic.ca/en/Facebook, stranica posjećena 17.12.2022.

[58] Gu L., Kropotov V., Yarochkin F., The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public. (June 3, 2017), dostupno na https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.247008519.2007575061.1601718271-287436439.1592572077, stranica posjećena 4. i 12.10.2020.

[59] Guess A., Nyha B., Reifler J., Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign, (January 9, 2018), dostupno na https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf, stranica posjećena 13.10.2022

[60] Europska komisija (priopćenje za tisak), Borba protiv dezinformiranja na internetu: Komisija predlaže uvođenje kodeksa prakse na razini EU-a, dostupno na https://ec.europa.eu/commission/presscorner/detail/hr/IP_18_3370, stranica posjećena 16.10.2022.

[61] Kazneni zakon, NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19

[62] NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI, NN br. 108/2015

[63] Beth Hendricks, How Social Networks are Used in Cybercrime dostupno na https://study.com/academy/lesson/how-social-networks-are-used-in-cybercrime.html, stranica posjećena 18.14.2022

[64] Nacionalni CERT, dostupno na https://www.cert.hr/socijalni_inzenjering/, stranica posjećena 18.10.2022.

[65] Bisson D., Global Cost of Cybercrime Exceeded $600 Billion in 2017, Report Estimates, (February 23, 2018), dostupno na https://securityintelligence.com/news/global-cost-of-cybercrime-exceeded-600-billion-in-2017-report-estimates/, stranica posjećena 16.5.2023.

[66] Irshad S., Soomro T.R., Identity Theft and Social Media, IJCSNS International Journal of Computer Science and Network Security (February 2018), 43-55.

[67] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, NN108/2015

[68] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN br. 64/18

[69] Acquisti A., Carrara E., Stutzman F., Callas J., Schimmer K., Nadjm M., Gorge M., Ellison N., King P., Gross R., Mellon C., Hewlett-Packard H., Security Issues and Recommendations for Online Social Networks. ENISA, (October 2007), dostupno na https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks, stranica posjećena 17.1.2023.

[70] International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services, Rome Memorandum, (Rome, 4 March 2008), dostupno na https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/berlin-group/2008/2008-Rome_Memorandum-en.pdf 13.5.2023.

[71] Domagoj J., Zaštita privatnosti na internetu, Repozitorij Fakulteta hrvatskih studija , Zagreb 2017, dostupno na https://repozitorij.hrstud.unizg.hr/islandora/object/hrstud%3A1036/datastream/PDF/view, stranica posjećena 16.3.2023

[72] IDX, 2019 Study on Social Media Privacy and Security Concerns, (2019) https://www.idx.us/knowledge-center/2019-study-on-social-media-privacy-and-security-concerns, stranica posjećena 20.9.2022

[73] APWG, Phishing Activity Trends Report, (8 June 2021) dostupno na https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf, stranica posjećena 13.5.2023

POPIS GRAFOVA

POPIS SLIKA

POPIS TABLICA

ŽIVOTOPIS

Luka Delonga rođen je 16. travnja 1976. u Sinju gdje je završio Tehničku i industrijsku školu Ruđer Bošković, smjer „Strojarski tehničar opći“. Diplomirao je 2010. godine na Fakultetu prometnih znanosti Sveučilišta u Zagrebu, smjer Pošta i telekomunikacije s temom „Utjecaj elektromagnetskog zračenja na zdravlje čovjeka i okoliš“. Od 2009. do 2011. godine radio je u COM GROUP d.o.o., na poziciji Regionalni koordinator, na poslovima implementacije naplate parkinga putem SMS-a, te implementaciji sustava upravljanja prometom u mirovanju na daljinu. Od 2012. do 2014. godine bio je zaposlen u ACNielsen d.o.o., na poziciji database operator, na poslovima obrada i analiza prikupljenih podataka u svrhu analize tržišta. Od 2014. zaposlen je u Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM), u početku u Odjelu komunikacijskih mreža i usluga, na poziciji Stručnjaka za komunikacijske usluge, a od 2019. godine u Odjelu infrastrukture, kao viši specijalist te zamjenik rukovoditelja odjela. Aktivno je sudjelovao na više seminara i konferencija te je koautor nekoliko radova koji su predstavljeni na međunarodnim konferencijama.

BIOGRAPHY

Luka Delonga was born on April 16, 1976 in Sinj where he graduated from the Ruđer Bošković Technical and Industrial School, majoring in "General Mechanical Technician". He graduated in 2010 from the Faculty of Transport and Traffic Sciences of the University in Zagreb, majoring in Post and Telecommunications with the thesis "The impact of electromagnetic radiation on human health and the environment". From 2009 to 2011 he worked in COM GROUP d.o.o., in the position of Regional Coordinator, on the implementation of parking billing via SMS, and the implementation of the remote traffic management system. From 2012 to 2014, he was employed at ACNielsen d.o.o., in the position of database operator, processing and analyzing collected data for the purpose of market analysis. Since 2014 he is employed at the Croatian Regulatory Agency for Network Activities (HAKOM), initially in the Department of Communication Networks and Services, in the position of Expert for Communication Services, and since 2019 in the Department of Infrastructure, as a senior specialist and deputy head of the department. He actively participated in several seminars and conferences and is the co-author of several papers that were presented at international conferences.