UNIVERZITET U BEOGRADU

FAKULTET POLITIČKIH NAUKA

Marta S. Mitrović

ULOGA DRŽAVE I INTERNET INTERMEDIJATORA U ZAŠTITI PRAVA INTERNET KORISNIKA

doktorska disertacija

Beograd, 2019

UNIVERSITY OF BELGRADE

FACULTY OF POLITICAL SCIENCES

Marta S. Mitrović

THE ROLE OF THE STATE AND INTERNET INTERMEDIARIES IN PROTECTING INTERNET USERS' RIGHTS

Doctoral Dissertation

Belgrade, 2019

Mentor:

Doc. dr Ana Milojević, Univerzitet u Beogradu, Fakultet političkih nauka

Članovi komisije:

Prof. dr Snježana Milivojević, Univerzitet u Beogradu, Fakultet političkih nauka

Doc. dr Jelena Kleut, Univerzitet u Novom Sadu, Filozofski fakultet, Odsek za žurnalistiku

Datum odbrane: _____

Uloga države i internet intermedijatora u zaštiti prava internet korisnika

Rezime:

U ovom radu istražuje se pravo na slobodno izražavanje i pravo na privatnost internet korisnika, što se analizira kroz uloge tri aktera: države, internet intermedijatora i internet korisnika. Cilj doktorskog rada je da se na osnovu analize uloga navedenih aktera i poređenjem različitih nacionalnih praksi ponudi model upravljanja internetom. Ponuđeni model bi za centralni koncept imao odgovornost, čime bi osiguravao i poštovanje prava internet korisnika. Istraživanje je sprovedeno na četiri nivoa.

U okviru prvog nivoa razmatra se uloga države u zaštiti prava internet korisnika. S obzirom na to da je uloga države najvidljivija kroz njen regulatorni okvir, u ovom delu rada se najpre predstavljaju pozitivni i negativni aspekti regulacije informaciono-komunikacionog sistema u tradicionalnom okruženju, a zatim se razmatraju i izazovi regulisanja internet prostora. Problematizovanje uloge države u globalizovanom informaciono-komunikacionom sistemu, odnosno očuvanje državne jurisdikcije u doba interneta, takođe je predmet teorijske analize ovog dela rada. Navedeno se ostvaruje kroz sukobljavanje stavova autora koji ulozi države u novom okruženju pristupaju iz ugla realista i liberala. Nakon razmatranja uloge države u novom okruženju i definisanja njene pozicije u gobalizovanom informaciono-komunikacionom sistemu, pristupa se analizi njene uloge u zaštiti prava internet korisnika. Kroz studiju slučaja Srbije, analizira se način na koji se mlade demokratije, postsocijalističke zemlje, odnose prema pravima internet korisnika. Hipoteza kojom se tvrdi da regulatorni okvir Srbije nije u dovoljnoj meri posvećen zaštiti prava na slobodno izražavanje i prava na privatnost internet korisnika, potvrđena je. Pri testiranju hipoteze, pored analize regulatornog okvira Srbije, u obzir su uzete i analize civilnog sektora, izveštaji Poverenika za informacije od javnog značaja, kao i primeri iz prakse kojima se ilustruju kršenja prava.

Drugi nivo analize podrazumeva ispitivanje uloge privatnih aktera – internet intermedijatora u zaštiti prava internet korisnika. Internet intermedijatore Tomas Koter (Thomas Cotter) definiše kao: „bilo koji subjekt koji omogućava prenos informacija od jedne do druge strane", odnosno bilo koji „pružilac komunikacijskih usluga" (2005: 2). Intermedijatori su, dakle, posrednici u internet kominikaciji. Za analizu njihove uloge u zaštiti prava internet korisnika odabrani su intermedijatori koji su u najneposrednijoj vezi sa internet korisnicima – pretraživači i društvene mreže. Ovi akteri odbijaju da se deklarišu kao mediji, tvrdeći da su u osnovi tehnološke kompanije čija je uloga samo neutralno prenošenje sadržaja na internetu. Jakubovič (Jakubowicz, 2009) ih prepoznaje kao *aktere nalik-medijskim*, ističući da su pojedine njihove funkcije suštinski medijske. Argument u ovom radu je da internet intermedijatori ne moraju biti nedvosmisleno određeni kao mediji u tradicionalnom smislu, ali ih to ne oslobađa odgovornosti prema korisnicima. Njihova uloga u zaštiti prava internet korisnika istraživana je na primeru kompanija Gugl i Fejsbuk, analizom njihove samoregulatorne politike u delu koji se tiče prava na slobodno izražavanje i prava na privatnost. Hipotezom se pretpostavilo da navedene kompanije ne garantuju apsolutnu zaštitu prava svojim korisnicima. Analizom uslova korišćenja Gugla i Fejsbuka, kroz poređenje sa EU regulativom, hipoteza je potvrđena. Najzanačajniji nalazi pokazuju 1) da korisnicima nije zagarantovan afirmativni pristanak, 2) da je jezik kojim su napisani uslovi korišćenja složen i pretežno tehnički, 3) da korisnici nisu nedvosmisleno upoznati sa načinima na koje se njihovi podaci dele sa trećim licima, niti u koje svrhe se to čini, 4) da obe kompanije imaju mogućnost uticaja na slobodu izražavanja, kroz upravljanje informacijskim iskustvom korisnika (*News Feed* na Fejsbuku, rezultati pretrage na Gugl),

5) da je način čuvanja i brisanja ličnih podataka netransparentan, 6) ; da obe kompanije prikupljaju prekomernu količinu ličnih podataka.

Treći nivo analize podrazumeva istraživanje stavova internet korisnika kada je reč o zaštiti njihovih prava na internetu. Veb-anketom, koja je sprovedena *tehnikom grudve*, ispitani su stavovi 783 internet korisnika o načinu na koji se država (Srbija) i privatni akteri (Fejsbuk i Gugl) odnose prema pravu na slobodno izražavanje, te prema privatnosti na internetu. Pored ovoga, anketom je ispitana i individualna odgovornost korisnika pri korišćenju internet usluga. Pretpostavljeno je da internet korisnici u Srbiji nemaju poverenje ni u državu ni u privatne aktere, kada je reč o zaštiti njihovih prava, ali da ni oni ne iskazuju zadovoljavajući stepen individualne odgovornosti. Sve hipoteze u ovom delu rada potvrđene su. Najznačajniji nalazi pokazuju sledeće: 1) samo šestina ispitanika smatra da Vlada Republike Srbije ne narušava privatnost internet korisnika, 2) skoro polovina ispitanika ne oseća se u dovoljnoj meri slobodno da bi objavljivala stavove kojima kritikuje Vladu, 3) približno 12% ispitanika zadovoljno je kako Fejsbuk štiti njihovu privatnost, dok je taj procenat za Gugl veći za jedan odsto, 4) trećina ispitanika potvrdno je odgovorila na pitanje da li su pročitali uslove korišćenja analiziranih kompanija, ali polovina njih nije dala tačne odgovore na kontrolna pitanja, 5) svega 8,9% ispitanika, koji su tvrdili da su pročitali uslove korišćenja, znaju da kompanija Fejsbuk deli njihove podatke sa trećim licima.

U okviru ***četvrtog nivoa analize*** poređeni su različiti pristupi zemalja u upravljanju internetom, kako bi se definisao model državnog upravljanja internetom. Zemlje koje su predmet analize u ovom delu disertacije odabrane su prateći klasifikaciju medijskih sistema Halina i Mančinija (Hallin & Mancini, 2004): liberalni model – Sjedinjenje Američke Države, demokratsko-korporativni model – Nemačka, mediteranski model – Francuska. Pretpostavljeno je da će odnos prema tradicionalnom medijskom sistemu imati uticaj i na odnos prema internet komunikaciji. Odabiru je dodata i Rusija, kao predstavnica postsocijalističkih zemalja sa, i dalje, autoritarnim tipom vladanja. Odabrane zemlje analizirane su korišćenjem sekundarne istraživačke građe, pre svega, izveštaja Fridom hausa (Freedom House) *Internet sloboda* za 2018. godinu, ali i pregledom istraživačkih radova i literature iz relevantne oblasti. Definisane su četiri intervenišuće varijable koje imaju presudni uticaj na izgradnju generalnog odnosa analiziranih zemalja prema internetu: *sloboda u internet komunikaciji, dostojanstvo u komunikaciji na internetu, bezbednost internet korisnika kroz nadzor* i *etatizam*. U odnosu na to koja je varijabla intervenišuća u određenom sistemu definisana su tri modela državnog upravljanja internetom: liberalni model (*sloboda u internet komunikaciji*), model državne kontrole (*etatizam*) i balansirani model upravljanja internetom (*dostojanstvo u komunikaciji, bezbednost kroz nadzor*). SAD je predstavnik prvog modela, Rusija je predstavnik modela državne kontrole, Nemačka i Francuska su određene kao najbliže balansiranom modelu, dok je Srbija pozicionirana između dva modela: modela državne kontrole i balansiranog modela.

Na osnovu svih prethodnih analiza, predložen je ideal-tipski model upravljanja internetom, koji uključuje sva tri aktera: državu, privatne aktere i internet korisnike, i za centralni koncept ima odgovornost. Model je nazvan ***model cirkularne odgovornosti upravljanja internetom***. Predloženi model je funkcionalistički i ima dva tipa: **Tip A** – kada je država dominatni akter, ali ne narušava ravnotežu; i **Tip B** – kada su privatni akteri dominatni, ali ne narušavaju balans. Disbalans ovog ideal-tipskog modela vodi stvaranju tri nova modela: ***etatistički model*** – kada je država dominantni akter, a etatizam centralni koncept; ***komercijalni model*** – kada su privatni akteri dominatni, a komercijalna isplativost centralni koncept oko koga se model izgrađuje i ***model apsolutne slobode ili anarhični model*** – kada korisnici preuzimaju dominantnu poziciju, težeći da izbegnu svaki vid kontrole, i model se izgrađuje oko koncepta anarhije (*Deep web*). Navedeni disbalansi mogu biti i kratkotrajni sa izgledom vraćanja u ravnotežu, ali mogu biti i permanentno stanje, kada više nije moguće govoriti o disbalnsu, jer je disbalans zapravo stanje ravnoteže.

Zaključak izveden na kraju rada zasnovan je, kao i ideal-tipski model, na konceptu odgovornosti. Odgovornost i kooperacija sva tri analizirana aktera ključni su pri upravljanju internetom. Jedino odgovorno poslovanje privatnih aktera i odgovoran odnos države pri izgradnji politika upravljanja internetom mogu biti garant poštovanja prava korisnika. Korisnicima ne preostaje ništa drugo nego da imaju *poverenje u apstraktne sisteme* i da veruju da će ekspertski sistemi delovati odgovorno (Giddens, 1998).

Ključne reči: regulacija, samoregulacija, internet intermedijatori, društvene mreže, pretraživači, sloboda izražavanja, pravo na privatnost, upravljanje internetom, internet korisnici.

Naučna oblast: Kulturološke nauke i komunikologija

Uža naučna oblast: Komunikologija i informatika

UDK broj: 316.774:321.01:342.7(043.3)

The Role of the State and Internet Intermediaries in Protecting Internet Users' Rights

Summary

The starting points for the research in this dissertation are the right of freedom of expression and the right of privacy of Internet users, which are being analyzed through the roles of three agents: the state, Internet intermediaries and Internet users. The purpose of the doctoral thesis is to offer a model of Internet governance, based on the analysis of the roles of the aforementioned agents and a comparison of different national practices, which would have responsibility as its central concept, and in that way would ensure the respect of Internet users' rights. The research was conducted on four levels.

The first level investigates the role of the state in protecting the rights of Internet users. Since the state's role is the most visible through its regulatory framework, this part of the thesis introduces the positive and negative aspects of regulating the communication and information system in the traditional environment, with the challenges of Internet space regulation being discussed subsequently. The complication of the role of the state in the globalized communication and information system, more precisely, the preservation of the state's jurisdiction is also the subject of the theoretical analysis in this part of the thesis, which is done by clashing views of authors who approach the role of the state in the new environment from the perspective of realists and liberals. After examining the role of the state in the new environment and defining its position in the globalized information and communication system, the following step is to approach the analysis of its role in the protection of the rights of Internet users. In the case study of Serbia, the subject of analysis is the relation of young democracies, post-socialist countries, towards the rights of Internet users. The hypothesis suggesting that the regulatory framework of Serbia is not sufficiently dedicated to protecting the rights of freedom of expression and privacy of Internet users, was confirmed. Along with the analysis of Serbia's regulatory framework, in the process of testing the hypothesis, the civil sector analysis, reports of the Commissioner for information of pubic importance, as well as practical examples of the violation of rights, that were the subject of the analysis, were also taken into account.

The second level of the analysis involves examining the role of private agents – Internet intermediaries in protecting the rights of Internet users. Thomas Cotter defined Internet intermediaries as: "any subject enabling the transfer of information from one party to the other", or any "communication service provider" (2005, p.2). Therefore, intermediaries are the mediators in the Internet communication. For the analysis of their role in protecting Internet users' rights, the intermediaries with the most direct connection to Internet users were chosen – search engines and social media. These agents refuse to declare themselves as the media, claiming that they are primarily technological companies, whose role is to neutrally transmit the content on the Internet. Jakubowicz (2009) recognizes them as the *media-like agents*, indicating that some of their functions are essentially media-like. The argument in the thesis is that Internet intermediaries need not be unambiguously defined as the media in the traditional sense, but that does not absolve them of responsibility toward users. Their role in protecting the rights of Internet users was examined through the example of companies such as Google and Facebook, that is, by analyzing their self-regulatory policy in the section concerning the rights of freedom of expression and privacy. The hypothesis suggested that the aforementioned companies did not guarantee the absolute protection of rights to their users. From the analysis of terms of use of Google and Facebook, that implied a comparison with EU regulations, the hypothesis was confirmed. The most significant findings indicate that users are not guaranteed the affirmative consent; that the language used to write terms of use is complex and predominantly technical; that users are not unequivocally informed of the ways in which their data is shared with third parties and for what purposes; that both companies

have the ability to influence the freedom of expression, by managing the information experience of users (*News Feed* on Facebook, *Search Results* on Google), that the method of saving and deleting personal data is non-transparent; that both companies collect excessive amounts of personal data.

The third level of the analysis implies examining the views of Internet users concerning the protection of their rights on the Internet. The web survey, conducted by the snowball sampling, included 783 Internet users who expressed their views regarding the ways the state (Serbia) and private agents (Facebook and Google) relate to the right of freedom of expression and privacy on the Internet. Also, the survey was used to examine the individual responsibility of users when it comes to the use of Internet services. Several hypotheses suggested that Internet users in Serbia do not have confidence in the country and private actors on the issue of protecting their rights. However, users also do not demonstrate a satisfactory level of individual responsibility. All of the hypotheses in this part were confirmed. The most important findings indicate that only one-sixth of the respondents consider that the Government of the Republic of Serbia does not violate the privacy of Internet users.

In addition, almost half of the respondents do not feel free to express their views criticizing the government; approximately 12% of respondents are satisfied with the way Facebook is protecting their privacy, while it is 1% higher in the case of Google; a third of respondents answered positively to the question whether they had read terms of use of the analyzed companies, but half of them did not give a correct answer to the main questions; only 8.9% of respondents who claimed to have read terms of use are aware of the fact that Facebook shares their data with third parties.

In **the fourth level of the analysis** there is a comparison of different approaches of cuntries in Internet governance, with the aim of defining a model of the state's governance of the Internet. The states that were the subject of the analysis in this part of the thesis, were selected according to Hallin and Mancini's classification of media systems (Hallin & Mancini, 2004); *the Liberal model* – the United States of America, *the Democratic Corporatist model* – Germany; *the Mediterranean model* – France. It was assumed that the relation towards the traditional media system will have an impact on the relation towards the Internet communication. As the representative of the post-socialist countries with continuing autocracy, Russia was also added to the selection. Selected countries were analyzed using the secondary research material, particularly, the Freedom House report (*Freedom on the Net for 2018),* but also by using an inspection of research papers and literature from that field. Four intervening variables were defined, which have a crucial influence on building the general relationship of the analyzed countries towards the Internet: freedom in Internet communication, dignity in Internet communication, safety of Internet users through surveillance and statism.

In reference to the intervening variable in a particular system, three models of the state's Internet governance were established: the liberal model (*freedom in Internet communication*), the model of state control (*statism*) and the balanced model of Internet governance (*dignity in communication, safety through surveillance*). The United States is the representative of the first model, Russia is the representative of the state control model, Germany and France are defined as the closest ones to the balanced model, while Serbia is positioned between the two models: the state control model and the balanced model.

Based on the previous analyses, an ideal-type model of Internet governance was proposed, including all three agents: the state, private agents and Internet users, and emphasizes responsibility as its central concept. The model was called **the circular responsibility model of Internet governance.**

The proposed model is functionalist and has two types: *Type A* - when the state is the dominant agent, but does not disrupt the balance; and *Type B* – when private agents are dominant, but do not disrupt the balance. The disparity of this ideal-type model leads to the

creation of three new models: **the *statism model*** – when the state is the dominant agent, while statism is the central concept; ***the commercial model*** – when private agents are dominant, while commercial profitability is the central concept around which the model is built and ***the model of absolute freedom or the anarchic model*** – when users take over the dominant position, striving to avoid any form of control and the model is built around the concept of anarchy (Deep web). The suggested imbalances can be momentary with the prospect of returning into balance, but they can also be a permanent condition when it is no longer possible to speak of imbalance, since the imbalance is actually the state of balance.

The conclusion drawn at the end of the thesis is based, like the ideal-type model, on the concept of responsibility. Cooperation and responsibility of all three analyzed agents are crucial for Internet governance. Moreover, only the responsible management of private agents and the responsible attitude of the state in building policies regarding Internet governance can guarantee respect of users' rights. The only choice users have is to trust the abstract systems and believe that expert systems will act responsibly (Giddens, 1998).

Key words: regulation, self-regulation, Internet intermediaries, social media, search engines, freedom of expression, privacy rights, Internet governance, Internet users

Scientific field: Cultural and Communication Sciences

Specific scientific field: Communication Science and Informatics

UDK: 316.774:321.01:342.7(043.3)

Sadržaj

1. Uvod

1.1. Formulacija istraživačkog problema

Informaciono-komunikacioni sistem, nekada jasno zaokružen i definisan u okvirima država i nacionalnih regulativa, usled tehnološkog razvoja i globalizacije postaje otvoren, čini se, neomeđen prostor. Ekspanzija komunikacije na internetu predstavlja izazov za tradicionalne forme regulisanja aktivnosti koje mogu ugroziti prava građana, u ovom slučaju internet korisnika. Ukoliko su prava internet korisnika narušena, ko se smatra odgovornim? Ko su akteri koji bi trebalo da garantuju bezbednu onlajn-komunikaciju? Drugim rečima, ko štiti interes korisnika?

U kompleksnom informaciono-komunikacionom okruženju postoje najmanje tri zainteresovane strane: **država**, **privatni akteri** i **korisnici**. Shodno tome, odgovor na postavljena pitanja može se potražiti u trijadi nacionalni – komercijalni – javni interes.

Pod **nacionalnim interesom** u ovom radu podrazumeva se interes države da posredstvom regulacije ostvari kontrolu nad informacijama koje se šire „mrežom". **Komercijalni interes** odnosi se na interes internet intermedijatora da stvore okruženje u kome će nesmetano obavljati funkciju posredovanja informacijama uz maksimalno ostvarivanje profita. **Javni interes** odnosi se na interes internet korisnika i prenosi na analizu mogućnosti ostvarivanja prava na slobodno izražavanje i prava privatnost.

Dva navedena prava zagarantovana su Članom 8 i 10 *Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda*:

> **Član 8**. *Pravo na poštovanje privatnog i porodičnog života:*
>
> „1) Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.
>
> 2) Javne vlasti neće se mešati u vršenje ovog prava sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih."

Član 10. *Sloboda izražavanja*:

„1 Svako ima pravo na slobodu izražavanja. Ovo pravo uključuje slobodu posedovanja sopstvenog mišljenja, primanja i saopštavanja informacija i ideja bez mešanja javne vlasti i bez obzira na granice. Ovaj član ne sprečava države da zahtevaju dozvole za rad televizijskih, radio i bioskopskih preduzeća.

2 Pošto korišćenje ovih sloboda povlači za sobom dužnosti i odgovornosti, ono se može podvrgnuti formalnostima, uslovima, ograničenjima ili kaznama propisanim zakonom i neophodnim u demokratskom društvu u interesu nacionalne bezbednosti, teritorijalnog integriteta ili javne bezbednosti, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, zaštite ugleda ili prava drugih, sprečavanja otkrivanja obaveštenja dobijenih u poverenju, ili radi očuvanja autoriteta i nepristrasnosti sudstva.” [1]

Polazeći od tumačenja nacionalnog interesa, jasno je da je uloga države, u delu koji se odnosi na intenzitet kontrole nad informacijama koje prožimaju njen (virtuelni) prostor, promenjena. Kako ističe Prajs (Price), „svuda je dovedena u pitanje sposobnost bilo koje države da u potpunosti kontroliše slike koje prožimaju njenu teritoriju” (2002: 3), ali država ostaje odgovorna da zaštiti svoje građane, u ovom kontekstu internet korisnike, i omogući poštovanje njihovih prava. Trebalo bi da država tu ulogu ostvaruje kroz regulaciju aktivnosti koje mogu dovesti do narušavanja prava internet korisnika. I premda jedan deo autora tvrdi da je država izgubila deo suvereniteta, kada je reč o onlajn-aktivnostima (Castells 2013; Price, 2002; Lessing, 2006), postoje i oni autori koji ističu jačanje pozicije države u borbi za povratkom kontrole nad svojim (virtuelnim) prostorom (Flew&Waisbord, 2015; Stein&Sinha, 2002).

Druga strana, zainteresovana za ostvarivanje komercijalnog interesa, jesu globalne privatne kompanije, koje posreduju u internet komunikaciji – tzv. internet intermedijatori. Iako su predstavnici privatnog sektora, intermedijatori se obavezuju na poštovanje prava korisnika kroz ostvarivanje samoregulatorne politike. Naime, internet intermedijatori omogućavaju korisnicima pristup sadržaju i, prema istom ključu, pristup provajderima sadržaja javnosti (Jakubowicz, 2009). Oni posreduju između proizvođača sadržaja, trećih lica i korisnika. Pod tako definisanim intermedijatorima, u ovom radu podrazumevaju se **pretraživači** i **društvene mreže**.

Internet intermedijatori direktno su uključeni u globalni informaciono-komunikacioni lanac. Njihova značajna uloga u privatnom sektoru podstiče debate o različitim aspektima njihove odgovornosti. S tim u vezi, Evropska komisija u *Strategiji o bezbednosti u sajber prostoru* navodi da „privatni sektor poseduje i posluje u značajnom delu sajber prostora, i svaka inicijativa koja ima za cilj da bude uspešna u ovoj oblasti mora da prepozna njegovu vodeću ulogu”[2].

[1] Dostupno na: http://www.sostelefon.org.rs/zakoni/14.%20Evropska%20konvencija%20za%20zastitu%20ljudskih%20prava%20i%20osnovnih.pdf (pristupljeno 02. 02. 2017. godine).

[2] Engl. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, dostupno na: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (pristupljeno 03. 02. 2017. godine).

Aktivno učešće internet intermedijatora u oblikovanju informaciono-komunikacionog okruženja podstiče debate i o tome kako se njihovo poslovanje odražava na pojedince, odnosno korisnike njihovih usluga. S obzirom na to da su intermedijatori privatne kompanije sa komercijalnim interesom, postavlja se pitanje kakva je njihova odgovornost u zaštiti javnog interesa. Odnosno, u kotekstu ovog rada, da li se može zahtevati njihova odgovornost kada je reč o zaštiti prava na slobodno izražavanje i privatnost korisnika. Da li se od intermedijatora može očekivati, pa i zahtevati, da se mimo svojih komercijalnih interesa obavežu i na zaštitu interesa svojih korisnika u jednom opštijem smislu?

Debate stručne javnosti imaju pravac definisanja odgovornosti intermedijatora po ugledu na tradicionalne masovne medije (Andrews 2016; Helbereger, 2016). Međutim, privatne kompanije koje posreduju u onlajn-komunikaciji odbijaju da budu svrstane u medijske organizacije[3], jer bi to značilo implicitno priznavanje odgovornosti za sadržaj koji se širi mrežom, ali i za šire društvene posledice.

Kada je reč o poštovanju ljudskih prava, očigledna je potreba za podjednakom odgovornosti države i privatnog sektora – intermedijatora. Da li je rešenje povećanje uloge države u regulisanju ove oblasti ili jačanje samoregulatornog okvira? Koji tip komunikacione politike bi pospešio zaštitu prava korisnika, a da pritom ne ugrozi ideal slobodanog protoka informacija, na čijim načelima je internet sazrevao? U najopštijem smislu, kako pomiriti nacionalni, komercijalni i javni interes?

UNESKO (engl. *United Nations Educational Scientific and Cultural Organiz*ation – UNESCO) od 2009. godine objavljuje seriju publikacija koje se tiču slobode na internetu – „Serije o internet slobodi"[4]. Među objavljenim publikacijama najveći je broj onih čije su centralne teme istraživanja: sloboda izražavanja i poštovanje prava na privatnost na internetu. Daton i saradnici (Dutton et al. 2011) u izveštaju „Sloboda pristupa sloboda izražavanja"[5], objavljenom u okviru UNESKO studije, analiziraju digitalnu arenu sa aspekta poštovanja slobode izražavanja. Autori su zaključili da sloboda izražavanja nije nešto što je dato, niti su, uprkos očekivanjima, tehnološke inovacije zagarantovale njeno ostvarivanje. Sloboda izražavanja na internetu zavisi od mnogo faktora, pre svega od politike i prakse industrije i nacionalnih država, pa u tom odnosu može biti gotovo potpuno ostvarena ili poništena.

Mendel i saradnici (Mendel et al., 2012) u izveštaju „Globalno istraživanje privatnosti na internetu i slobodnog izražavanja"[6] ističu tradicionalni značaj ova dva prava i problematizuju njihovo ostvarivanje u onlajn-okruženju. U delu koji se tiče prava na privatnost na internetu autori ističu nove izazove koje donosi novonastali kontekst. Pre svega to su: novi načini prikupljanja i skladištenja personalnih informacija, tehnološki omogućeni u obimu koji je do skoro bio nezamisliv; mogućnosti lociranja korisnika; novi kapaciteti vlada i privatnog sektora u analizi ličnih podataka korisnika; upotreba ličnih informacija u komercijalne svrhe; izazovi u regulisanju dela aktivnosti koji se tiču

[3] Na primer, kompanija Fejsbuk napravila je novu aplikaciju *FacebookPaper*, koja generiše vesti i omogućava pristup svojim korisnicima. Čelnici kompanije tvrde da Fejsbuk samo posreduje između medija, sa kojima sarađuju, i korisnika i da ne proizvode sopstveni sadržaj, stoga se ne mogu svrstati u medijske kompanije (Ulanoff, 2014). Pogledati na: http://mashable.com/2014/01/30/facebook-paper-app-analysis/#QAVeHyWSpqqq (pristupljeno, 03. 02. 2017. godine).

[4] UNESCO (2009). *Series of Internet Freedom*. Dostupno na: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publications-by-series/unesco-series-on-internet-freedom/ (pristupljeno 03.02.2017. godine).

[5] Engl. *Freedom of Connection Freedom of Expression*. Dostupno na: https://unesdoc.unesco.org/ark:/48223/pf0000191594 (pristupljeno 03. 02. 2017. godine).

[6] Engl. *Global Survey on Internet privacy and Freedom of Expression*. Dostupno na: https://unesdoc.unesco.org/ark:/48223/pf0000218273 (pristupljeno 03. 02. 2017. godine).

privatnih podataka, s obzirom na internacionalnu prirodu interneta. Pored ovog, autori analiziraju moguće načine koji bi doprineli boljoj zaštiti privatnosti i pozivaju internet intermedijatore na odgovornost. U empirijskom delu izveštaja, Mendel i saradnici analiziraju pojedinačne nacionalne okvire i njihove regulatorne prakse, ali i moguće načine samoregulacije privatnih aktera. Komparativnim analizama potvrđuju se različiti pristupi u regulaciji ove oblasti, koji su u direktnoj vezi sa nacionalnim politikama država u kojima internet posrednici posluju. Sumirano, rezultati raznovrsnih istraživanja, objavljenih u okviru studije „Serije o internet slobodi", ukazuju na rastući značaj problematizacije poštovanja ljudskih prava u onlajn-okruženju.

Kada je reč o stavovima internet korisnika, zainteresovanih za ostvarivanje njihovih prava na slobodno izražavanje i privatnost, u „eri nakon Snoudena" čak 91% odraslih Amerikanaca smatra da nema kontrolu nad tim kako njihove privatne podatke skladište i koriste privatne kompanije (Pew Research Centre, 2016)[7]. Korisnici snose deo odgovornosti, koju prepoznajemo kao individualnu odgovornost. Međutim, suočeni sa mnogobrojnim samoregulatornim aktima – politikama privatnosti, uslovima korišćenja – pred njima je nefer izbor da gotovo bespogovorno prihvate načine poslovanja privatnih kompanija, ili da jednostavno ne koriste njihove usluge; te da veruju da ni njihove vlade neće zloupotrebiti njihove lične podatke, niti im neopravdano uskratiti slobodu onlajn-izražavanja.

Pokušaj da se pomire interesi tri navedena aktera u onlajn-okruženju – države, internet intermedijatora i internet korisnika u ovom radu, gradiće se oko koncepta *odgovornosti*. Polazeći od ovog koncepta, najpre će biti analizirana uloga države, sa akspekta *odgovorne regulacije* u oblasti interneta; zatim uloga internet intermedijatora sa aspekta *odgovorne samoregulatorne* politike – na primeru kompanija Gugl i Fejsbuk; i na kraju, uloga internet korsnika sa aspekta *individualne odgovornosti* pri korišćenju onlajn-usluga. Poređenjem praksi u različitim zemljama, biće ponuđen okvir za klasifikaciju različitih pristupa internet upravljanju, kada je reč o poštovanju prava internet korisnika; sumiranjem svih rezultata dobijenih istraživačkim poduhvatom, biće definisan i ideal-tipski model upravljanja internetom.

1.2. Značaj i opravdanost istraživanja

Značaj teme ogleda se u tome što doprinosi aktuelnoj debati o ulozi države i internet intermedijatora u globalnom informaciono-komunikacionom sistemu, kao i njihovoj odgovornosti za zaštitu prava korisnika. S obzirom na to da se u radu ne analizira samo njihova uloga u opštem smislu, već i pojedinačni informaciono-komunikacioni sistemi i njihove politike prema novom komunikacionom okruženju, doprinos se ogleda i u nastojanju da se analizom pojedinačnih pristupa predloži održiv model politike upravljanja internetom. Takav model podrazumevao bi jasno definisane uloge internet intermedijatora i države, kojim bi se garantovalo poštovanje prava internet korisnika.

Naučni doprinos disertacije je u tome što će pokušati da odgovori na pitanje na koji način se menja uloga države i njena odgovornost za zaštitu prava građana, onda kada su oni u ulozi internet korisnika. Takođe, naučni doprinos ogleda se i u pokušaju da se ukaže na specifičnu ulogu inernet intermedijatora, privatnih aktera, kada je reč o zaštiti prava korisnika. Naučni doprinos predstavlja i

[7] Dostupno na: https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (pristupljeno 04. 02. 2017. godine).

iskorak iz teorijske dihotomije sloboda – regulacija, kojim želi da se pokaže da je kombinacija regulacije i samoregulatorne politike intermedijatora moguća i nužna, naročito u slučajevima kada komercijalni interes narušava javni, pretećи da ugrozi prava korisnika.

Društveni doprinos teze ogleda se, pre svega, u analizi studije slučaja Srbije. Zbog specifičnog istorijskog i društveno-političkog konteksta, a kao predstavnik postsocijalističkih mladih demokratija, analiza Srbije u ovoj oblasti daje doprinos istraživačkom polju koje se odnosi na izazove posttranzicionih zemalja u oblasti informaciono-komunikacionih sistema. U zemljama gde je država istorijski imala neprikosnovenu ulogu u regulisanju, kontroli, ali i socijalnoj zaštiti građana, kakva je i Srbija, prenošenje dela odgovornosti na globalne privatne kompanije predstavlja veliki izazov. Kroz studiju slučaja u obzir se uzima odnos države prema zaštiti prava internet korisnika i odnos građana, u ovom slučaju internet korisnika u Srbiji, prema odgovornosti državne politike i politike intermedijatora za zaštitu njihovih prava. Kroz analizu navedenih korelacija traži se odgovor na pitanje koju politiku Srbija uspostavlja u odnosu prema zaštiti prava na privatnost i slobodno izražavanje na internetu, ali i kakav je stav korisnika prema odgovornosti države i intermedijatora pri zaštiti njihovih prava. Doprinos rada prepoznaje se i u tome što će pružiti smernice za uspostavljanje komunikacione politike, odnosno predložiti model koji bi pomirio prava korisnika sa interesima države i intermedijatora.

2. Teorijsko-metodološki okvir istraživanja

2.1. Teorijski okvir

Ven Kulinberg i Mek Kvejl (Van Cuilenburg & McQuail, 2003), analizirajući etape u razvoju komunikacione politike u zapadnim zemljama, ističu tri paradigmatične faze, o kojima će biti reči u nastavku. Prvu fazu, do Drugog svetskog rata, karakteriše brzi tehnološki razvoj i primarni interesi države i korporacija. Drugu fazu, koja je trajala od Drugog svetskog rata do osamdesetih/devedesetih godina 20. veka, oblikovali su sociopolitički interesi, koji su preuzeli primat pred ekonomskim i nacionalnim interesima. Treća faza, od osamdesetih/devedesetih godina do danas, karakteriše se opštom privatizacijom, pri čemu se dovode u pitanje normativne medijske politike, što stvara izazov koji se ogleda u stvaranju nove paradigme komunikacione politike (Van Cuilenburg & McQuail, 2003: 186–203).

Ven Kulinberg i Mek Kvejl nude skicu nove paradigme komunikacione politike čiji je krajnji cilj ostvarivanje javnog interesa. Tri su ključna koncepta pri uspostavljanju nove paradigme komunikacione politike: sloboda komuniciranja, pristup i kontrola/odgovornost (Van Cuilenburg & McQuail, 2003: 203–206). Upravo su ta tri koncepta u osnovi ovog rada. Dok se prva dva podupiru i ogledaju u poštovanju prava na slobodno izražavanje, treći se posredno odnosi na politike odgovornosti države i internet intermedijatora, koja proizlazi iz mogućnosti da kontrolišu protok informacija i uređuju novo komunikaciono okruženje. Zbog toga je uspostavljanje komunikacione politike koja bi podrazumevala njihovu veću odgovornost u odnosu prema pravima korisnika nužna i predstavlja fokus ovog rada.

Ven Kulinber i Mek Kvejl navode da „koreni komunikacijskih politika leže u interakciji između težnje država za ostvarivanjem nacionalnih interesa i poslovanja komercijalnih/industrijskih preduzeća" (2003: 182). Sa promenom u informaciono-komunikacionim sistemima, a pod uticajem razvoja tehnologije i globalizacije, uloge države i privatnih aktera, uključenih u informaciono-komunikacioni lanac, menjaju se. U tradicionalnom informaciono-komunikacionom sistemu država je imala najznačajniju ulogu u regulaciji. U skladu sa tim, Radojković i Stojković ističu šest osnovnih normativa države, kao zakonodavca: ustavna načela o slobodi izražavanja, zakoni o vlasništvu nad medijima, zakoni o telekomunikacijama, zakoni koji se odnose na industriju kulture, zakoni kojima se štite ugledi pojedinaca ili državnog interesa ograničavanjem slobode govora, zakoni o autorskim pravima i intelektualnoj svojini (2004: 48–50). Jasno je da je država bila entitet u čijem su okviru nastajale tradicionalne forme informisanja i komunikacije, stoga je njena uloga u regulisanju (često i upravljanju) celokupnim informaciono-komunikacionim sistemom bila gotovo neprikosnovena. Država je u tom kontekstu imala moć da pravnom regulativom štiti svoje interese, ali i interese medija i građana (zabrana koncentracije, zahtev za pluralizmom, zaštita privatnosti, sloboda izražavanja itd).

Kastels (Castells) u knjizi "Moć komunikacije" piše o gubitku suvereniteta države; države koja je tradicionalno definisana kao jasno omeđena teritorija, sa krutim granicama i jasnim centrom moći. Kastels negira nestajanje države kao entiteta, ali uvodi pojam *network state,* odnosno *umrežene države,* čime objašnjava trenutno stanje država, koje su, usled globalizacije, doživele transformaciju. Kastels ih smatra samo jednim "čvorom" u umreženom društvu; kako bi zadržale deo nekadašnjeg suvereniteta, države postaju deo "mreže", dele svoju moć sa globalnim centrima, internacionalnim telima (2013: 38–42). Kada je reč o informaciono-komunikacionom lancu, jasno je da se države, usled nemoći da samostalno kontrolišu svoj prostor, okreću internacionalnim telima, kakva su Savet Evrope ili Evropska Unija.

Prajs (Price, 2002), istovetno Kastelsu, piše o globalnoj informacijskoj revoluciji, koja vodi gubitku centralizovane moći države i okretanju ka nadnacionalnim propisima. Prajs, u novonastalom globalnom kontekstu, značaj daje pregovaranju pri susretu sa izazovima u informaciono-komunikacionom okruženju, nasuprot strogim nacionalnim propisima, koji su tradicionalno bili primarni. Takođe, autor ističe značaj istorijskog, društvenog i geopolitičkog polazišta država, jer u skladu sa njima države grade i sprovode svoje komunikacione politike.

Promenjena uloga države očigledna je i kada je reč o intenzitetu kontrole informacija. Države su suočene sa trendom razvoja globalnog komunikacionog sistema, koji prevazilazi granice nacionalnog i povećava ulogu privatnih aktera koji posreduju u informacijskoj razmeni. Herman i Mekčesni (Herman & McChesney, 2004) ističu da je korporativni kapitalizam sa svojim transnacionalnim kompanijama prevladao svetskom scenom, koristeći se principima slobode izbora i ljudskih prava. Ukoliko kroz tu prizmu posmatramo globalni razvoj informaciono-komunikacionih sistema, jasno je da privatne transnacionalne kompanije, kakve su i internet intermedijatori, preuzimaju primat, zagovarajući slobodan protok informacija i apsolutnu slobodu izražavanja i informisanja. Međutim, Herman i Mekčesni ukazivali su i na negativnu stranu takvog trenda. Globalna korporativna ideologija ima za cilj da slobodu dovede u direktnu vezu sa potpunim odsustvom kontrole i da kritikuje države koje regulacijom pokušavaju da zaštite svoje interese, jer na taj način ometaju njihovo funkcionisanje i sticanje profita. Privatne kompanije, internet intermedijatori, koje su okosnica komunikacije na internetu, imaju slične imperijalističko-korporativne namere.

Međutim, uporedo sa insistiranjem na sajber prostoru bez granica i smanjenju jurisdikcije pojedinačnih država, primetni su i pokušaji država da povrate kontrolu nad svojim prostorom, u ovom slučaju virtuelnim, i redefinišu pojam medijskog ekosistema, vraćajući ga na tradicionalni pojam

medijskih nacionalnih sistema, koji bi uključivao i internet prostor. O tome pišu Flu i Vejsbord (Flew & Waisbord, 2015). Analizirajući medijske sisteme Kine, Brazila i Australije, autori izvode zaključak da: "aktuelne debate o internet neutralnosti, slobodi i privatnosti, svedoče i o naporima u drugom pravcu – konkretno, o nameri da se 'nacionalizuje' sajber prostor i izgradi parohijalni, fragmentirani internet usidren u nacionalnim zakonima" (str. 18).

Stajn i Sinha (Stein & Sinha, 2002) navode tri ključna razloga zbog kojih je državama važno da imaju kontrolu nad informacijama koje se distribuiraju putem interneta. Prvi razlog ogleda se u tome što je komunikacioni sistem tradicionalno bio centralan u političkom procesu. Države imaju potrebu da kontrolišu onaj deo prostora u kome se generiše društveno znanje, podstiče na političku aktivnost i na osnovu koga građani donose političke odluke. Drugo, države su zabrinute zbog uticaja koji globalne informaciono-komunikacione tehnologije mogu imati na društveni i kulturni život građana. I treće, virtuelni prostor nije odvojiv od realnog. Kako autori smatraju, svaki pojedinac koji preduzme neku aktivnost u virtuelnom prostoru jeste pojedinac koji postoji u realnom prostoru, građanin je neke države i odgovoran je za svoje delovanje (str. 415–416).

Dakle, tradicionalno shvaćen, pojedinac je, kao internet korisnik, odgovoran za delovanje u virtuelnom prostoru. Međutim, značajna uloga internet intermedijatora, odnosno posrednika, u informaciono-komunikacionom lancu otvara i pitanja njihove odgovornosti prema internet korisnicima. Jakubovič (Jakubowicz, 2009) funkciju intermedijatora definiše kao nalik-medijskoj, prepoznajući mnoge aktivnosti internet posrednika kao klasično medijske (uloga vratara, postavljanje standarda), ali ističe da oni ne proizvode sopstveni sadržaj, te se ne mogu smatrati medijima u klasičnom smilu. Međutim, njihova velika uloga u diseminaciji informacija pokreće pitanje implikacija intermedijatora, ne samo na internet korisnike već i na čitav niz informaciono-komunikacionih praksi, i društvo u celini. S obzirom na to da su intermedijatori privatne kompanije sa komercijalnim interesom, postavlja se pitanje kakva je njihova odgovornost u zaštiti javnog interesa. Jakubovič (2009) smatra da oni ne moraju biti prepoznati kao klasične medijske organizacije da bi se obavezali na zaštitu prava korisnika, jer ih na to obavezuju njihove funkcije slične medijskim.

Značaj intermedijatora, i opravdanost instistiranja stručne javnosti na povećanju njihove odgovornosti, potvrđuje i istraživanje[8] koje su 2015. godine, u okviru Istraživačkog centra Pju, sproveli Mičel i saradnici (Mitchel et al.). Ovo istraživanje pokazuje da je šest od deset ispitanika milenijumske generacije navelo Fejsbuk kao glavni izvor za političke vesti. Navedeni podatak ukazuje da internet intermedijatori uzimaju primat i kada je o informisanju reč, pa Helbergerova (Helbereger, 2016)[9] navodi da je došao trenutak da i intermedijatori budu podvrgnuti zvaničnoj politici, sličnoj medijskoj. Prvi impuls prepoznaje u nastojanju da se izvrši revizija *Direktive audio-vizuelnih medijskih servisa*, kako bi se uključila i odgovornost intermedijatora. Saglasan je i Andrjus (Andrews, 2016)[10], koji smatra da bi gigante poput Gugla i Fejsbuka trebalo regulisati na nivou Evropske Unije i smatrati ih medijima, pa u skladu sa tim se i odnositi prema njihovoj odgovornosti.

[8] Dostupno na: https://www.journalism.org/2015/06/01/facebook-top-source-for-political-news-among-millennials/ (pristupljeno 05.02.2017. godine).
[9] Helberger, (2016). "Facebook is a news editor: the real issues to be concerned about". *LSE blog*. Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2016/05/26/facebook-is-a-news-editor-the-real-issues-to-be-concerned-about/ (pristupljeno: 25.03.2018. godine).
[10] Leighton Andrews. (December 13, 2016). We need European regulation of Facebook and Google. *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/12/13/we-need-european-regulation-of-facebook-and-google/ (pristupljeno 03.02.2017. godine).

Međutim, da li su intermedijatori zaista zainteresovani da posluju u skladu sa poštovanjem prava korisnika i da li mogu da ugroze, pre svega, slobodu izražavanja? Notn (Naughton, 2016)[11] ističe ogroman uticaj ovih kompanija na javnu sferu, a samim tim i demokratiju, pa analiziranje njihove odgovornosti smatra ključnim. Međutim, autor smatra da velike kompanije, poput Gugla ili Fejsbuka, nisu posebno zainteresovane za poštovanje ljudskih prava. Notn objašnjava da im industrija komunikacije nije primarna pri sticanju profita. Autor na primeru Gugla pojašanjava svoje stanovište, navodeći da su oni koji vode ovu kompaniju shvatili da je primarno ulagati u zdravstvo, energetiku ili transport, pa su svoje poslovanje proširili na ove oblasti, smatrajući ih primarnim pri ostavarivanju profita.

U tako kompleksnom komunikacionom okruženju pokreću se pitanja implikacija na postojeću regulatornu praksu. Da li bi zaštitom prava korisnika trebalo da se bavi tržište ili država, da li regulacija novog okruženja treba da bude nametnuta odozgo (*top-down)* ili da dolazi odozdo (*bottom-up*), i da li bi poštovanje prava korisnika trebalo da bude regulisano od strane države i njenog zakonskog okvira, ili pak, da budu u domenu samoregulacije?

Trebalo bi da samoregulatorna politika internet posrednika, naročito kada je reč o njihovoj odgovornosti za poštovanje prava korisnika, pomiri interes korisnika da budu „zaštićeni na mreži“ i privatni, odnosno ekonomski interes privatne kompanije, koja pruža informaciono-komunikacione usluge. Dalje, trebalo bi pomiriti interes države i njenog nacionalnog zakonskog okvira sa internacionalnim okvirom, a u skladu sa slobodnim protokom informacija. Zbog toga je jedan od najvećih regulatornih izazova uspostavljanje regulatornog balansa između suprotstavljenih interesa internet intermedijatora – države i internet korisnika. Taj balans bi podrazumevao da jača regulacija ove oblasti omogući zaštititu prava korisnika, što ne znači veću kontrolu države, jer, kako navode Ven Kulinberg i Mek Kvejl (Van Cuilenburg & McQuail) „kroz istoriju država je često percipirana kao glavni neprijatelj slobode izražavanja, dok je u isto vreme ona takođe postala, putem ustava i pravnih sistema, učinkoviti garant slobode u važnim aspektima” (2003:183). To bi bilo moguće ukoliko bi nova komunikaciona politika prepoznala intermedijatore kao značajne aktere u informaciono-komunikacionoj praksi, čime bi njihova odgovornost bila formalno povećana, a mogućnost države da zaštiti građane, kroz određeni sistem regulatorne politike, bila izvesna.

Internet prostor je često percipiran kao anarhična necentralizovana struktura, koju je nemoguće kontrolisati. Međutim, Lesing (Lessing, 2006) ističe da je osnovni problem u takvom viđenju interneta, kao neregulisanog monolitnog prostranstva, u tome što se sastoji iz mnoštva slojeva, kojima bi, prilikom analize, tako trebalo i pristupiti. Lesing ističe da je česta zabluda da je arhitektura sajber prostora takva da onemogućava kontrolu i regulaciju. Međutim, autor objašnjava da je kod, koji se nalazi ispod površine vidljive infrastrukture i čini internet takvim kakav jeste, itekako podložan upravljanju. Lesing kao primarnu ističe indirektnu kontrolu, koju smatra opasnijom, jer nemogućnost idnetifikovanja centara moći oslobađa od odgovornosti (2006: 138-157).

Države imaju različite politike u oblasti regulisanja rada interneta. Pristupi bi se mogli grupisati u dva najopštija tipa: tip koji podrazumeva strožu regulaciju i tip koji podrazumeva samoregulaciju, kao primarni pristup. U skladu sa tim i Stajn i Sinha (2006) navode dva opšta modela politike regulacije: *tržišno orjentisana politika* i *politika zasnovana na javnom interesu*. Prvi model ograničava suverenu moć države, a osnovna kritika odnosi se na eroziju vrednosti javnog dobra, koje tradicionalno

[11] Naughton, J. (2016). Digital Dominance: forget the ‘digital’ bit. *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/07/12/digital-dominance-forget-the-digital-bit/ (pristupljeno 04.02.2017. godine).

održava država. Ovaj model podrazumeva veću ulogu samoregulatorne politike. Sa druge strane, kritika drugog modela prepoznaje se u sledećem: država može da iskoristi svoju moć i da narušava ljudska prava umesto da ih sama brani, dok je očigledna prednost u zakonom zagarantovanom poštovanju opšteg interesa, nasupot komercijalnom. Zbog toga autori predlažu i treći model *internacionalni* ili *multinacionalni režim*, koji bi podrazumevao internacionalne institucije i instrumente, što bi obezbeđivalo slobodan protok informacija, ali i zaštitu ljudskih prava (Stein & Sinha 2006: 425–436). Ovaj model podrazumeva smanjenje ingerencija pojedinačnih država i obavezujuća dokumenta usvojena na nivou internacionalnih tela, kojima se uređuje oblast delatnosti internet intermedijatora. Takav je slučaj sa Savetom Evrope.

Odgovornost intermedijatora najčešće se ogleda kroz politiku samoregulacije. Jedan od primera samoregulatorne prakse jeste postupak „uoči i ukloni" (engl. *notice and takedown*), koji podrazumeva obavezu intermedijatora da kada uoče „štetni sadržaj", isti uklone sa platforme u određenom vremenskom roku. Međutim, kako Alert i saradnici (Ahlert et al.) smatraju, to se ne može činiti na osnovu nekog algoritamskog proračuna, niti su intermedijatori adekvatni za takav vid samoregulacije, što u krajnjem može dovesti do "drastičnih posledica po slobodu izražavanja" (2004: 3). Helbergerova (Helberger, 2016) ide i korak dalje, pa ističe da bi takva politika, na primeru Fejsbuka, dovela do stvaranja „privatno kontrolisane javne sfere".

Tomson (Thomson, 2016; Thomson, 2015) pak smatra da bi normativni pristup odgovornosti intermedijatora bio najbolje rešenje (2015: 803-816); samoregulatorni okvir, koji pretpostavlja da će intermedijatori reagovati na kršenje ljudskih prava, ne bi ugrozio slobodu izražavanja, dok bi istovremeno štitio pravo na privatnost korisnika. Autor tvrdi da bi traženje pravde na sudu, ukoliko dođe do povrede prava, bilo nerazumno, jer sudovi ne funkcionišu isto u vreme interneta (2015: 816–827). Takođe, Tomson smatra da problem nije u tome što bi u samoregulatornom postupku privatne kompanije bile one koje donose sud o tome šta je ispravno već bi se trebalo fokusirati na to kako one to čine, odnosno, da li je njihove delovanje u skladu sa opštim interesom.

Sledeći tvrdnju Mek Kvejla (1994) da će brz razvoj tehnologije dovesti do urušavanja normi i dovesti u pitanje tradicionalnu društvenu teoriju, koja je po svojoj prirodi neizbežno normativna, dolazimo do pitanja da li će novi akteri u komunikaciono-informacionom lancu u potpunosti urušiti stari normativni poredak, sledeći korporativnu logiku, ili će pak pokušaji da se regulacijom sačuva javni interes i odbrane ljudska prava, rezultirati uspehom. U svakom slučaju, kako je predviđao Mek Kvejl (1994), u jednom trenutku će komunikaciona politika morati da se suoči sa normativnim pitanjima.

2.2. Istraživačke metode

Analiza poštovanja prava na slobodno izražavanje i pravo na privatnost internet korisnika zahteva interdisciplinarni pristup i korišćenje više metoda. Analiza u disertaciji obuhvata četiri integralna dela: analizu regulatornog okvira Srbije, analizu politike samoregulacije internet intermedijatora (Gugl i Fejsbuk), stavove internet korisnika i komparativnu analizu politika upravljanja internetom.

Prilikom prikupljanja podataka najpre će biti korišćena **opšte naučna metoda**, kojom će biti analizirana reprezentativna literatura iz oblasti. Analizom prethodnih istraživanja iz oblasti **dedukcijom** će biti izvedeni najznačajniji aspekti istraživačkog problema. U empirijskom delu rada biće prezentovana **studija slučaja** Srbije. S obzirom na to da je pristup studije slučaja kompleksan, on obuhvata korišćenje više izvora podataka i različite analitičke metode (Perecman & Curran, 2006).

Fokus istraživanja je na zaštiti dva prava internet korisnika: pravo na slobodno izražavanje i pravo na privatnost, te je neophodno definisati šta se podrazumeva pod kršenjem tih prava. Pod ugrožavanjem prava na slobodno izražavanja koje, kako definiše *Evropska konvencija za zaštitu ljudska prava i osnovnih sloboda*, uključuje "slobodu posedovanja sopstvenog mišljenja, primanja i saopštavanja informacija i ideja bez mešanja javne vlasti i bez obzira na granice"[12] smatraće se neopravdani nadzor od strane države, sajber napadi koji imaju za cilj ometanje pristupa određenim sadržajima, pravna uznemiravanja korisnika zbog iskazivanja onlajn mišljenja i ostale pravne posledice.

Poštovanje prava na privatnost biće drugo analizirano pravo u ovom radu. Ugroženo pravo na privatnost podrazumeva nemogućnost korisnika da ostvare jasan uvid u to ko, kada i na koji način može da raspolaže njihovim ličnim podacima. Premda samoregulatorna politika intermedijatora uglavnom garantuje zaštitu ličnih podataka podeljenih na mreži, mnoge podstavke podrazumevaju slobodno korišćenje podataka u komercijalne svrhe. Takav vid raspolaganja privatnim podacima podrazumeva da intermedijatori dele informacije o korisnicima sa privatnim firmama partnerima, kako bi im omogućili direktan pristup ciljnoj grupi. Takođe, moguće kršenje prava na privatnost podrazumeva da intermedijatori mogu proslediti vladama podatke o korisnicima, ukoliko se proceni da je određena informacija od značaja za državu, a ukoliko je takav ustupak zakonom uslovljen, odnosno zagarantovan[13].

Prvi deo analize podrazumeva **analizu regulatornog okvira Srbije**, kojim se uređuje zaštita prava na privatnost i sloboda izražavanja na internetu. Stoga će osnovnu građu analize predstavljati odredbe zakonske regulative, kojima se uređuje analizirana oblast. Ovakav pristup omogućava detaljnu

[12] Dostupno na: http://www.sostelefon.org.rs/zakoni/14.%20Evropska%20konvencija%20za%20zastitu%20ljudskih%20prava%20i%20osnovnih.pdf (pristupljeno 02. 02. 2017. godine).

[13] Takav je slučaj, na primer, sa *Tehničkim uslovima* iz 2009. koje je usvojio RATEL i kojima se direktno ugrožava pravo na privatnost korisnika, ali i na slobodu izražavanja. U prvom članu ovog akta navodi se: "Ovim aktom definišu se tehnički uslovi za podsisteme, uređaje, opremu, instalacije, sistemski i aplikativni softver i baze podataka javnih telekomunikacionih operatora (mrežni operatori, pružaoci usluga i pružaoci pristupa) za potrebe vršenja elektronskog nadzora određenih telekomunikacija od strane nadležnih državnih organa u skladu sa zakonom". Dostupno na: http://www.ratel.rs/editor_files/File/dozvole/uputstva/Tehnicki_uslovi-internet.pdf (pristupljeno 07. 02. 2017. godine).

analizu celovitog okvira, korišćenjem raznovrsnih izvora podataka, od nacionalnih do međunarodnih zakonskih dokumenata, koji se primenjuju u Srbiji.

Drugi deo analize podrazumeva detaljnu **analizu samoregulatornih politika kompanija Gugl i Fejsbuk**, u oblasti kojom se uređuje pravo na privatnost i sloboda izražavanja korisnika. Analiza samoregulatorne politike internet intermedijatora značajna je kako bi se ukazalo na neophodnost jasno definisane odgovornosti privatnih aktera prema korisnicima, onda kada je reč o zaštiti prava korisnika.

Treći deo analize odnosi se na stav internet korisnika o zaštiti njihovih prava. Korišćenjem kvantitativne **metode anketiranja internet korisnika u Srbiji**, cilj je utvrditi njihov stav o zaštiti prava na privatnost i slobodno izražavanje na internetu. Ova metoda, kao najčešće korišćena u društvenim naukama, ima za cilj da omogući razumevanje načina na koji društvo funkcioniše (Groves et al, 2004). U ovom konkretnom istraživanju značaj primene navedene metode, odnosno značaj dobijenih rezultata, ogleda se u dolaženju do zaključaka koji se implicitno odnose na politike odgovornosti, kako države tako i intermedijatora. Detektovanje problema korisnika značajno je u delu koji se tiče definisanja regulatornih mera države, ali i samoregulatornih politika intermedijatora, koji bi vodili ka sigurnom internet prostoru.

Za potrebe ovog istraživanja najpogodniji je uzorak koji se ne zasniva na teoriji verovatnoće, odnosno namerni uzorak, baziran na *tehnici grudve*. Naime, kada je reč o ovom tipu uzorkovanja, ispitanici se biraju na osnovu unapred utvrđenih karakteristika i aktivnosti. U slučaju ovog istraživanja ispitanici su aktivni internet korisnici, stoga bi metod uzorkovanja koji pretpostavlja teoriju verovatnoće bio nepogodan. Očigledan nedostatak je to što uzorak ne može biti reprezentativan, ali je prednost to što su karakteristike i aktivnosti ispitanika u direktnoj vezi sa unapred utvrđenim predmetom i ciljem istraživanja (Vanderstoep & Johnston, 2009).

U četvrtom delu analize **komparativnim metodom** biće upoređene različite politike upravljanja internetom, naročito u oblasti poštovanja prava na slobodno izražavanje i privatnost. Poređenja će omogućiti klasifikaciju modela državnog upravljanja internetom i predlog novog modela upravljanja internetom, koji će uključiti sve prethodno analizirane aktere: državu, intermedijatore i korisnike.

Prilikom obrade podataka, dobijenih teorijsko-analitičkom metodom, biće korišćena analitičko-deskriptivna metoda, kojom će se teorijska građa detaljno obrazložiti i analizirati. Za obradu podataka dobijenih metodom ankete, biće korišćena statistička metoda obrade podataka. Metodom sinteze, dobijeni rezultati biće uobličeni i prezentovani u zaključnom delu rada.

2.3. Predmet i cilj istraživanja

Predmet ove doktorske disertacije jesu **pravo na privatnost** i **pravo na slobodu izražavanja internet korisnika**. Predmet istraživanja biće analiziran sa **četiri aspekta**:

1. Sa jedne strane biće analiziran ***odnos države Srbije prema pravima internet korisnika***, odnosno poštovanju na privatnost i slobodno izražavanje, koji se ogleda u regulatornoj politici, ali i primerima iz prakse.

2. Drugi aspekt podrazumeva ***analizu politike odgovornosti internet intermedijatora***, kada je reč o poštovanju prava korisnika, a koja se, pre svega, ogleda u samoregulatornoj praksi.

3. Treći aspekt analize jeste ***stav internet korisnika u Srbiji prema poštovanju njihovih prava na slobodno izražavanje i privatnost na internetu*** od strane države i privatnih kompanija, ali i dolaženje do podataka koliko su internet korisnici u Srbiji upoznati sa politikama u ovoj oblasti, te da li su i sami odgovorni korisnici internet usluga.

4. Četvrti aspekt podrazumeva ***komparaciju različitih nacionalnih politika upravljanja internetom*** u ovoj oblasti i dolaženje do klasifikacije modela državnog upravljanja internetom, ali i definisanje ideal-tipskog modela upravljanja internetom, koji bi uključio sve dobre prakse kompariranih modela, a one negativne sveo na minimum.

Cilj ove disertacije jeste da ukaže na značaj izgradnje komunikacione politike kojom bi se garantovala zaštita prava na privatnost i slobodno izražavanje na internetu. Istraživanja koja preispituju ovu delatnost u Srbiji tek su u povoju, stoga, predloženo istraživanje ima za cilj da nadogradi postojeće rezultate prikupljanjem podataka za Srbiju. Detaljnom analizom regulatorne politike Srbije i samoregulatorne politike intermedijatora u oblasti poštovanja dva navedena prava, cilj je da se doprinese globalnoj raspravi o izazovima pri zaštiti prava na slobodu izražavanja i prava na privatnost internet korisnika. Takođe, cilj je da se, na osnovu dosadašnjih istraživanja u drugim državama, definišu preliminarni tipovi politika odgovornosti pri zaštiti navedenih prava, odnosno da se izvrši njihova klasifikacija. Cilj je i da se na osnovu komparativne analize nacionalnih primera ponudi model koji bi uključio sve tri strane: državu, intermedijatore i korisnike, a koji bi mogao da bude održiv u različitim okolnostima internet okruženja i nacionalnih politika.

S obzirom na to da se u Srbiji niko nije detaljno bavio izazovima regulacije i samoregulacije u oblasti novog informaciono-komunikacionog okruženja, posebno odgovornosti internet intermedijatora za poštovanja prava korisnika, **teorijski cilj rada** jeste i upotpunjavanje domaće literature iz ove istraživačke oblasti.

Praktični cilj jeste ukazivanje na sukobljene pozicije državne politike i biznis politike intermedijatora, dolaženje do odgovora ko u tim sukobima ipak uspeva da nametne svoj interes i da li je presudan interes vlade, komercijalni interes tržišta ili javni interes građana.

2.4. Istraživačka pitanja i hipoteze

U nastavku su navedena istraživačka pitanja iz kojih proizlaze hipoteze koje će biti testirane u doktorskoj tezi. Svako od istraživačkih pitanja odnosi se na jedan aspekt analize zaštite prava na privatnost i slobodno izražavanje na internetu: državu, internet intermedijatore i internet korisnike.

Istraživačko pitanje 1 (IP 1): Na koji način je u Srbiji regulisana zaštita prava na privatnost i slobodu izražavanja internet korisnika?

Hipoteza 1 (H1): Regulatorni okvir Srbije, u delu koji se tiče slobode izražavanja i prava na privatnost na internetu, nije u potpunosti posvećen zaštiti građana/korisnika, već jednim delom ide u prilog intermedijatora i same države, narušavajući prava korisnika.

Ova hipoteza testiraće se analizom dokumenata kojima se reguliše istraživana oblast. Regulatorni okvir Srbije biće analiziran na nivou tela izvršne vlasti, koja regulišu oblast informisanja i telekomunikacija: Ministarstvo kulture i informisanja i Ministarstvo trgovine, turizma i telekomunikacija; i na nivou regulatornih tela: Regulatorno telo za elektronske medije i Regulatorna agencija za elektronske komunikacije i poštanske usluge. Takođe, biće analizirana i međunarodna dokumenta, koja regulišu ovu oblast, a koja su primenljiva u Srbiji. Za ilustraciju primene zakona, biće korišćeni i primeri iz prakse.

- **IP2: Da li je samoregulatorna politika internet intermedijatora u delu koji se tiče poštovanja prava na privatnost i slobodu izražavanja u skladu sa interesima korisnika?**

- *H2: Samoregulatorna politika internet intermedijatora ne garantuje apsolutnu zaštitu prava na privatnost i slobodno izražavanje korisnicima.*

Kada je reč o samoregulatornoj praksi internet intermedijatora, biće analizirani *Uslovi korišćenja* Fejsbuk kompanije o pravima i obavezama u delu koji se tiče zaštite privatnosti i slobode izražavanja i zvanični *Uslovi korišćenja* kompanije Gugl, te u delu koji se tiče politike privatnosti, kao i izveštaji o transparentnosti, koji se tiču ugrožavanja slobode izražavanja korisnika, uglavnom pod pritiskom vlada različitih zemalja. Da bi se testirala postavljena hipoteza, biće analizirana i usklađenost politika privatnosti i uslova korišćenja sa evropskom regulativom.

IP3: Kakav je stav internet korisnika u Srbiji o zaštiti njihovih prava u onlajn prostoru?

- H3: Internet korisnici u Srbiji osećaju se nesigurno prilikom deljenja ličnih podataka na internetu.

- *H3a. Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožava država.*

- *H3b. Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožavaju privatni akteri (Gugl i Fejsbuk)*

- H4: Internet korisnici u Srbiji ne veruju u odgovornost internet intermedijatora i pravne mogućnosti države, kada je reč o zaštiti njihovog prava na slobodno izražavanje u onlajn-prostoru.

- *H4a. Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožava država.*

- *H4b. Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožavaju privatni akteri (Gugl i Fejsbuk).*

- H5. Internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti kada je reč o zaštiti njihovih prava na internetu**.**

H5a: *Internet korisnici u Srbiji ne čine dovoljno da zaštite svoju privatnost, iako su svesni rizika od zloupotrebe ličnih podataka*.

- H5b: *Internet korisnici u Srbiji nisu u dovoljnoj meri upoznati sa Uslovima korišćenja kompanija čije usluge koriste***.**

Navedene hipoteze testiraće se kroz anketno ispitivanje internet korisnika u Srbiji, odnosno statističkom analizom njihovih odgovora. Testiranje postavljenih hipoteza pružiće uvid u to kakav je stav internet korisnika o zaštiti njihovih prava u onlajn-prostoru. Većina istraživanja koja se bave poštovanjem prava korisnika u onlajn-prostoru ne bave se analizom stavova korisnika, već samo regulatornom, odnosno samoregulatornom politikom. Ispitivanje stavova korisnika važno je zbog dobijanja uvida u to koliko je korisnicima značajna zaštita njihovih prava i da li se osećaju dovoljno zaštićenim od strane (inter)nacionalnih zakona i samoregulatorne politike intermedijatora. Takođe, značajan je i nalaz koliko su sami korisnici svesni rizika i u skladu sa tim odgovorni prilikom korišćenja internet usluga.

3. Regulatorni izazovi i uloga države u globalizovanom informaciono-komunikacionom sistemu

Moć države nikada nije bila više problematizovana u istoriji nego u poslednjih nekoliko decenija. Suverenitet države u doba interneta često se dovodi u pitanje, jer globalizovanim informaciono-komunikacionim sistemom (IKS) ne mogu samostalno da upravljaju pojedinačne države, pri čemu je fokus je na kooperaciji i umreženom upravljanju, koje uključuje kako države i nadnacionalna tela, tako i privatne kompanije i civilni sektor.

Ključni koncepti u ovom poglavlju jesu ***država*** i ***regulacija*** – u skladu sa tim, biće analizirana uloga države u regulaciji protoka informacija u dva okruženja: najpre u *tradicionalnom*, a potom i *internet okruženju*, koje je u najvećoj meri uticalo na izgradnju *globalizovanog IKS*. Pod globalizovanim IKS u ovom radu smatraju se međusobno povezani nacionalni informaciono-komunikacioni sistemi, koji su u eri interneta više nego ikada ranije upućeni jedni na druge i prinuđeni na saradnju.

Praćenjem regulatorne uloge države od tradicionalnog okruženja do učešća u regulisanju internet prostora, nastojaće se da se ukaže na značaj slobodnog tržišta, kako u tradicionalnom IKS, tako i u globalizovanom, ali i na neophodnost regulisanja odnosa u takvom okruženju, u cilju ostvarivanja javnog interesa. Jedan od ciljeva ovog poglavlja je oduzmanje negativnog predznaka regulaciji, ali i ukazivanje na regulatorne zloupotrebe, kojima su sklone uglavnom autoritarne vlade.

Kroz faze razvoja regulacije internet prostora, biće ukazano na sve veće učešće država u regulisanju internet okruženja, bilo ono samostalno ili u kooperaciji sa međunarodnom (ne)vladinim institucijama i drugim državama. U ovom delu posebno će biti analizirana promenjena uloga države i polemisaće se o njenoj moći i suverenitetu u novom okruženju. Takođe, biće analizirani i različiti modeli upravlja informacijama u novom IKS.

U drugom delu poglavlja tema će biti uloga države u zaštiti ljudskih prava, ali će analiza obuhvatiti i nadnacionalne sisteme zaštite. Pravo na privatnost i slobodno izražavanje na internetu biće posebno analizirana u okviru ovog potpoglavlja. Država će ponovo biti jedan od centralnih aktera, kada je reč o izazovima koji se tiču zaštite pomenuta dva prava na internetu, premda će i privatni akteri i međunarodne institucije imati značajnu ulogu.

Argument u ovom poglavlju je da je regulatorna uloga države u globalizovanom IKS promenjena i suočena sa mnogobrojnim izazovima, ali ne i ništavna. Promenjena uloga ne znači nužno i slabljenje suvereniteta – pojedinačni sistemi jesu umreženi, prelivaju se jedni u druge, a ponekad je teško jasno im odrediti granice, ali ipak nacionalni sistemi ostaju stub globalizovanog IKS. U globalizovanom IKS prepoznaje se prostor za distinkciju nacionalnih sistema, koje je novo okruženje promenilo, ali ne i poništilo.

Poslednji deo ovog poglavlja ima za cilj da predočene teorijske postavke o regulatornoj ulozi države u novom okruženju primeni na studiju slučaja Srbije, odnosno da se na primeru jednog nacionalnog regulatornog okvira ukaže na ulogu države u regulisanju prava na slobodno izražavanje i privatnost na internetu. Analizom zakonodavnog okvira Srbije, koji se odnosi na dva prava koja su predmet analize, biće prikazano da su izazovi koje donosi internet komunikacija i poštovanje ljudskih

prava „na mreži" još izraženiji u zemljama mlade demokratije. Pretpostavka od koje se polazi jeste da da regulatorni okvir Srbije ne štiti u potpunosti navedena dva prava svojih građana/internet korisnika.

3.1. Regulacija tradicionalnih medija i javni interes

Jedino slobodni mediji mogu služiti građanima, odnosno javnom interesu, i biti stožer demokratiji. Napisana teza vremenom je postala aksiom, podrazumeva se i predstavlja polaznu osnovu za mnogobrojna istraživanja medija i njihovog delovanja. Kada kažemo da bi mediji morali biti slobodni, podrazumevamo slobodu u najopštijem smislu – slobodni od stega države, političkih, ekonomskih i drugih interesnih pritisaka. Kako Veljanovski ističe: „Iskustvo je pokazalo, a teorija utvrdila da demokratskog društva nema bez slobodne sfere javnosti, a da, opet, slobodne sfere javnosti nema ako u njoj postoji bilo čiji monopol: države, politike, biznisa ili drugih centara moći" (2009: 58). Međutim, pitanje koje se nameće je: Da li slobodu i ostvarivanje javnog interesa omogućava apsolutno slobodno tržište ili regulisano medijsko okruženje? U razvijenim zemaljama, gde je gotovo svaki segment života podređen kapitalizmu i konzumerizmu, da li bi trebalo i informaciju podrediti isključivo tržišnoj potražnji ili je pak, shodno njenoj moći i značaju, potrebno tretirati je drugačije od ostalih roba koje su u opticaju (Bal, 1997; Lorimer, 1998)?

U dobu razvijenog kapitalizma informaciju možemo grubo okarakterisati kao robu, jer je činjenica da je ona glavni produkt medijskih preduzeća. Međutim, ovako formulisan odnos informacije (robe) i medija (preduzeća) blizak je upravo kapitalističkoj percepciji, koja u prvi plan ističe profit, zamagljujući suštinu medija – rad u javnom interesu.

Pristup koji medije vidi isključivo kao privatna preduzeća, a njihove usluge, samo kao komercijalne, informaciju izjednačava sa robom, kojoj bi se trebalo pristupiti kao i bilo kom drugom proizvodu na otvorenom i konkurentnom tržištu. Međutim, pravila koja važe za medije ne mogu se izjednačiti sa pravilima koja važe za naftnu, farmaceutsku ili ma koju drugu industriju. Ukoliko to učinimo, informacija postaje ono što Fransis Bal (Francis Balle) naziva „namirnica među drugim namirnicama", ili „big business" (1997: 48). Informacija nije materijalna roba lišena smisla i uticaja. Informacija je moć; ona koja upravlja životima ljudi i u krajnjem utiče na njihove postupke i odluke.

Polemišući o informaciji kao robi, Veljanovski staje u odbranu informacije kao nematerijalnog dobra, koji se ne može tretirati kao roba: „Ovakav rezon mnogo se više poklapa sa zalaganjima koja medije vide kao konstruktivan element u podsticanju demokratskih tokova i širenja prostora građanskih sloboda" (2009: 58). Upravo je ta moć upravljanja smislom sveta u kojem živimo ono što je odvaja od svih ostalih roba i iziskuje drugačiji pristup. Međutim, svaka moć privlači kontrolu. Naročito onda kada je ta moć upravo ona koja osnažava korisnike medija kao građane da odlučuju o tome kome će poveriti političku moć.

Bal (1997) se u knjizi „Moć medija“ fokusira, pre svega, na odnos između medija, tržišta i državnih službenika, odnosno „posrednika, trgovaca i mandarina”[14] i na njihovu borbu za uspostavljanje kontrole. Ističući značaj slobodnih medija, autor odbacuje sve vidove kontrole i postulira tržište kao jedini okvir kojim se može regulisati protok informacija, ideja, a u skladu sa demokratskim principima, oslikanim u logici liberalne tržišne konkurentnosti. Ipak, Bal, još na početku postavlja ključno pitanje: „Dokle se tržište može prostirati a da pri tom ne ode predaleko? [...] Ukoliko tržišna ekonomija prati političku demokratiju, ne dogodi li se, ponekad, da postane neposlušna? Pa da, putem, zagubi svog pratioca, izlažući ga tako opasnosti da izgubi razum, štaviše i dušu?” (1997: 5).

U zemljama sa demokratskim uređenjem jedino tržište (Balovi „trgovci”) može da ponudi okvir koji nudi ispunjenje osnovnog postulata slobode medija. Međutim, da li bi pojedine sfere društvenog života trebalo da budu izuzete iz surove logike kapitalizma? Bal zaključuje da je mogućnost izbora neophodna, predstavlja prioritet i polaznu osnovu za demokratiju, ali ono što je takođe neophodno jeste „znati u kojim granicama se to zbiva; mediji, državni službenici i tržište moraju da sarađuju i čine „trougao demokratije” (1997: 108, 126).

Rolend Lorimer (Rowland Lorimer, 1998), takođe, naglašava tezu „slobodna štampa, slobodno tržište” (str. 113). Međutim, Lorimer nudi i načine za ublažavanje „surovih zakona tržišta” kroz „državnu intervenciju na tržištu, odnosno političku ekonomiju, to jest ubacivanje kulturno-političkih ciljeva pri određivanju okvira, unutar kojih ekonomska aktivnost sme da se odigra” (str. 111). Silvija Harvi (Silvia Harvey) to naziva „intervencionizam u javnom interesu osmišljen da bi bila omogućena 'prava na komunikaciju'” (u Brigs i Kobli, 2005: 340). Načelno, to bi značilo da državna intervencija, u smislu regulacije medijskog tržišta i šire informaciono-kounikacionog sistema, može biti pozitivna kada ***za cilj ima odbrane javnog interesa***.

Pojam ***javni interes***, zbog svoje opštosti i apstraktnosti, teško je ograničiti na pojedinačine aspekte i definisati. Takođe, trebalo bi imati na umu da: „nema *javnog interesa* koji bi bio nepromenljiva, istorijski i kontekstualno nezasvisna i zbog toga *trajna kategorija*” (Radojković, 2016: 15). Javni interes je koncept koji izaziva dosta polemika, zbog svoje nestalne prirode, podložne različitim interpretacijama u različitim prilikama i periodima. U ovom delu rada koristi se Mekvejlov (McQuail, 1994; 1995) pristup prilikom definisanja javnog interesa.

Denis Mekvejl, pozivajući se na Helda, (Held, 1970, u McQuail, 1995) navodi tri najopštija razmatranja ovog pojma kroz tipologiju ideja o javnom interesu: *teorija prevladavanja, teorija zajedničkog interesa* i *unitarna teorija*. *Teorija prevladavanja* podrazumeva da je javni interes volja većine. Ovakav pristup javnom interesu može se najjednostavnije prepoznati kroz praksu glasanja. Teorija prevladavanja sugeriše da je volja većine merilo javnog interesa, a njena slabost ogleda se u potencijalnom konfliktu sa onim delom javnosti koji javni interes doživaljava kao „nešto više od skupa individualnih preferencija” (McQuail, 1995: 23).

Teorija zajedničkog interesa pretpostavlja da javni interes predstavlja najopštije zajedničke interese svih ljudi, potrebne da bi jedno društvo funkcionisalo (električnu energiju, vodu, zakone itd).

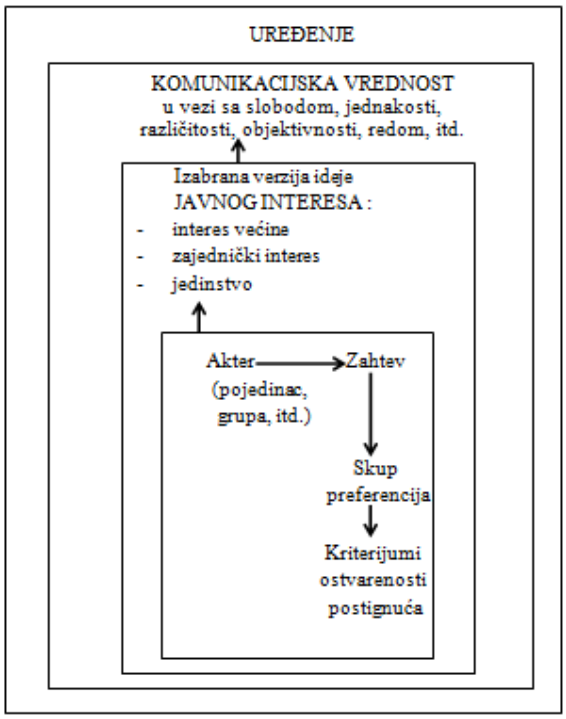
[14] Fransis Bal pod *mandarinima* podrazumeva državne službenike, umetnike, naučnike, koji su nekada imali monopol nad sredstvima informisanja. *Trgovci* su za Bala igrači na tržištu, koji se vode isključivo komercijalnim idealima definisanim tržištem. *Posrednici* su, u ovoj raspodeli uloga, mediji; oni koji posreduju između centara moći i publike, odnosno građana. Kontrolu nad informacijom u najvećoj meri imaju trgovci, ali Bal smatra da posrednici mogu povratiti kontrolu, ukoliko se pridržavaju standarda profesionalizma i etičkih principa i na taj način zaista samo nezavisno posreduju, štiteći javni interes.

Slabost ove teorije je u tome što se zalaže za određene ciljeve, ali ne iskazuje potrebu za ispunjenjem nekih posebnih ciljeva. *Unitarna teorija*, bliska antičkim filozofima i marksistima, kao merilo onog što je javni interes uzima neke apsolutne normativne principe, koji su deo veće ideologije (McQuail, 1995: 22–23).

Mekvejl ističe da, tragajući za definicijom javnog interesa koji bi trebalo da ostvaruju mediji, možemo prepoznati različite elemente svake od navedenih teorija, ali da bismo razumeli koncept javnog interesa moramo ga raščlaniti na elemente i pratiti njihove korelacije u konkretnom društvu. Zbog toga Mekvejl nudi okvir za identifikovanje procena zahteva za javnim interesom u medijima (kako je prikazano u Grafikonu 1).

Najopštiji agens jeste *uređenje*, pod kojim pored državnog uređenja, koje se ogleda u regulatornom okviru, Mekvejl podrazumeva i druge vrste „javnog foruma", profesionalnog i samoregulatornog, koji utiču na donošenje odluka. *Komunikacijske vrednosti* odnose se na „opšte dobro" koje se od komunikacije očekuje, a koje su u vezi sa *odabranom idejom o javnom interesu*, koja, kako Mekvejl navodi „pomaže da se izdvoje potencijalno relevantna pitanja pri istraživanju medijskih performansi od čisto sektorskih, individualnih ili idiosinkratičkih tački gledišta" (1995: 29). *Akteri* ili *agenti preferencija* jesu oni koji određuju standard, često mogu imati lične interese, ali mogu i braniti javni interes; njih prepoznajemo kao javnu vlast, političke i društvene institucije, industrijske unije, istraživače, medijske profesionalce itd. *Zahtevi*, koji su u središtu, ima najznačajniju ulogu; „ovi zahtevi zapravo predstavljaju ciljeve ili uopštene težnje za ostvarenjem komunikacijskih vrednosti i obezbeđivanje podrške za sveobuhvatne i dugoročne ciljeve i koristi za društvo. Često se dešava da su takvi zahtevi kontradiktorni i kontrastni" (str. 29). *Skup preferencija* odnosi se na željene forme informacija, pristupa, slobode, ali i na restrikcije, dok se poslednji element tiče *kriterijuma postignuća*, odnosno uspešnosti, koji daje detaljnije indikatore za evaluaciju konkretnih performansi.

U kojoj meri će se zahtevati ostvarivanje javnog interesa, i na koji način će javni interes biti percipiran u konkretnom društvenom uređenju zavisi od mnogobrojnih agenasa koji na to utiču, a koji su obuhvaćeni Mekvejlovim okvirom za identifikovanje. Proces, od ideje javnog interesa koja je dominantna u jednom društvu do kriterijuma kojima se evaluira postignuće, odnosno ostvareni javni interes u medijima jeste kompleksan.



Grafikon 1 Okvir za identifikovanje procena zahteva za javnim interesom u medijima (prema McQuail 1995: 28)

Mekvejl je u članku *Masovno komuniciranje i javni interes: ka društvenoj teoriji strukture i funkcije medija* (u Denis Mekvejl, Stari kontinent – novi mediji, 1994: 85–113), između ostalog, pokušao da odgovori na pitanje koji su to zahtevi koji se najčešće stavljaju pred medije i medijske profesionalce, kada je reč o ostvarivanju javnog interesa. Autor navodi pet takvih zahteva: *sloboda, raznovrsnost, kvalitet informacija, društveni poredak i solidarnost* i *kulturni poredak* (str. 102-109).

Sloboda je zahtev koji se podrazumeva, kako u radu medija, tako i uopšte u odnosima u demokratskim društvima. Međutim, Mekvejl ističe da je sloboda koncept koji je kompleksan za definisanje, ali i ostvarivanje, naročito zbog raznovrsnih okolnosti pod kojima se teži njenom ostvarenju. Autor navodi da se pod slobodom u komuniciranju najčešće podrazumevaju: nepostojanje cenzure, neometan pristup izvorima informacija, kritički odnos prema društvenoj zbilji i slično. Međutim, ostvarivanje ovih zahteva može često biti i kontradiktorno. U tom kontekstu Mekvejl navodi primere sledećih protivurečnosti: apsolutna sloboda nije moguća, jer može narušiti prava drugog; „vlada ili javna tela nekad nužno moraju da intervenišu da bi osigurali slobode koje, u praksi, sam sistem ne omogućava automatski" (1994: 103). Zbog sveprisutne komercijalizacije medija, Miroljub Radojković slobodi pripisuje i „zahtev da se spreči prikriveni uticaj vlasnika i oglašivača na učitavanje značenja u vestima i komentarima" i dodaje da se sloboda danas „sučeljava sa vrednostima koje su po definiciji takođe sastojak javnog interesa kao što su duhovno i fizičko zdravlje dece, očuvanje privatnosti i dostojanstva građana" (Radojković, 2016: 11).

Raznovrsnost je, kao i sloboda, često upotrebljavan koncept u teoriji medija, koji je vremenom izgubio jasno značenje, jer uključuje mnogo raznolikih elemenata, a sa druge strane ima svoje pritivurečnosti i različito se interpretira u odnosu na okolnosti pod kojima se ostvaruje. Najopštije,

raznovrsnost podrazumeva pluralizam izvora informacija, raznovrsne sadržaje, dok „raznovrsnost u užem smislu podrazumeva široku lepezu proizvoda medijske kulture za sve uzraste, ukuse i interesovanja" (Radojković, 2016: 12). Mekvejl u ovom zahtevu naročito vrednuje dobrobiti koje iz njega proizlaze, a odnose se na učešće manjinskih glasova i doprinos društveno-kulturnom bogatstvu.

Kvalitet informacije naročito je dovedena u pitanje u savremenom digitalnom dobu. Internet pruža mogućnost da svako sebe nazove "komunikatorom" i širi informacije koje mogu biti ne samo manjeg kvaliteta, jer nisu uobličene kroz prizmu profesionalizma, već mogu biti poluinformacije, govor mržnje, dezinformacije, pa i puke laži (Radojković, 2016). Mekvejl se pri određenju koncepta kvaliteta informacije poziva na tradicionalne zahteve za objektivnim, pravovremenim, verodostojnim, potpunim informacijama, premda ukazuje na poteškoće pri njihovom ostvarivanju u praksi, jer navedeni pojmovi nisu statični i nepromenljivi, pa ni kruto definisani.

Kada je reč o *društvenom poretku i solidarnosti*, ključna su pitanja integracije društva, poštovanje zakona i poretka, pridržavanje moralnih normi društva i slično. Međutim, ispunjavanje ovog zahteva, možda više od svih prethodnih, može dovesti do sukoba sa javnim interesom. O tome piše Radojković, navodeći primer vanrednih stanja kada je, nekada i ustavom, cenzura medija dozvoljena, jer je nacionalna bezbednost opravdava. Na taj način se sukobljavaju zahtev za očuvanjem društvenog poretka sa zahtevom za slobodu (Radojković, 2016: 13). Mekvejl ističe da je ovaj zahtev teško proceniti mimo društveno-političkog konteksta i nezavisno od vremena i okolnosti pod kojima se posmatra.

Kulturni poredak je zahtev oko koga postoji najmanje saglasnosti. Mekvejl piše da bi mediji trebalo da podstiču kulturnu kreativnost, da reflektuju kulturu društva, međutim, iako poželjni, ovi imperativi se teško mogu ostvariti prinudno. Kao primer suprostvaljenih mišljenja, Radojković navodi sukob onih koji smatraju da bi mediji trebalo da reflektuju etablirane kulturne vrednosti i zagovornika kontrakulturnih vrednosti, jer svako iz svog ugla javnim interesom smatra upravo vidljivost svojih vrednosti (Radojković, 2016: 13).

Zahtevi koji su navedeni ne mogu se istovremeno u svakom trenutku ostvariti u jednom društvu. Radojković u tom kontekstu piše o *usaglašavanju* navedenih zahteva, i pod time podrazumeva davanje na značaju nekim zahtevima na račun drugog/drugih, i obrnuto, u zavisnosti od trenutnih okolnosti (Radojković, 2016: 15). Mekvejl u skladu s tim i ističe da svaki od pet navedenih zahteva možemo posmatrati u konkretnom društvu, uređenju i trenutku, jer mimo konteksta ovi zahtevi predstavljaju samo ideal koji se postavlja pred medije i novinare.

Mekvejl (1995) kao najopštiji okvir, kojim se procenjuju zahtevi za javnim interesom, postulira *uređenje*, koje se pre svega ogleda u regulatornim merama. Regulacija IKS uopšte podrazumeva državnu intervenciju zbog očuvanja javnog interesa, ali i iz ekonomskih i tehničkih razloga. U tom kontekstu, Fejntak i Varni (Feintuck, Varney, 2006) iznose zanimljivu tezu: „efektivna komunikacija zavisi od efektivne regulacije komunikacije" (str. 56). Autori ističu da će ovo možda zvučati paradoksalno, ali u nastavku daju slikovito obrazloženje: „Kao što dvoje ljudi koji govore simultano ne dovodi do efektivne komunikacije, emitovanje dve radio stanice na istoj frekvenciji ili mešanje u transmisiju podjedanko je nezadovoljavajuće" (str. 56). U tom smislu, kontrola koja se ostvaruje regulacijom medija poželjna je u meri koja osigurava javni interes i sprečava korišćenje medija u destruktivne svrhe, bilo da je reč o destrukciji javnog interesa, pluralizma, demokratskog postupanja ili, u širem smislu, destrukciji ljudskih prava. Kako ističu Fejntak i Varni, činjenica da su demokratskom društvu neophodni mediji ne može biti prenaglašena, iz čega sledi „da demokratija zahteva građane

koji su informisani, ukoliko su efektivni kao građani, jeste *prima facie* opravdanje za regulaciju u okviru demokratskog konteksta" (2006: 5).

Fejntak i Varni (2006: 55–66) navode četiri razloga kojima opravdavaju regulaciju medija: *efektivnu komunikaciju*, *političku i kulturnu raznolikost*, *ekonomsku opravdanost* i *javnu službu*. Autori pod *efektivnom komunikacijom* ne podrazumevaju samo slobodu govora, već i pristup raznovrsnim izvorima, što se oslanja na drugi argument *političke i kulturne raznolikosti*. Jasno je da raznolikosti nema onde gde vlada monopol nad izvorima informacija, bilo da je reč o monopolu države ili privatnog sektora. Dalje, navedeni argumenti odnose se na treći razlog, koji podrazumeva *ekonomsku opravdanost* regulacije, što daje državi mogućnost da regulacijom medijskog tržišta pospeši pluralitet i spreči monopol u medijskom sektoru. Sva tri razloga, uzeta zajedno, govore u prilog poslednjem, koji se odnosi na *javnu službu*. Slično, Mekvejl i Van Kulinberg (Van Cuilenburg & McQuail, 2003) u modelu nacionalne komunikacione politike definišu javni interes kroz političko, društveno i ekonomsko blagostanje.

Uopštavajući odnos vladinih regulatornih mera i zahteva za slobodom, Mekvejl navodi da:

> „istorijska progresija može biti sumirana kao pomeranje od *gušenja* (u ime države i religije), ka *prohibiciji* (selektivno primenjenoj), ka *ovlašćenju* (ograničenom, u ime sloboda i biznisa), ka *preporukama* (koje ohrabruju obrazovne i kulturne ciljeve), ka *libertarijanizmu* (zahteva tržišta za nesmetanom slobodom funkcionisanja). Neizbežno, trenutno stanje medijskih institucija nudi mešavinu svih ovih elemenata, iako *gušenje* nije više legitimna ili upotrebljiva moderna opcija" (McQuail, 1995: 9).

Regulacija medija počela je sa regulacijom štampanih medija, odnosno sa masovnom distribucijom knjiga, sredinom 15. veka, da bi se kasnije nastavila sa razvojem štampe, kao prvog medija masovnog komuniciranja. Pojava radija, kasnije i televizije označila je nastavak regulatornih aktivnosti, sada radiodifuzije, koja nikada nije dostigla nivo slobode kao štampa. Naime, štampa je od svih medija masovnog komuniciranja najmanje podložna regulaciji. U većina razvijenih zemalja štampa se oslanja samo na samoregulaciju, odnosno poštovanje kodeksa i etičkih standarda uspostavljanih unutar profesije[15]. Međutim, kao što je već bilo reči, ukoliko je tržište jedini regulator, postoji opasnost od koncentracije, komercijalizacije i urušavanja javnog interesa.

Sa druge strane, regulacija radiodifuzije je kompleksnija i jača. Potreba za regulacijom elektronskih medija može se objasniti kroz dva najopštija razloga. Prvi se odnosi na to da je spektar, kojim se koriste elektronski mediji, vlasništvo države, odnosno u širem smislu vlasništvo građana i da je ograničen, premda u doba digitalizacije ovaj argument gubi na značaju[16]. S druge strane, moć medija, o kojoj je bilo reči, da bi bila upotrebljena u svrhu javnog, a ne privatnog ili pojedinačnog

[15] Na primer, štampa u Britaniji nije podvrgnuta nijednom vidu regulacije. Samoregulativni mehanizam je do septembra 2014. godine ostvarivan putem *Žalbene komisije za štampu* (*Press Complaints Commission*). Informacija o zatvaranju *Žalbene komisije* dostupna je na njihovom zvaničnom sajtu: http://www.pcc.org.uk/ (pristupljeno 12.11.2017. godine). *Žalbenu komisiju* je, usled afere o hakovanju telefona iz 2011. godine, u koju su bili umešani tabloidi u vlasništvu Ruperta Mardoka (o ovom slučaju izveštavao je BBC - "News of the World phone-hacking scandal" . Dostupno na: http://www.bbc.com/news/uk-11195407 (pristupljeno 12. 11. 2017. godine) zamenila *Nezavisna organizacija za standarde u štampi* (*Independent Press Standards Organisation* , dostupno na: https://www.ipso.co.uk/ (pristupljeno 12. 11. 2017. godine)).

[16] Sa razvojem tehnologije, pojavom kablovskih i satelitskih emitera, iluzija o ograničenom spektru je razbijena. Broj stanica se povećavao, a regulacija slabila, gubeći argument limitiranosti spektra (Barvajz i Gordon, u Brigs i Kobli, 2005: 315–316).

interesa, mora da podlegne regulatornoj kontroli, zakonski propisanim pravilima poslovanja, koji bi u idealnom slučaju sprečili koncentraciju te moći. O tome piše i Ralf Negrin (Ralph Negrin), koji težnju evropskih zemalja za državnom kontrolom nad radiodifuzijom vidi „kao način da se izbegne haos na radio frekvencijama za emitovanje […] i istovremeno da se ne zanemari 'javni interes'" (u Brigs i Kobli, 2005: 357).

Javni interes trebalo bi da bude verovatniji tamo gde su sloboda govora, pluralitet izvora i vlasništva prisutni. Svakako da samo postojanje medijskog pluralizma nije garant odbrane javnog interesa i sprečavanja koncentracije moći (Klimkiewicz, 2009; Ward, 2005), ali je preduslov za demokratskiji pristup izgradnji medijskog okruženja. Na primer, u Francuskoj *Vrhovni audio-vizuelni savet* (*Conseil supérieur de l'audiovisuel*[17]), od 1989. godine, garantuje slobodu radiodifuzije. Regulacija radiodifuzije u Francuskoj usmerena je pre svega na zaštitu diverziteta i slobodu izražavanja; „instrumenti kojima se štiti pluralizam u medijima veoma su različiti i smešteni u okviru tri oblasti: Zakona Zajednice (*Community law*), Francuskom opštem pravu (*French common law*) i posebnom zakonodavstvu uvedenom posebno za ovu oblast" (Almiron-Roig, 2010: 474). Međutim, kompleksna medijska regulativa u Francuskoj nije uspela da obezbedi pluralizam. Almiron-Roig ističe da je Francuska primer borbe između demokratskih principa i neoliberalnog kapitalizma; Francuska zakonskim okvirom pokušava da odbrani pluralizam i standarde, ali je upliv politike i biznisa očigledan (2010: 482). Upravo zbog toga je u poznatoj klasifikaciji medijskih sistema Halina i Manćinija (Hallin, Mancini, 2004) Francuska okarakterisana kao mediteranski tip, medijski sistem bliži zemljama južne, nego zemljama zapadne i severne Evrope.

Regulacija medija, u kontekstu liberalnog shvatanja slobode medija, često ima negativni prizvuk. Naročito u eri sveopšte deregulacije. Međutim, trebalo bi napraviti razliku između državne kontrole nad medijima, koja je izražena u nedemokratskim zemljama, i regulative koja podrazumeva stvaranje jasno definisanog prostora u čijim okvirima mediji koegzistiraju. Zbog toga pojedini autori (Harvi, 2005; Feintuck, Varney, 2006) govore o procesu *re*regulacije, jer deregulacija, kao proces povlačenja države iz vlasništva i kontrole medija, podrazumeva i jasan regulatorni okvir, kojim se definišu uslovi pod kojima je moguće uspešno deregulisati medijsku sferu. U suprotnom, dolazi do "divlje deregulacije"[18], karakteristične za postsocijalističke zemlje.

Međutim, čak i jasno definisan zakonski okvir u oblasti medija može da dovede do zloupotrebe regulatornih mera od strane države. Kako ističe Mekvejl: „Pojam 'javnog interesa' je nekada upotrebljen ili viđen kao ideološki uređaj dizajniran da prikrije neopravdane regulatorne ambicije od strane vlade" (McQuail, 1995: 3). U tom smislu regulacija može imati negativne posledice po rad medija, onda kada država koristi zakonodavni okvir kao instrument za uspostavljanje kontrole nad radom medija. Reč je o rigoroznim zakonima o medijima, koji mogu gušiti slobodu izražavanja[19].

[17] Dostupno putem linka: http://www.csa.fr/en/The-CSA/An-Independent-Authority-to-Protect-Audiovisual-Communication-Freedom (pristupljeno 12. 11. 2017. godine).

[18] Ovaj termin upotrebljava se da opiše deregulaciju u zemljama mlade demokratije, koje su taj proces pokušale da sprovedu u slabo regulisanim uslovima, što je u krajnjem dovelo do negativnog ishoda – loše privatizacije, koja podrazumeva netransparentno vlasništvo, koncentraciju, osnivanje velikog broja medija bez dozvola za rad itd. (Tomić, 2016).

[19] Primer takvog zakona u bivšoj Jugoslaviji je Zakon o javnom informisanju iz 1998. godine, koji je, između ostalih rigoroznih mera, predviđao enormne novčane kazne, zatvorske kazne i zabranu rada medija. Tekstu Zakona pristupiti putem linka: http://anem.org.rs/sr/medijskaScena/uFokusu/story/7452/Zakon+o+javnom+informisanju.html (pristupljeno 11. 11. 2017. godine).

Jedan od takvih medijskih sistema pronalazimo u Narodnoj Republici Kini, koja preko *Centralnog departmana za propagandu*[20] i *Državne uprave za štampu, izdavaštvo, radio, film i televiziju* u potpunosti kontroliše sadržaj svih medija u Kini. Medijski sadržaj u Kini mora biti u skladu sa ideologijom Komunističke partije Kine, stoga je cenzura u oblasti medija na visokom nivou, o čemu svedoči i godišnji izveštaj o slobodi medija Fridom hausa (Freedom House) za 2017. godinu[21], prema kome je Kina dobila 87 od 100 negativnih poena.

Međutim, regulacija je, takođe, jedan od načina da se spreči koncentracija vlasništva i stvaranje monopola, obezbedi pluralizam, poštuju ljudska prava i ostvari javni interes[22]. Velika Britanija je dobar primer medijske politike koja insistira na odbrani javnog interesa, što se ostvaruje kroz regulatorna, nezavisna samoregulatorna tela i javni servis, koji je u službi građana. U vreme konzervativaca u Velikoj Britaniji (1984-1996) oslabljena je regulacija, otvoreno tržište za nove stanice (*Channel 4*), ali „nekomercijalni BBC prepoznat je kao 'kamen temeljac' sistema i ostavljen je relativno nedirnut" (Harvi, u Brigs i Kobli, 2005: 342–349)[23].

Barvajz i Gordon (Barwise & Gordon) navode primer britanske *ideje radiodifuzije javnih servisa*: „elektronski mediji moraju, u zamenu za dozvolu za emitovanje, da emituju izvesne stvari u izvesno vreme kao javna služba, čak i ako im to ne donosi profit" (u Brigs i Kobli, 2005: 316). Velika Britanija spada u red zemalja u kojima je sloboda medija na zadovoljavajućem nivou. To potvrđuje i izveštaj Fridom hausa[24] za 2017. godinu, prema kojem je Britanija dobila 25 od 100 negativnih poena, čime je klasifikovana kao zemlja slobodnih medija.

Poslednjih decenija pažnja je usmerena ka međunarodnom pravu i internacionalnim telima. U tom kontekstu najznačajnije organizacije koje utiču na rad medija na nadnacionalnom nivou jesu: Evropska Unija, Savet Evrope, Ujedinjene nacije, UNESKO itd. Međutim, nacionalni zakonodavni okvir ostaje značajan u smislu regulisanja medija koji posluju u okviru nacionalnih granica. Mediji su

[20] O funkciji i ulozi Centralnog departamana za propagandu Komunističke partije Kine videti više u Brady, A. M. (2006). *Guiding hand: The role of the CCP Central Propaganda Department in the current era.*

[21] Izveštaju za Kinu pristupiti putem linka: https://freedomhouse.org/report/freedom-press/2017/china (pristupljeno 12. 11. 2017. godine).

[22] Lorimer (1998), između ostalih zakona koji su relevantni za funkcionisanje medija, navodi zakone o slobodi komuniciranja, koji uključuju i vlasništvo, zakone o slobodi informisanja, zakone o autorskim pravima itd.

[23] U Velikoj Britaniji od kada je usvojen *Komunikacijski akt 2003* (*Act of Communication 2003*) radiodifuziju reguliše *Ofkom*, odnosno *Kancelarija za komunikacije* (*Office of Communications*). Pored elektronskih medija, *Ofkom* reguliše i fiksne telefonske i mobilne linije, kao i internet. Javni medijski servis *BBC* (*British Broadcasting Corporation*) od njegovog nastanka, 1922. godine, regulisan je internim BBC nadzorom (*BBC Trust*). Međutim, *Kraljevskom poveljom* (*Royal Charter*), koja je stupila na snagu 2017. godine, BBC podleže regulaciji *Ofkoma* zajedno sa komercijalnim medijima.
Tekstu *Komunikacijskog akta 2003* pristupiti putem linka:
http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf (pristupljeno 12. 11. 2017. godine).
Sajtu *Ofkoma* pristupiti putem linka: https://www.ofcom.org.uk/ (pristupljeno 12. 11. 2017. godine).
Review of BBC Internal Governance videti putem linka:
http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/about/how_we_govern/governance_review_2013.pdf
(pristupljeno 12. 11. 2017. godine).
Tekstu Povelje pristupiti putem linka:
http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/about/how_we_govern/2016/charter.pdf (pristupljeno 12.11.2017. godine).

[24] Izveštaju za Veliku Britaniju iz 2017. godine pristupiti putem linka: https://freedomhouse.org/report/freedom-press/2017/united-kingdom (pristupljeno 12. 11. 2017. godine).

deo medijskih sistema koji postoje u konkretnom društveno-političkom okviru, koji ih umnogome oblikuje (Siebert, Peterson, Schramm, 1956; Hallin, Mancini, 2004; Hallin, Mancini, 2011). Negrin navodi da će „u mnogim aspektima, svaki nacionalni sistem radiodifuzije (a isto važi i za novine) reprezentovati naročito – ponekad jedinstveno – uređenje; uređenje koje, za uzvrat, odražava različite društvenopolitičke tradicije, ekonomske sile, geografske karateristike i tako dalje" (u Brigs i Kobli, 2005: 356).

Razvoj novih tehnologija i široka upotreba interneta donele su nove i kompleksnije izazove državnoj regulaciji. Pitanja brisanja nacionalnih granica i globalnog komuniciranja stalni su predmet debata s početka 21. veka. Država je uspela da odgovori na mnogobrojne izazove, ali konstantni razvoj novih tehnologija doprinosi regulatornoj neizvesnosti do koje dovodi novo informaciono-komunikaciono okruženje.

3.2. Izazovi regulisanja internet prostora

Uzimajući u obzor Mekvejlove hronologije istorijskog odnosa regulacije i zahteva za slobodom medija, koja se kretala od *gušenja*, od strane države i religije, do *libertarijanskog* pristupa, u ime slobodnog tržišta (McQuail, 1995: 9), može se zaključiti da je ona primenljiva na tradicionalne medije, ali da joj se, kada je reč o internetu, može pristupiti obrnuto. Naime, na primeru štampe uočava se da je zahtev za regulacijom i kontrolom slabio sa razvojem ovog medija. Promena odnosa države i štampe, od potpune kontrole do apsolutne samoregulacije, značila je osvajanje slobode, oslobađanjem od stega države i regulacije. Razvojni put interneta kreće se u suprotnom smeru. Nastao kao samoregulatorni otvoreni prostor, internet se vremenom suočavao sa mnogobrojnim ograničenjima, od *preporuka* i *prohibicija*, pa i do *gušenja* u autoritarnim režimima.

Iako smo danas svesni mnogobrojnih ograničenja interneta, njegov virtuelni prostor i dalje često posmatramo kroz vizuru prvobitne bezgraničnosti, i to najamnje u dva smisla. Prvo, bezgraničnost možemo tumačiti kao nepregledno virtuelno prostranstvo, nesagledivo ljudskom umu. Drugo, internet ne poznaje fizičke granice, dok povezuje svaki segment planete, tačnije, koliko god mu to infrastruktura omogućava. Ukoliko se pođe od te pretpostavke, da je internet izbrisao fizičke granice u svakom smislu, nameću se sledeća pitanja: Ko kontroliše internet? Da li je regulacija interneta moguća? Na kraju, da li je ona uopšte potrebna?

Međutim, period vere u apsolutno slobodni sajber prostor završio se u prošlom veku. Prateći faze razvoja regulacije interneta, kako ih je definisao Polfrej (Palfrey, 2010)[25], u nastavku će biti predstavljen osnovni hronološki pregled svake od njih. Naime, Polfrej regulaciju interneta posmatra

[25] Polfrej je sa još nekoliko svojih kolega objavio tri knjige koje se bave drugom, trećom i četvrtom fazom regulacije interneta. Prva knjiga odnosi se na drugu fazu "Pristup odbijen": Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. (2008). *Access denied: The practice and policy of global internet filtering*. Mit Press. Druga knjiga objavljena dve godine kasnije posvećena je trećoj fazi kontrolisanog pristupa: Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Haraszti, M. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Mit Press. Dok su trećom knjigom, objavljenom 2011. godine, autori na primeru azijskog kontinenta pokušali da pojasne trenutnu fazu koja se karakteriše takmičenjem države i privatnih kompanija za prevlast u sajber prostoru: Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: security, identity, and resistance in Asian cyberspace*. MIT Press.

kroz četiri faze: *Otvoreni internet*, *Pristup odbijen*, *Kontrolisani pristup* i *Osvajanje pristupa*. Sa prelaskom u svaku sledeću fazu uviđa se jačanje regulatornih mehanizama i potreba za uspostavljanjem kontrole nad internet prostorom.

3.2.1. Prva faza regulacije interneta – *Otvoreni internet*

U prvoj fazi regulacije interneta, koju Polfrej (Palfrey, 2010: 981–985) naziva *Otvoreni internet*, a koja je trajala od šezdesetih godina prošlog veka do 2000. godine, verovanje da je sajber prostor, prostor koji je potpuno odvojen od fizičkog, bio je polazni argument za odbranu apsolutne slobode od teritorijalnih i regulatornih stega. Zastupnici ove teze bili su, pre svih, osnivači interneta, inženjeri i rani korisnici interneta, koji su verovali da su stvorili komunikacioni prostor kojem nije potrebna spoljna regulativa, prostor na koji oni polažu sva prava, te prostor u kojem mogu da uživaju izuzeće od državne kontrole. Njihova vizija bila je stvaranje paralelnog sveta, gde ljudi žive „pod svojim pravilima, oslobođeni stega ma kakvog opresivnog društva i slobodni od mešanja vlade" (Goldsmith & Wu, 2006: 13).

Prvu fazu regulacije interneta obeležila je borba za kontrolom nad internetom između industrije i vlade. Konkretno reč je o vladi SAD, s obzirom na to da je internet kakav danas poznajemo razvijen na teritoriji Amerike. Početak razvoja okarakterisan je nemešanjem vlade i dominacijom "izumitelja" i "žitnika" interneta, koji su verovali da internet pripada njima i da, kao takav, ne može biti pod kontrolom vlade. Kako navodi Polfrej, "sve do devedesetih većina država je ili ignorisala onlajn-aktivnosti ili su ih regulisale veoma slabo" (2010: 982). Međutim, period nemešanja vlade nije dugo trajao[26].

Izumitelji su imali idealizovanu viziju sajber prostora i bili su vođeni željom za stvaranjem jedne nove vrste demokratizovanog prostora, kojim bi se upravljao samoregulatorni mehanizam. Sajber libertarijanci smatrali su da je bilo kakav vid državne intervencije zapravo napad na Prvi amandman, koji bezuslovno štiti slobodu izražavanja u Americi. Jedan od najpoznatijih sajber aktivista, Džon Peri Barlou (John Perry Barlow) osnovao je 1990. godine zajedno sa još dvojicom sajber aktivista *Elektronsku graničnu fondaciju* (engl. *Electronic Frontier Foundation – EFF*), "organizaciju koja je – kroz političku participaciju, parnice, obrazovanje, seminare i kampanje različitih vrsta – posvećena razvoju pravne koncepcije sajber prostora kao zasebnog mesta i odbrani od upada teritorijalne vlade" (Goldsmith & Wu, 2006:18). Međutim, 1996. godina poljuljala je suverenost sajber prostora. Goldsmit i Vu o tom događaju pišu: „Došlo je odeveno kao 'regulisanje nepristojnosti' koje je bilo poznato kao 'Zakon o pristojnosti u komunikaciji' (CDA). CDA je kažnjavao svo prenošenje 'nepristojnih' seksualnih komunikacija ili slika na internetu 'na način dostupan osobi ispod 18 godina'" (2006: 19). Donošenje ovog zakona libertarijanci su doživeli kao udar na slobodno komuniciranje na internetu, koje je bilo srž njihove ideologije. Barlou je, izrevoltiran ovim činom, napisao *Deklaraciju o nezavisnosti sajber prostora*, koja sumira i sve značajne ideje sajber libertarijanaca:

> „Vlade Industrijskog sveta, vi iznureni divovi od mesa i čelika, dolazim iz sajber prostora, novog doma uma. U ime budućnosti, molim vas da nas ostavite na miru. Niste dobrodošli kod nas. Nemate suverenitet tamo gde se skupljamo.

[26] O tom periodu i borbi za prevlast detaljno pišu Goldsmit i Vu (2006: 13–46).

> Nemamo izabranu vladu, niti bismo je voleli imati […] Proglašavam globalni društveni prostor koji gradimo kako bismo bili prirodno nezavisni od tiranije koju nam pokušavate nametnuti. Nemate nikakvo moralno pravo da nama vladate […] Ne poznajete našu kulturu, našu etiku ili nepisane kodove koji već pružaju našem društvu više reda, nego što se može dobiti bilo kojim vašim nametanjem […] Vaši pravni pojmovi imovine, izražavanja, identiteta, kretanja i konteksta ne odnose se na nas. Svi se temelje na materiji, a ovde nemaju nikakve važnosti.
>
> Naši identiteti nemaju tela […] Mi ćemo stvoriti civilizaciju uma u sajber prostoru. Možda će biti humanija i poštenija od onog sveta koje su vaše vlade napravile do sada" (Davos, Switzerland, February 8, 1996)[27].

Sličnog je mišljenja i internet optimista Nikolas Negropont (Nicholas Negroponte) – on u knjizi "Biti digitalan" (1996) iznosi zanimljive teze o bezgraničnom internetu koji prkosi kontroli; „Internet omogućava svetski komunikacijski kanal koji se suprotstavlja bilo kom vidu cenzure" (Negroponte, 1996: 158). Sajber optimisti smatrali su da bi internet regulacija poništila njegovu pravu prirodu i funkciju, stoga regulisanje onlajn-aktivnosti, u njihovoj viziji, nije bilo potrebno.

Sa druge strane, vođene su debate, ne o potrebi, već o mogućnosti regulisanja interneta, s obzirom na njegovu internacionalnu prirodu. Džonson i Post (Johnson & Post) smatraju da je bespredmetno govoriti o postojanju granica u sajber prostoru. Obrazlažući regulatorne izazove koje donosi ovaj bezgranični prostor autori navode:

> „Uspon globalne kompjuterske mreže uništava vezu između geografske lokacije i: (1) *moći* lokalnih vlasti da uspostave kontrolu nad onlajn ponašanjem; (2) *efekata* onlajn-ponašanja na individue ili stvari; (3) *legitimiteta* lokalnih suverenih napora da regulišu globalni fenomen; (4) mogućnosti fizičke lokacije da *izvesti* o tome koji skup zakona se primenjuje" (1996: 1370).

O irelevantnosti fizičke lokacije Negropont piše: „Adresa postaje više poput broja socijalnog osiguranja nego ulična koordinata. To je virtualna adresa" (1996:166), i dodaje: „Bitovi će biti bezgranični, skladišteni i upravljani apsolutno bez poštovanja geopolitičkih granica" (1996: 228).

Međutim, Goldsmit i Vu (Goldsmith & Wu, 2006: 49–63) osporavaju argumente o beznačajnosti geografske lokacije iz nekoliko razloga. Prvo, internet korisnici ne govore istim jezikom, iako je engleski jezik označen kao svetski. Privatne kompanije koje posluju onlajn ubrzo su shvatile značaj ove razlike i modifikovale svoje sadržaje, prilagođavajući ih jeziku država u kojima posluju. Pored jezika postoje i značajne razlike u preferencijama, koje su uslovljene kulturom, običajima, normama; „Opcija 'izaberi zemlju' pokušava da zadovolji ove preferencije i očekivanja" (Goldsmith & Wu, 2006: 51). Autori navode da je uprošćena opcija 'izaberi zemlju' bila samo prvi impuls u pokušaju da se korisnici lociraju fizički. Kasnije su osmišljene mnogobrojne algoritamske tehnike koje neprimetno lociraju geografske koordinate, što je značajno iz najmanje dva razloga; prvi, kako je već pojašnjeno, ide u prilog korisnicima, jer im omogućava da shodno svojim preferencijama dobijaju ponude sadržaja; drugi je komercijalne prirode, jer olakšava targetiranje ciljnih geografskih grupa

[27] Ceo tekst *Deklaracije* videti putem linka: https://www.eff.org/cyberspace-independence (pristupljeno 05.12.2017. godine).

kojima treća lica, oglašivači, preko intermedijatora, lakše pristupaju. Zastupajući tezu da su granice značajne i na internetu, Goldsmit i Vu zaključuju: „Ironično, za medijum koji je trebalo da uništi granice, geografija je postala važan način za dobro povezivanje" (Goldsmith & Wu, 2006: 52).

Internet libertarijanci nisu predvideli značaj "ograničenog interneta", te je prvih nekoliko decenija postojanja interneta obeležilo verovanje u internet bez granica i regulatornih ograničenja. Internet je tih decenija bio utopijski posmatran kao jedna nova sfera ljudskih delatnosti, koja ne poznaje „ovozemaljske zakone" i ne povinuje se nametnutim pravilima ponašanja. Međutim, decenije koje su usledile pokazale su da internet nije ostao imun na regulaciju, kao što su liberterijanci i futorolozi optimisti predviđali u drugoj polovini 20. veka.

Kada su pitanja regulisanja interneta postala sve učestalija, pojavili su se i prvi problemi koji se tiču uspostavljanja komunikacione politike koja bi bila dovoljno opšta da obuhvati stalno promenljive globalne aktivnosti, ali i da odgovori na specifičnosti nacionalnih zakonskih okvira. Pamela Samjuelson (Pamela Samuelson u Marsden, 2000), za razliku od Džonsona i Posta (Johnson & Post, 1996) ne negira potrebu regulisanja internet prostora, ali izdvaja pet najopštijih izazova sa kojima se suočavaju kreatori regulatorne politike, kada je reč o internetu:

> „1 mogu li primeniti ili prilagoditi postojeće zakone i politike za regulaciju internet aktivnosti ili su potrebni novi zakoni ili politike za regulisanje ponašanja na internetu;
>
> 2 kako formulisati razumni i proporcionalni odgovor kada je potrebna nova regulacija;
>
> 3 kako izraditi zakone koji će biti dovoljno fleksibilni da se prilagode uslovima koji se brzo menjaju;
>
> 4 kako sačuvati temeljne ljudske vrednosti pri suočavanju sa ekonomskim ili tehnološkim pritiscima koji nastoje da ih potkopaju; i
>
> 5 kako uskladiti internet pravo i stvaranje politike s drugim državama tako da postoji dosledno pravno okruženje na globalnom nivou" (2000: 318).

Početak 21. veka obeležilo je suočavanje sa prethodno navedenim izazovima. Pitanja teritorijalnih jurisdikcija, učešća država i uspostavljanje regulatornih mehanizama predstavljaju izazove koji su aktuelni danas, kao i 2000. godine.

3.2.2. Druga faza regulacije interneta – *Pristup odbijen*

Period od 2000. do 2005. godine Polfrej prepoznaje kao drugu fazu regulacije interneta i naziva je *Pristup odbijen* (2010: 985–989). Iluzija o onlajn-prostoru odvojenom od geografskih koordinata ostala je neostvareni san internet optimista. Ova faza donela je različita ograničenja i predvidela mnoge preventivne i restriktivne mere, kojima se reguliše komunikacija i poslovanje na internetu. Najočiglediji razlog potrebe za regulacijom internet aktivnosti odnosio se na sadržaj koji se nesmetano širio mrežom, a koji je prepoznat kao štetan. Reč je, pre svega, o pornografskom sadržaju i o potrebi

zaštite maloletnika. Vlade su bile saglasne da bi takve sadržaj na internetu trebalo regulisati kao i u ma kom drugom prostoru.

Jasno je da je u ovoj fazi ideja o virtuelnom prostoru koji je odvojen od fizičkog i o virtuelnim identitetima, koji su bestelesni u onlajn-prostoru, u potpunosti odbačena. Subjekti koji krstare mrežom nemaju dvojne identitete, od kojih je onaj koji je virtuelni oslobođen od svake vrste odgovornosti i gotovo nespojiv sa identitetom koji ima fizičku manifestaciju. Takođe, kompanije koje posluju na internetu ne mogu biti izuzete od zakonskih propisa, niti mogu da sprovode svoje aktivnosti bez poštovanja država u kojima posluju. Na primer, u zamenu za nesmetano poslovanje na njihovoj teritoriji države zahtevaju kontrolu nad sadržajem, koju će im omogućiti upravo privatne kompanije. Poznati primer takve vrste "simbioze" države i internet intermedijatora jeste poslovanje kompanije Jahu! (*Yahoo!)* u Kini (Palfrey, 2010; Goldsmith & Wu, 2006). Ukratko, Jahu! je pristao da kineskoj vladi na njihov zahtev dostavlja informacije o aktivnostima internet korisnika. Reč je o korisnicima, koji, prema mišljenju kineske partije, šire politički nepogodne informacije. Poznat je i slučaj kineskog novinara koji je osuđen na deset godina zatvora, pošto je kompanija Jahu! dostavila kineskoj vladi sadržaj njegovih mejlova.

Na primeru kompanije Jahu! može se uvideti promena u načinu rada i javno zastupanim principima od strane internet intermedijatora. Jahu! je svoje bazične principe poslovanja menjao u skladu sa promenama faza u regulaciji interneta, odnosno sa sve većim učešćem vlada u kontrolisanju internet prostora. Jahu! se prvo opirao učešću vlada u regulisanju interneta, u skladu sa prvom fazom otvorenog interneta. Kasnije je, vođen komercijalnim razlozima, svoj odnos prema slobodi na internetu prilagodio drugoj fazi i u skladu sa njom gradio svoju politiku prema slobodi na interentu, što se pokazalo na primeru poslovanja kompanije Jahu! na kineskom tržištu.

Naime, samo nekoliko godina pre ulaska na kinesko tržište Jahu! jeste bio subjekt međunarodne afere koja se ticala ingerencija država u kojima posluje – u ovom slučaju reč je bila o Francuskoj (Surčulija, 2010). Naime, zakon SAD ne prepoznaje određene nacističke simbole i retoriku na internetu kao sadržaj koji bi trebalo filtritati, dok su u Francuskoj takvi sadržaji zabranjeni. Jahu! je kompanija koja je registrovana u Americi, ali je korisnicima u Francuskoj omogućila pristup takvim sadržajima. Korisnik iz Francuske tužio je Jahu! i dobio parnicu na sudu u Francuskoj. Jahu! nije odstupio od svojih principa, pozivajući se na zakone SAD i negirao odgovornost za nepoštovanje zakona Francuske. Međutim, sud u Americi je potvrdio presudu i naložio uklanjanje sadržaja. Sud je utvrdio da je Jahu! imao tehničke mogućnosti da spreči širenje nacističkog sadržaja mrežom u Francuskoj, te da je imao stranice na francuskom jeziku koje su očigledno bile namenjene upravo francuskim korisnicima. Jahu! je postupio prema naloženim sudskim merama (Goldsmit & Wu, 2006: 1–10).

Ovaj primer pokazuje kako je verovanje u brisanje granica i pozivanje na irelevantnost nacionalnih jurisdikcija bilo neosnovano. Države imaju mogućnost filtriranja, blokiranja i uklanjanja sadržaja sa interneta, bez obzira na lokaciju intermedijatora. Takođe, primer intermedijatora Jahu! jeste dobar primer promene standarda poslovanja (od pozivanja na bezuslovnu slobodu izražavanja u Francuskoj, do pristajanja na učešće u nadzoru internet korisnika u Kini) privatnih kompanija, kada je prioritet intermedijatora osvajanje tržišta i komercijalna isplativost.

Uspostavljanje regulatorne prakse imalo je, svakako, i negativne posledice. Takvi primeri se najbolje ogledaju u državama sa represivnim sistemima, koje su u zakonski okvir ugradile i mere pomoću kojih filtriraju i one sadržaje koji su politički nepodobni. Robert Feris i Nart Vilnev (Robert Faris & Nart Villeneuve, u Deibert, et. al, 2008: 5–29) istraživali su filtriranje interneta u 40 zemalja,

kao deo organizacije "Inicijativa za otvoreni internet" (*OpenNet Initiative*[28]). Rezultati njihovog istraživanja pokazuju da je sadržaj koji je podložan filtriranju raznolik, nije samo pornografski i politički, i da se razlikuje od države do države. Kao najčešće kategorije koje su predmet internet filtriranja, autori navode sledeće: slobodu izražavanja, opozicione partije, ekstremiste, ljudska prava, prava manjina, međunarodne odnose, prava žena, govor mržnje, kontroverznu istoriju, umetnost, gej sadržaj, pornografiju, kockanje, alkohol, drogu, hakovanje, sajtove za reklame i mnoge druge (Robert Faris & Nart Villeneuve, u Deibert, et. al, 2008: 7). Iz ponuđene liste postaje jasno da društvene i kulturne okolnosti igraju veliku ulogu pri odabiru sadržaja koji će biti filtrirani.

Inicijativa za otvoreni internet od 2006. godine intenzivno prati promene u regulaciji sajber prostora, i objavljuje regionalne i nacionalne izveštaje o filtriranju i cenzurisanju internet sadržaja. Objašnjavajući metodologiju kojom se služe prilikom analize regulacije internet prostora, identifikuju četiri nivoa kontrole internet sadržaja: 1. nivo kičmenog stuba interneta (*internet backbone*), čijom kontrolom mogu onemogućiti pristup internetu na teritoriji cele zemlje; 2. nivo internet servis provajdera najčešće je primenjen i sprovodi se metodama tehničkog blokiranja, uklanjanja rezultata pretraga, uklanjanja nakon objavljivanja sadržaja i indukovanom autocenzurom; 3. na nivou institucija, najčešće na radnim mestima, u kafićima i drugim javnim mestima; i 4. na nivou individualnih kompjutera, posredstvom specijalnih softvera.[29]

Dakle, države mogu regulisati sadržaj na internetu i to regulacijom softvera i hardvera (Wu, 1996: 649–656). Praksa filtriranja internet sadržaja nije rezervisana samo za represivne režime i manje razvijene zemlje. Blokiranje internet sadržaja deo je regulatornih mehanizama i razvijenih zemalja, s tim što je filtriranje uglavnom usmereno ka pornografskom sadržaju, autorskim pravima, govoru mržnje i bezbednosti.

3.2.3. Treća faza regulacije interneta – *Kontrolisani pristup*

Mogućnost regulacije sa završetkom druge faze više nije bila centralna tema debata o kontroli interneta. Ključna pitanja odnosila su se na granice regulacije – jer je druga faza "odbijenog pristupa" pokazala značajne zloupotrebe – i na odgovornost privatnih kompanija, koje su sa godinama razvoja interneta dobijale na značaju. Prema Polfreju (2010: 989–991), nakon 2005. godine usledila je treća faza regulacije interneta, koju naziva *Kontrolisani pristup* i koja traje do 2010. godine. Osnovna karakteristika ove faze jeste pojačana kontrola države i jačanje regulatornih mera. Međutim, u ovoj fazi kontrola nije toliko očigledna, kao što je to bio slučaj sa prethodnom. Metode su sofisticiranije i države ih sprovode u saradnji sa privatnim akterima, čija je uloga sve značajnija. Države su pronašle mnogobrojne načine da uspostave kontrolu nad internet aktivnostima. Polfrej to opisuje na sledeći način:

> „Kontrole prvog reda povezane sa cenzurom kombinuju se sa pravnom kontrolom i nadzorom čiji je zadatak da onima koji objavljuju onlajn daju do znanja da ih neko

[28] Dostupno putem linka: https://opennet.net/about-filtering (pristupljeno 09. 12. 2017. godine).
[29] Celokupni rad *Inicijative za otvoreni internet*, njihova metodologija rada, izveštaji i naučne publikacije dostupni su na njihovom sajtu: https://opennet.net/about-filtering (pristupljeno 09. 12. 2017. godine).

posmatra i da država može da ih ugasi ili da ih pošalje u zatvor. Ove kombinovane metode regulacije vrlo su učinkovite" (Palfrey 2010: 990).

Dajbert i Rohozinski (Deibert & Rohozinski, 2010) klasifikuju internet kontrolu na kontrolu *prve*, *druge* i *treće generacije*, koje se razlikuju po načinu sprovođenja, od ogoljene cenzure, preko zakonskih restriktivnih mera, do poslednje generacije kontrole koja se ostvaruje posredstvom nadzora. Kao primer efikasne kombinacije druge i treće generacije kontrole navedeni autori analiziraju Rusiju i ruski sajber prostor – *Runet*, za čiji sistem kontrole navode sledeće: „strategije nadzora imaju tendenciju da budu suptilnije i sofisticiranije i dizajnirane tako da oblikuju i utiču na to kada i na koji način korisnici primaju informacije, umesto da im potpuno onemoguće pristup" (Deibert & Rohozinski, 2010: 16). Primer prve generacije kontrole bio bi kineski sajber prostor, čija vlada blokira protok informacija na svojoj teritoriji. Sa druge strane, *Runet*, koji je široko rasprostranjen u postsovjetskim zemljama, kontrolisan je perfidnijim merama.

Dajbert i Rohozinski ih klasifikuju u odnosu na to koju generaciju kontrole koriste: od isključivo cenzorskih mera (Turkmenistan), ili isključivo druge generacije kontrole (Ukrajina i Jermenija), preko kombinovanja sve tri vrste kontrole (Belorusija) i najčešće kombinovanjem druge i treće generacije kontrole (Rusija, Moldavija, Kirgistan, Azerbejdžan) (Deibert & Rohozinski, 2010: 29).

Međunarodna organizacija digitalnih aktivista i boraca za ljudska prava *Global Voices Advocacy* (GVA) objavila je jula 2008. godine vest o ruskom blogeru koji je osuđen na godinu dana zatvora zbog komentara na blogu[30]. Godinu dana ranije bloger *LiveJournal*-a suočavao se sa trogodišnjom kaznom zatvora zbog objavljivanja fikcije na svom blogu, koja je bila protumačena kao „lažno upozorenje na terorisitičke pretnje"[31]. U martu 2010. godine opozicioni internet sajt u Rusiji zatvoren je po nalogu policije[32]. Svi ovi primeri pokazuju da postsovjetske zemlje sprovode specifičnu vrstu kontrole internet prostora. Pojedini primeri iz postsovjetskih zemalja podsećaju na rigoroznu "kinesku" kontrolu. Često je kontrola ugrađena u zakonski okvir koji joj daje legalitet. Međutim, sofisticiranost njihovih metoda ogleda se u širenju straha i indukovanju samocenzure, kao posledice jasnog stava postsovjetskih vlada koji bi se mogao opisati rečenicom "samo te posmatramo".

[30] Veronica Khokhlova, (15 July 2008). "Russia: One Year in Prison for Blog Comment", *Global Voices Advocacy*. Dostupno na: https://advox.globalvoices.org/2008/07/15/russia-one-year-in-prison-for-blog-comment (pristupljeno 06. 12. 2017.godine).

[31] Sami Ben Gharbia, (18 September 2007). "Russian LiveJournal blogger could face three-year sentence ". Dostupno na: https://advox.globalvoices.org/2007/09/18/russian-livejournal-blogger-could-face-three-year-sentence (pristupljeno 06. 12. 2017.godine).

[32] Alexey Sidorenko, (26 March 2010). "Russia: Website Closed By Police Order". Dostupno na: https://advox.globalvoices.org/2010/03/26/russia-website-closed-by-police-order (pristupljeno 06.12.2017.godine).

3.2.4. Četvrta faza regulacije interneta – *Osvajanje pristupa*

Nakon 2010. godine počela je faza koju Polfrej prepoznaje kao četvrtu i naziva *Osvajanje pristupa* (2010: 991–993). Ova faza predstavlja period borbe za kontrolom nad internet prostorom. Jasno je, iz prethodnih faza, da su države uvidele moć koju mogu da ostvare kontrolisanjem internet aktivnosti i, što je za njih još značajnije, pronašle su načine da to uspešno sprovode. Sa druge strane, privatni akteri su se nametnuli kao dominantni u novom prostoru, a država sa njima može da sarađuje da bi ostvarila svoje ciljeve (kako je to slučaj u Kini) ili da pokušava da ograniči njihovu moć i kontroliše njihov rad, kako bi zaštitila svoje građane i njhova prava, što je to slučaj u većini demokratskih zemalja – međutim, trebalo bi imati na umu da su zloupotrebe česte i u demokratskim zemljama. U ovoj fazi privatni akteri dobijaju na značaju i sami su suočeni sa pitanjima odgovornosti.

Zbog čega je sajber prostor mesto koje je vredno osvajanja? Period od 2010. godine doneo je niz globalnih društveno-političkih promena koje su se većim delom odvijale onlajn ili su tu počinjale. Za primer možemo uzeti niz revolucija, poznatih kao tviter-revolucije, koje su dokazale da početna teza o odvojenom sajber prostoru, ako je ikada i važila, u ovom trenutku razvoja sigurno više nema značaja. Prelivanja iz onlajna u oflajn i obrnuto zapravo su toliko kompleksna da više ne možemo sa sigurnošću tvrditi da li je nešto započelo na internetu pa se preselilo u oflajn-svet ili je put pratio pravac oflajn-onlajn.

Isprepletane aktivnosti savremenog čoveka čine nemogućim odvajanje ova dva sveta krutom granicom, što se pokazalo i na primerima sankcionisanja onlajn-ponašanja. Tviter-revolucije, "curenje" poverljivih informacija preko Vikiliksa (Wikileaks) i Snoudenovo (Edward Snowden) objavljivanje dokaza o nelegalnom prisluškivanju građana od strane Nacionalne bezbedonosne agencije (NSA), samo su neki od najpoznatijih primera koji su pitanja bezbednosti i kontrole sajber prostora stavili u fokus svetske javnosti. Nije trebalo mnogo vremena da bi se shvatilo da je internet prostor, prostor od geopolitičkog značaja, na kojem se pokreću revolucije, objavljuju tajne informacije, grupišu ljudi i poziva na oflajn-akcije. Jasno je da su sve te prilike uticale na to da mnoštvo zainteresovanih strana, država, privatni akteri, društvene grupe, pojedinci, pristupe takmičenju za osvajanje interneta, odnosno za uspostavljanjem kontrole nad sajber prostorom. Delbert i saradnici pišu o značaju internet prostora: „Sada se smatra domenom jednake važnosti kao i zemlja, vazduh, more i prostor, to je medij kroz koji se odvija trgovina, obrazovanje, hobi, politika i rat" (Deibert et. al. 2011: 4).

3.2.5. Borba za net neutralnost

Godina 2017. ostaće upamćena i po jednoj specifičnoj internet borbi – borbi za otvoreni internet i očuvanje principa net neutralnosti (*Net neutrality*). Pod ovim pojmom podrazumeva se zabrana internet servis provajderima da na bilo koji način stvaraju uska grla i diskriminišu sadržaj. Ganli i Olgrov (Ganley & Allgrove) suštinu debate o net neutralnosti vide u pitanju da li bi internet trebalo da nastavi da funkcioniše po principu prenosa bez diskriminacije ili bi „operatorima koji poseduju ili kontrolišu različite aspekte fizičkog sloja trebalo biti dozvoljeno da 'diskriminišu' podatke koji prolaze njihovom mrežom" (2006: 455–457).

Telo evropskih regulatora za elektronske komunikacije (BEREC) u avgustu 2016. godine objavilo je *Smernice za implementaciju evropskih pravila o net neutralnosti za nacionalne regulatore*[33]. U Americi je net neutralnost garantovana Glavom II Zakona o komunikacijama iz 1934. godine:

> „(a) Biće nezakonito da bilo koji provajder čini nepravednu ili bezrazložnu diskriminaciju u pogledu troškova, praksi, klasifikacija, propisa, sadržaja ili usluga u vezi sa komunikacijskom uslugom, direktno ili indirektno, na bilo koji način ili bilo kojim uređajem, ili da daje nepotrebnu ili nerazumnu prednost bilo kojoj određenoj osobi, klasi ili lokalitetu, zbog nepotrebne ili nerazumne predrasude ili nedostatka.
>
> […]
>
> (c) Svaki provajder koji svesno krši odredbe ovog odeljka platiće Sjedinjenim Državama iznos od 6.000 dolara za svaki takav prekršaj i 300 dolara za svaki dan nastavka takvog prekršaja" (Communication Act of 1934, Title II, str. 36)[34].

Najavljeno ukidanje neutralnosti interneta u Americi, zakazano za 14. decembar 2017. Godine, izazvalo je lavinu komentara. Američka javnost podeljena je u dva tabora, proponente i oponente ukidanja net neutralnosti. Deo javnosti koji se protivi ukidanju iznosi svoje argumente, predviđajući kraj interneta kakav poznajemo. Sumirano njihovi argumenti odnose se na stvaranje uskih grla od strane provajdera kojima bi se usporili sajtovi koji ne plaćaju premijum pakete, povećali troškovi za korisnike, slabile pozicije malih *start-up* kompanija itd. Predsednik Federalne komisije, Adži Paj (Ajit Pai), jedan do najglasnijih zagovornika ukidanja neutralnosti i kritičara Glave II Zakona o komunikacijama, smatra da je internet bio u usponu do pre dve godine, kada je 2015. godine formalno usvojen princip neutralnosti, i naglašava da nije bilo potrebe popravljati nešto što nije bilo pokvareno: „Ništa u vezi sa internetom nije bilo pokvareno u 2015. godini. Ništa se u zakonu nije promenilo. I nisu

[33] BEREC *Guidelines*, videti putem linka: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules (pristupljeno 10. 12. 201. godine).

[34] *Communication Act of 1934* dostupan putem linka: https://transition.fcc.gov/Reports/1934new.pdf (pristupljeno 10. 12. 2017. godine).

internet servis provajderi blokirali korisnike da pristupaju sadržaju, aplikacijama ili uslugama po svom izboru. Ne, sve je bilo o politici" (Pai, *The Future of the Internet Freedom*, april 2017)[35].

Paj smatra da je politika neutralnosti, nasuprot očekivanom, dovela do blokiranja inovacija, služila monopolu i usporila razvoj interneta. Dalje, Paj navodi argument kojima brani ukidanje principa neutralnosti interneta:

> „Prvo, doneće većem broju Amerikanaca brži pristup internetu. […] Drugo, stvoriće nove poslove. Više Amerikanaca će raditi na izgradnji ovih novih mreža. […] Treće, pospešiće konkurenciju. […] Četvrto, ovaj predlog je najbolji put za zaštitu onlajn-privatnosti Amerikanaca […] To znači da će najstručniji i najiskusniji regulatori ponovo štititi onlajn-privatnost Amerikanaca" (Pai, *The Future of the Internet Freedom*, april 2017).

Zagovornici net neutralnosti smatraju da će se ukidanjem principa neutralnosti ugroziti i sloboda izražavanja, a Paj im odgovara: „Vladina regulacija nije prijatelj slobode govora, nego njen neprijatelj. Uostalom, Prvi amandman ne daje vlasti moć da je reguliše. On opovrgava vladi tu moć" (Pai, 2017). Jasno je da zagovornici neutralnosti smatraju da će slobodan i jednak pristup internetu i sloboda izražavanja biti mogući samo ukoliko su regulisani Glavom II Komunikacijskog akta i u nadležnosti Federalne komisije za komunikacije. Sa druge strane, protivnici neutralnosti ističu da je najbolja regulacija ona koja nije u rukama vlade i Komisije. Trenutni epilog ide u prilog ovim drugim, jer je Komisija 14. decembra 2017. godine izglasala ukidanje principa poznatih kao net neutralnost regulacija[36]. Reakcije dela javnosti koji se protivio takvom ishodu burne su. Amerikanci izražavaju svoj protest na onlajn-trgovima i gradskim ulicama. Mnoge kompanije najavljuju sudske tužbe. Ono što je sada izvesno jeste da se promene neće osetiti preko noći, a koji će se argumenti potvrditi tačnim pokazaće se u narednom periodu, koji je već definisan kao „nova era interneta".

***

Razvoj interneta i faze regulacije interneta ne mogu se sagledati globalno. Postoje razlike u pristupu internetu u okviru komunikacionih politika različitih regiona, ali i pojedinačnih zemalja. Uopšteno, pristup internetu možemo da podelimo na demokratski i autoritarni, ukoliko za indikator uzmemo odnos države prema slobodi interneta. U tom kontekstu regulaciju internet aktivnosti mogu se posmatrati ili kao gušenje internet poslovanja i sloboda (autoritarne zemlje), ili kao pokušaj uređenja internet prostora, sa ciljem jačanja sloboda, ali i sankcionisanja štetnih aktivnosti (demokratske zemlje).

[35] Remarks Of FCC Chairman Ajit Pai at the Newseum, Washington DC, April 26, 2017. Videti putem linka: https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0426/DOC-344590A1.pdf (pristupljeno 05. 12. 2017. godine).

[36] Cecilia Kang, (December 14, 2017). "F.C.C. Repeals Net Neutrality Rules". *The New York Times*. Dostupno na: https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.html (pristupljeno 05. 12. 2017. godine).

Regulacija interneta, kao i ma kog drugog dela informaciono-komunikacionog sistema, poželjna je u meri koja osigurava pluralizam i slobodu mišljenja i izražavanja, sprečava ugrožavanje slobode drugih i sprovodi se sa ciljem zaštite javnog interesa. Odsustvo regulatornih mehanizama značilo bi apsolutnu slobodu, koju, u ovoj fazi razvoja interneta, lako može zameniti anarhija.

Počeci razvoja interneta i aktivnosti tadašnjih korisnika ne mogu se uporediti sa načinom primene interneta danas. Komercijalizacija interneta, odnosno eksploatisanje internet prostora od strane gigantskih kompanija, koje su još u njegovom začetku uvidele ogroman potencijal za stvaranje krupnog kapitala "na mreži", promenile su njegovu prvobitnu prirodu. Od prostora koji su iznedrili kreativni pojedinci, preko forum grupa i kolektiva koji se sam regulisao, internet je postao "biznis prostor".

Potpuno odsustvo regulacije interneta danas, značilo bi prepuštanje privatnim kompanijama da same regulišu svoje aktivnosti. Stoga se sprovođenje regulatornih mera u demokratskim zemljama ne može posmatrati kao gušenje slobode pojedinaca od strane država, već kao način da se građanima garantuje zaštita osnovnih ljudskih prava. Smisao učinkovite regulacije je, dakle, u obezbeđivanju sigurnog prostora za nesmatano poslovanje, uz poštovanje ljudskih prava i ostvarivanje javnog interesa.

Odgovornost države je da uspostavi regulatorni mehanizam koji može da odgovori na navedene zahteve. Pitanje zloupotrebe uvek je otvoreno, kao i kada je reč o regulaciji tradicionalnih načina komunikacije i informisanja. Zbog toga je jedan od najvećih izazova državama danas, naročito mladim demokratijama, pronalaženje prave mere pri regulaciji informaciono-komunikacionog sistema.

3.3. Promenjena uloga države u globalizovanom informaciono-komunikacionom sistemu

Rasprave o ulozi države u globalizovanom informaciono-komunikacionom sistemu uglavnom se svode na polemisanje o suverenitetu države i promeni njene moći sa razvojem interneta i prekogranične komunikacije i poslovanja. Kako je već bilo reči u prethodnom poglavlju, internet libertarijanci slavili su internet kao medijum koji će poljuljati moć države da kontroliše onlajn-aktivnosti. Mnogobrojni kasniji primeri govorili su upravo suprotno – država u velikoj meri može da kontroliše intrenet aktivnosti. Međutim, da bismo razumeli promene o kojima se raspravlja i argumente autora koji spore ili veličaju moć države u novim okolnostima, moramo najpre da pojasnimo različita stanovišta o ulozi države u međunarodnom sistemu. Upravo u različitim polazištima pri definisanju uloge države leže aktuelna neslaganja o jačanju ili slabljenju moći države (Perritt, 1998; Post, 1998; Drezner, 2004).

3.3.1. Država iz ugla realista i libarala

An-Mari Sloter (Anne-Marie Slaughter, 1994) ukazuje na značajne razlike u poimanju uloge države od strane realista i liberala. Realisti državu posmatraju u okvirima njene teritorijalnosti i u skladu sa tim se odnose prema njenoj moći, dok je liberalima država sekundarna u odnosu na potrebe društva, koje mogu da prevaziđu njene okvire.

Naime, prema tradicionalnom realističnom shvatanju, država je ta koja je primarni akter u međunarodnim odnosima – ona ima koncentrisanu moć i njena teritorijalnost je neprikosnovena. Sloterova o realistima piše:

> „Prvo, oni veruju da su države primarni akteri u međunarodnom sistemu, racionalni unitarni akteri koji su funkcionalno identični. Drugo, pretpostavljaju da je organizacijsko načelo međunarodnog sistema anarhija, koju ne mogu posredovati međunarodne institucije. Treće, država se može tretirati kao da je njena dominantna preferencija želja za moći. [...] Za realiste, teritorijalne granice definišu područje iz kojeg se mogu izvući resursi potrebni za vojnu i ekonomsku moć" (Slaughter, 1994: 722, 723).

Sa druge strane, liberali koncept moći menjuju interesom(ima), i to interesima društvenih grupa i civilnog sektora:

> „Gde realisti traže koncentraciju državne moći, liberali se usredsređuju na načine iz kojih međuzavisnost proizlazi i omogućava pojedincima i grupama da vrše različite pritiske na nacionalne vlade [...] Državno ponašanje, pak, ne određuje međunarodna ravnoteža moći, bez obzira na to da li je posredovana od strane institucija, već odnos između tih društvenih aktera i vlada koje zastupaju njihove interese" (Slaughter, 1994: 728).

Promena uloge države u novom IKS može se, dakle, posmatrati iz ugla ova dva stanovišta i ona će se shodno tome i razlikovati. U prvom slučaju, gde se država primarno određuje na osnovu svoje teritorijalnosti i moći koja je skoncentrisana u njenim jasno definisanim okvirima, razvoj novih tehnologija, na čelu sa internetom, svakako urušava koncepciju realista o neprikosnovenoj ulozi države. Sa druge strane, liberali koji insistiraju na potrebama društva, pre nego na moći države kao prioritetnog aktera u međunarodnom sistemu, imaju drugačiji pogled na promene koje donose nove tehnologije. Dejvid Post (David Post) smatra da, posmatrana sa liberalnog aspekta, država sa razvojem prekograničnih tehnologija ne samo da neće izgubiti moć i suverenitet, već će dobiti priliku da se bolje organizuje i funkcioniše: „Budući da se liberalne države ne oslanjaju na vezu između teritorija i moći, one mogu bolje da funkcionišu u svetu u kojem se ta veza uništava. Liberalne države naći će načine kako da koriste internet za jačanje liberalnog upravljanja, da rade bolje nego sada", dok "Realistične države – one koje se oslanjaju isključivo na teritoriju i moć kao izvor svog autoriteta – neće. Internet svakako komplikuje državnost i državnu pripadnost, ali teško da ih čini irelevantnim" (1998: 525–526).

Međutim, ukoliko internet omogućava širok pristup informacijama i potencijalno osnažava internet korisnike kao građane, postavlja se pitanje zbog čega države percipiraju internet aktivnosti kao pretnju po svoju moć i suverenitet? O tome piše Henri Perit (Henry Perritt, 1998) i ističe da je otvoren internet prostor pretnja jedino autokratskim režimima, koji imaju za cilj sprečavanje slobodnog protoka informacija i isključivanje građana iz procesa odlučivanja. Perit navodi da države doživljaju internet kao pretnju po svoju suverenost zbog toga što smatraju da ugrožava njihove osnovne tri funkcije

„osiguravanje nacionalne bezbednosti, regulisanje ekonomskih aktivnosti i zaštitu i promovisanje civilnih i moralnih vrednosti" (Perritt, 1998: 427).

Perit, nasuprot velikom broju autora koji problematizuju suverenitet države u novom okruženju, iznosi tezu da internet zapravo jača poziciju države. Njegov osnovi argument, iz pozicije liberala, jeste da internet jača vladavinu prava; „na primer, država ga koristi da bi informisala i upoznala građane sa zakonima, njihovom efikasnošću, naročito je značajan za zemlje u tranziciji" (1998: 435–436). Navedeno je u saglasnosti sa njegovim tvrdnjama da internet ugrožava samo zatvorene zemlje, sa autokratskim režimom, koje strahuju od gubitka moći ukoliko svojim građanima omoguće nesmetani pristup informacijama.

Otvoreni internet predstavlja izazov svim državama, bile one demokratske ili autokratske, s tim što se izazovi rešavaju na različite načine u skladu sa državnim uređenjem. Na primer, u kineskom sistemu pristup regulisanju interneta poznat je kao *Veliki zaštitni zid Kine* (engl. *The Great Firewall of China*) i podrazumeva primenu restriktivnih nacionalnog zakona. Ruski sajber prostor – *Runet* takođe je jedan od načina na koji države mogu kontrolisati svoj internet prostor. Jasno je da države mogu u potpunosti da kontrolišu internet prostor, makar to vodilo potpunoj izolaciji. Međutim, takva rešenja nisu primenljiva u razvijenim demokratskim zemljama. Jednostavno filtriranje ili blokiranje svih nepoželjnih sadržaja ne bi bilo u skladu sa poštovanjem osnovnih ljudskih prava, na čelu sa slobodom izražavanja. Zbog toga je pitanje uloge države u regulisanju protoka informacija internetom kompleksnije u demokratskim zemljama.

Demokratska država kao garant poštovanja ljudskih prava i spečavanja ilegalnih aktivnosti svoje osnovne funkcije ne gubi u onlajn-prostoru. Građani svake uređene zemlje očekuju od države da ih zaštiti i onda kada je zaštita njihovih prava u vezi sa aktivnostima na internetu. Goldsmit i Vu navode da ne primećujemo svakodnevno koliko uživamo zaštitu od strane naših vlada, „ali primetimo kada ona nedostaje: kada se prekrše ugovori, kada je imovina ukradena, i kada je prevara osiona" (2006: 140). To možemo videti na primeru kompanije *eBay*, koja je u periodu nastanka, 1995. godine, insistirala na slobodnom internetu i poslovanju zasnovanom isključivo na smoregulaciji. Međutim, usled neočekivano brzog porasta broja korisnika[37], *eBay* se okrenuo državi za pomoć. Prevare na ovoj platformi nije bilo moguće sprečiti bez regulatornih mera i sprovođenja sankcija (Goldsmith & Wu, 2006: 129–139). U tom smislu uloga države ostala je značajna, ali je promenjen način na koji država sprovodi regulatorne mere, odnosno njena uloga je prilagođena novonastalom okruženju i njegovim izazovima.

[37] „Do kraja 1999. godine *eBay* imao je preko pet miliona korisnika" (Goldsmith&Wu, 1996: 132).

3.3.2. Međunarodna saradnja – umreženo delovanje

Ne može se sporiti da internet jeste veći izazov državama od prethodnih tehnoloških dostignuća. Jedan od izazova tiče se i udruženog delovanja država, odnosno internacionalne koooperacije kao načina rešavanja problema nastalih „na mreži". Na primeru slučaja kompanije Jahu! u Francuskoj pokazalo se kako je moguće odgovoriti izazovu preplitanja jurisdikcija država i neusaglašenosti zakonskog okvira po pitanju zabranjenih sadržaja na internetu.

Još jedan poznati primer tiče se prava na privatnost u evropskom zakonodavstvu i načina skladištenja ličnih podataka kompanije Majkrosoft (Microsoft), koji detaljno opisuju Goldsmit i Wu (2006). Ukratko, 1999. godine Majkrosoft je osmislio sistem koji skladišti i čuva sve lozinke i lične podakte korisnika na jednom mestu, tako da kada korisnik želi da pristupi sajtu, na kojem je registrovan, sistem prepoznaje i nudi podatke, bez obaveze korisnika da pamti ili pri svakom pristupu unosi svoje lične podatke. Ovakav način skladištenja i raspolaganja ličnim podacima u Americi nije predstavljao problem, međutim, politika privatnosti na evropskom kontinentu pretila je da ugrozi poslovanje Majkrosofta na tom tržištu. S obzirom na to da je Majkrosoft imao veliki broj korisnika u Evropi, a veličina tržišta diktira i pravila ponašanja, Majkrosoft je promenio svoju politiku poslovanja i uskladio je sa evropskom regulativom. Kompanija Majkrosoft otišla je i korak dalje i primenila isti princip u svim zemljama u kojima posluje, jer je bilo isplativije da ima jedinstven sistem za sva tržišta (Goldsmith & Wu, 2006: 173–177).

U ovim primerima može se prepoznati promenjena uloga države, u odnosu na način na koji je definišu realisti. Slučaj kompanija Jahu! i Majkrosoft nije mogao da se reši samo u okvirima nacionalnog zakonodavstva, već je bilo neophodno uključiti i druge aktere, u ovim konkretnim slučajevima druge države. Mnogi izazovi današnjice mogu se kontrolisati jedino posredovanjem međunarodnih institucija i saradnjom na internacionalnom nivou, što se odražava na koncentrisanu moć države.

Milton Mjuler (Milton Mueller, 2010) smatra da je upravo dihotomija, sajber libertarijanci – liberali, nasuprot teoretičarima koji insistiraju na teritorijalnosti i suverenitetu države – realisti, pogrešna pozicija pri definisanju promenjene uloge države u globalizovanom IKS. Mjuler zauzima poziciju centra i navodi: „moramo biti svesni revolucionarnog potencijala novih društvenih odnosa koje omogućavaju internet i digitalni mediji; ali istovremeno moramo biti veoma realistični o političkim, pravnim, institucionalnim, ekonomskim i kulturnim silama koje oblikuju i ograničavaju bilo kakve promene" (Mueller, 2010: 5). Mjuler kao rešenje uvodi koncept *umreženog upravljanja,* koje „pruža jedan mogući način premošćavanja jaza između nacionalnih institucija i globalne povezanosti" (2010: 6).

Umreženo upravljanje internetom ne isključuje državu kao značajnog aktera u informacionom društvu. Međutim, uloga države se menja u meri u kojoj je neophodno partnerstvo vlada sa ostalim značajnim akterima u novom okruženju. Na primer, mnoge ilegalne aktivnosti na internetu nije moguće rešiti u okvirima samo jedne države, oni kompleksniji zahtevaju udružene napore država. Pored pozitivnih primera uspešnih saradnji država na suzbijanju ilegalnih aktivnosti, brojni su i oni koji se ne mogu nazvati uspešnom kooperacijom:

> „Aleksej Vladimirovič Ivanov, dvadesetogodišnji kompjuterski štreber iz Čeljabinska, Rusije, sa planine Ural, zarađuje tako što hakuje kompjuterske mreže

američkih kompanija. Nakon što provali u servere firmi, kontaktira ih u ime 'Ekspertske grupe za zaštitu od hakera' i traži hiljade dolara u zamenu za savete kako da zapuši njihove sigurnosne rupe. [...] Ukoliko kompanija ne odgovori na njegove pretnje, Ivanov će izbrisati njihove kompjuterske datoteke ili će objaviti podatke kreditnih kartica njihovih klijenata na internetu. Nije iznenađujuće, što je većina kompanija pristala na iznudu" (Goldsmith & Wu, 2006: 163).

Navedeni primer sajber kriminala uključuje jurisdikcije dve države, Rusije i Amerike. Rusija nije omogućila uvid u kompjuterske podatke hakera, pa je FBI hakovao kompjutere u Rusiji da bi dobio potrebne podatke, što je Rusija okvalifikovala kao narušavanje suvereniteta i podnela krivičnu prijavu protiv FBI (Godsmith &Wu, 2006: 163–164).[38]

Između ostalog, sajber kriminal je jedna od oblasti koja zahteva međunarodnu saradnju. Savet Evrope je 2001. godine usvojio ***Konvenciju o visokotehnološkom kriminalu***:

„Uvereni u potrebu da se, kao prioritet, nastavi zajednička kaznena politika usmerena na zaštitu društva od sajber kriminala, između ostalog, usvajanjem odgovarajućeg zakonodavstva i podsticanjem međunarodne saradnje. [...] Sa uverenjem da efikasna borba protiv sajber kriminala zahteva povećanu, brzu i veoma funkcionalnu međunarodnu saradnju" (Convencion on Cybercrime[39], 2001: 2).

Problem širenja dečje pornografije internetom takođe je jedan od problema kojem se mora pristupiti internacionalno, odnosno kooperativno[40]. Nart Vilnev (Nart Villeneuve u Deibert et. al. 2010: 55–70) analizira ograničenu internacionalnu kooperaciju po pitanju zaštite dece, odnosno dečje pornografije na internetu. Vilnev navodi da svaka država može da zaštiti svoj nacionalni internet prostor ili blokiranjem sadržaja na granici ili različitim filter sistemima, međutim, kooperacija je potrebna u onom delu koji se odnosi na identifikaciju i sankcionisanje servera sa kojih se takav sadržaj šalje. U tom kontekstu neophodno je uspostavljanje "dinamične kooperacije", koja podrazumeva: „kontinuiranu komunikaciju i interakciju između zajednice različitih aktera koji obuhvataju nadnacionalne institucije kao što su Europska unija, nacionalne vlade, privatne industrije, uključujući internet servis provajdere (ISP) i nevladine organizacije" (Villeneuve u Deibert et. al. 2010: 55). Vilnev zaključuje da međunarodna saradnja još uvek nije na nivou efikasne dinamične kooperacije kada je u pitanju distribucija dečjeg pornografskog sadržaja.

U prethodno navedenim primerima pokazuje se da je neophodno prilagođavanje države većoj međunarodnoj saradnji u rešavanju problema koji se javljaju na internetu. Međutim, uloga države u donošenju i sprovođenju nacionalnih zakona kojima se reguliše sajber prostor i dalje je stub

[38] Brendan I. Koerner. (June 2002) "From Russia with Lopht". *Legal Affairs* Dostupno na: http://www.legalaffairs.org/issues/May-June-2002/feature_koerner_mayjun2002.msp (pristupljeno 13. 12. 2017. godine).

[39] Originalni tekst Konvencije videti putem linka: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (pristupljeno 14. 12. 2017. godine).

[40] Pored Konvencije o sajber kriminalu, koji u članu 9. sadrži odredbe o suzbijanju dečje pornografije, postoji niz dokumenata koji se bave ovim problemom na evropskom nivou: Savet Evrope je 2012. godine usvojio Konvenciju o zaštiti dece od seksualne eksploaticije i seksualnog zlostavljanja (dostupno na: https://rm.coe.int/168046e1e1) , Evropski Parlament je 2012. godine usvojio Rezoluciju o zaštiti dece u digitalnom svetu (dostupno na: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012IP0428&from=EN) (pristupljeno 14. 12. 2017. godine).

nacionalnih zakonodavnih okvira. Najveći broj međunarodnih dokumenata ističe značaj nacionalnih specifičnosti i insistira na implementaciji u skladu sa domaćim zakonodavstvom, kulturom, običajima, domaćim normama i očekivanjima. Na predstavljenim primerima Francuske i Amerike uviđa se da postoji značajna razlika u poimanju slobode izražavanja na internetu. U SAD se ne sankcioniše nacistička onlajn-propaganda, dok je u Francuskoj ili Nemačkoj takav sadržaj zabranjen i shodno tome filtriran.

3.3.3. Modeli upravljanja protoka informacija

Kompleksnost novog okruženja zahteva nove modele upravljanja protoka informacija internetom. Kako je već bilo reči, države kao akteri u međunarodnom sistemu ne mogu samostalno da odgovore na sve izazove uspešno, zbog toga je ključ u međunarodnoj saradnji, odnosno umreženom delovanju zasnovanom na kooperaciji. Specifičnost globalizovanog IKS ogleda se i u uključivanju privatnih aktera u proces upravljanja. Pojam upravljanja (*governance*) sve češće menja pojam vladanja (*governing*), jer podrazumeva sistem u koji nisu uključene samo vlade i nacionalne države, već i ne-državni akteri; takođe, pojam upravljanja je pogodniji za opisivanje aktuelnih odnosa, jer se ne odnosi na klasično hijerarhijsko vladanje, već pre na pregovaranje i postizanje konsenzusa u koji su uključene mnogobrojne zainteresovane strane, privatni akteri i civilni sektor pored država (Mayntz, 2002).

Borzel i Ris (Börzel & Risse, 2005) grafički prikazuju područje upravljanja u zavisnosti od aktera koji su uključeni u proces upravljanja (prikazano u Grafikonu 2). Autori razlikuju načine upravljanja u koje su uključeni samo javni akteri (nacionalne i nadnacionalne institucije), udruženo upravljanje privatnog i javnog sektora i upravljanje koje obuhvata samo privatne aktere.

<table>
<tr><th>Uključeni akteri

Načini upravljanja</th><th>Samo javni akteri</th><th>Privatni i javni akteri</th><th>Samo privatni akteri</th></tr>
<tr><td>Hijerarhijsko: Odozgo prema dole (pretnja od) sankcija</td><td>• Tradicionalna nacionalna država
• Nadnacionalne institucije (EU, delimično STO)</td><td></td><td></td></tr>
<tr><td>Ne-hijerarhijsko 1: Pozitivni podsticaji; pregovaranje</td><td>• Internacionalno pregovaranje</td><td rowspan="2">• Delegiranje javnih funkcija privatnim akterima
• Korporativizam
• Javno-privatno

• Mreže i partnerstva
• vrednovanje</td><td rowspan="2">• Privatni interes vlade/privatn i režimi

• Privatno-privatno partnerstvo (nevladine komapnije)</td></tr>
<tr><td>Ne-hijerarhijsko 2: Ne-manipulativno ubeđivanje (učenje, raspravljanje itd)</td><td>• Institucionalno rešavanje problema</td></tr>
</table>

Grafikon 2 Područje upravljanja. Osenčano područje = područje upravljanja u užem smislu; tamno osenčano područje = područje javno-privatnog partnerstva (Börzel & Risse, 2005: 3).

U prvom tipu prepoznat je hijerarhijski model upravljanja, karakterističan za tradicionalnu regulaciju nametnutu odozgo, dok u preostala dva načina upravljanja takav model nije prepoznat. Osnovna karakteristika upravljanja u koje su uključeni i (ili samo) privatni akteri jesu, pre svega, nehijerarhijski modeli koji podrazumevaju pozitivne podsticaje, pregovaranje, nemanipulativnu persuaziju itd.

Model koji uključuje privatne i javne aktere prepoznat je i kada je reč o upravljanju internetom, odnosno novim informaciono-komunikacionim tehnologijama. Već je bilo reči o tome da tradicionalno hijerarhijsko upravljanje zasnovano samo na nacionalnim državama kao suverenim akterima u međunarodnom sistemu nije moguće. Odnosno, nije moguće u meri koja bi za ishod imala pozitivno razrešenje aktuelnih izazova u globalnoj komunikacionoj politici. Način upravljanja koji dominira u toj oblasti je onaj koji Borzel i Ris (2005) prepoznaju kao kooperaciju privatnih i javnih aktera, i takve režime definišu na sledeći način:

> „međunarodni režimi s eksplicitnim normama, pravilima i postupcima donošenja odluka, ali i neformalno upravljanje koje se odnosi na specifična pitanja – područja međunarodnog života. Ne-državni akteri mogu biti (domaće i transnacionalne) neprofitne organizacije (uključujući [multinacionalne] korporacije), najčešće grupe (biznis grupe, sindikati) i neprofitni sektor" (Börzel & Risse, 2005: 4).

Potrebu da se u rešavanje izazova novog informacionog okruženja intenzivno uključe i ne-državni akteri uvidele su, 2001. godine, Ujedinjene nacije. *Rezolucijom 56/83*[41] Generalna skupština Ujedinjenih nacija donela je odluku o organizovanju *Svetskog samita o informacionom društvu*, koji je održan u dve faze; prva faza u Ženevi 2003. godine, druga faza u Tunisu 2005. godine.

Akcioni plan[42] iz Ženeve kao glavne aktere informacionog društva navodi nacionalne vlade, privatni sektor, civilno društvo i internacionalne i regionalne institucije, insistirajući na njihovoj saradnji i partnerstvu. Država, odnosno vlade, ostaju na prvom mestu akcionog plana, ali u skladu sa planom, preporuka je da deluju udruženo, umreženo, sa ostalim zainteresovanim stranama (*stakeholders*) u informacionom društvu:

> „Vlade imaju vodeću ulogu u razvoju i implementaciji sveobuhvatnih, budućih i održivih nacionalnih e-strategija. Privatni sektor i civilno društvo, u dijalogu sa vladama, imaju važnu konsultativnu ulogu u osmišljavanju nacionalnih e-strategija. […] Zalaganje privatnog sektora je važno u razvoju i širenju informaciono-komunikacionih tehnologija (ICT), za infrastrukturu, sadržaj i aplikacije. Privatni sektor nije samo tržišni igrač već igra i ulogu u širem kontekstu održivog razvoja (WSIS-03/GENEVA/DOC/5-E, poglavlje A, stavka 3a i 3b)[43]".

Akcionim planom poziva se Generalni sekretar UN da organizuje radnu grupu koja će se baviti upravljanjem internetom (*Internet governance*) i koja će uključiti vlade, privatni i civilni sektor. Radna

[41] Tekst *Rezolucije* videti putem linka : http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf (pristupljeno 14.12.2017. godine).
[42] Tekst *Akcionog plana* videti putem linka: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf (pristupljeno 14. 12. 2017. godine).
[43] Ibid.

grupa je 2005. godine podnela *Izveštaj o upravljanju internetom (*WGIGR)[44] kojim je upravljanje internetom definisala kao:

> „Razvoj i primena zajedničkih načela, norma, pravila, postupaka donošenja odluka i programa, koji oblikuju evoluciju i korišćenje interneta, od strane vlada, privatnog sektora i civilnog društva, shodno njihovim ulogama" (WGIGR, Château de Bossey, June 2005).

Drugom fazom, održanoj u Tunisu 2005. godine, potvrđena je značajna uloga države i privatnog sektora:

> „Politički autoritet za pitanja javne politike koji se odnose na internet suvereno je pravo država. Države imaju prava i odgovornost za međunarodna pitanja javne politike u vezi sa internetom. […] Privatni sektor imao je i mora i dalje imati važnu ulogu u razvoju interneta, kako u tehničkim tako i ekonomskim oblastima" (WSIS-05/TUNIS/DOC/9(Rev.1)-E, stav 35a i 25b)[45].

Svetski samit o infromacionom društvu nastavio je da se održava na godišnjem nivou[46], insistirajući na partnerstvu svih zainteresovanih strana, javnih i privatnih aktera u izgradnji boljeg informacionog društva. Uključivanje privatnih aktera, kao neizbežnog dela upravljanja IKS, ne odnosi se samo na „delegiranje javnih funkcija privatnim akterima" (Börzel & Risse, 2005: 3) u smislu jačanja pozicija ne-državnih aktera, već sa sobom nosi i podelu odgovornosti. Odgovornost se, pre svega, odnosi na izgradnju okruženja koje će osiguravati slobodan, nediskriminatoran pristup, sigurnu onlajn zonu, uz poštovanje ljudskih prava.

U tom kontekstu, Savet Evrope je, u martu 2016. godine, usvojio *Strategiju Saveta Evrope za upravljanje internetom 2016-2019*[47], u čijem se uvodu navodi:

> „Upravljanje internetom treba da omogući dijalog i interakciju između svih segmenata stanovništva da promoviše poštovanje, jednakost, toleranciju i zajednički život, čime se podstiče angažovanje i participacija u demokratskom društvu" (paragraf 1).

Ističući značaj unapređenja demokratskih vrednosti, garantovanja onlajn-bezbednosti i poštovanja osnovnih ljudskih prava, *Strategijom* se posebno naglašava odgovornost svih učesnika pri postizanju ovih ciljeva:

> „Delotvorna zaštita i promocija demokratije, ljudskih prava i vladavine prava u digitalnom svetu zajednički je zadatak i zajednički cilj mnogih aktera. Zahteva partnerstvo i sinergiju između država, međunarodnih organizacija, civilnog društva, privatnog sektora, tehničkih i akademskih zajednica" (Paragraf 15).

---

[44] Tekst videti putem linka: https://www.wgig.org/docs/WGIGREPORT.pdf (pristupljeno 14. 12. 2017. godine).
[45] Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16–18. November 2005. Dostupno na: http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf (pristupljeno 17. 12. 2017. godine).
[46] Svim godišnjim izveštajima Samita može se pristupiti putem linka: http://www.itu.int/net/wsis/review/reports/ (pristupljeno 17. 12. 2017. godine).
[47] Tekst Strategije videti putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60 (pristupljeno 17. 12. 2017. godine).

Model upravljanja internetom, kao *novom javnom sferom* (Papacharissi, 2002), uključuje udružene napore javnog i privatnog sektora. Stoga, uloga države u međunarodnom sistemu komunikacija jeste izmenjena, međutim, teoretičari koji su predviđali kraj teritorijalnim granicama i apsolutni gubitak suvereniteta i jurisdikcije preuranjeno su državi otpisali moć. Država je i dalje značajan akter, kako Prajs ističe „verovatnije su redifinisana moć države i promene u maniru i praksama autoriteta, od onog što je često okarakterisano kao negiranje države" (Price, 2002: 3).

3.4. Uloga države u zaštiti ljudskih prava u novom informacionom okruženju

„Ljudska prava su, dakle, moralnog porekla, a urođena su baš zato što ih ima svako ljudsko biće samim tim što je ljudsko biće. Ona se ne duguju državi, koliko god ona demokratska bila, i postoje bez države i nezavisno od njene volje. […]S druge strane, mada su ljudska prava urođena i postoje nezavisno od države, ona svoj pravi smisao ostvaruju upravo u regulisanju odnosa pojedinca i države" (Hadži-Vidanović, Milanović, 2006: 7).

Ljudska prava su prava zagarantovana svakom čoveku, bez diskriminacije i ograničenja. Mnogo je faktora koji utiču na to u kojoj će se meri zaštita ljudskih prava zaista i sprovoditi. Uvođenje informaciono-komunikacionih praksi u svakodnevicu građana razvijenih zemalja donelo je mnogobrojne izazove promociji i zaštiti ljudskih prava. Dok, sa jedne strane, globalna povezanost i brzina protoka informacija mogu da pospešuju i brzu reakciju međunarodne zajednice, kada do kršenja ljudskih prava dođe, sa druge strane javlja se novi izazov: zaštita ljudskih prava na internetu.

S obzirom na to da su predmet analize u ovom radu pravo na slobodno izražavanje i pravo na privatnost na internetu, njihova zaštita i uloga države u obezbeđivanju ova dva prava na internetu biće centralna tema ovog potpoglavlja. Međutim, da bi odnos države prema pravima u novom okruženju bio analiziran, neophodno je najpre da se pojmovno odredi termin ljudskih prava i ukazaže na tradicionalnu ulogu države u njihovoj zaštiti.

Proporcionalno sve većem insistiranju internacionalne zajednice na poštovanju ljudskih prava, literatura o ovoj tematici, kao što su različiti uvodi u ljudska prava, priručnici i udžbenici, umnožava se decenijama (Dimitrijević, Paunović, Đerić, 1997; Robertson, 2004; Wolfgang & Minna, 2005; Andrew, 2007; Beitz, 2011; Smith, 2014). Pojmu ljudskih prava može se pristupiti sa različitih aspekata. Osnovne teze u vezi sa operacionalizacijom ovog termina u tradicionalnom okruženju mogu se svesti na sledeća problemska pitanja: Da li su ljudska prava nešto što svakom čoveku pripada rođenjem, ili su pak ljudska prava različita za različite zajednice ljudi? Odnosno, ko definiše šta jesu ljudska prava i u kojoj meri će biti ostvarena ili uskraćena: država, međunarodno ili prirodno pravo? Novo okruženje donosi i nova pitanja: Ko je garant poštovanja ljudskih prava na internetu: država, međunarodne institucije ili privatni akteri? Da li država ima kapacitete da zaštiti prava svojih građana na internetu? Da li država može da ugrozi prava svojih građana na internetu? Ova pitanja i izazovi biće razmotreni u nastavku.

3.4.1. Definisanje ljudskih prava

Dimitrijević, Paunović i Đerić u knjizi *Ljudska prava: udžbenik* (1997), navode različita teorijska shvatanja ljudskih prava, od pozitivističkih do marksističkih (str. 42–59). Naime, prema pozitivističkom shvatanju ljudska prava su propisana zakonom i kao takva moraju se poštovati. Pozitivisti izvorište ljudskih prava pronalaze u zakonodavstvu, pre svega u ustavu, kao najvišem aktu jedne države. Međutim, autori kritikuju takav stav pozitivista: „Podrazumeva se mogućnost da ljudska prava budu ukinuta promenama pravnih normi pod uticajem novog političkog konsenzusa" (Dimitrijević, Paunović, Đerić, 1997: 43). Odnosno, sa svakom promenom vlasti, jednostavnim preglasavanjem manjine, katalog ljudskih prava mogao bi da se menja i na taj način obesmišljava, jer podilazi volji većine na čelu sa predstavnicima vlasti. U tom kontekstu Klapam (Clapham) navodi dodatni argument: „Ljudska prava mogu i da štite ljude od 'tiranije' većine" (2007: 2).

Sa druge strane, naturalističko polazište izvor ljudskih prava pronalazi mimo volje države (Beitz, 2011: 49–74), jer, kako tvrde naturalisti: „Postoje pravne norme i subjektivna prava iznad i van pozitivnih propisa i volje države, odnosno zakonodavca" (Dimitrijević, Paunović, Đerić, 1997: 45). Pored ova dva suprotna shvatanja, autori navode i utilitarističko polazište, koje poštovanje ljudskih prava opravdava načelom korisnosti i marksističko, koje spori potrebu za postojanjem ljudskih prava u besklasnom društvu, jer će svi biti jednaki i ravnopravni (str. 51–59).

Jasno je da se analizi ljudskih prava može pristupiti sa različitih aspekata, međutim, ono što je značajno i što pronalazimo u većini teorijskih utemeljenja jeste da su ljudska prava nesporno postala značajan deo državnih i međunarodnih politika, naročito nakon Drugog svetskog rata i porasta svesti o potrebi da se prava čoveku garantuju, ne samo kroz apstraktnu misao o njihovoj neophodnosti već i kroz konkretne pozitivističke norme i propise (Simmons, 2009: 36–42).

Katalog ljudskih prava je opširan, ali sva ljudska prava možemo kategorizovati na dve velike grupe i njihove podgrupe: **građanska i politička prava** i **ekonomska, socijalna i kulturna prava** (Dimitrijević, Paunović, Đerić, 1997; Hadži-Vidanović, Milanović, 2006). Ova podela odnosi se na različite oblasti koje ljudska prava obuhvataju, ali je i u vezi sa odnosom države prema njima. Naime, obaveza svake pravne demokratske države je zaštita osnovnih ljudskih prava svojih građana. Međutim, razlika u odnosu države prema ovim dvema grupama ljudskih prava ogleda se u potrebi za pasivnom ili aktivnom reakcijom države[48]. Kako ističu Hadži-Vidanović i Milanović: „Građanska i politička prava potiču iz klasičnih shvatanja liberalne demokratije, koja traži od države da se ne meša u privatnu sferu pojedinca osim ako je to apsolutno neophodno, dok ekonomska, socijalna i kulturna zahtevaju od države da se aktivno angažuje radi boljeg života svojih građana" (2006: 8–9). Dimitrijević, Paunović i Đerić pojašnjavaju da su građanska prava zasnovana na *autonomiji* pojedinca, politička na *participaciji*, odnosno oba na *načelu slobode*, dok je osnovna funkcija ekonomskih, socijalnih i kulturnih prava da omoguće pojedincu da zaista dostigne građanska prava (1997: 174). Tako, na primer, pravo na slobodno izražavanje i pravo na privatnost spadaju u prvu grupu i od države se u tom kontekstu očekuje pasivna reakcija, odnosno nemešanje u slobodu izražavanja pojedinaca ili

[48] Hadži-Vidanović i Milanović daju pojašnjenje: „Najveći broj ljudskih prava postoji baš prema državi: njima se ona ili ograničava ili se traži njeno aktivno delovanje. Među prva, spada npr. pravo na privatnost – ono nalaže državi da se ne meša u nešto što su naša lična, privatna posla. Među druga spada npr. pravo na obrazovanje, odnosno obaveza države da svojim građanima obezbedi određeni nivo svima dostupnog školovanja" (2006: 7–8).

nezadiranje u privatnu sferu, dok su, na primer, pravo na obrazovanje ili pravo na minimalne uslove egzistencije, prava druge grupe i zahtevaju aktivno učešće države, radi njihovog ostvarivanja.

3.4.2. Institucionalni nivoi zaštite ljudskih prava

Regulacija poštovanja ljudskih prava odvija se na tri nivoa: državnom, regionalnom i međunarodnom ili internacionalnom. Pojedinci su najčešće svesni prvog nivoa, odnosno unutrašnjeg prava, koje dolazi od strane države i reguliše odnose u jednom društvu. Međutim, ljudska prava su i međunarodno regulisana, čime se sprečava samovolja pojedinih država,u regulisanju ljudskih prava[49]. Na državnom nivou ljudska prava regulišu se nacionalnim zakonodavnim okvirom, a i sastavni su deo svakog ustava demokratskih zemalja. Primer regionalnog sistema u zaštiti ljudskih prava pronalazimo u Evropi. Volfgang i Mina (Wolfgang & Minna, 2005: 31) navode tri sloja evropske regulacije ljudskih prava: Savet Evrope, Organizacija za evropsku bezbednost i saradnju i Evropska unija (videti Grafikon 3).

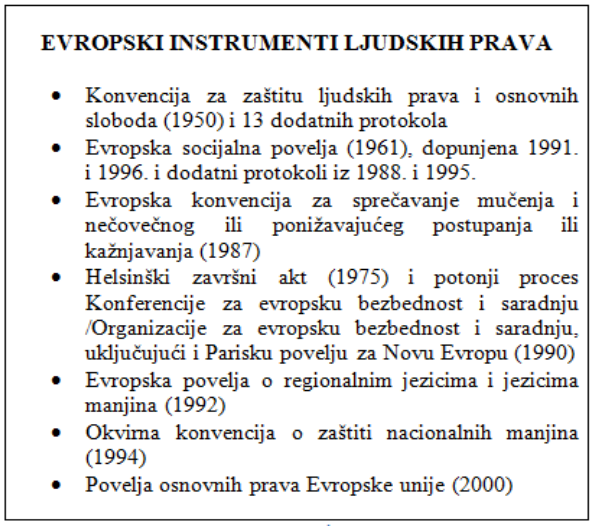
EVROPSKE INSTITUCIJE I TELA ZA LJUDSKA PRAVA	
Savet Evrope: • Evropski sud za ljudska prava (jedinstveni sud od 1998) • Evropski komitet za socijalna prava (izmenjen 1999) • Evropski komitet za sprečavanje mučenja (CPT, 1989) • Savetodavni komitet Okvirne konvencije o zaštiti nacionalnih manjina (1998) • Evropska komisija za rasizam i netoleranciju (ECRI, 1993) • Evropski komesar za ljudska prava (1999) • Komitet ministara Saveta Evrope	**OSCE:** • Kancelarija za demokratske institucije i ljudska prava (ODIHR, 1990) • Visoki predstavnik za nacionalne manjine (OSCE, 1992) • Predstavnik za slobodu medija (OSCE, 1997) **Evropska unija:** • Evropski sud pravde • Evropski centar za praćenje rasizma i ksenofobije (EUMC, 1998) P • Povelja o osnovnim pravima u EU (2000)

Grafikon 3 Evropske institucije i tela za ljudska prava (Wolfgang & Minna, 2005: 32).

Najznačajniji instrumenati za zaštitu ljudskih prava u Evropi obuhvataju značajne konvencije i povelje (videti Grafikon 4), među kojima je, za naše istraživanje, najznačajnija *Konvencija za zaštitu*

[49] „Da mogućnost države da oduzme prava nije samo terorijska, pokazuje praksa država čije su vlade došle na valast revolucionarnim putem ili koje tvrde da sprovode revolucionarne promene. Nama su najbliži primeri tzv. 'socijalističkih zemalja', čiji su zakonodavni organi ukinuli mnogobrojna subjektivna prava stečena u prethodnim porecima, pa čak i prava koja su sticana u prvo vreme revolucionarne vlasti. [...] U najrigidnijim sistemima ove vrste, za neke kategorije stanovništva (plemiće, pripadnike građanske klase) bilo je ukinuto i pravo na više obrazovanje, a u SSSR, Kini, Severnoj Koreji i sličnim zemljama eliminisana su mnoga druga prava, kao na primer pravo na slobodno biranje prebivališta i zapošljavanja, stupanje u brak sa strancima itd“ (Dimitrijević, Paunović, i Đerić, 1997: 25).

ljudskih prava i osnovnih sloboda iz 1950. godine, koja članom 8 i 10 štiti pravo na privatnost, odnosno slobodu izražavanja[50].



Grafikon 4 Evropski instrumenti ljudskih prava (Wolfgang & Minna, 2005: 31).

Borba za pravnu zaštitu ljudskih prava i ograničavanje apsolutnih vlasti na internacionalnom nivou uglavnom se dovodi u vezu sa *Deklaracijom o pravima čoveka i građanina* iz 1789. godine, koja je plod Francuske buržoaske revolucije. Iako nije prvi akt kojim se proklamuju osnovna ljudska prava, ova *Deklaracija* jeste „bila prva koja im je dala opšte, svetsko značenje. Donesena je u jednoj državi, ali s obzirom na širinu pristupa ima univerzalno značenje, jer je okrenuta svetu i budućnosti" (Huseinspahić, 2009: 242). *Deklaracija* iz 1789. godine kao prirodna prava čoveka navodi slobodu, vlasništvo i otpor ugnjetavanju. Takođe, u članu 18 navodi se da „niko ne može biti pozvan na odgovornost zbog mišljenja, pa i religioznog, ukoliko njegovo iskazivanje ne ometa javni red utvrđen zakonom"[51]. Tumačen u opštijem smislu, član 18 odnosi se na slobodu izražavanja, odnosno iskazivanja mišljenja, kao pravo pojedinca koje ne podleže sankcijama, ukoliko ne narušava druga prava i slobode propisane zakonom.

Ideal poštovanja ljudskih prava kao neodvojiv element vladavine prava od 18. veka postaje preduslov za izgradnju budućeg pravednijeg društvenog poretka. Danas svaka demokratska država garantuje poštovanje osnovnih ljudskih prava, čiji začetak prepoznajemo u francuskoj *Deklaraciji*, ali koji je vremenom širio svoje granice, uključujući mnoga prava, zagarantovana nacionalnim zakonima

[50] Pored evropskog regionalnog okvira i drugi delovi sveta imaju svoje regionalne sisteme. O zaštiti prava na evropskom tlu, ali i o Americi i Africi i njihovoj regionalnoj zaštiti ljudskih prava opširnije videtu u: Smith, R. K. (2014). *Textbook on international human rights*. Oxford University Press, pp. 86–153.

[51] Tekst Deklaracije dostupan putem linka: https://www.slideshare.net/GordanaComic/francuska-deklaracija-o-pravima-oveka-i-gradjanina-iz-1789 (pristupljeno 10. 01. 2018. godine).

pojedinačnih država, ali i međunarodnih organizacija[52]. Kako ističe Veljanovski: „Oblast ljudskih prava postaje univerzalna, sveobuhvatna te uključuje ostvarivanje svih potreba ljudi koje u savremeno doba, razvojem demokratije i ravnopravnosti, postaju legitimne" (2017: 8).

O kompleksnom sistemu zaštite ljudskih prava na nadnacionalnim nivoima, Jurišić navodi da se zaštita odvija na tri nivoa: kroz bileteralne odnose pojedinačnih država, preko međunarodnih vladinih organizacija i putem nevladinih organizacija, specijaliziranih za datu oblast (1998: 70–82). Prvi nivo podrazumeva saradnju između država koja pored diplomatsko-konzularnih aktivnosti[53] ima i ulogu zaštite svojih sunarodnika, sa privremenim ili trajnim prebivalištem na teritoriji nematične države. Drugi nivo odnosi se na međunarodne vladine organizacije, kakve su na primer Ujedinjene nacije[54], koje su kao svetska organizacija nezaobilazne kada je o poštovanju ljudskih prava na međunarodnom nivou reč, dok treći nivo obuhvata specijalizovane nevladine organizacije[55], kao što su *Amnesty International* ili *Human Rights Watch*.

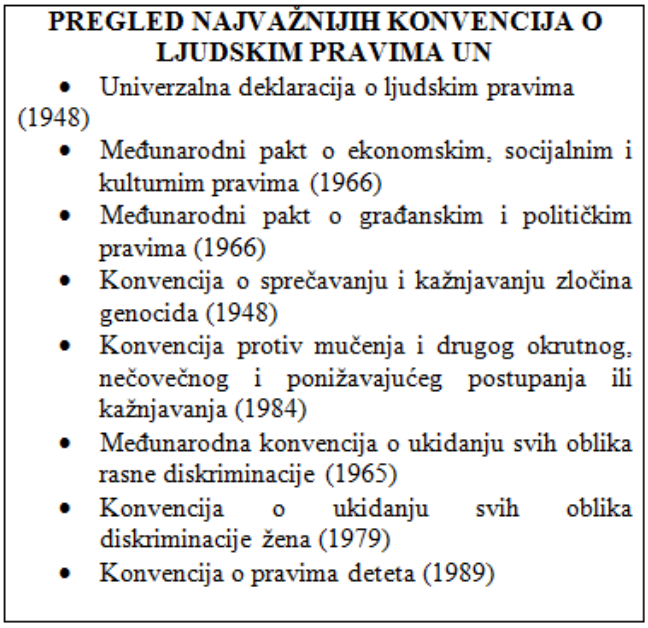
Ujedinjene nacije, kao vladina internacionalna organizacija, imaju kompleksni sistem zaštite ljudskih prava, koji se ogleda u brojnim poveljama (videti Grafikon 5). Jedna od najznačajnijih deklaracija Ujedinjenih nacija, u kontekstu ovog rada, jeste *Univerzalna deklaracija o ljudskim pravima* iz 1948. godine, koja članom 19 brani slobodu izražavanja bez obzira na granice.

[52] Dejvid Robertson u knjizi *Rečnik ljudskih prava* (Robertson, D. (2004). *A dictionary of human rights*. Routledge) daje pregled svih ljudskih prava abacednim redom. Takođe, navodi i sve značajne nacionalne i međunarodne organizacije i dokumenta, koje garantuju poštovanje ljudskih prava.

[53] Radojković i Stojković detaljno opisuju ulogu države kao subjekta međunarodnog komuniciranja i ukazuju na značaj vladinih aktivnosti u odnosima sa drugim državama (2004: 79–86).

[54] O strukturnoj organizaciji Ujedinjenih nacija videti u: Smith, R. K. (2014). *Textbook on international human rights*. Oxford University Press. pp. 52–86. O značaju Ujedinjenih nacija na međunarodnom planu, ali i o ulozi njenih specijalizovanih agencija (UNESCO i Međunarodna telekomunikaciona unija) videti u: Radojković, M. (1987). *Međunarodno komuniciranje*. Beograd: Zavod za udžbenike i nastavna sredstva, str. 128–144.

[55] Videti više u: Ibid. str. 144–156.



Grafikon 5 Konvencije Ujedinjenih nacija o ljudskim pravima (Wolfgang & Minna, 2005: 27).

3.4.3. Internet i ljudska prava

Komercijalna upotreba interneta donela je mnogobrojne izazove kada je reč o zaštiti ljudskih prava. Mnogi autori bavili su se upravo ovim pitanjem, odnosom ljudskih prava i novog informacionog okruženja (Metzl, 1996; Khor, 2011; Gregg, 2012; Maletić, Dakić, 2012; Hick, Halpin & Hoskins, 2016). Džejmi Mecl (Jemie Metzl, 1996) analizira odnos informacione tehnologije i ljudskih prava, ističući i koristi i potencijalne opasnosti, koje novo okruženje donosi. Autor ne spori benefite koji se, pre svega, ogledaju u boljoj globalnoj povezanosti i brzni informisanja o kršenju ljudskih prava, ali ističe da one nekada nisu presudne da bi reakcija bila adekvatna. Primer koji autor u tom kontekstu navodi jeste kršenje ljudskih prava u Ruandi, o kojem su zapadne zemlje bile blagovremeno obaveštene, ali je pravovremena reakcija ipak izostala (Metzl, 1996: 707–708).

Mecl analizira i ulogu nevladnih organizacija specijalizovanih za pitanja ljudskih prava i načine na koje one koriste nove tehnologije. Ukazujući na potencijalnu korist, ali i opasnosti od, na primer, nadzora države ili zagušenja informacionih kanala od strane autoritarnih vlada, autor zaključuje da grupe za odbranu ljudskih prava imaju zadatak da: „maksimiziraju benefite ovih sistema i minimizuju značajnu opasnost koju oni predstavljaju. […] U isto vreme, zajednica zaštitnika ljudskih prava može biti značajan igrač u naporima da se odredi ko će izvući korist od ovog dramatičnog tehnološkog napretka" (Metzl, 1996: 746). Kako Hik, Halpin i Hoskins (Hick, Halpin & Hoskins) navode: „Aktivisti za ljudska prava mogu koristiti internet, ali isto tako mogu i neprijatelji ljudskih prava širiti svoje informacije i propagandu" (2016: 13).

Slično, Bendžamin Greg (Benjamin Gregg, 2012) ukazuje na pozitivne i negativne aspekte novih tehnologija, kada je reč o jačanju politike ljudskih prava. Kao pozitivne on navodi to što je internet manje kontrolisan, decentralizovan i relativno jeftin, povezuje ljude širom sveta i ne diskriminiše marginalizovane grupe. Sa druge strane, autor ističe da je verovatnije ostvarivanje ovih prednosti u demokratskim zemljama, nasuprot autoritarnim, stoga navodi i potencijalne probleme koji se ogledaju u opresiji od strane države, korporativnoj kontroli privatizovnog javnog prostora, pitanjima privatnosti na internetu, nejednakom pristupu i slično (str. 212–214).

Mogućnost bržeg protoka informacija i umrežavanje sa udaljenim delovima sveta, išli su, dakle, u prilog zaštiti ljudskih prava, naročito onda kada je prioritet brza reakcija međunarodnih organizacija, vladinih i nevladinih, za zaštitu ljudskih prava. Internet je u tom smislu „postao alat za promociju i zaštitu ljudskih prava, koji se koristi za dobijanje, prenošenje i diseminaciju informacija" (Hick, Halpin & Hoskins, 2016: 7). Sa druge strane, internet je nesumnjivo doneo i nove izazove u oblasti zaštite ljudskih prava. Vatni (Watney) ambivalnetnu prirodu novog okruženja slikovito opisuje: „Kada se duh (komercijalizacija interneta) jednom pusti iz boce, njegove moći su oslobođene za oba, i dobro i zlo" (2007: 42). U tom kontekstu, odnos javnosti prema internetu Vatni opisuje na sledeći način: „Kada internet i tehnologija promovišu ljudska prava tehnologija se magijski vrednuje. Kada internet olakšava kontrolu države, tehnologija se proklinje" (Watney, 2007: 43).

Uloga države u ovoj oblasti usložnjava se sa sve složenijim informacionim okruženjem. Pojedinac je odgovoran za svoja dela u onlajn-prostoru, podjednako kao i u oflajn-zajednici. Pravila ponašanja ne menjaju se sa promenom medijuma, niti se odgovornost briše zajedno za geografskim granicama. Slično je i sa ulogom države, kao stožera u zaštiti prava svojih građana. Ukoliko država ne uvaži prekršaj nekog prava pojedinca, on, nakon što iscrpi sve mogućnosti žalbe u nacionalnom zakonodavnom okviru, može uputiti žalbu i Međunarodnom sudu za ljudska prava, koji ima mogućnost donošenja suprotne odluke i bukvalnog poništavanja nacionalne presude. Kooperacija države i međunarodnih tela, ali i privatnih aktera, neophodna je i pri zaštiti ljudskih prava onlajn.

3.4.4. Sloboda izražavanja na internetu

Pravo na slobodno izražavanje jedno je od centralnih prava u demokratskim zemljama. Ovim pravom građanima se garantuje primanje i širenje informacija, bez obzira na granice. „U slobodi izražavanja se istovremeno otelotvoravaju čovekova sloboda od države i njegovo pravo da utiče na državu u kojoj živi" (Dimitrijević, Paunović, Đerić, 1997: 319). Pravo na slobodno izražavanje zagarantovano je članom 19 *Univerzalne deklaracije o ljudskim pravima* iz 1948. godine, kao i članom 10 *Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda* iz 1950. godine. Oba pravna dokumenta ističu značaj prava na slobodno izražavanje bez diskriminacije. Moglo bi se pretpostaviti da je upravo sa sve većom upotrebom interneta ovo pravo dobilo svoj pravi smisao. Međutim, sloboda izražavanja poznaje granice i na internetu (Surčulija, 2010).

Zaštita prava na slobodno izražavanje na internetu kompleksni je izazov u novom okruženju, i jedan od predmeta ovog istraživanja. Ugrožavanje prava na slobodno izražavanje na internetu javlja se u različitim oblicima i može biti narušeno od strane različitih aktera. Pravo na slobodno izražavanje

podrazumeva pravo na širenje, ali i na prijem informacija iz različitih izvora, stoga svaka zabrana širenja ili prijema informacija, izuzev kada one škode drugom, predstavlja kršenje prava na slobodno izražavanje.

Nekada je kršenje ovog prava na internetu evidentno, na primer, kada govorimo o autoritarnim vladama, koje čak i infrastrukturno blokiraju pristup internetu ili određenim sadržajima; ili kada je reč o blokiranju, uklanjanju i filtriranju sadržaja od strane privatnih kompanija, koje može biti sprovedeno pod nalogom vlada, ali i zarad zaštite drugih prava. Sa druge strane, kršenje ovog prava može biti sofisticiranije i kada je reč o državi i kada je reč o privatnim akterima. Navedeno se može ilustrovati sledećim primerima:

1) mogućnost vlada (čak i demokratskih) da nadziru aktivnosti građana na internetu, dok saznanje o tome vodi građane u autocenzuru, odnosno bojazan korisnika interneta da objavljuju kritičke sadržaje o radu svojih vlada, zbog straha od odmazde i sankcija, ili

2) mogućnost privatnih kompanija na internetu, na primer društvenih mreža, da upravljaju informacijama, odnosno da favorizuju određene sadržaje iz komercijalnih ili drugih interesa.

Prethodni primeri su primeri uticanja na slobodu izražavanja korisnika, koji nisu tako očigledni kao prvonavedene pretpostavljene situacije.

Međunarodne institucije svojim regulatornim okvirom štite pravo slobodnog izražavanja na internetu:

- ***Evropska unija***, odnosno Savet EU, 2014. godine u Briselu usvojio je *Smernice EU za ljudska prava o slobodi izražavanja onlajn i oflajn*[56]. Smernice se posebno odnose na poštovanje ljudskih prava onlajn, kao što je to slučaj sa ljudskim pravima oflajn. Kada je reč o dvama pravima, koja su predmet analize u ovoj disertaciji, navodi se sledeće: „Sva ljudska prava koja postoje oflajn takođe moraju biti zaštićena onlajn, posebno pravo na slobodu mišljenja i izražavanja, kao i pravo na privatnost, što takođe uključuje i zaštitu ličnih podataka" (član 6). U delu *Opštih razmatranja* navodi se: „**Pravo na slobodu mišljenja i izražavanja je univerzalno pravo:** Sloboda mišljenja i izražavanja odnosi se na sve osobe jednako. Treba ga zaštititi svugde i za svakoga, bez obzira na to ko su i gde žive. Mora biti poštovano i zaštićeno jednako onlajn i oflajn" (član 23). U sledećem članu posebno se ističe odgovornost država u zaštiti prava na slobodno izražavanje na internetu: „**Države imaju primarnu obavezu zaštite i osiguravanja prava na slobodu mišljenja i izražavanja**" (član 24).

- ***Ujedinjene nacije*** su 1966. godine usvojile *Međunarodni sporazum o civilnim i političkim pravima*[57] (MSCPP), koji je stupio na snagu 1976. godine. Članom 19 *Sporazum* štiti slobodu izražavanja. Međutim, sa razvojem novih informaciono-komunikacionih tenologija i komercijalizacijom interneta, javila se i potreba da se članu 19 pristupi iz novog aspekta, shodno tehnološkim promenama. Komitet za ljudska prava Ujedinjenih nacija

[56]Engl. *EU Human Rights Guidelines on Freedom of Expression Online and Offline,* videti putem linka: https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf (pristupljeno 29. 01. 2018. godine).
[57]Engl. *International Covenant on Civil and Political Rights,* videti putem linka http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf (pristupljeno 28. 01. 2018. godine).

objavio je 2011. godine opšti komentar broj 34, CCPR/C/GC/34[58], o članu 19, kojim se ukazuje na značaj slobode izražavanja na internetu, ističući u članu 12 da sloboda izražavanja uključuje: „sve forme audio-vizuelnih kao i elektronskih i na internetu zasnovanih načina izražavanja" (CCPR/C/GC/34, član 12). Takođe, članom 15 ukazuje se na promene koje donosi novo okruženje pri tumačenju prava na slobodno izražavanje: „Države članice trebaju uzeti u obzir u kojoj meri je razvoj informacionih i komunikacionih tehnologija, kao što su internet i mobilni sistemi za distribuciju elektronskih informacija, bitno promenio komunikacijske prakse širom sveta" (CCPR/C/GC/34, član 15).

- ***Savet Evrope***, odnosno Komisija ministara pri Savetu Evrope, 2003. godine usvojila je *Deklaraciju o slobodi komunikacije na internetu*[59]. Kroz sedam principa koji se odnose na: pravila o sadržaju na internetu, podsterkivanje samoregulacije i koregulacije, odsustvo državne kontrole, uklanjanje barijera za pristup, slobodu provajdera, ograničenu odgovornost servis provajdera kada je reč o sadržaju i anonimnost, *Deklaracija* osnažava slobodu izražavanja na internetu.

Pravo na slobodno izražavanje na internetu Savet Evrope štiti i Političkom deklaracijom *Sloboda izražavanja i demokratija u digitalnoj eri: Mogućnosti, prava, odgovornosti*[60], usvojenom 2013. godine u Beogradu. Članom 5 ove *Deklaracije* navodi se sledeće:

> „Pristup internetu neodvojivo je povezan sa ljudskim pravima, posebno sa ostvarivanjem prava na slobodu izražavanja. Potvrđujemo da je od fundamentalnog značaja da ljudi imaju mogućnost da se izraze i pristupe informacijama na internetu bez prekomernih ograničenja, čime im se omogućava da efektivno ostvaruju svoja prava u skladu sa članom 10 Evropske konvencije o ljudskim pravima".

Uz *Deklaraciju* usvojene su i tri rezolucije. *Rezolucija broj 1: Sloboda interneta* posebno ističe značaj slobode izražavanja na internetu, koja u svom prvom članu navodi: „Internet, koji je stvoren radi razmene informacija i znanja, ima jedinstvenu ulogu, pomažući pojedincima da rade i budu politički i kulturni angažovani, da se okupljaju i udružuju i, pre svega, da komuniciraju i izražavaju različite stavove i mišljenja, uključujući i nezadovoljstvo i protest" [61]. Ovim članom se jasno apostrofira potreba za zaštitom slobode izražavanja na internetu, koja ima ogroman društveni i politički značaj. *Rezolucijom* se države članice Saveta Evrope pozivaju da postupaju u skladu sa poštovanjem slobode interneta: „Neopravdano uplitanje ugrožava univerzalnost i integritet interneta, negativno utiče na poverenje ljudi prema internetu i umanjuje vrednost njegove javne uloge. Neophodno je da zemlje članice Saveta Evrope postupaju u skladu sa svojim obećanjem da neće ugroziti internet" (član 10).

---

[58] Engl. *International Covenant on Civil and Political Rights, General comment No. 34*, videti putem sajtu: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (pristupljeno 28. 01. 2018. godine).

[59] Engl. *Declaration on freedom of communication on the Internet*, videti putem linka: http://www.osce.org/fom/31507?download=true (pristupljeno 28. 01. 2018. godine).

[60] Tekst Deklaracije videti putem linka: http://www.kultura.gov.rs/cyr/aktuelnosti/politicka-deklaracija---sloboda-izrazavanja-i-demokratija-u-digitalnoj-eri (pristupljeno 29. 01. 2018. godine).

[61] Tekst Rezolucije videti putem linka: http://www.kultura.gov.rs/cyr/aktuelnosti/politicka-deklaracija---sloboda-izrazavanja-i-demokratija-u-digitalnoj-eri , kao deo *Političke deklaracije* (pristupljeno 29. 01. 2018. godine).

Mogućnost ostvarivanja prava na slobodno izražavanje na internetu zagarantovana je dakle i međunarodnim pravom, ali svaka država svojim zakonskim okvirom reguliše ostvarivanje ovog prava, odnosno garantuje njegovo poštovanje. S obzirom na to da pravo na slobodno izražavanje mogu ugroziti privatni akteri, ali i države, Smit navodi: „Države su dužne da osiguraju da nacionalno pravo štiti slobodu izražavanja na oba nivoa, pružajući odgovarajuće mere zaštite i pravne lekove u slučaju kršenja zakona" (Smith, 2014: 306).

3.4.5. Pravo na privatnost na internetu – Veliki podaci (*Big Data*)

Pravo na privatnost još jedno je od prava koje je suočeno sa mnogobrojnim izazovima u novom informaciono-komunikacionom okruženju. Mnoga pitanja o zaštiti privatnosti internet korisnika ostaju otvorena: Ko upravlja našom privatnosti na internetu (Bennett & Raab, 2006)? Da li nas je nečemu naučilo Snoudenovo otkriće (Rainie, 2016)? Da li bi trebalo da pristupimo internetu kao mestu koje „nikada ne zaboravlja" (Rosen, 2011)? Da li je moguće osloniti se na državu kada je reč o zaštiti ovog prava (Schwartz, 1999), ili je ključ u zaštiti koja se garantuje samoregulacijom (Ang, 2001)?

U doba gotovo nekontrolisanog deljanja ličnih podataka "na mreži", zaštita prava na privatnost internet korisnika nameće se kao ključni izazov. Doba „velikih podataka" (engl. *big data*) posledica je brzog i sveobuhvatnog razvoja komunikacionog okruženja. „Oblaci" (engl. *clouds*) interneta skladište nezamisliv broj metapodataka o korisnicima. Gotovo da ne postoji veb-stranica ili aplikacija koja u zamenu za pristupanje ili preuzimanje ne zahteva pristup ličnim podacima korisnika, kao što su telefonski imenik, mejl kontakti, galerija fotografija ili istorija pretraga. Pored komercijalnih pružaoca usluga i operatori od posebnog značaja, kakve su i vladine agencije ili državne ustanove, prateći trend *e*-poslovanja, skladište i zadržavaju ogroman broj ličnih podataka građana. Stoga pravo na privatnost biva potencijalno ugroženo pri korišćenju javnih, kao i pri korišćenu komercijalnih onlajn-usluga. Kako je navedeno u članu 5 *Direktive o privatnosti i elektronskim komunikacijama* (2002/58/EZ)[62]: „Pristup digitalnim pokretnim mrežama postao je dostupan i prihvatljiv široj javnosti. Ove digitalne mreže imaju ogromne kapacitete i mogućnosti obrade ličnih podataka. Uspešan prekogranični razvoj ovih usluga delom zavisi od poverenja korisnika da njihova privatnost neće biti ugrožena".

Podaci koji se odnose na korisnike interneta nazivamo ličnim podacima, i kada govorimo o zaštiti privatnosti na internetu pre svega mislimo na zaštitu *ličnih podataka*, koje internet korisnici svojim aktivnostima (ne)svesno ostavljaju „na mreži".

Fondacija *Share* u Vodiču „Moji podaci, moja prava" definiše šta se sve smatra ličnim podacima na internetu:

> „Lozinke i naši nalozi za poruke, mejl ili društvene mreže, istorija aktivnosti koje smo sa tih naloga preduzeli (metapodaci, šerovi, lajkovi, klikovi), istorija pretrage interneta u aplikacijama koje koristimo, IP adresa našeg kompjutera ili smartfona, IMEI broj uređaja kojim pristupamo mreži i slično. Takođe, svi podaci iz fizičkog sveta koje unosimo pri

[62] Tekst Direktive videti putem linka: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058 (pristupljeno 03. 02. 2018. godine).

korišćenju usluga (adresa, broj telefona, računa, itd) kao i jedinstvene numeričke vrednosti u kojima su takvi podaci izraženi" (Krivokapić, Petrovski, 2018: 7).

Međutim, pored ovih podataka za koje većina ljudi može da pretpostavi da su lični podaci, jer imaju jasnu vezu sa korisnicima, postoje i podaci koje korisnici interneta ostavljaju korišćenjem određenih usluga, a da ih često i nisu svesni. Možemo čak i da pretpostavimo da takve podatke prosečni korisnik ni ne prepoznaje kao lične:

> „Snimak pande iz Kine ili citat poznatog pisca, koje smo podelili na svom profilu, nisu lični podaci. Međutim, vreme kada smo objavili post, geolokacija uređaja koji smo koristili, profili od kojih smo sadržaj preuzeli i koji su dalje delili naš post, mogu se smatrati podacima o ličnosti. Takođe, sama informacija da volimo pande ili određenog pisca predstavlja lični podatak.
>
> […]
>
> Sve što nas može identifikovati, direktno ili posredno, jeste podatak o ličnosti. Ako su uređaj ili pretraživač naši, personalizovani, onda i kolačići preuzeti sa sajtova spadaju u naše podatke o ličnosti. Na primer, kolačič za Guglovu analitiku koji registruje posetu i interakcije danas se nalazi na većini sajtova na svetu. To znači da će Gugl imati podatke o posetiocima tih sajtova, čak i kada posetioci ne koriste nijedan od Guglovih proizvoda" (Krivokapić, Petkovski, 2018: 7).

Dakle, prilikom korišćenja internet usluga svaka aktivnost korisnika ostavlja trag koji može biti očigledan (ime, prezime, mejl adresa), ali i nevidljiv, kao što su lokacija i vreme pristupa, pa čak i lične preferencije – na primer, trag o tome koji sadržaj se korisniku sviđa, a koji ne. Na osnovu ovih (meta)podataka može se izgraditi profil svakog pojedinačnog korisnika sa preciznim informacijama o njegovim preferencijama, koji potom može biti iskorišćen u komercijalne ili neke druge svrhe. Hose Van Dijk (Jose Van Dijck) u tom konkstu piše: „čak su i veze (prijatelji, sviđanja, trendovi) pretvoreni u podatke" (2013: 9); „Fejsbuk je društvene aktivnosti kao što su 'prijateljstvo' i 'sviđanje' pretvorio u algoritamske odnose" (Van Dijck, 2014: 198).

Autorka Van Dijk (2014), analizirajući primenu velikih podataka, piše o tri ključna koncepta: o procesu *datifikacije*, ideologiji *dataizma* i *nadzoru podataka* (engl. *dataveillance*, kovanica reči *data* – podaci i *surveillance* – nadzor). Datifikacija je „transformacija društvene akcije u onlajn-kvantifikovane podatke , čime se omogućava praćenje u realnom vremenu i prediktivna analiza" (Maier-Schoenberger i Cukier, 2013. prema Van Dijck, 2014: 198). Drugim rečima, svako onlajn-ponašanje i aktivnost korisnika ostavlja trag koji se beleži, skladišti i koristi za predviđanje budućeg ponašanja korisnika. S tim u vezi, ideologija dataizma pretpostavlja da svako onlajn-ponašanje može biti kvantifikovano i precizno mereno. Međutim, dataizam uključuje i poverenje u institucije koje se služe procesom datifikacije (Van Dijck, 2014). Prema Van Dijkovoj, reč je o raznovrsnim institucijama i organizacijama, ali se sve one mogu svrstati u tri velike grupe: država, privatne kompanije i akademci. Svi se oni koriste ličnim podacima internet korisnika, ali ih mogu primenjivati na različite načine. Akademci ove podatke uglavnom primenjuju za društvena istraživanja ljudskog ponašanja u onlajn-sferi.

S druge strane, korporacijama, naročito društvenim mrežama, primarni cilj je da prikupljene podatke pretvore u sredstvo plaćanja, odnosno da korisnicima naplate svoje usluge tako što će njihove podatke prodati trećim stranama: „Metapodaci i podaci postali su redovna *valuta* kojom građani plaćaju

svoje usluge komunikacije" […] Vlasnici platforme rutinski dele zajedničke metapodatke korisnika sa trećim stranama u svrhu prilagođenog marketinga u zamenu za besplatne usluge" (Van Dijck, 2014: 197). Jasno je da su veliki podaci postali veliki biznis. Privatne kompanije, na čelu sa društvenim mrežama, korisnicima stvaraju iluziju o besplatnom korišćenju njihovih usluga, dok ličnim podacima korisnika stiču profit.

Nadgledanje i skladištenje podataka o aktivnostima i ponašanju korisnika može se okarakterisati kao nadzor onlajn podataka. Međutim, za razliku od nadzora u tradicionalnom smislu, nadzor onlajn-podataka „podrazumeva neprekidno praćenje (meta)podataka za neistražene i unapred neodređene svrhe" (Van Dijck, 2014: 205). Može se pretpostaviti da će privatne kompanije koristiti podatke uglavnom u komercijalne svrhe, sa druge strane bilo je primera korišćenja onlajn-podataka u političke svrhe (na primer, Bregzit ili izbori u Americi 2016. godine). Takođe, može se pretpostaviti da će države koristiti nadzor onlajn podataka kako bi sprečile sajber kriminal, ali ne možemo da budemo sigurni da ih neće zloupotrebiti i koristiti i u druge svrhe. O tome piše Daton: „postoji bojazan da će internet i povezani društveni mediji i veliki podaci narušiti privatnost i dovesti demokratiju u rizik - budući da političari, vlade, privreda i industrije ne mogu da odole potencijalima ovih novih alata da im pomognu u posmatranju i manipulisanju javnim mišljenjem i ponašanjem" (Dutton, 2018: 4).

Na izazove koje je donelo doba velikih podataka nadnacionalne institucije odgovaraju mnogobrojnim pravnim aktima. Podaci o ličnosti i privatnost korisnika zaštićeni su brojnim međunarodnim dokumentima:

- ***Evropska unija*** članovima 7 i 8, *Povelje Evropske unije o ljudskim pravima*[63], pravo na privatnost i pravo na zaštitu podataka o ličnosti, definiše kao temeljna ljudska prava. Do 2016. godine *Direktiva 95/46/EZ Evropskog parlamenta i Veća (1995) o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka*[64] bila je najznačajnija direktiva u ovoj oblasti. Godine 2016. *Direktiva 95/46* zamenjena je *Uredbom (EU) 2016/679 Evropskog parlamenta i Veća (2016) o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka*[65] (*General Data Protection Regulation* – GDPR). EU je maja 2018. godine izdala *Komunikaciju Komisije Evropskom parlamentu i Veću: Veća zaštita i nove prilike – Komisija daje smernice za direktnu primenu Opšte uredbe o zaštiti podataka od 25. maja 2018. godine*[66]. Ovim dokumentom Evropska komisija nalaže direktnu i nedvosmislenu primenu GDPR. Kako se navodi u ovoj *Komunikaciji*, period od dve godine, koliko je prošlo od usvajanja GDPR, bio je period predviđen za prilagođavanje i pripremu za potpuno primenu novog regulatornog okvira. Kompleksni regulatorni okvir, GDPR, na kojem je EU radila poslednjih godina, definitivno je stupio na snagu 25. maja, 2018. godine.

[63] Povelja je dostupna putem linka: http://ravnopravnost.gov.rs/wp-content/uploads/2012/11/images_files_Povelja%20Evropske%20unije%20o%20osnovnim%20pravima.pdf (pristupljeno 20. 06. 2018. godine).
[64] Direktiva je dostupna putem linka: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A31995L0046 (pristupljeno 20.06.2018. godine).
[65] Uredba je dostupna putem linka: http://esigurnost.org/wp-content/uploads/2018/01/GDPR-Uredba-2016.679.pdf (pristupljeno 20. 06. 2018. godine).
[66] Dostupno putem linka: https://ec.europa.eu/transparency/regdoc/rep/1/2018/HR/COM-2018-43-F1-HR-MAIN-PART-1.PDF (pristupljeno 20. 06. 2018. godine).

- ***Savet Evrope*** je 2013. godine usvojio Političku deklaraciju *Sloboda izražavanja i demokratija u digitalnoj eri: Mogućnosti, prava, odgovornosti*[67] na konferenciji ministara održanoj u Beogradu. Pravo na privatnost internet korisnika *Politička deklaracija* garantuje članovima 6 i 7:

> „Pravo na privatan život zaštićeno je u skladu sa članom 8 Evropske konvencije o ljudskim pravima. Zaštita ličnih podataka, koja predstavlja jednu od njegovih posledica, detaljnije je obrađena, između ostalog, u Konvenciji 108, zakonodavstvu Evropske unije i drugim relevantnim međunarodnim i nacionalnim zakonima ili principima. Zaštita ličnih podataka predstavlja pravo samo po sebi, ali i preduslov koji omogućava ostvarivanje drugih prava" (član 6).

Ukazujući na rastuću opasnost od nadzora internet korisnika i neovlašćenog prikupljanja podataka, *Političkom deklaracijom* ističe *se*:

> „Podaci mogu biti prikupljeni i obrađeni zbog legitimnog cilja, uključujući ciljeve definisane u Statutu Saveta Evrope. Svako prikupljanje podataka ili nadgledanje u cilju zaštite nacionalne bezbednosti mora biti izvršeno u skladu sa postojećim zahtevima ljudskih prava i vladavine zakona, uključujući član 8 Evropske konvencije o ljudskim pravima. Imajući u vidu rastuće tehnološke kapacitete za masovno elektronsko nadziranje i opasnosti koje iz toga proizlaze, naglašavamo da moraju postojati odgovarajuće i efikasne garancije protiv zloupotreba koje mogu ugroziti ili čak uništiti demokratiju" (član 7).

- Generalna skupština ***Ujedinjenih nacija*** 2013. godine usvojila je Rezoluciju 68/167 *Pravo na privatnost u digitalnom dobu*[68]. Rezolucijom se ističe potreba da se prepozna značaj poštovanja ljudskih prava onlajn, u istoj meri kao i oflajn. Ukazuje se na promenjeno okruženje koje zahteva nove pristupe i pozivaju se države da odgovore na nove izazove uz poštovanje ljudskih prava, sa posebnim akcentom na poštovanje privatnosti „na mreži".

***

Slično kao i kada je bilo reči o ulozi države u upravljanju internetom, uloga države u zaštiti prava njenih građana na internetu promenjena je u meri u kojoj svoje zakonodavstvo oslanja na međunarodnu regulaciju u ovoj oblasti. Ipak, značaj države nije poništen, niti je njena uloga centralnog aktera u tom procesu umanjena. Ključ uspešne realizacije zaštite ljudskih prava u onlajn-svetu pronalazimo u kooperaciji država sa drugim državama, nadnacionalnim telima i privatnim akterima. Zaštita ljudskih prava oduvek se bazirala na međunarodnoj saradnji. Internet je tom modelu upravljanja ljudskim pravima samo potvrdio značaj, jer su izazovi koje donosi preplitanje jurisdikcija država u eri globalizovanog IKS mnogo verovatniji.

---

[67] Dostupno putem linka: http://www.kultura.gov.rs/cyr/aktuelnosti/politicka-deklaracija---sloboda-izrazavanja-i-demokratija-u-digitalnoj-eri (pristupljeno 29. 01. 2018. godine).

[68] engl. *Reolution 68/167: The right to privacy in the digital age*, dostupno putem linka: https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf (pristupljeno 28. 01. 2018. godine).

Kao što je bio pokazano na primeru gotovo svih međunarodnih deklaracija pomenutih u ovom delu rada, država se jasno ističe kao lider u zaštiti građana onlajn. U isto vreme, privatni akteri, nevladine organizacije i civilni sektor uključeni su u svaki segment upravljanja. Postojanje više nivoa zaštite može se posmatrati i kao model međusobne kontrole uključenih strana. Naime, uloga država i međunarodnih organizacija ogleda se u sprečavanju zloupotreba od strane privatnih aktera; u isto vreme međunarodne organizacije, bile one vladine ili nevladine, kontrolišu države u ovom procesu.

3.5. Regulisanje prava na slobodno izražavanje i prava na privatnost (zaštita podataka) na internetu u Srbiji

Srbija, kao članica Saveta Evrope i kandidat za članstvo u EU, u obavezi je da poštuje sve prethodno navedene deklaracije i rezolucije Saveta Evrope, ali i da svoje zakonodavstvo usaglašava sa regulatornim okvirom EU, što je jedan od uslova za pristup evropskoj zajednici. Sledeća dva poglavlja imaju za cilj da odgovore na pitanje da li je i u kojoj meri zakonodavni okvir Srbije u skladu sa regulatornim okvirom EU u oblasti poštovanja prava na slobodno izražavanje i privatnost na internetu, i da se analizom regulatornog okvira utvrdi da li je sloboda izražavanja i pravo na privatnost internet korisnicima u Srbiji zaista zagarantovana.

Kroz studiju slučaja Srbije odgovoriće se na postavljeno istraživačko pitanje: **Na koji način je u Srbiji regulisana zaštita prava na privatnost i slobodu izražavanja internet korisnika?** Odnosno, analizom regulatornog okvira Srbije biće testirana prva postavljena hipoteza:

(H1) ***Regulatorni okvir Srbije, u delu koji se tiče slobode izražavanja i prava na privatnost na internetu, nije u potpunosti posvećen zaštiti građana/korisnika, već jednim delom ide u prilog intermedijatora i same države, narušavajući prava korisnika.***

Tokom analize regulatornog okvira Srbije (januar/februar 2018. godine) na snazi je bio stari Zakon o zaštiti podataka o ličnosti. Međutim, 21. novembra 2018. godine, na snagu je stupio novi Zakon o zaštiti podataka o ličnosti[69], koji će se u potpunosti primenjivati od leta 2019. godine. S obzirom na to da je analiza prvobitno obuhvatila stari Zakon, jer je u tom trenutku on bio važeći, naknadno je dodato i potpoglavlje (3.5.3.) u kojem se analizira novi Zakon i njegova usklađenost sa GDPR. Potpoglavlje (3.5.2.) u kojem je analiziran stari Zakon ostavljeno je nepromenjeno, jer nudi dobar okvir za komparaciju sa novim Zakonom.

[69]Novi ZZPL dostupan je na sajtu Poverenika: https://www.poverenik.rs/sr-yu/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B84.html (pristupljeno: 11. 01. 2019. godine).

3.5.1. Regulisanje prava na slobodno izražavanje na internetu u Srbiji

Vlada Republike Srbije 2010. godine usvojila je *Strategiju razvoja informacionog društva u Republici Srbiji do 2020. godine* (*"Sl. glasnik RS", br. 51/2010*)[70]. U *Strategiji* se posebno ističe da je razvoj informaciono-komunikacionih tehnologija pokretač razvoja mnogih drugih oblasti, od ekonomije do razvoja demokratskog društva. Takođe, kao osnovne ciljeve *Strategija* postulira pristup informaciono-komunikacionim tehnologijama bez diskriminacije, ali i ističe da je osiguravanje bezbednosti u novom okruženju ključno.

Prema podacima Svetske internet statiske[71] za 2017. godinu, pristup internetu u Srbiji ima 67,1 procenat stanovništva, što je za skoro 20 procenata manje od proseka Evropske unije (85,7 procenata). Procentualni porast upotrebe interneta u Srbiji pokazuju podaci Republičkog zavoda za statistiku[72], prema kojima je od 2010. do 2016. godine porast iznosio 25,7 procenata. *Strategijom* je predviđeno da do 2020. godine ***svim*** građanima Srbije bude omogućen pristup internetu visokog kvaliteta.

Najznačajnija zakonodavna tela kojima se u Srbiji reguliše oblast informisanja jesu: Ministarstvo kulture i informisanja, Ministarstvo trgovine, turizma i telekomunikacija i Regulatorno telo za elektronske medije. Shodno tome, najznačajniji zakoni kojima se reguliše pravo na slobodno izražavanje jesu: *Zakon o javnom informisanju i medijima, Zakon o elektronskim komunikacijama,* ali i drugi zakoni, kao što je *Krivični zakonik*[73].

Ustav Republike Srbije (*"Sl. glasnik RS", br. 98/2006*)[74] već u članu 1 ukazuje na značaj poštovanja ljudskih prava u skladu sa demokratskim načelima, ističući i značaj vladavine prava, demokratskih načela, ali i ljudskih i manjinskih prava, koja su u saglasnosti sa evropskim strandardima. U drugoj Glavi *Ustav* Srbije posebno definiše osnovna ljudska prava i slobode, Član 46 garantuje pravo na slobodu mišljenja i izražavanja, bilo da je reč o govoru, pisanoj reči ili mislima koje se prenose *na druge načine*, gde možemo prepoznati i onlajn-izražavanje, premda nije direktno istaknuto. Takođe, ističe se da sloboda izražavanja ne podrazumeva samo širenje, već i traženje i prijem informacija. Sloboda izražavanja, međutim, može biti zakonski ograničena u specifičnim situacijama, o čemu se u nastavku Člana 46 navodi: „Sloboda izražavanja može se zakonom ograničiti, ako je to neophodno radi zaštite prava i ugleda drugih, čuvanja autoriteta i nepristrasnosti suda i zaštite javnog zdravlja, morala, demokratskog društva i nacionalne bezbednosti Republike Srbije".

---

[70] Strategija je dostupna putem linka: http://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html (pristupljeno 03. 02. 2018. godine).

[71] Engl. *Internet World Stats,* dostupno putem linka: http://www.internetworldstats.com/stats9.htm (pristupljeno 03. 02. 2018. godine).

[72] Dostupno na sajtu: http://www.stat.gov.rs/WebSite/repository/documents/00/02/64/26/17-Informacione_tehnologije.pdf Republičkog zavoda za statistiku (pristupljeno 03. 02. 2018. godine).

[73] Za detaljnu analizu prava na slobodu izražavanja i njeogovo ograničavanje u Republici Srbiji pogledati: Surčulija Milojević, J. (2016). *Dozvoljenost ograničenja slobode izražavanja u skladu sa evropskim instrumentima i medijskim zakonodavstvom Republike Srbije* (Doktorska disertacija, Univerzitet u Beogradu-Pravni fakultet).

[74] Tekst Ustava Republike Srbije dostupan je putem linka: http://www.paragraf.rs/propisi/ustav_republike_srbije.html (pristupljeno 30. 01. 2018. godine).

Komunikacija na internetu podleže sankcijama ukoliko krši neku navedenu stavku iz Člana 46. Na primer, *Krivični zakonik*[75] Članom 170 predviđa da:

> „(1) Ko uvredi drugog, kazniće se novčanom kaznom od dvadeset do sto dnevnih iznosa ili novčanom kaznom od četrdeset hiljada do dvesta hiljada dinara. (2) Ako je delo iz stava 1. ovog člana učinjeno putem štampe, radija, televizije ili sličnih sredstava ili na javnom skupu, učinilac će se kazniti novčanom kaznom od osamdeset do dvestačetrdeset dnevnih iznosa ili novčanom kaznom od stopedeset hiljada do četristopedeset hiljada dinara" (*Krivični zakonik,* član 170).

Kazna se ne primenjuje:

> „ako je izlaganje dato u okviru ozbiljne kritike u naučnom, književnom ili umetničkom delu, u vršenju službene dužnosti, novinarskog poziva, političke delatnosti, u odbrani nekog prava ili zaštiti opravdanih interesa, ako se iz načina izražavanja ili iz drugih okolnosti vidi da to nije učinio u nameri omalovažavanja" (*Krivični zakonik,* član 170).

Ovaj član *Krivičnog zakonika* primenjuje se i na komunikaciju ostvarenu putem interneta, u tom slučaju se, na primer, društvene mreže tumače kao javna glasila, pa shodno tome pojedinac koji tim putem uputi pretnju ili uvredu može odgovarati pred sudom.

Poslednjih nekoliko godina česti su primeri koji ilustruju primenu ovog zakona zbog objava na društvenim mrežama. Septembra 2017. godine u Kruševcu su privedene dve osobe zbog pretnji koje su putem Fejsbuka uputile predsedniku Srbije i direktoru Bezbednosno-informativne agencije. Privedene osobe optužene su da su prekršile član 138 i 138a *Krivičnog zakonika*[76]. Član 138 odnosi se na ugrožavanje sigurnosti i ukoliko se prekršaj čini prema nosiocima javnih funkcija predviđena je kazna zatvora od šest meseci do pet godina, dok član 138a predviđa kazne za krivično delo proganjanja.

Još jedan slučaj iz 2017. godine jeste privođenje jedne osobe u Obrenovcu zbog pretnji na Tviter nalogu. Pretnja se, kako je izvestila N1[77], odnosila na fizički obračun i upućena je vladajućoj stranci u Srbiji. Jasno je da se *Krivični zakonik* primenjuje podjednako i na komunikaciju na internetu, međutim, ono što je bilo sporno u konkretnom slučaju, a o čemu je predstavnik *Share* fondacije[78] govorio za N1, jeste nezakonito oduzimanje pasvorda za Tviter i mejl nalog optuženog, kao i zaplena mobilnog telefona, jer ja za takav postupak neophodan sudski nalog, u suprotnom je reč o ugrožavanju prava na zaštitu podataka o ličnosti.

---

[75] Tekst Krivičnog zakonika (*"Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016)* dostupan je putem linka: http://www.paragraf.rs/propisi/krivicni_zakonik.html (pristupljeno 31. 01. 2018. godine).

[76] "Privedene dve žene zbog pretnji Vučiću i Gašiću na Fejsbuku". (08. septembar 2017. godine). *N1*. Dostupno na: http://rs.n1info.com/a316666/Vesti/Vesti/Privedene-dve-zenske-osobe-zbog-pretnji-Vucicu-i-Gasicu.html (pristupljeno 31. 01. 2018. godine).

[77] Maja Nikolić. (05. jun, 2017. godine). „Kad policija "hapsi" tviter, imejl i mobilni telefon". *N1*. Dostupno na: http://rs.n1info.com/a273957/Vesti/Vesti/Kad-policija-hapsi-tviter-imejl-i-mobilni-telefon.html (pristupljeno 31.01.2018. godine).

[78] *Share* fondacija je neprofitna organizacija koja se bavi zaštitom prava internet korisnika: http://www.shareconference.net/sh . (pristupljeno 31. 01. 2018. godine).

Zakon o javnom informisanju i medijima[79] u članu 3 navodi:

„Ovim zakonom uređuje se način ostvarivanja slobode javnog informisanja koja posebno obuhvata slobodu prikupljanja, objavljivanja i primanja informacija, slobodu formiranja i izražavanja ideja i mišljenja, slobodu štampanja i distribucije novina i slobodu proizvodnje, pružanja i objavljivanja audio i audio-vizuelnih medijskih usluga, slobodu širenja informacija i ideja preko interneta i drugih platformi, kao i slobodu izdavanja medija i obavljanja delatnosti javnog informisanja" (*Zakon o javnom informisanju i medijima,* član 3).

Ovaj *Zakon* pod medijima ne podrazumeva:

„platforme, poput internet foruma, društvenih mreža i drugih platformi koje omogućavaju slobodnu razmenu informacija, ideja i mišljenja njenih članova, niti bilo koja druga samostalna elektronska publikacija, poput blogova, veb-prezentacija i sličnih elektronskih prezentacija, osim ako nisu registrovane u Registru medija, u skladu sa ovim zakonom" (član 30).

U tom smislu, ovim *Zakonom* se uređuje oblast javnog informisanja pod kojim se podrazumevaju samo mediji koji su registrovani, stoga ne postoji direktna povezanost sa pravom na slobodu izražavanja i privatnosti internet korisnika, premda pojedini članovi podrazumevaju poštovanje slobodnog protoka informacija i zabranu cenzure. Međutim, ugrožavanje slobode izražavanja onlajn-medijima direktno se odnosi i na ograničavanje prava na prijem informacija bez ograničenja i na slobodu izbora izvora informacija. U tom kontekstu, ukoliko se cenzurisanjem sprečava objavljivanje informacija onlajn-medijima, dovodi se u pitanje i slobodno izražavanje pojedinca.

Zakonom o elektronskim komunikacijama[80] uređuju se: „uslovi i način za obavljanje delatnosti u oblasti elektronskih komunikacija. […] zaštita prava korisnika i pretplatnika; bezbednost i integritet elektronskih komunikacionih mreža i usluga" (član 1). Član 3 ističe ciljeve koji se, između ostalog, zasnivaju na: „obezbeđivanju mogućnosti krajnjih korisnika da, prilikom korišćenja javnih komunikacionih mreža i usluga, slobodno pristupaju i distribuiraju informacije, kao i da koriste aplikacije i usluge po svom izboru". Dakle, ovim *Zakonom* predviđa se sloboda izražavanja korisnika, u smislu pristupa i slobodnoj distribuciji informacija elektronskim putem.

Godina 2014. bila je ključna u spoznavanju mogućnosti cenzure na internetu u Srbiji, koja je u suprotnosti sa prethodno navedenim članovima zakona. Naime, u vreme poplava koje su u maju 2014. godine zahvatile gotovo celo Balkansko poluostrvo, Srbija je bila jedna od zemalja koje su pretrpele najveću štetu. Bilo je mnogo oprečnih izveštaja o šteti, ljudskim žrtvama i odgovornim licima, ali je bilo i dosta objava koje bismo danas nazvali "lažnim vestima" (*fake news*). Analizirajući stanje na terenu, predstavnica Misije OEBS za slobodu medija, Dunja Mijatović, iznela je u izveštaju zabrinutost zbog internet cenzure od strane Vlade Srbije. Kako se navodi u izveštaju, onlajn-stranice pojedinih

[79] Tekst Zakona (*"Sl. glasnik RS", br. 83/2014, 58/2015 i 12/2016 - autentično tumačenje*) dostupan je putem linka: http://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html (pristupljeno 30.01.2018. godine).

[80] Tekst Zakona (*"Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014*) dostupan je putem linka: http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html (pristupljeno 01. 02. 2018. godine).

medija bile su blokirane, uklanjani su tekstovi pojedinih autora i privedeno je više od dvadesetoro ljudi na saslušanje zbog objava na društvenim mrežama. Mijatovićeva tim povodom izjavljuje:

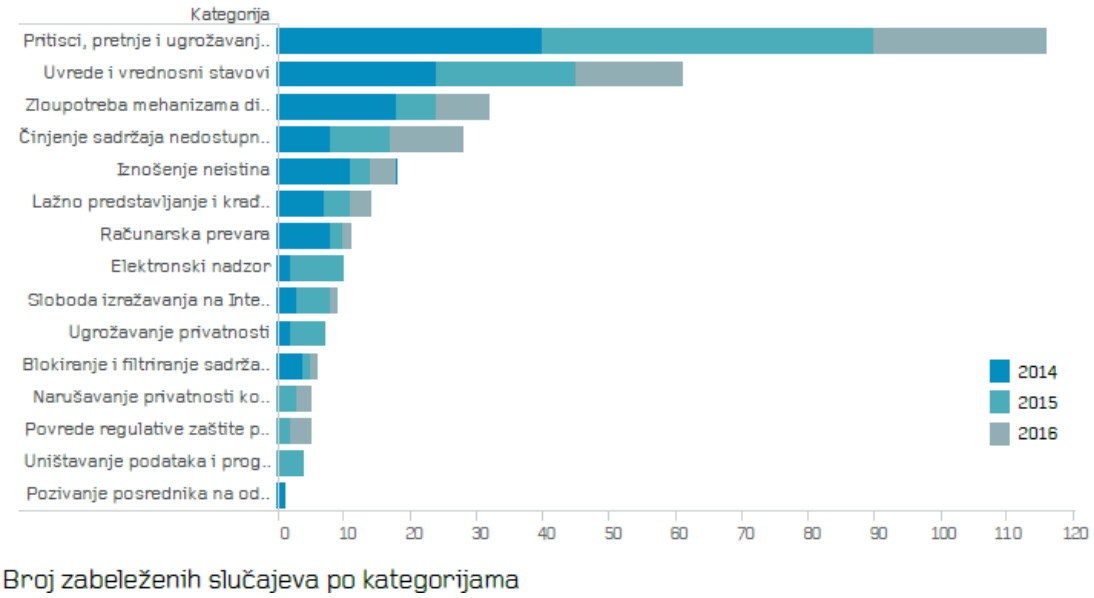
> „Duboko sam zabrinuta zbog tvrdnji da su veb stranice i onlajn sadržaj blokirani. To je jasno kršenje prava na slobodno izražavanje. Internet pruža neuporedive mogućnosti za podršku pravima i veoma je značajan za slobodan protok i pristup informacijama. U kriznim vremenima slobodan protok informacija je od vitalne važnosti kako bi ljudi mogli samostalno da procene situaciju" (Mijatović, 2014)[81].

Značajnu ulogu u zaštiti prava na slobodno izražavanje, pored Vladinih tela, imaju i nevladine organizacije. Njihova uloga ogleda se, pre svega, u monitoringu poštovanja prava i izveštajima koji ukazuju na stanje u praksi. Usvojene strategije i zakoni su slovo na papiru ukoliko njihova primena izostane ili ukoliko se selektivno primenjuju. Fondacija *Share*, kao neprofitna nevladina organizacija, bavi se analizom poštovanja ljudskih prava u onlajn-sferi. *Fondacija* objavljuje godišnje izveštaje o stanju u Srbiji, koje ilustruje reprezentativnim primerima. Poslednji izveštaj *Monitoring digitalnih prava i sloboda u Srbiji* objavili su 2016. godine[82]. Poseban deo izveštaja odnosi se na slobodu izražavanja na internetu i sa tim u vezi se u izveštaju navodi:

> „Netransparentne procedure suspenzije, brisanja pojedinih statusa i čitavih naloga na društvenim medijima, pre svega na fejsbuku i jutjubu, sve češće su u fokusu globalne javnosti. Patroliranje granicama slobode govora u onlajn sferi preuzele su gigantske korporacije, čiji ljudski i algoritamski cenzori preuzimaju ovlašćenja da uređuju javni prostor i sprovode selekciju informacija koje razmenjujemo" (2016: 21).

Kada je reč o Srbiji, autori izveštaja posebno skreću pažnju na česte suspenzije naloga na društvenim mrežama ili blokiranje stranica onlajn-medija neposredno nakon objavljivanja kritičkih stavova: „Tokom 2016. SHARE tim je registrovao petnaestak tehničkih slučajeva povreda prava u onlajn okruženju. Najmanje dva slučaja vezana su za medije (Danas, Pištaljka), na koje je napad lansiran neposredno nakon objave izveštaja vezanih za najviše državne funkcionere i njihovo neposredno okruženje" (2016: 21). Njihova analiza pokazuje da je broj tehničkih napada bio veći 2014. i 2015. godine (videti Grafikon 6), ali da to ne znači da se pitanjem bezbednosti ne bi trebalo intenzivnije baviti, naročito zato što napadi na pojedine sajtove, učinjeni prethodnih godina, još uvek nisu dobili sudski epilog.

[81] *Government online censorship in Serbia worrying trend,* says OSCE media freedom representative, (May 2014). Stockhlom. Dostupno na: http://www.osce.org/fom/119173 (pristupljeno 01. 02. 2018. godine).
[82] *Izveštaj* Fondacije *Share* dostupan je putem linka: https://labs.rs/Documents/Monitoring_digitalnih_prava_i_sloboda_izvestajza_2016_srb.pdf (pristupljeno 28. 01. 2018. godine).



Grafikon 6 Broj zabeleženih tehničkih napada po godinama, Fondacija Share, 2016: 20.

Hakerski napad na sajt *Centra za istraživačko novinarstvo Srbije* (CINS) dogodio se decembra 2013. godine, o čemu je CINS izdao zvanično saopštenje[83] u kojem objašnjava da je tom prilikom sa njihovog sajta uklonjen samo jedan tekst „Protekcije za ćerku Jorgovanke Tabaković u RFZO". Sajt *Telepromptera* hakovan je aprila 2015. godine, i kako tvrdi glavni i odgovorni urednik ovog portala, Danilo Redžepović, sajt je bio meta hakerskog napada zbog tekstova koji su kritički analizirali rad članova vladajuće stranke i njihovih simpatizera[84]. Takođe, Redžepović u autorskom tekstu navodi da je napad bio delo profesionalaca koji su imali pristup skupoj opremi i bili jako dobro organizovani. Tom prilikom obrisane su sve baze podataka *Telepromptera*. Iste godine dogodili su se i hakerski napadi na sajt Peščanika, neposredno nakon što je na sajtu objavljen tekst o analizi doktorata Ministra unutrašnjih poslova Srbije[85].

Napadi na onlajn-medije se u širem smislu mogu smatrati i napadom na slobodu izražavanja građana, u ovom slučaju internet korisnika, jer sloboda izražavanja podrazumeva i nesmetano primanje informacija, što je u ovim slučajevima bilo ili otežano ili onemogućeno. Građani su bili sprečeni da pristupe nefiltriranom ili obrisanom sadržaju određenih medija i internet stranica. Uprkos tome što su povodom ovih slučajeva pokrenuti sudski postupci, ovi sporovi do danas nisu rešeni. Takođe, činjenica da su pomenuti sajtovi bili mete napada nakon kritičkih tekstova o stranci koja je na vlasti dodatno uliva sumnju u spremnost države Srbije da se na pravi način odnosi prema slobodi izražavanja, kako onlajn-medija, tako i onlajn-korisnika.

[83] *Saopštenje Centra za istraživačko novinarstvo Srbije* dostupno je putem linka: http://www.nuns.rs/info/statements/20821/saopstenje-centra-za-istrazivacko-novinarstvo-srbije.html (pristupljeno 02. 01. 2018. godine).
[84] Danilo Redžepović. (april 2015. godine). "Kako je hakovan Teleprompter". Peščanik. Dostupno na: http://pescanik.net/kako-je-hakovan-teleprompter/ (pristupljeno 01. 02. 2018. godine).
[85] Beta. (18. jun 2015. godine). "Sajt Peščanika pod žestokim hakerskim napadima". *N1*. Dostupno na: http://rs.n1info.com/a70020/Vesti/Hakerski-napad-na-sajt-Pescanika.html (pristupljeno 02. 02. 2018. godine):

Rezultati monitoringa Fondacije *Share* pokazuju da su najčašće žrtve sajber napada:

> „Korisnici koji su smatrali da im je pristup uskraćen zbog iznošenja kritičkih stavova ili njihove uloge u društvu, kao što su novinari, odbornici u lokalnoj vlasti, akteri iz nevladinog sektora i onlajn aktivisti. Zasad ostaje nejasno u kojim se situacijama aktivira automatski servis platforme za zaključavanje naloga, 'usled neuobičajenih aktivnosti', pokušaja pristupa sa drugog uređaja ili većeg broja prijava koje upućuju politički oponenti, po raznim osnovama navodne povrede pravila korišćenja (govor mržnje, kršenje autorskih prava, i slično)" (2016: 21).

Za postupanje u ovakvim slučajevima *Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* (*Sl. glasnik RS", br. 61/2005 i 104/2009*)[86] članom 4 uspostavlja posebno odeljenje za borbu protiv visokotehnološkog kriminala pri Višem javnom tužilaštvu. Ovim *Zakonom* se pod visokotehnološkim kriminalom podrazumevaju krivična dela „kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku" (član 2). Član 3 u trećem stavu navodi i krivično gonjenje zbog kršenja „prava i sloboda čoveka i građanina", među kojima svakako prepoznajemo i pravo na slobodno izražavanje.

Predstavnici *Yucoma*, Komiteta pravnika za ljudska prava, u tekstu: „Sudska praksa o internetu u Srbiji suprotna Evropskom sudu", kao glavne probleme u oblasti poštovanja prava na slobodno izražavanje i privatnost na internetu, između ostalih, navode neusaglašenost sudskih praksi sa evropskim standardima, sudije koje nisu dovoljno upoznate sa ovom oblasti i ne prate evropske presude u sličnim situacijama i medijske zakone koji ne uključuju nove platforme i nove oblike komunikacije i informisanja (npr. društvene mreže)[87].

Yucom je 2017. godine sproveo projekat *Sloboda izražavanja i zaštita privatnosti na internetu u Srbiji*[88]. Cilj ovog projekta bila je analiza međunarodnog prava u ovoj oblasti, ali i analiza regulatornog okvira Srbije, kada je reč o dva navedena prava. Preporuke koje su rezultat njihove iscrpne analize odnose se na neophodnost pojačanog učešća pravosudnih organa kada do kršenja prava dođe, kao i na neselektivnu i blagovremenu primenu zakonskih mera, sa ciljem ostvarivanja optimalnih uslova za izgradnju poverenja u pravni lek. Svako drugačije postupanje dovodi do kršenja ne samo nacionalnih zakona već i međunarodnih dokumenata primenljivih u Srbiji. Svako izostajanje reakcije dovodi do gubitka poverenja građana u državu i njenu moć zaštite, što u krajnjem vodi do otežanog razvoja informacionog društva, kakvo *Strategija* iz 2010. godine predviđa.

[86] Tekst Zakona dostupan je putem linka: http://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html (pristupljeno 02. 02. 2018. godine).

[87] Yucom. (decembar 2017. godine). "Sudska praksa o internetu u Srbiji suprotna Evropskom sudu". Dostupno na: http://www.yucom.org.rs/sudska-praksa-o-internetu-u-srbiji-suprotna-evropskom-sudu/ (pristupljeno 02. 02. 2018. godine).

[88] Projekat je dostupan putem linka: http://www.yucom.org.rs/sloboda-izrazavanja-i-zastita-privatnosti-na-internetu-u-srbiji/ (pristupljeno 02. 02. 2018. godine).

3.5.2. Regulisanje prava na privatnost na internetu u Srbiji: Stari Zakon o zaštiti podataka o ličnosti

Zaštitita privatnosti građana na internetu zagarantovana je mnogobrojnim međunarodnim dokumentima. Već je bilo reči o deklaracijama Evropske unije, Saveta Evrope i Ujedinjenih nacija, koje sledeći trend razvoja informacionih tehnologija, posebnu pažnju posvećuju i zaštiti privatnosti internet korisnika i ličnih podataka "na mreži". Međutim, i države su obavezne da svojim građanima osiguraju informacionu bezbednost.

Republika Srbija, kao kandidat za članstvo u EU, i članica Saveta Evrope, obavezna je da poštuje međunarodne standarde u ovoj oblasti, pa da shodno njima gradi i sopstveni pravni okvir pri zaštiti privatnosti internet korisnika u Srbiji. U *Strategiji razvoja informacionog društva u Republici Srbiji do 2020. godine* državi se, kao jedan od ključnih ciljeva, postavlja odgovor na izazove, „kao što su: novi aspekti bezbednosti, ugrožavanje privatnosti, tehnološka zavisnost, nedovoljna interoperabilnost i otvorena pitanja zaštite intelektualne svojine."[89] *Strategijom* se predviđa da do 2020. godine bude formiran potpun institucionalni okvir za apsolutnu garanciju informacione bezbednosti, kako bi se građanima omogućilo sigurno informaciono okruženje, koje podrazumeva zaštitu ličnih podataka i privatnosti korisnika, a sve sa ciljem izgradnje poverenja u zakonsku zaštitu korisnika. *Ustav* Republike Srbije članom 42 garantuje zaštitu podataka o ličnosti i navodi da se podaci obrađuju samo onda kada je to zakonom predviđeno i da svako ima pravo da bude obavešten kada se o njemu prikupljaju lični podaci.

Zakon o elektronskim komunikacijama, između ostalog, uređuje i oblast elektronskih podataka, odnosno tajnost podataka korisnika, presretanje i zadržavanje podataka. Članom 126 *Zakon* ustanovljava da se sadržaj elektronske komunikacije korisnika može presretati ukoliko je to u skladu sa zakonom, na primer, ako je u vezi sa krivičnim delom, ugrožavanjem nacionalne bezbednosti i slično, uz neophodnu odluku suda za takvo postupanje. U suprotnom korisnik mora biti upoznat sa radnjom i mora da dâ pristanak. Član 127 navodi dužnosti operatora[90] kada je reč o zakonitom presretanju i zadržavanju podataka. Operator je dužan da ustupi podatke vladinim agencijama, ukoliko je lice čiji su podaci zadržani prekršilo član 126.

Međutim, Fondacija *Share* u Monitoringu za 2016. godinu navodi da se pojedinim podacima pristupalo u suprotnosti sa odredbama *Zakona o elektronskim komunikacijama*: „Tokom 2014. Telenorov IKT sistem registrovao je 201.879 samostalnih pristupa zadržanim podacima, i to: MUP 199.818, BIA 993, VBA: 1068. Naredne godine ukupno je ostvareno 300.845 samostalnih pristupa" (2016: 68). Autori Monitoringa zaključuju da pristupanje podacima korisnika bez prethodno zvanično upućenog zahteva ili pristanka korisnika sugeriše potencijalnu zloupotrebu Vladinih tela, što vodi do kršenja prava na privatnost i tajnost ličnih podataka. *Share* upozorava da prikupljanje elektronskih podataka ne podrazumeva samo sadržaj komunikacije:

[89] *Strategija* je dostupna putem linka: http://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html (pristupljeno 02. 01. 2018. godine).

[90] „*Operator* je lice koje obavlja ili je ovlašćeno da obavlja delatnost elektronskih komunikacija" (Zakon o elektronskim komunikacijama, str. 6).

„Nadzor i praćenje, kao najčešći oblici narušavanja privatnosti, u popularnim predstavama uglavnom se vezuju za prisluškivanje sadržaja komunikacije. Međutim, podaci o komunikaciji, tzv. metapodaci, otkrivaju daleko više informacija od samog razgovora. […] Pažljivim kombinovanjem velike količine metapodataka može se dobiti kompletan digitalni profil određene ličnosti: lokacija, dnevne rutine, mreža ljudi, izvori informacija, interesovanja" (2016: 91).

S obzirom na to da su operatori zakonski u obavezi da na zahtev Vlade i njenih agencija pruže ovakve informacije o svojim korisnicima, oni se ipak prema njima moraju ophoditi u skladu sa *Zakonom o zaštiti podataka ličnosti.*

Zakon o zaštiti podataka o ličnosti (*"Sl. glasnik RS", br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012*)[91] ima za cilja da „u vezi sa obradom podataka o ličnosti, svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda" (član 2). *Zakon* je pretrpeo mnogobrojne kritike stručne javnosti. Poverenik za informacije od javnog značaja u izveštaju za 2016. godinu navodi sledeće: „Brojni ekscesi odnosno povrede prava na zaštitu podataka o ličnosti, neki i izuzetno krupnih dimenzija ili značaja, imperativno zahtevaju da se odnos države i društva u celosti prema zaštiti podataka o ličnosti, odnosno privatnosti uopšte, potpuno, iz korena promeni," i obrazlaže:

„Unutrašnji pravni okvir u oblasti zaštite podataka o ličnosti u Srbiji je krajnje neodgovarajući i time krajnje nefunkcionalan. Razloga tome je više. Kao prvo, brojne odredbe Zakona o zaštiti podataka o ličnosti (dalje u tekstu: ZZPL) su neodgovarajuće, odnosno nepotpune, a pojedina pitanja uopšte nisu ni uređena ZZPL, kao što na sistemski način nisu uređena ni drugim, posebnim zakonima" (Izveštaj Poverenika, 2016: 6, 23)[92].

U delu *Izveštaja* u kojem se navode pojedini primeri kršenja *Zakona*, Poverenik, kao vrlo čest prekršaj, navodi zadržavanje podataka o elektronskoj komunikaciji i posebno naglašava da se povodom nezakonitog zadržavanja i presretanja elektronskih podataka korisnika više puta obraćao državnim organima, ali da državni organi ne reaguju na prijave Poverenika. Poverenik u *Izveštaju* upozorava da se takvim praksama krši, pre svega, *Ustav* Srbije i da svakako nije u skladu ni sa nacionalnim zakonskim okvirom, ni sa evropskim standardima u ovoj oblasti, te zaključuje da neadekvatna usklađenost ZZPL sa evropskim standardima ali i izostanak primene *Zakona* u praksi dovode do nepoverenja građana i do narušavanja njihovog prava na privatnost.

Takođe, Fondacija *Share* za zaštitu digitalnih prava uputila je kritiku na račun ZZPL, zbog odugovlačenja pri usvajanju novog zakona, o čemu je pisao i CINS[93], ali i zbog neusklađenosti sa evropskim standardima. Naime, Evropski parlament i Savet Evrope su 27. aprila 2016. godine usvojili

[91] Tekst Zakona dostupan je putem linka: http://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html (pristupljeno 02.02.2018. godine).
[92] Izveštaj Poverenika za 2016. godinu dostupan je putem linka: https://www.poverenik.rs/sr-yu/izvetaji-poverenika.html (pristupljeno 02. 02. 2018. godine).
[93] CINS u tekstu „Neobaveštena ministarka: Da li je gotov nacrt zakona o zaštiti podataka o ličnosti?", novembar 2017. godine, navodi: „Protivrečne izjave nadležnih o fazi izrade nacrta, netransparentnost u radu i nedovoljna komunikacija sa zainteresovanom javnošću, kao i tretiranje pitanja privatnosti građana i zaštite njihovih ličnih podataka iz perspektive interesa bezbednosnih službi, stvaraju atmosferu nepoverenja i zabrinutosti". Tekst je dostupan putem linka: https://www.cins.rs/news/srpski/article/neobavestena-ministarka-da-li-je-gotov-nacrt-zakona-o-zastiti-podataka-o-licnosti (pristupljeno 03. 02. 2018. godine).

Opštu uredbu o zaštiti podataka o ličnosti (*Regulation (EU) 2016/679*)[94], koja stupa na snagu u maju 2018. godine. Ova *Uredba* najintenzivnije do sada štiti pravo na privatnost i lične podatke korisnika. Srbija u skladu sa pregovorima za članstvo u EU, a kako je predviđeno Poglavljem 23[95], mora da uskladi ZZPL sa evropskim okvirom, što se do danas nije desilo.

O tome kako ZZPL funkcioniše u praksi govore i mnogobrojni primeri poslednjih godina. Marta 2017. godine "procureli" su lični podaci 400.000 ljudi u Srbiji. Kako je izvestio N1: „JMBG, broj lične karte, adresa, kućni i mobilni telefon tih ljudi našli su se na jednom javnom serveru. Uz podatke na pojedinim mestima stoje i napomene koje ukazuju na to da su podaci korišćeni u stranačke svrhe"[96]. Poverenik je o ovom slučaju rekao da je učinjen ogroman broj krivičnih dela, ali da njegova kancelarija nema ovlašćenje niti resurse da se ovim propustom bavi[97].

Međutim, ovo nije prvi slučaj otkrivanja ličnih podataka velikog broja građana Srbije. CINS je 2017. godine podsetio na slučaj o javno dostupnim matičnim brojevima preko pet miliona građana Srbije tokom 2014. godine na sajtu Agencije za privatizaciju[98]. Poverenik je povodom ovog slučaja podneo krivične prijave, međutim do sudskog epiloga nije došlo, jer je slučaj zastareo.

Izgradnja institucionalnog okvira za informacionu bezbednost, koja podrazumeva i zaštitu ličnih podataka "na mreži" i privatnosti uopšte, zahteva uključivanje stručne javnosti, predstavnika industrije i civilnog sektora, kako je istaknuto i u *Strategiji za razvoj informacionog društva u Republici Srbiji do 2020. godine*. Preporuke da nevladina tela imaju podjednaku ulogu u rešavanju gorućih problema zaštite prava na internetu deo su svih nacionalnih i nadnacionalnih obavezujućih dokumenata. Međutim, Srbija je bez javne rasprave[99] u maju 2017. godine usvojila *Strategiju razvoja informacione bezbednosti za period od 2017. do 2020. godine*[100].

Prilikom analize regulatornog okvira Srbije kojim se garantuje u širem smislu informaciona bezbednost, a u užem zaštita privatnosti internet korisnika, koja podrazumeva i zaštitu ličnih podataka, uočeno je dosta negativnih trendova. Neusaglašenost novih zakonskih okvira sa evropskim

---

[94] engl. *General Data Protection Regulation,* dostupno putem linka: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 (pristupljeno 02. 02. 2018. godine).

[95] Pregovaračka poglavlja 23 i 24 – O čemu pregovaramo?, dostupno putem linka: https://www.mpravde.gov.rs/tekst/7029/vodic-za-novinare-poglavlja-23-i-24-o-cemu-pregovaramo.php (pristupljeno 03. 02. 2018. godine).

[96] Primer podataka objavljenih na javnom severu: „6209: Do sada glasao za DS. Neće više. Invalid. Deca 20 i 22 godine. Nezaposlena, žena radi u kafani za 11.000. On invalid iz Bosne. 34142: Veliki protivnik ove vlasti. Ne kontaktirati". „Šta stranke znaju o vama: Nađena baza podataka 400.000 ljudi", *N1*, mart 2017. godine. Tekst dostupan putem linka: http://rs.n1info.com/a237644/Vesti/Vesti/Sta-stranke-znaju-o-vama-Procurili-podaci-400.000-gradjana.html (pristupljeno 03. 02. 2018. godine).

[97] Miodrag Sovilj. (25. mart 2017. godine). „Šabić o iscurelim podacima: Ogroman broj krivičnih dela", *N1* Dostupno na: http://rs.n1info.com/a237666/Vesti/Vesti/Sabic-o-iscurelim-podacima-Ogroman-broj-krivicnih-dela.html (pristupljeno 02. 02. 2018. godine).

[98] Anđela Milivojević, Milica Stojanović. (28. jun 2017. godine). „Privatnost građana godinama na izvolite". *CINS.* Dostupno na: https://www.cins.rs/privatnost-gradjana-godinama-na-izvolite/ (pristupljeno 02. 02. 2018. godine).

[99] Fondacija *Share*. (maj 2017. godine). „Strategija informacione bezbednosti usvojena bez javne rasprave". Dostupno na: http://www.shareconference.net/sh/vesti/strategija-informacione-bezbednosti-usvojena-bez-javne-rasprave (pristupljeno 04. 02. 2018. godine).

[100] Tekst Strategije dostupan je putem linka: http://www.srbija.gov.rs/vesti/dokumenti_sekcija.php?id=45678 (pristupljeno 04. 02. 2018. godine).

preporukama i standardima jedan je od negativnih primera u radu Vlade na osiguravanju onlajn-okruženja, koje bi za cilj trebalo da ima zaštitu privatnosti i ličnih podataka internet korisnika. Naime, iako se u Evropi usvajaju deklaracije i preporuke koje intenzivnije uređuju ovu oblast, Srbija nedosledno prati preporuke, i, dok strategijama i akcionim planovima najavljuje značajno poboljšanje zakonskog okvira, u praksi se sa donošenjem zakona kasni. Upravo je odlaganje datuma donošenja zakona iz ove oblasti, pored neusaglašenosti, drugi uočeni negativni trend. Naveden je primer *Zakona o zaštiti podataka o ličnosti*, koji kada je poslednji put usvojen, pre skoro deset godina, nije mogao da predvidi brz razvoj informaciono-komunikacionih tehnologija, stoga nije primenljiv na okruženje koje se drastično promenilo u protekloj deceniji. Usvajanje novog *Zakona* najavljuje se poslednjih nekoliko godina, Poverenik je dostavljao predlog *Zakona*, ali niko iz resornog ministarstva još uvek nije dao precizan odgovor javnosti kada će *Zakon* konačno biti donesen.

Sledeća kritika upućena je zbog izostanka javnih rasprava i nedovoljnog uključivanja nevladinih organizacija, civilnog sektora i stručne javnosti pri donošenju strategija i zakona. Nespremnost Vlade Srbije da u izradu strategija uključi i civilni sektor, govori o nepoštovanju standarda koje je Vlada donela u prethodnim strategijama. Takođe, ovakvim odnosom prema civilnom sektoru Vlada direktno krši međunarodne preporuke, u kojima je jasno istaknuto da civilni sektor i industrija moraju biti sastavni deo izgradnje boljeg informacionog okruženja, pri čemu je uloga države i dalje centralna, ali svakako ne i dovoljna da samostalno ponudi najbolja rešenja za krajnje korisnike. Sve ovo govori o odsustvu volje Vlade Srbije da se pitanjima informacione bezbednosti bavi shodno propisima EU, i na kraju u interesu svojih građana, internet korisnika.

Poslednji negativni trend odnosi se na nerešene sudske sporove iz ove oblasti. Kada krivična dela koja se odnose na „curenje“ ličnih podataka pet miliona građana, ili objavljivanje baze podataka građana u stranačke svrhe, ne podležu sankciji, odugovlače se do zastarivanja slučaja, a dopisi Poverenika ostaju samo slovo na papiru, onda sve to ukazuje na nezainteresovanost države Srbije za aktuelna pitanja informacione bezbednosti.

Ukoliko se nastave ovi negativni trendovi, Srbija neće ostvariti cilj koji je postavila *Strategijom za razvoj informacionog društva*, te neće ni omogućiti svojim građanima apsolutnu informacionu bezbednost do 2020. godine. Kako su najznačajniji zakoni u oblasti zaštitite privatnosti na internetu, *Zakon o elektronskoj komunikaciji*, *Zakon o informacionoj bezbednosti* i *Zakon o zaštiti podataka o ličnosti*, a sva tri su pretrpela kritike nevladinog sektora, zbog već navedenih razloga, moglo bi se zaključiti da Srbija nije napredovala u zaštiti ovog prava, pa građani Srbije, kao internet korisnici, nisu bezbedni u onlajn-prostoru.

3.5.3. Regulisanje prava na privatnost na internetu u Srbiji: Novi Zakon o zaštiti podataka o ličnosti

Dugo najavljivan novi Zakon o zaštiti podataka o ličnosti, usvojen 9. novembra 2018. godine, stupio je na snagu 21. novembra 2018. godine, a u potpunosti će se primenjivati od leta 2019. godine. Naime, Srbija se, kao kandidat za članstvo u EU, Akcionim planom za poglavlje 23[101] obavezala da će zaštitu podataka o ličnosti uskladiti sa evropskom regulativom. Novi ZZPL bi u tom kontekstu trebalo da bude usklađen sa evropskim standardima u ovoj oblasti, tačnije da bude u skladu sa GDPR. S obzirom na to da će se novi ZZPL u potpunosti primenjivati od leta 2019. godine, te da se u ovom trenutku ne može sa sigurnošću govoriti o njegovoj efikasnosti i praktičnoj primeni, kako je to bio slučaj pri analizi starog Zakona, cilj ovog potpoglavlja je da novi Zakon sagleda u kontekstu evropskih standarda i regulacije, kao i da ukaže na najčešće kritike stručne javnosti.

Novi ZZPL predstavlja gotovo preslikan GDPR. Njime se proširuju prava građana u oblastima koje starim ZZPL nisu bile regulisane. Kao što to propisuje i GDPR i ZZPL iz 2018. godine uključuje ograničenje obrade podataka, transparentnost u pogledu deljanja ličnih podataka sa trećim licima, afirmativni i nedvosmisleni pristanak lica čiji se podaci obrađuju itd. Međutim, ono što dodatno komplikuje već složene odredbe Zakona jeste činjenica da je novi ZZPL zapravo integrisana verzija GDPR i policijske Direktive EU (2016/680)[102], kojom se uređuje zaštita obrade podataka o ličnosti od strane nadležnih tela za sprečavanje krivičnih dela.

Evropska komisija je još pre usvajanja Zakona dala Komentar[103] na nacrt Zakona, kojim je ukazala na propuste, posebno na komplikovanu strukturu nacrta, zbog konstantnog mešanja tzv. policijske Direktive (2016/680) i odredbi GDPR. U tom kontekstu u Komentaru se ističe: „Zaštita podataka je fundamentalno pravo u Evropskoj uniji, posebnu pažnju bi trebalo posvetiti tome da zakon svojom jasnoćom omogući građanima brojna važna prava. Čini se da to nije slučaj u ovom nacrtu" (Komentar EK)[104]. Komisija predlaže da se ova dva segmenta, policijska Direktiva i GDPR, odvoje, odnosno da se Nacrt odnosi samo na GDPR i prava građana. Međutim, to se nije desilo. Novousvojeni Zakon u sebe uključuje i policijsku Direktivu EU.

Propusti, koji se u Komentaru EK navode, odnose se i na neadekvatnu *strukturu*, *nerazumljivost*, koja vodi *nečitljivosti* teksta nacrta, pogrešnu interpretaciju *suštine pojedinih odredbi*, *nedostatak informacija o instituciji Poverenika*, neophodnih za procenu nacrta Zakona. Nakon upućenih komentara i smernica, Zakon je minimalno izmenjen u skladu sa njima, ali suštinski problemi ostali su nepromenjeni: nečitljivost, nerazumljivost, nejasno istaknuta prava građana itd.

---

[101] Akcioni plan dostupan je putem linka: https://www.mpravde.gov.rs/files/Akcioni%20plan%20PG%2023%20Treci%20nacrt-%20Konacna%20verzija1.pdf (pristupljeno: 11. 01. 2019. godine)

[102] DIREKTIVA (EU) 2016/680 EVROPSKOG PARLAMENTA I VEĆA od 27. aprila 2016. o zaštiti pojedinaca u vezi sa obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili progona krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka o stavljanju izvan snage Okvirne odluke Veća 2008/977/PUP. Dostupno putem linka: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L0680&from=EN (pristupljeno: 11. 01. 2019. godine).

[103] Komentar Evropske komisije na Nacrt Zakona o zaštiti podataka o ličnosti dostupan putem linka: http://www.partners-serbia.org/komentari-evropske-komisije-o-nacrtu-zakona-o-zastiti-podataka-o-licnosti-konacno-dostupni-javnosti/ (pristupljeno: 11. 01. 2019. godine).

[104] Ibid.

Kao primer nejasnih konstrukcija, odnosno kako to EK opisuje – *veoma zakomplikovanih odredbi*, u Komentaru se navodi član 40, često kritikovan i od strane domaće stručne javnosti. Naime, Poverenik Rodoljub Šabić i Fondacija *Share* smatraju da je ovaj član, koji se odnosi na ograničenje zaštite prava, protivustavan[105]. Nevladine organizacije ukazale su na to da je član 40 izmenjen nakon javne rasprave, pa je 41 organizacija civilnog društva podnela amandman na član 40[106]. Amandmanom[107] se ukazuje na nejasne konstrukcije, koje ostavljaju prostor za različite interpretacije, a samim tim i različitu primenu. Na primer, u članu 40 navodi se da se prethodnim članovima garantovana prava građana „mogu ograničiti ako ta ograničenja ne zadiru u suštinu osnovnih prava i sloboda" (ZZPL, član 40, stav 1) dok se Amandmanom dodaje da se ta prava „mogu ograničiti **zakonom**". Dalje, Amandman menja i stav 2 člana 40, i konstrukciju „prilikom primene ograničenja" menja „zakonskim odredbama kojima se ograničavaju", i „ prema potrebi" menja konstrukcijom „kada je to od značaja"[108].

Dakle, organizacije civilnog sektora koje su podnele amandman insistirale su na jasnim jezičkim konstrukcijama kojima bi se nedvosmisleno istaklo da je ograničavanje prava propisanih Zakonom moguće samo u zakonskim okvirima. Evropska komisija je u pomenutom Komentaru na nacrt Zakona, takođe, imala slične primedbe i ukazala na to da pojmovi "legitimni interes" i "interes na osnovu zakona" nisu sinonimi, kako se u Nacrtu Zakona koriste (Komentar EK)[109]. Takođe, Poverenik je mesec dana pre stupanja na snagu novog Zakona uputio pismo Narodnoj skupštini, kojim ukazuje na ovaj propust i navodi:

> „Upozoravam narodne poslanike da ovakvo rešenje vodi drastičnom urušavanju pravnog sistema, u potpunoj je suprotnosti sa Ustavom, zakonom i međunarodnim dokumentima i konvencijama i ozbiljno narušava princip vladavine prava. Gotovo je izlišno ukazivati na to da je ovakvo rešenje u potpunom nesaglasju sa duhom demokratskog društva, te da su štetne posledice po osnovna prava i slobode građana nesagledive" (Pismo Poverenika Narodnoj skupštini, 22.10.2018. godine)[110].

Međutim, Skupština nije uvažila pismo Poverenika, ni Amandman civilnih organizacija nije usvojen u Parlamentu. S obzirom na to da nisu usvojene izmene predložene Amandmanom, ostavlja se prostor za subjektivne interpretacije ograničavanja prava propisanih Zakonom, što u krajnjem može voditi i njegovoj zloupotrebi, pre svega, od strane rukovalaca i obrađivača podataka o ličnosti.

---

[105] Insajder. (09. novembar 2018. godine). „Zakon o zaštiti podataka o ličnosti usvojen bez predloženih korekcija". Dostupno na: https://insajder.net/sr/sajt/vazno/12512/ (pristupljeno: 11. 01. 2019. godine).
[106] Fondacija *Share*. (15. novembar 2018. godine). „Usvojen Zakon o zaštiti podataka o ličnosti". Dostupno na: https://www.sharefoundation.info/sr/usvojen-zakon-o-zastiti-podataka-o-licnosti/ (pristupljeno: 11. 01. 2019. godine).
[107] Tekst Amandmana civilnog sektora na član 40. Zakona o zaštiti podataka o ličnosti dostupan je na sajtu: https://www.sharefoundation.info/wp-content/uploads/Predlog-amandmana-na-ZZPL-Partneri-Srbija-i-Share-fondacija.pdf (pristupljeno: 11. 01. 2019. godine).
[108] Ibid.
[109] Komentar Evropske komisije na Nacrt Zakona o zaštiti podataka o ličnosti dostupan je putem linka: http://www.partners-serbia.org/komentari-evropske-komisije-o-nacrtu-zakona-o-zastiti-podataka-o-licnosti-konacno-dostupni-javnosti/ (pristupljeno: 11. 01. 2019. godine).
[110] Pismo Povrenika Šabića Narodnoj skupštini Republike Srbije povodom člana 40 Zakona o zaštiti podataka o ličnosti dostupno je putem linka: https://www.poverenik.rs/images/stories/dokumentacija-nova/pismaorganima/pismoposlanicimaZZPLCL40.pdf (pristupljeno 11. 01. 2019. godine).

O tome šta konkretno može da se desi ukoliko se u ZZPL ne vrati reč „zakon", koja je bila deo starog ZZPL, govorili su Poverenik Rodoljub Šabić i Danilo Krivokapić iz Fondacije *Share*, mesec dana pre stupanja na snagu novog Zakona: „Izbačena je jedna reč na dva mesta, koja se zove – zakon, to znači da ono što je zakonom osigurano da ta ograničenja podrazumevaju, da se neće više utvrđivati zakonom nego – nekako, a nije najjasnije ni ko će to raditi. Ko je tu reč obrisao. Ko personalno?" (Šabić za *N1*)[111]. Krivokapić dodaje da podatke građana na taj način lako mogu da zloupotrebe države i njene agencije, ali i velike privatne kompanije koje poslovanje zasnivaju na podacima, te da novi predlog Zakona obesmišljava svoj naziv, jer upravo čini suprotno (Krivokapić za *N1*)[112].

Čini se da su sve pozitivne odredbe koje uvodi novi ZZPL dovedene u pitanje prospustom u samo jednom članu – članu 40. Ukoliko se prava građana, garantovana ovim Zakonom, mogu ograničavati prizvoljno, to ostavlja prostor za zloupotrebu podataka o ličnosti, kako od strane države i njenih agencija, tako i od strane privatnih kompanija.

***

Država – centralna tema ovog poglavlja – i dalje ima značajnu ulogu u upravljanju IKS, koliko god on bio globalizovan. Država ima pravne mogućnosti da kontroliše svoj nacionalni internet prostor, premda, ukoliko pretenduje da bude deo demokratskog poretka, ne bi smela da tu svoju moć zloupotrebi. Međutim, ostaje činjenica da je internetom nemoguće upravljati bez saradnje država sa međunarodnom zajednicom, privatnim akterima i civilnim sektorom.

Pravo na privatnost i sloboda izražavanja na internetu, predmet istraživanja ovog poglavlja, garantovana su brojnim međunarodnim dokumentima, ali ih garantuju i države svojim regulatornim okvirima. Cilj analize regulatornog okvira Republike Srbije bio je da se da odgovor na postavljeno istraživačko pitanje: *Na koji način je u Srbiji regulisana zaštita prava na privatnost i slobodu izražavanja internet korisnika?*. U skladu sa tim, prvom hipotezom se pretpostavilo da regulatorni okvir Srbije nije u potpunosti posvećen zaštiti internet korisnika, kada je reč o pravu na privatnost i slobodnom izražavanju onlajn, već da delom narušava prava korisnika u Srbiji, te da svojim nejasnim i neodređenim odredbama ide u prilog državi i internet intermedijatorima.

Na osnovu sprovedenog istraživanja i dobijenih rezultata, možemo zaključiti da je prva hipoteza potvrđena. Sumirano, trendovi uočeni analizom su sledeći:

a) Trendovi u oblasti zaštite prava na slobodno izražavanje na internetu u Srbiji:

- Negativna praksa isključivanja civilnog sektora i stručne javnosti iz javnih rasprava o strategijama i zakonima u ovoj oblasti.

- Negativna praksa kreatora zakona da ignorišu preporuke i smernice civilnog sektora.

[111] *N1*. (21. oktobar 2018. godine). „Iz novog zakona obrisana reč zakon, svi građani u opasnosti". Dostupno na: http://rs.n1info.com/Vesti/a429536/Sabic-i-Krivokapic-o-Predlogu-zakona-o-zastiti-podataka.html (pristupljeno 11. 01. 2019. godine).
[112] Ibid.

- Negativna praksa hapšenja građana koji su na društvenim mrežama iskazivali svoj politički stav.

- Negativna praksa hakerskih napada na onlajn-medije, nakon što su objavili tekstove koji kritikuju Vladu Republike Srbije ili neke njene članove.

b) Trendovi u oblasti zaštite prava na privatnost na internetu u Srbiji:

- Pozitivna praksa pokušaja usklađivanja zakona sa EU regulativom, usvajanjem novog Zakona o zaštiti podataka o ličnosti, čime se znatno proširuju prava građana u ovoj oblasti.

- Kritike upućene na račun novog ZZPL odnose se na pokušaj države da neustavnom odredbom člana 40 ograniči građanima pravo na zaštitu podataka o ličnosti, kompleksan i nerazumljiv jezik, nejasnu strukturu itd. O efikasnosti novog ZZPL govoriće se tek narednih godina, nakon njegove potpune primene – ipak, aktuelne kritike govore u prilog neizvesnoj budućnosti zaštite ovog prava.

- Negativna praksa izmene delova nacrta Zakona o zaštiti podataka o ličnosti nakon javne rasprave u kojoj su učestvovale civilne organizacije.

- Negativna praksa ignorisanja preporuka i smernica Evropske komisije, civilnog sektora, Poverenika i stručne javnosti od strane kreatora zakona i poslanika.

- Negativna praksa odugovlačenja sudskih sporova, sa tendencijom zastarevanja slučajeva, na koje je više puta ukazivao Poverenik Rodoljub Šabić.

- Negativna praksa nereagovanja tužilaštva na prijavljene slučajeve masovnih kršenja prava na zaštitu podataka o ličnosti, o kojima je Poverenik izvestio tužilaštvo i podneo zvanične izveštaje.

- Negativna praksa neovlašćenog nadzora internet komunikacije građana od strane države i njenih agencija, što je Fondacija *Share* potvrdila monitoringom.

Uzevši u obzir uglavnom negativne trendove u oblasti zaštite dva prava koja su bila predmet analize, jasno je da se internet korisnici u Srbiji ne mogu osloniti na zaštitu koju bi trebalo da im pruža zakonski okvir Republike Srbije. U kojoj meri internet korisnici mogu da se oslone na privatne aktere i koliko su zaista svesni opasnosti po navedena dva prava na internetu, teme su sledećih poglavlja.

4. Politike odgovornosti internet intermedijatora

Jedni od najznačajnijih aktera u globalizovanom IKS jesu internet intermedijatori. Pod njima podrazumevamo privatne kompanije koje posluju na internetu i predstavljaju sponu – *intermedijatore* – između korisnika i internet usluga. Usluge koje ove kompanije pružaju mogu biti raznovrsne, od internet konekcije preko onlajn-plaćanja do posredovanja u internet komunikaciji. Predmet istraživanja u ovom radu jesu intermedijatori koji su u direktnoj i najočiglednijoj vezi sa internet korisnicima – **pretraživači** i **društvene mreže**.

U ovom poglavlju definisaćemo internet intermedijatore, odredićemo im mesto u globalizovanom IKS i analizirati njihove uloge i značaj. Posebno ćemo analizirati njihovu ulogu nemedijskih aktera – koji obavljaju funkcije nalik medijskim, te njihovu ulogu „vratara" u komunikaciji posredovanoj internetom.

Iako ćemo se prema njima odnositi kao prema privatnim kompanijama čiji je osnovni cilj sticanje profita i isplativost poslovanja, nastojaćemo da ukažemo na značaj ostvarivanja javnog interesa „na mreži", naročito zbog njihove dominantne uloge u globalizovanom IKS. Njihova odgovornost ne može se sagledavati samo kroz logiku tehno-kompanija, kako se internet intermedijatori najčešće samoreprezentuju. Njihova značajna uloga posrednika u internet komunikaciji nalaže i društveno odgovorno poslovanje i rad u interesu korisnika.

Prava internet korisnika garantuju međunarodni i nacionalni zakonodavni okviri, ali i samoregulatorni mehanizmi internet intermedijatora. Shodno uslovima korišćenja njihovih usluga korisnicima se predočavaju obaveze, ali i garantuju prava. Pravo na slobodno izražavanje na internetu zagarantovano je brojnim pravnim aktima, ali ga i intermedijatori garantuju svojom samoregulatornom politikom. Pravo na privatnost takođe je posebno tretirano pravo uslovima korišćenja intermedijatora, prvenstveno zbog nesagledive količine ličnih podataka koje korisnici dele korišćenjem internet usluga.

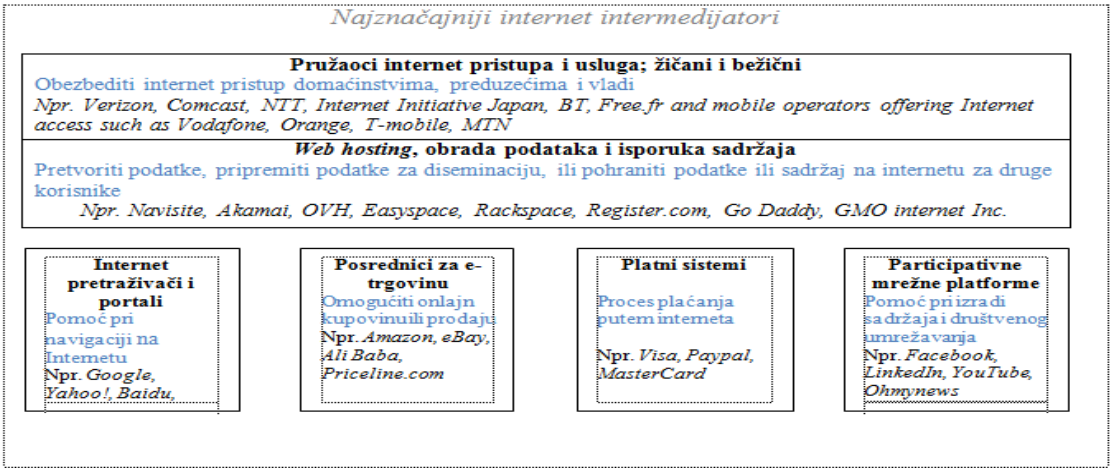
Nakon teorijskih određenja ključnih koncepata u ovom poglavlju: *internet intermedijatora* – pretraživača i društvenih mreža i *samoregulatornih mehanizama*, u drugom delu poglavlja analiziraćemo samoregulatorne mehanizame internet intermedijatora u oblasti poštovanja prava korisnika. Tačnije, analiziraćemo uslove korišćenja Gugla i Fejsbuka u oblasti poštovanja prava na slobodno izražavanje i prava na privatnost njihovih korisnika.

4.1. Novi akteri u globalizovanom informaciono-komunikacionom sistemu

Novo okruženje dovodi do promene u preraspodeli kontrole i moći. Moć se sa država pomera na međunarodne organizacije, kontrola se iz javnog preliva i u privatni sektor. Internet, koji je u svom nastajanju težio da poništi državnu jurisdikciju, u čemu je nakratko i uspevao, postao je prostor čija se kontrola sve intenzivnije uključuje u državne i međunarodne zakone. Međutim, država, iako i dalje ima centralnu ulogu, regulatorne aktivnosti na internetu sprovodi u kooperaciji sa privatnim akterima.

Privatni akteri, oličeni u privatnim kompanijama koje posluju na internetu, nisu novina u onlajn-prostoru. Svaka aktivnost na internetu oduvek je za posrednike imala privatne aktere, koji na više nivoa (infrasturkturno, arhitektonski, sadržinski) uređuju virtuelna krstarenja korisnika. Međutim, sa rastućim izazovima potencijalno štetnih aktivnosti (pornografija, govor mržnje, kršenje autorskih prava, nepoštovanje ljudskih prava) privatni akteri dobijaju na značaju, posebno oni koje s pravom možemo okarakterisati kao onlajn-imperije, stecišta moći.

Upravo na njih misli Martin Mur (Martin Moore, 2017) kada kaže: „Društvo će biti definisano načinom na koji se odnosimo prema tehnološkim gigantima"[113]. Pod tehnološkim gigantima podrazumevamo privatne kompanije koje obuhvataju raznolike internet intermedijatore. Tomas Koter (Thomas Cotter) definiše intermedijatore kao „bilo koji subjekt koji omogućava prenos informacija od jedne do druge strane", odnosno bilo koji „pružilac komunikacijskih usluga" (2005: 2). Shodno svom mestu u informaciono-komunikacionom sistemu, internet intermedijatori imaju različite uloge: od omogućavanja pristupa internetu, preko diseminacije podataka, do onlajn-navigacije, plaćanja i umrežavanja (videti Grafikon 7).



Grafikon 7 Stilizovana reprezentacija uloga internet intermedijatora (Perest, 2010: 9).[114]

[113] Martin Moore. (2 April 2017)."Society will be defined by how we deal with tech giants". *The Guardian*. Dostupno na: https://www.theguardian.com/commentisfree/2017/apr/01/brexit-britain-respond-tech-giants-civic-role-googleapple-facebook-amazon-eu (pristupljeno, 14. 02. 2018. godine).

[114] Karin Perset (Karine Perset, 2010) analizirajući društvenu i ekonomsku ulogu internet intermedijatora, sagledava prve dve grupe intermedijatora (internet servis provajdere i *web* hosting), kao upućene na treća lica, dok poslednju grupu (pretraživači, posrednici e-trgovine, platni sistemi i društvene mreže) definiše u okvirima korisnika ili potrošača sadržaja, proizvoda i usluga.

Karin Perset (Karine Perset, 2010) u Izveštaju za OECD (*Organisation for Economic Co-operation and Development*), kao što je prikazano u Grafikonu 7, deli intermedijatore na tri velike grupe: internet servis provajdere koji obezbeđuju pristup internetu, privatne kompanije koje pružaju usluge obrade i isporuke podataka i intermedijatore koji su u direktnom kontaktu sa krajnjim korisnicima, pružajući im usluge pretraživanja, kupovine, plaćanja i participacije. Fokus ovog istraživanja jesu intermedijatori koji su u najneposrednijoj vezi sa korisnicima, pretraživači i društvene mreže, odnosno **Gugl** i **Fejsbuk**.

Iako je prva pomisao na ove gigante njihova ekonomska pozicija i moć, ono što intrigira istraživače humaniste pre svega je njihova društvena uloga, koja je delom neodvojiva od ekonomske, ali svakako manje primetna od miliona dolara, koliko takve kompanije zarađuju. Mur ističe da pitanje odnosa prema tehnološkim gigantima nije samo ekonomsko, jer oni oblikuju naš svakodnevni život, stoga imaju i značajnu građansku ulogu (Moore, 2016, 2017).

Na prvi pogled, mogli bismo da pretpostavimo da su ove kompanije tehnološke, da njima upravljaju algoritmi i da ih stoga možemo okarakterisati kao neutralne platforme za prenošenje sadržaja. Međutim, bolji uvid u njihov način rada razbija iluziju o njihovoj neutralnosti i ukazuje na novi vid konstruisanja društveno-političke zbilje kroz „algoritamsko upravljanje javnim interesom" (Napoli, 2015: 757). Gudman i Povels (Goodman & Powles, 2016) poentiraju iskazom o Guglu i Fejsbuku: „Zovemo ih platformama, mrežama ili vratarima. Ali ove etikete jedva da im odgovaraju. […] Postali su nešto mnogo značajnije. Postali su medijum kroz koji doživljavamo i razumemo svet"[115]. Da bismo mogli da govorimo o ulozi i uticaju koji pretraživači i društvene mreže, kao novi akteri, imaju u informacionom ekosistemu, moramo najpre da se upoznamo sa načinom rada ovih intermedijatora.

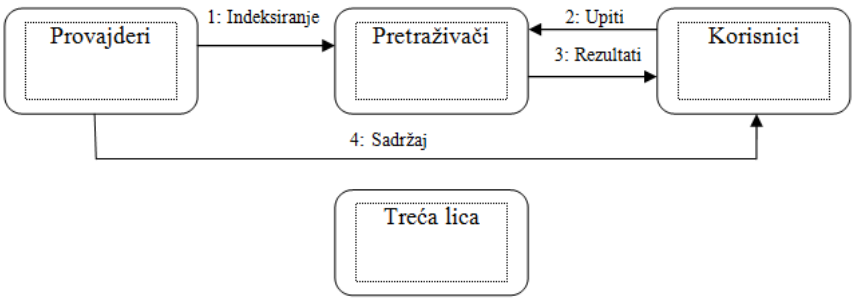
4.1.1. Pretraživači

Grimelman (Grimmelmann) pretraživače opisuje slikovito i višeznačno:

> „Oni su bibliotekari koji uvode red u haotičnu onlajn-akumulaciju informacija. Oni su glasnici koji povezuju pisce i čitaoce. Oni su kritičari koji sadržaju daju značaj ili ga šalju u zaborav. Oni su inovatori koji razvijaju nove tehnologije ili poslovne modele kako bi popravili internet. I oni su špijuni, od kojih se traži da sprovedu pretragu sa diskrecijom" (2007: 3).

Grimelman je analizirao tok informacija u okruženju koje je direktno zavisno od pretraživača, ali oni nisu jedini akteri uključeni u ovaj proces. Proces pretraživanja je kompleksan i zahteva analizu na najmanje dva nivoa, tehničkom i, kako ćemo kasnije videti, ideološkom, odnosno značenjskom nivou. Autor daje jedostavan prikaz procesa protoka informacija i pregled aktera uključenih u operaciju pretraživanja (videti Grafikon 8).

[115] Goodman, E. P., & Powles, J. (September, 28, 2016). "Facebook and Google: Most powerful and secretive empires we've ever known". *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2016/sep/28/google-facebook-powerful-secretive-empire-transparency (pristupljeno, 14. 02. 2018. godine).



Grafikon 8 Protok informacija u pretrazi (Grimmelmann, 2007: 7).

Indeksiranje podrazumeva proces u kome pretraživači sarađuju sa onima koji nude sadržaje kako bi se upoznali sa njihovom ponudom i organizovali ponuđene sadržaje u skladu sa upitom. Pod *upitom* se podrazumeva akcija korisnika kojom potražuje određenu informaciju. *Pretraživač* daje povratnu informaciju u vidu *rezultata* pretrage korisnika, odnosno listu sajtova koji nude sadržaje, a koji prema algoritamskom proračunu pretraživača najviše odgovaraju potraživanom pojmu (Grimmelmann, 2007: 7–11).

Takođe, i Van Eijk (Van Eijk) piše o načinima na koji funkcioniše pretraga na internetu putem pretraživača. Uprošćeno, on ističe da se pretraga može shvatiti kao proces u kome korisnik potražuje informaciju putem pretraživača koji je već unapred indeksirao informacije, na osnovu određenih kriterijuma; pretraživač šalje tzv. „detektive", „pauke" ili „botove" (2006: 2) da među informacionim provajderima pronađu onog koji ima najbolju ponudu za određenu pretragu. Proces se odvija i u drugom smeru, kada „detektivi" pronađu informacije koje su u skladu sa upitom i šalju ih nazad, od informacionog provajdera do korisnika; „to je usko grlo, sa dve boce povezane sa njim" (2006: 2).

Ovaj je proces primer korišćenja veštačke inteligencije, odnosno sistema u kojem mašine uče i oponašaju ljudske akcije i reakcije, koja je danas široko primenjena. Gugl koristi tehniku mašinskog učenja u skoro svim svojim aplikacijama i uslugama povezanim sa njima. Tako Guglov Android sistem reaguje na glas i poziva traženu osobu iz imenika, dalje: „od *Gmail*-a, preko Android menadžmenta baterije, do prikupljanja vesti, prikupljanja glasova robota koji zvuče kao ljudski" (Chlarton, 2018)[116] Gugl se koristi veštačkom inteligencijom. Glavni urednik Guglovog bloga Kristijan Hovar (Christian Howard) u blogu *Predstavljanje Guglove veštačke inteligencije* piše: „mi sve više stavljamo naglasak na implementaciju mašinskog učenja u skoro sve što Gugl radi" (Howard, 2018)[117]. Dakle, pretraživanje i radnje povezane sa njim nisu samo mehaničke, mašinske radnje, već unapred instruirane reakcije, plod veštačke inteligencije mašina koje su naučene da oponašaju ljudsku inteligenciju.

[116] Alistair Chalrton.(May 09 2018). "Artificial intelligence has become the backbone of everything Google does". *Gear Brain*. Dostupno na: https://www.gearbrain.com/google-uses-artificial-intelligence-everywhere-2567302875.html (pristupljeno 05. 01. 2019. godine).
[117] Christian Howard. (07 May 2018). "Introducing Google AI". *Google AI Blog*. Dostupno na: https://ai.googleblog.com/2018/05/introducing-google-ai.html (pristupljeno 05. 01. 2019. godine).

U tom kontekstu, Grimelman (Grimmelmann, 2007) usložnjava proces pretrage informacija kroz komparativni prikaz zainteresovanih strana, njihovih pojedinačnih interesa i potencijalnih problema, koji se konkretizuju kroz pravna pitanja i teorijske postavke (videti Grafikon 9). Sada pitanje protoka informacija više nije lišeno značenjskih slojeva, prevazilazi samo tehničko pitanje upita i rezultata i uključuje dodatne elemente.

Autor daje detaljan pregled interesa svih uključenih strana u proces pretraživanja: korisnika, provajdera, trećih lica i pretraživača, i izdvaja potencijalne izazove pri ostvarivanju tih interesa. Interes korisnika odnosi se primarno na kvalitet i privatnost pretrage, a najčešći problem u vezi sa ostvarivajem ovih zahteva jeste ugrožavanje privatnosti, odnosno zaštita korisnika, koja se najčešće ogleda u prihvatanju uslova korišćenja. Kada je reč o informacionim provajderima, njihovi interesi tiču se troškova, konkurentnosti i plasmana, odnosno fer rangiranja od strane pretraživača. Treća lica, kada je reč o internet okruženju, jesu raznovrsne zainteresovane strane, poput na primer agencija za oglašavanje, statističku obradu i slično, a njihovi interesi obuhvataju širok spektar pitanja, koja uključuju i reputaciju, privatnost i odnos sa korisnicima. Pretraživači, kao centralni akteri u sistemu pretrage informacija na internetu, posebno su zainteresovani za pitanja konkurencije, inovacija, ali i sprečavanja "prevara na klik" i pitanja optimizacije pretraživača, pod kojim se podrazumevaju različite tehnike pri rangiranju *veb* pretrage (Grimmelmann, 2007: 15-50).

Oblast	Interes	Protok informacija	Primer pravnih teorija
Korisnici	Privatnost	Upiti	Privatnost, ugovor
	Kvalitet	Rezultati	Zaštita korisnika
Provajderi	Troškovi	Indeksiranje, Sadržaj	Prestup, Ugovor
	Nepravedna konkurencija	Sadržaj	Autorska prava, Zaštiti znak, Ugovor
	Plasman	Rezultati	Zaštitni znak, Poslovni delikti
Treća lica	Vlasništvo	Sadržaj	Autorka prava, Zaštitni znak
	Reputacija	Sadržaj	Kleveta
	Privatnost	Sadržaj	Privatnost
	Vrline korisnika	Sadržaj	Direktna regulacija
Pretraživači	Optimizacija pretraživača	Indeksiranje, Rezultati	Prevara
	Klik prevara	Rezultati	Ugovor
	Inovacija	Sve	Pravo intelektualne svojine
	Konkurencija	Sve	Zakon o konurentnosti

Grafikon 9 Interesi u pretraživanju (Grimmelmann, 2007: 17)

Dakle, pretraživanje uključuje i interese i potencijalne probleme, analizirane u okviru raznovrsnih teorijskih i pravnih postavki. Pretraživače moramo sagledati šire od samog procesa potraživanja informacija; „pretraživači pokreću ne samo tehnička već i politička pitanja" (Introna & Nissenbaum, 2000:169). U tom kontekstu, Van Eijk ističe da pretraga informacija na internetu nije neutralna, unapred algoritamski uređena tako da uvek nudi najbolje rezultate pretrage. Zapravo, autor govori o „manipulaciji rezultatima pretrage", jer „ako je pauk instruiran da zanemari određene informacije, te se informacije nikada neće pojaviti kao rezultat pretraživanja" (2006: 3). Na taj način pretraživači postaju više od pukog kanala, oni su u ulozi vratara koji sistemom selekcije i eliminacije informacija mogu odlučivati o tome koji će rezultati pretrage stići do krajnjeg korisnika i na kom mestu će biti listirani u rezultatima pretrage.

Operacija pretraživanja u tom kontekstu zadire u polje prava na slobodno izražavanje. Van Ejik navodi brojne primere kojima ilustruje navedeno. Polazeći od plaćanja informacionih provajdera za bolje rangiranje u rezultatima pretrage, do filtriranja rezultata na različitim nacionalizovanim pretraživačima, kao što je to slučaj sa Guglovim domenom u Nemačkoj, koji blokira pretragu nacističke propragande, ili poznati slučaj Jahua u Kini, koji filtrira pretragu u skladu sa politikom Komunističke partije.

4.1.2. Društvene mreže

Pored pretraživača, drugi značajni akteri u novom IKS jesu društvene mreže. Kaplan i Henlejn (Kaplan & Haenlein) navode da društvene mreže nisu čedo 21. veka, već da imaju korene u samom začetku interneta i njegovoj prvobitnoj ideologiji, koja je podrazumevala povezivanje korisnika i razmenu poruka onlajn. Međutim, oni takođe ističu da se prvobitne forme ne mogu smatrati istovetnim, samo drugačije upakovanim proizvodima, pre svega zbog vrtoglavog razvoja tehnologije poslednjih decenija i inovacija koje su te promene donele. U tom kontekstu najznačajnije promene su pojava i razvoj *veb* 2.0 i proizvodnja sadržaja od strane korisnika (Kaplan & Haenlein, 2010: 60).

Obar i Vajdmen (Obar & Wildman) takođe smatraju da je okretanje *vebu* 2.0 ključno za razvoj i popularizaciju društvenih mreža, jer je upravo to pretvorilo internet u interaktivno polje. „Okretanje *vebu* 2.0 može se okarakterisati kao promena od korisnika kao konzumenata ka korisnicima kao učesnicima" (Obar & Wildman, 2015: 746). Pozivajući se na Toflerov (1980) *Treći talas*, autori koriste kovanicu „prokonzumer" ili „propotrošač" (engl. *prosumer*), koja se dobija spajanjem reči proizvođač (engl. *producer*) i potrošač/konzument (engl. *consumer*) kako bi opisali korisnika u digitalnom dobu, koji i sam proizvodi sadržaj i ima centralnu ulogu u razvoju društvenih mreža. Društvene mreže jesu, dakle: „*Veb* 2.0 aplikacije bazirane na internetu", dok je sadržaj kreiran od strane korisnika „životna snaga društvenih mreža" (Obar & Wildman, 2015: 746).

Kaplan i Henlejn razlikuju šest tipova društvenih mreža: *blogove*, *sajtove društvenih mreža*, *svetove virtuelnih društava*, *kolaborativne projekte*, *zajednice sadržaja* i *svetove virtuelnih igara*. Sve njih klasifikuju na osnovu nivoa *društvene prisutnosti* i *samoprezentacije* (videti Grafikon 10). U tom smislu sajtovi društvenih mreža, kakav je i Fejsbuk, imaju srednji nivo društvene prisutnosti i visok nivo samoprezentacije, za razliku od, na primer, svetova virtuelnih zajednica, poput „Drugog života" (*Second life*), koje imaju i visok nivo prisutnosti i visok nivo samoprezentacije. Sa druge strane,

kolaborativni projekti, na primer Vikipedija (*Wikipedia*), imaju oba niska nivoa, i društvene prisutnosti i samootkrivanja.

	Društvena prisutnost/bogatstvo medija		
	nisko	**srednje**	**visoko**
visoko **Samoprezentacija/** **Samooktrivanje** **nisko**	Blogovi	Sajtovi društvenih mreža (*Facebook*)	Svetovi virtuelni društava (*Second Life*)
	Kolaborativni projekti (*Wikipedia*)	Zajednice sadržaja (*YouTube*)	Svetovi virtuelnih igara (*World of warcraft*)

Grafikon 10 Klasifikacija društvenih medija na osnovu društvene prisutnosti/medijskog bogatstva i samoprezentacije/ samootkrivanja (Kaplan & Haenlein, 2010: 62).

Međutim, šire od pukog definisanja načina na koji društvene mreže funkcionišu i određenja učesnika u tom procesu, ostaje pitanje njihove društveno-političke uloge i uticaja. Iz prethodno objašnjenih tehničkih radnji i procesa možemo zaključiti da pretraživači imaju ključnu ulogu u onlajn-svetu. Prvi kontakt sa internetom ostvaruje se putem pretraživača. Njihova pretraga nije neutralna, niti je samo tehničke prirode (Goodman & Powles, 2016; Miller, 2014; Carlson, 2007; Grimmelmann, 2007; van Eijk, 2006; Introna & Nissenbaum, 2000). Sa druge strane, ključni deo društvenih mreža čini učešće korisnika. Međutim, ni Fejsbuk nije samo neutralna platforma za deljenje sadržaja korisnika i njihovo međusobno povezivanje (Griffith, 2017; Helberger & Trilling, 2016; Gottfried & Shearer, 2016; DeNardis & Hackl, 2015; Mueller, 2015; Napoli, 2015; Obar & Wildman, 2015). Gotovo sve radnje na ovim platformama obikovane su određenim kulturnim, društvenim, političkim, u najširem smislu građanskim procesima ili ih same oblikuju.

4.2. Uloge i značaj internet intermedijatora

Analizirajući uticaj koji tehno-giganti, između ostalih i Gugl i Fejsbuk, mogu da imaju na proces demokratije i civilno društvo, Mur identifikuje šest ključnih moći, koje mogu biti i prednost i opasnost: „1. moć upravljanja pažnjom, 2. moć prenošenja vesti, 3. moć omogućavanja kolektivne akcije, 4. moć davanja glasa ljudima, 5. moć da se utiče na glasače, 6. moć pozivanja na odgovornost" (2016: 24). Gotovo sve navedene moći svojstvene su i tradicionalnim medijima. Moć upravljanja pažnjom, na primer, svakako je jedna od osnovnih karakteristika tradicionalnih medija. Usmeravanje pažnje ka određenim, sugerisanim temama, koje samim tim dobijaju na značaju u javnom prostoru, osnova je tradicionalne *teorije dnevnog reda*, prema kojoj nam mediji *ne govore šta da mislimo, već o čemu da mislimo* (McCombs & Shaw, 1972). Prenošenje vesti, pozivanje na odgovornost, takođe su moći koje prepoznajemo kod tradicionalnih medija. Dakle, mogli bismo preuranjeno zaključiti da navedene moći i uticaj na građane nisu novina, niti su nastale sa pojavom tehno-giganata i interneta. Međutim, ono što ih razlikuje od dosadašnjih informaciono-komunikacionih medijuma jeste ogromna

moć u pozivanju na kolektivnu akciju i njihov, do sada neslućeni, uticaj na političke izbore (Moore, 2016).

Primer koji ilustruje navedenu Murovu tvrdnju jeste uloga društvenih mreža u organizovanju građanskih protesta na Bliskom istoku, tzv. „tviter revolucije" (Parmelee & Bichard, 2011; Bruns, Highfield & Burgess, 2013). Društvene mreže pokazale su ogromnu moć u pozivanju na kolektivnu akciju, okupivši stotine hiljada građana, koji su svoje nezadovoljstvo i politički bunt akumulirali na virtuelnim agorama, a sprovodili ga na gradskim trgovima i ulicama. Sve značajniju ulogu ovih kompanija na demokratske procese uočava i Napoli:

> „Mantre tehnoloških kompanija, poput Guglove 'ne budi zao', ili Fejsbukove 'davanje moći ljudima da dele' čine se neadekvatnim u evoluiranju medijskog ekosistema u kojem algoritamski usmerene platforme igraju sve značajniju ulogu u proizvodnji, širenju i konzumiranju vesti i informacija koje su od suštinskog značaja za funkcionalnu demokratiju" (Napoli, 2015: 757).

Intermedijatori, dakle, svakako imaju značajan uticaj na oblikovanje političkog i društvenog života građana, čime potvrđuju svoju značajnu civilnu, odnosno građansku ulogu. Njihova moć odražava se i na navike i odluke pojedinaca i političku participaciju, što je još jedna distinktivna moć, o kojoj Mur govori.

Pojava "lažnih vesti", na primer, imala je ulogu u izborima za predsednika Amerike 2016. godine, kao i u referendumskom izjašnjavanju Velike Britanije (Brexit) (Allcott & Gentzkow, 2017; Rainie, Anderson & Albright, 2017), što samo dodatno potvrđuje da su društvene mreže, kao UGC (*User Generated Content*) platforme, jedne od veoma uticajnih aktera u procesu političkog odlučivanja.

Prema istraživanju *Pew Research* Centra šest od deset Amerikanaca dobija vesti preko društvenih mreža, pri čemu je Fejsbuk najuticajnija društvena mreža u tom kontekstu. Naime, 67% odraslih Amerikanaca koristi Fejsbuk, od toga dve trećine dobija vesti upravo sa ove društvene mreže (Gottfried & Shearer, 2016). Međutim, „tehnološke kompanije preferiraju da ne ostavljaju utisak moćnih, već radije ističu kako njihovi alati i servisi opunomoćavaju javnost" (Moore, 2017: 22).

Slično Muru, Frančeska Muzijani (Francesca Musiani) ističe da pri analizi upravljanja internetom ne smemo zanemariti ni „inherentno političke" osobenosti algoritamskih proračuna pretraživača, jer „privatni akteri u informacijsko-tehnološkom sektoru trenutno igraju sve značajniju ulogu u medijaciji sadržaja, kao i u regulaciji onlajn-forme izražavanja, sa implikacijama na oba, internet prava i ekonomske slobode" (2013: 5, 1).

Glavna i odgovorna urednica Gardijana, Ketrin Vajner (Katharine Viner) smatra da goruća uloga Fejsbuka predstavlja pretnju za demokratiju i profesionalno novinarstvo:

> „Fejsbuk je postao najbogatiji i najmoćniji izdavač u istoriji zamenivši urednike algoritmima – razbio je javnu sferu na milione personalizovanih vesti , pomerajući čitavo

društvo daleko od otvorenog terena istinske debate i argumenata, dok zarađuje milijarde od naše pažnje" (Ruddick, 2017).[118]

Gugl i Fejsbuk donose petinu prihoda od oglasa na globalnom nivou, sa zaradom skoro duplo većom u odnosu na analizu od pre pet godina[119]. Pogled na listu najznačajnijih internet intermedijatora već nagoveštava njihovu moć i višestruki uticaj. Navedene kompanije (Gugl, Fejsbuk, Amazon i dr) upravljaju gotovo svakim segmentom onlajn-aktivnosti koje čine rutinu svakodnevnog života korisnika. Takođe, zaključujemo da onlajn-pejzaž oblikuju, i njime upravljaju, oligopoli, i to uglavnom američki. U tom kontekstu Kabir Čiber (Kabir Chibber, 2014) iznosi zanimljivu konstataciju: „Američki kulturni imperijalizam ima novo ime: GAFA"[120]. Akronim GAFA nastao je spajanjem početnih slova jednih od najmoćnijih intermedijatora: **G**ugla, Epla (**A**pple), **F**ejsbuka i **A**mazona.

Uloga ovih novih informaciono-komunikacionih aktera u demokratskim, političkim i kulturnim procesima značajna je. Međutim, još jedna značajna uloga intermedijatora, koju im dodeljuju same vlade, ogleda se u aktivnom učešću intermedijatora u regulaciji sadržaja. Naime, često se pred intermedijatore postavlja zahtev da detektuju i uklone ilegalan sadržaj na mreži, pri čemu se ovi novi akteri uključuju u upravljanje internetom, što pojedini autori smatraju privatizacijom javne sfere, davanjem prevelike moći internet intermedijatorima kroz regulatorne mehanizme (DeNardis, 2009, 2010, 2014; Musiani et al., 2016; Musiani, 2013).

Denardis i Hekl (DeNardis & Hackl, 2015) ističu da je značajnije pitanje *kako društvene mreže upravljaju internetom* od toga kako se upravlja društvenim mrežama i otvaraju pitanje „*privatizovanog upravljanja* putem platformi društvenih medija" (2015: 762). Autori se udaljavaju od čestih analiza sadržaja i okreću se analizi infrastrukture, kao ključnog momenta u upravljanju internetom. Suštinska pitanja individualnih prava, desiminacije informacija, zaštite slobode govora, biće, smatraju autori, oblikovana administrativnim, tehnološkim i poslovnim odlukama, pre nego zakonom zaštićena (DeNardis & Hackl, 2015: 762–763).

Sve navedene uloge intermedijatora, posebno Gugla i Fejsbuka, od aktivnog učešća u upravljanju internetom, preko uloge glavnih aktera u medijaciji informacija, čime se postuliraju kao centralni igrači u ostvarivanju prava na slobodno izražavanje, pa sve do rastuće uloge kada je reč o građanskom aktivizmu i političkoj participaciji, opravdavaju istraživanja koja su poslednjih godna vrlo intenzivna. Pitanja koja su veoma aktuelna tiču se i njihove odgovornosti koju sa sobom donose njihove uloge u IKS, o čemu će biti reči u narednim potpoglavljima.

[118] Graham Ruddick. (16 Nov 2017). "Katharine Viner: in turbulent times, we need good journalism more than ever". *The Guardian.* Dostupno na: https://www.theguardian.com/media/2017/nov/16/katharine-viner-we-need-public-interest-journalism-in-turbulent-digital-age (pristupljeno 20. 02. 2018. godine).
[119] Julia Kollewe. (2 May 2017). "Google and Facebook bring in one-fifth of global ad revenue". *The Guardian.* Dostupno na: https://www.theguardian.com/media/2017/may/02/google-and-facebook-bring-in-one-fifth-of-global-ad-revenue (pristupljeno 22. 02. 2018. godine).
[120] Kabir Chibber. (December 1 2014). "American cultural imperialism has a new name: GAFA", *Quartz.* Dostupno na: http://qz.com/303947/us-cultural-imperialism-has-a-new-name-gafa/ (pristupljeno 22. 02. 2018).

4.2.1. Internet intermedijatori: Akteri nalik medijskim akterima

Značajno mesto koje internet intermedijatori zauzimaju u novom informaciono-komunikacionom okruženju pokreće pitanja njihove odgovornosti. Mur (2016) ističe njihovu civilnu moć *pozivanja* vlada (prim. aut.) *na odgovornost*, ali je sagledava i kroz odgovornost samih intermedijatora. Naime, ukoliko privatne kompanije koje posluju na internetu vladama upućuju poruku: „odgovornost kroz transparentost" (Moore, 2016: 48), onda bi i one morale da posluju odgovorno i transparentno, kako bi opravdale titulu *petog staleža*[121].

Dok stručna javnost polemiše da li bi i za njih trebalo da važe „pravila ponašanja" kao i za tradicionalne medije, shodno njihovoj ulozi u novom informacionom ekosistemu (DeNardis, 2009; 2010; 2014; Helberger, 2014; Helberger & Trilling, 2016; Kohl, 2012; 2013; Moore, 2016; 2017; Milivojević, 2017; Musiani, 2013; Napoli, 2015; Goodman & Powles, 2016; Griffith, 2017; Kovach, 2017; Miller, 2014), ovi novi akteri, privatne imperije, odbijaju da sebe nazovu medijskim ili pak kompanijama nalik medijskim. Intermedijatori insistiraju na svojoj tehnološkoj prirodi, odnosno predstavljaju sebe samo kao tehnološku bazu za kreiranje i razmenu sadržaja, insistirajući na svojoj neutralnosti i, shodno tome, suženoj društvenoj odgovornosti.

Kako bismo im pronašli odgovarajuće mesto u novom okruženju, moramo najpre da ukažemo na tradicionalno poimanje medija, s obzirom na to da su „granice između novinara i ne-novinara postale zamagljene zbog razvoja komunikacije posredstvom interneta" (Vobič, Milojević, 2012: 470). Tek tada možemo da uporedimo tradicionalne uloge sa ulogama novih aktera, internet intermedijatora.

U *Preporuci Komiteta Ministara* CM/Rec(2007)15 pojam *medija* definiše se na sledeći način:

> „Termin 'mediji' odnosi se na one koji su odgovorni za periodično stvaranje informacija i sadržaja i njihovu diseminaciju nad kojom postoji urednička odgovornost, bez obzira na sredstva i tehnologiju koja se koristi za isporuku, a koja su namenjena za prijem i koja bi mogla imati jasan uticaj na značajan procenat javnosti"[122].

Ovakvo određenje medija bi na prvi pogled isključilo nove aktere, jer insistira na uređivačkoj odgovornosti koju ne prepoznajemo kod intermedijatora, bar ne u tradicionalnom smislu, o čemu će kasnije biti više reči. Takođe, intermedijatori ne proizvode sopstveni sadržaj, ali su najznačajniji akteri u njegovoj diseminaciji, i svakako, imaju ogroman uticaj na veliki procenat internet korisnika, onlajn javnost.

Pitanje novih aktera i njihovo teorijsko određenje bilo je fokus rada Karola Jakuboviča (Karol Jakubowicz) "Novo poimanje medija" (*A New Notion of Media*), izloženog na konferenciji Ministara Saveta Evrope zaduženih za pitanja medija i novih servisa u Rejkjaviku 2009. godine. Jakubovič identifikuje tri načina na koje možemo pristupiti pojavi novih aktera u IKS. Prvi pristup podrazumeva

[121] Štampa se naziva *četvrtim staležom* ili *četvrtom vlasti*, pored plemstva, sveštenstva i građanstva, odnosno sudske, izvršne i zakonodavne vlasti. Ovim se slobodnoj štampi priznaje ogromni značaj i uloga u demokratskom društvu. Izrazom *peti stalež* opisuje se uloga interneta u novom informacionom društvu.

[122] engl. *Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns*, dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4a3d (pristupljeno 03. 03. 2018. godine).

da će svi mediji postati novi mediji, odnosno da će sa sve većom upotrebom tehnoloških inovacija, a pod okriljem konvergencije, tradicionalni mediji inkorporirati nove trendove i transformisati se u nove medije. Primer za to su onlajn-izdanja tradicionalnih štampanih medija, onlajn-emitovanje tradicionalnih televizijskih programa i slično (Jakubowicz, 2009:19).

Drugi pristup tretira medijske forme koje su proizvod novih aktera. Jakubovič nudi tri moguća slučaja: zaobilažanje tradicionalnih medija u procesu diseminacije informacija, tzv. disintermedijaciju; širenje informacija od strane neprofesionalnih aktera, kao što su blogeri; i diseminaciju informacija od strane novih intermedijatora, kao što su pretraživači, internet servis provajderi i slično (Jakubowicz, 2009: 19). U kontekstu ovog istraživanja najznačajniji slučaj je poslednji, koji se odnosi na intermedijatore, i koji za Jakubovića predstavlja ujedno i treći način u pristupanju novog poimanja medija: „medijske ili aktivnosti nalik medijskim koje izvode ne-medijski akteri" (Jakubowicz, 2009: 24-26).

Oslanjajući se na Mekvejlov koncept „novinarstva kao javne profesije" (McQuail, 2008), Jakubovič navodi šest elemenata, na osnovu kojih definiše da li je određena aktivnost medijska ili je nalik medijskoj: da li je *svrha* služiti javnom interesu i kreirati prostor za javnu debatu; da li podrazumeva *uređivački proces i politiku* selekcije i odgovornosti; da li su *novinari i drugi kreatori sadržaja* uključeni u organizacionu strukturu; da li je *periodična diseminacija* podrazumevana; da li je omogućena *javna priroda* informacija; i da li postoji *usklađenost sa normativnim, etičkim, profesionalnim i pravnim standardima* (Jakubowicz, 2009: 9). Autor ističe da su svrha, uređivačka politika i poštovanje profesionalnih standarda ono što zaista pravi razliku između medijskih organizacija i onih koje su nalik njima.

Uzimajući u obzir navedene elemente, Jakubovič uvodi nove aktere i na njima primenjuje definisane odrednice medija. S tim u vezi, Jakubovič navodi da je *svrha*, kao prvi element kojim definišemo medijsku aktivnost, ostala nepromenjena, bilo da je reč o tradicionalnim medijima ili novim akterima, koji se javljaju u medijskom okruženju. Kada je reč o *uređivačkom procesu*, autor smatra da je on dosta izmenjen kada je reč o novim akterima: „uređivačka odgovornost poprima različite, često veoma ograničene, forme" (2009: 17). Treći element, koji podrazumeva *medijske profesionalce*, naročito novinare, kod novih aktera se razlikuje u meri u kojoj su kreatori sadržaja "volonteri", "građani", "amateri" (2009: 17). *Periodičnost*, kao četvrti element distinkcije, ne može se posmatrati kao uprošćena kategorija redovnog objavljivanja informacija, smatra Jakubovič. Naime, autor navodi primer Gugl vesti, koje se osvežavaju u proseku četiri puta na sat vremena, stoga bismo mogli zaključiti da zadovoljavaju ovaj kriterijum. Sa druge strane, „prirodno statični veb sajtovi teško se mogu kvalifikovati kao mediji" (2009: 17). Element *javne prirode komunikacije* ostaje i kod novih aktera, sa razlikom koju Jakubovič prepoznaje u "globalnoj dostupnosti", okrenutosti ka aktivnom učešću publike u odabiru informacija, ali i u personalizovanom targetigarnju, kojim se nišane određene kategorije ciljnih grupa (Jakubowicz, 2009: 17). Poslednji element, koji se odnosi *na normativne, etičke, profesionalne i zakonske standarde*, Jakubovič posmatra kao veoma značajan kriterijum, kojim se utvrđuje da li su pojedini akteri zaista i medijski akteri.

Savet Evrope je 2011. godine usvojio *Preporuku (CM/Rec(2011)7)*[123] *Komiteta Ministara državama članicama u vezi sa novim poimanjem medija*. Potrebu za postavljanjem novih standarda u definisanju medija i medijskih usluga Komitet obrazlaže:

> „Novi akteri preuzeli su funkcije u procesu proizvodnje i distribucije medijskih servisa koji su, do nedavno, izvršavali samo (ili uglavnom) tradicionalne medijske organizacije; ovo uključuje agregatore sadržaja, dizajnere aplikacija i korisnike koji su takođe prizvođači sadržaja. Brojni 'intermedijatori' ili 'pomoćnici' koji često potiču od informacionog i komunikacionog sektora (IKS) [..] od ključnog su značaja [...] Usluge koje pružaju ovi novi akteri postali su ključni u pronalaženju informacija, pretvarajući ponekad intermedijatore ili pomoćnike u vratare ili u igrače koji imaju aktivnu ulogu u uređivačkim procesima masovne komunikacije" (*CM/Rec(2011)7*: pargraf 6).

U ovoj *Preporuci* navodi se i šest kriterijuma, po ugledu na Jakubovičeve, na osnovu kojih države članice mogu sa sigurnošću da odrede da li određeni subjekt u IKS obavlja medijsku ili aktivnost nalik medijskoj i da se u skladu sa tim odnose prema ovim akterima i njihovoj odgovornosti. Prvi kriterijum je *namera da deluju kao medij*, što se određuje na osnovu indikatora: da li sebe nazivaju medijem, da li primenjuje medijske standarde u radu i slično. Drugi kriterijum podrazumeva *da imaju svrhu i osnovne ciljeve medija*, kao što su širenje medijskog sadržaja i periodičnost u objavljivanju. *Uređivačka kontrola* je treći kriterijum, dok je *poštovanje profesionalnih standarda* četvrti. *Rasprostranjenost i širenje informacija* koje je u skladu sa profesionanim standardima i koje je u srži medijske delatnosti jeste sledeći kriterijum. Poslednji, šesti, odnosi se na *očekivanja javnosti* i uključuje dostupnost, pluralizam, odgovornost, transparentnost i drugo. Nisu svi kriterijumi od jednake važnosti, pa se uređivačka kontrola, svrha i širenje informacija određuju kao značajniji, jer njihovo odsustvo gotovo zasigurno eliminiše aktera kao medijskog, dok su preostala tri „mekši kriterijumi". Međutim, u *Preporuci* se navodi da čak i odsustvo „tvrdih" kriterijuma ne znači automatsko isključivanje odgovornosti, naprotiv:

> „Intermedijatori i pomoćnici u medijskom ekosistemu mogu se razlikovati od medija [...] oni često ne ispunjavaju neke od osnovnih kriterijuma kao što su uređivačka kontrola (kriterijum 3) ili svrha (kriterijum 2). Međutim, oni često igraju bitnu ulogu što im daje značajnu moć u pogledu dostupnosti i kontrole ili nadzora nad sadržajem. Kao rezultat toga, intermedijatori i pomoćnici mogu preuzeti aktivnu ulogu u uređivačkim procesima masovne komunikacije. Stoga bi zemlje članice trebalo pažljivo da razmotre kreiranje politike u vezi sa medijima i trebalo da posvete posebnu pažnju pozitivnim i negativnim obavezama koje proizlaze iz člana 10 Evropske konvencije o ljudskim pravima ((*CM/Rec(2011)7*: paragraf 15)".

Danas je jasno da intermedijatori igraju aktivnu ulogu u uređivanju i kontrolisanju protoka informacija. Uredničko filtriranje sadržaja od strane intermedijatora pokreće pitanje uloge vratara. U vremenu disintermedijacije, koju definišemo kao „eliminisanje posrednika, npr. medijskih organizacija, jer svako može ponuditi informacije i drugim sadržajima mogu direktno pristupiti korisnici i primaoci" (Jakubowicz, 2009: 12), uloga čuvara kapije se smanjuje, ali se istovremeno i nameće kao kompleksno pitanje.

[123]Engl. *Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media*, dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0 (pristupljeno 03. 03. 2018. godine).

Uloga intermedijatora kao vratara u novom okruženju može se analizirati na primeru Gugl vesti (*Google news*)[124] (Jakubowicz, 2009; Carlson, 2007). Kompanija Gugl definiše Gugl vesti na sledeći način:

> „Gugl vesti je kompjuterski generisan sajt za vesti koji prikuplja naslove iz izvora širom sveta, grupiše slične priče i prikazuje ih u skladu sa individualnim interesima svakog čitaoca. [...] Naši tekstovi biraju i rangiraju kompjuteri koji, između ostalog, procenjuju koliko se često i na kojim mestima priča pojavljuje onlajn. Takođe, rangiramo tekstove i na osnovu određenih karakteristika sadržaja vesti kao što su aktuelnost, lokacija, relevantnost i raznolikost. Kao rezultat toga, priče se razvrstavaju bez obzira na politički stav ili ideologiju."[125]

Ovaj sajt isključuje ljude kao urednike, ali ulogu vratara preuzima kompjuterski algoritam, čiji se proračun vodi tradicionalnim značenjskim odrednicama vesti, kao što su *aktuelnost, blizina, relevantnost* i slično. Gugl vesti zaista nude različite izvore za istu temu, što korisnicima ostavlja mogućnost izbora, komparacije i zaključivanja, stvarajući „raznovrsnu agoru vesti" (Carlson, 2007: 1020). Međutim, da li to znači da algoritam može adekvatno da zameni urednika ako mu se zadaju parametri kojima se i urednici rukovode pri selekciji vesti? Polemišući o načinu na koji su pretraživači promenili, ili još uvek menjaju, tradicionalnu ulogu urednika i novinara, Met Karlson (Matt Carlson) zaključuje da „ideja o tome šta je 'novinarstvo' nije fiksna i nepromenljiva, već sklona menjanju u skladu sa promenom kulture koja je okružuje. Na ovaj način, pretraživači vesti najavljuju drugačiji konceptualni model onoga što vesti rade i kako se obraćaju publici" (2007: 1027).

Internet intermedijatori, dakle, nisu samo "nevini" prenosioci, agregatori sadržaja – intermedijatori sadržaj i rangiraju. Intermedijatori se pozivaju na argument neutralnosti tehnologije, odnosno algoritama i veštačke inteligencije koju koriste u rangiranju i diseminaciji sadržaja, u odbrani sopstvene „intermedijatorske" pozicije. Međutim, sa stanovišta društvenih nauka, alogoritmi se ne mogu smatrati neutralnom tehnologijom i mnogi autori ukazuju na problematičnost argumenta „mrežne neutralnosti".

Pretraživači i društvene mreže nisu oslobođene vrednosnih slojeva, komercijalnih interesa ili pravnih stega. Neutralnost, koju promoviše Gugl, a koja se pojednostavljeno može shvatiti kao jednaka šansa za sve ponuđače sadržaja, ostvaruje se upotrebom algoritama, čiji je način rada često neshvatljiv i nevidljiv za običnog korisnika. U krajnjem, način rangiranja pretrage dobro je čuvana poslovna tajna Gugla. Iznoseći niz kratkih i jednostavnih konstatacija, poput: "Gugl je internet", "Neutralni glasnik-čiji glasnik?", Kol (Kohl, 2013: 193,195) ukazuje na značaj Gugla u izgradnji virtuelnog sveta, predstavljajući ga kao tehno-giganta nesagledive moći. Naime, Kol pojašnjava da je čitavo iskustvo internet korisnika posredovano Guglovom pretragom. Pretraživač Gugl u nepregledni haos onlajn-sveta uvodi red, ali to ne čini neutralno, već se vodi određenim odrednicama i kriterijumima. Kao najdominantniji pretraživač, Gugl možemo nazvati i samim internetom, jer gotovo svaka aktivnost internet korisnika otpočinje Guglovom pretragom (Kohl, 2013: 191–193); po mišljenju Jakubovića na delu je "Guglaizacija pretraživanja" (Jakubowicz, 2009: 34). Međutim, Kol pojašnjava da pretraživanje nije neutralno, njegov automatizam nije jednak njegovoj neutralnosti. Upravo zbog toga pokušava da

[124] „Gugl vesti pokrenute su u septembru 2002. godine kao potpuno automatizovan servis vesti. Sajt ne zahteva urednike-ljude, za razliku od vodećih agregatora vesti, veb stranica kao što su AOL ili Jahu vesti. Naslovi se prikupljaju sa preko 4 500 web stranica i sajt se ažurira svakih 15 minuta" (Carlson, 2007: 1019).
[125] *About Google News*, videti putem linka: https://www.google.com/intl/en_us/about_google_news.html (posećeno: 10. 03. 2018. godine).

odgovori na pitanje čiji je Gugl glasnik, te u tom kontekstu pojašnjava da će ponuda potraživanih pojmova biti u vezi sa oglasnim porukama koje su ponuđači sadržaja platili, kako bi ih pretraživač povezao sa ciljanim korisnicima Guglovih usluga (Khol, 2013: 195–197).

Problemsko pitanje koje se nameće, onda kada se prihvate argumenti koji govore u prilog tome da pretraživači jesu onlajn-vratari, prelazi na jedan novi nivo na kojem Gugl evoluira od glasnika do kreatora. Kako objašnjava Kol: „U meri u kojoj organizovanje materijala ne može nikada biti neutralno, u istoj meri je zamućena i granica između organizacije sadržaja i kreiranja sadržaja" (Khol, 2013: 192). Jakubovič navodi: „Ako su posrednici zaista imali uređivačke i regulatorne funkcije u odnosu na dobavljače i korisnike sadržaja, to bi ih učinilo posrednicima i približilo njihov rad onima u medijima, implicirajući stepen uredničke odgovornosti i odgovornosti za distribuirani sadržaj" (Jakubowicz, 2009: 24).

Prema tradicionalnoj teoriji o čuvarima kapija, sa jedne strane, nalaze se sve vesti koje su u opticaju, koje zatim prolaze kroz uska grla, gde se obavlja selekcija, i sa druge strane zamišljenog puta ovog procesa nalaze se vesti koje su "vratari" propustili, dajući im legitimitet i značaj. Pojednostavljeno, u svaku novinarsku redakciju svakodnevno dospe veliki broj informacija, međutim, neće svaka od njih postati vest. O tome koja će informacija izaći u etar odlučuju vratari, koje uglavnom prepoznajemo u ulozi urednika, ali i mnoštvo vanmedijskih faktora može uticati na selekciju, na primer, različite društvene i političke grupe, oglašivači. Jakubovič ovaj proces opisuje na sledeći način: „Uloga čuvara kapije održava i sprovodi skup profesionalnih rutina i konvencija za koje se smatra da predstavljaju neku vrstu kontrolnog mehanizma kvaliteta u institucionalnom novinarstvu" (2009: 17). Ova teorija, koju je prvi uspostavio Kurt Levin (Kurt Lewin), vremenom modifikovana i revidirana (Milojević, Radojković, 2016; Barzilai-Nahon, 2008) ostavlja prostor za dodatne interpretacije u novom informaciono-komunikacionom okruženju.

Potreba za postojanjem čuvara kapija u okruženju koje je moć selekcije preselilo u ruke korisnika kroz mogućnosti interakcije i participacije možda deluje neosnovano. Međutim, „možda su informacione kapije danas svakom pojedincu potrebnije nego ikada, kao filteri koji će propuštati potrebne i odbacivati ogromnu količinu nepotrebnih informacija" (Milojević, Radojković, 2016: 185). Značajnije pitanje, od sumnje u potrebu postojanja vratara, možda bi bilo *ko su na internetu čuvari kapije?*, jer ono što sada već svaki prosečni korisnik zna jeste da filtriranje sadržaja na internetu neupitno postoji.

Emili Lejdlou (Emily Laidlaw) razlikuje dve vrste međuzavisnih čuvara kapija na internetu: internet čuvare kapije, koji „kontrolišu protok informacija" i internet informacione čuvare kapije, koji za posledicu te kontrole imaju uticaj na „participaciju i promišljanje u demokratskoj kulturi" (2010: 266). Lejdlou pojašnjava proces čuvanja kapije kroz:

> „kanalisanje (npr. pretraživači, hiperlinkovi), cenzuru (tj. filtriranje, blokiranje, zoniranje), dodatu vrednost (tj. alati za prilagođavanje), infrastrukturu (tj. pristup mreži), interakciju korisnika (tj. uobičajene stranice, hipertekstualni linkovi) i uređivačke mehanizme (tj. tehnička kontrola, informacijski sadržaj)" (Laidlaw, 2010: 267).

Dakle, mehanizmi kojima se različiti intermedijatori služe, od obezbeđivanja pristupa (internet sevis provajderi), do, na primer, filtriranja i blokiranja ilegalnog sadržaja, svakako upućuju na jaku ulogu vratara. Ukoliko, kao što to čini i autorka, tome dodamo i pitanja ljudskih prava, čija se zaštita dodatno problematizuje "na mreži", jasno je da internet intermedijatori imaju značajnu ulogu vratara,

koja prevazilazi samo algoritamski proračun i direktno utiče na demokratski proces. Jakubovič u tom kontekstu navodi primer sajtova koji samoregulišu objavljivanje komentara korisnika i ističe:

> „Takva moderacija zahteva uređivačku procenu zasnovanu na nizu kriterijuma i može dovesti do odbijanja komentara, pri čemu je autor lišen šanse da dođe do publike i publika lišena pristupa sadržaju komentara. Čak i u ovom malom obimu, ovo je veoma relevantno u pogledu slobode izražavanja" (Jakubowicz, 2009: 24).

Ukoliko ovim primerima dodamo i nesvesno učešće korisnika u uređivačkom procesu, pitanje selekcije informacija dodatno se usložnjava, a odgovornost intermedijatora kao vratara maskira. Aktivnosti korisnika na društvenim mrežama, na primer, unose se u logiku algoritama, koji potom određuje vrstu sadržaja koja će korisniku biti ponuđena. Uprošćeno, lajkovanje (*like* – sviđati se) na društvenim mrežama korisniku donosi veću ponudu sličnog sadržaja, čime sam korisnik, uglavnom nesvesno, uređuje ponudu informacija od strane intermedijatora.

Natali Helberger (Natali Helberger, 2014) analizira drugi aspekt internet intermedijatora kao čuvara kapija i fokusira se na njihov uticaj na pluralizam, odnosno diverzitet kao jedan od osnovnih ciljeva javnih politika. Naime, autorka ističe da je na snazi podela moći između tradicionalnih i internet čuvara kapija, kada je reč o kontroli pažnje korisnika, jer sada i novi akteri „utiču na dostupnost, pronalaženje, ocenu, preporuku i funkcionalnost medijskih ponuda" (2014: 10). Nilsen (Nielsen) takođe ukazuje na rastući značaj globalnih digitalnih intermedijatora, ističući pretraživače i društvene mreže, posebno mobilne platforme i aplikacije, kao „nove kapije vesti" (2013: 75).

Već je bilo reči o istraživanju Istraživačkog centra Pju koje svedoči da je za više od dve trećine Amerikanca glavni izvor vesti društvena mreža Fejsbuk (Gottfried & Shearer, 2016). Takođe, istraživanje iz 2018. godine, koje je obuhvatilo 38 zemalja, pokazuje da 42% ispitanika iz svih zemalja bar jednom dnevno traži vesti na internetu, dok skoro polovina od ukupnog broja ispitanika koristi društvene mreže kao izvor vesti (Mitchell et al., 2018). Rezultati ovih istraživanja govore u prilog tome da se sve veći broj ljudi, i to ne samo u rezvijenim zemljama, okreće internetu, odnosno društvenim mrežama kada je reč o izvorima vesti. Autorka Helberger s pravom naziva društvene mreže „novim kapijama vesti". Što je veći broj korisnika koji intermedijatore koristi kao novi prostor za informisanje o značajnim društveno-političkim temama, to je i veća uloga i odgovornost intermedijatora pri skretanju pažnje na određene medijske sadržaje.

Ističući ulogu intermedijatora kao čuvara kapije, Robin Mansel (Robin Mansell, 2014) navodi da su oni više od običnih prenosioca sadržaja i da im se tako treba pristupiti: „Umesto podvojenog fokusiranja na tržišne segmente poput prenosa/pristupa, sadržaja, pretraživanja/agregacije, fokus treba prebaciti na medijsku ekologiju, nove tačke kontrole i procenu da li je korisničko iskustvo u skladu sa javnim interesom za medijski pluralizam".[126]

Kompanije koje su predmet analize u ovom radu, Gugl i Fejsbuk, godinama odbijaju da preuzmu odgovornost koja bi bila proporcionalna njihovoj ulozi i uticaju. Isprovociran njihovom reakcijom, Miler postavlja sledeća pitanja:

> „Da li su ove kompanije malo neiskrene? Sa jedne strane, one žele biti otvorene i agnostičke platforme za distribuciju sadržaja [...] Sa druge strane, one najveći deo svojih

[126]Mansell, R. (2014). "Governing the gatekeepers: is formal regulation needed?" *Media Policy Blog.* Dostupno na: http://eprints.lse.ac.uk/80359/ (pristupljeno 05. 03. 2018. godine).

prihoda dobijaju od medijskog oglašavanja. Smatram da bi trebalo da budu iskrenije kada je reč o tome šta žele da budu: platforme bez uređivačke odgovornosti ili medijske kompanije sa organizacionim okvirom koji omogućava donošenje uređivačkih odluka?" (Miller, 2014)[127].

Ukoliko se odluče za drugu opciju onda bi, smatra autor, morale i da prihvate odgovornosti i regulatorne mere koje takva odluka sa sobom donosi. Na istom tragu je i izvršni direktor *Sky*, Džeremi Darok (Jeremy Darroch) koji opominje:

> „Naše društvo i naša industrija suočavaju se sa cunamijem štetnih sadržaja onlajn: od lažnih vesti do ekstremizma, od krađe identiteta do krađe sadržaja. Svako se bori sa kretanjem kroz uglavnom neregulisan internet krajolik. […] Pre ne tako mnogo godina, internet kompanije bile su male i prilično neuticajne . Danas su to neke od najvećih kompanija na planeti sa dostignućem i obimom finansijskih izvora daleko većim od prethodnih medijskih i komunikacionih kompanija . Mi smo regulisani zbog našeg uticaja na društvo, ali njihov uticaj na društvo danas je verovatno mnogo veći."[128]

Zbog njihove ogromne ekonomske moći i neupitnog uticaja na korisnike, ove kompanije bi trebalo da prihvate odgovornost koju imaju u kreiranju javne sfere i demokratskim procesima. Njihova dostupnost, brzina i količina informacija koje svakodnevno protiču njihovim sistemima, opravdano izazivaju bojazan zbog stvaranja onlajn prostora sa ogromnim uticajem i nesrazmernom odgovornosti. Međutim, društvene mreže izgleda ne žele da priznaju značaj i ulogu koju imaju u novom IK okruženju:

> „Ironično, dok se platforme društvenih mreža uspostavljaju kao jedne od najznačajnijih medijskih organizacija 21. veka, one često – delom zbog sopstvenih svesnih napora – nisu percipirane niti tretirane kao medijske kompanije, već pre kao nešto fundamentalno drugačije – tehnološke kompanije" (Napoli, 2015: 752).

Međutim, operativna direktorka Fejsbuka Šeril Sendberg (Sheryl Sandberg) u intervjuu za *Axios*, oktobra 2017. godine, izjavila je da Fejsbuk nije medijska kompanija: „u našoj srži mi smo tehnološka kompanija… mi ne zapošljavamo novinare"[129]. Izjava direktorke Fejsbuka izazvala je burne reakcije, pre svega zbog pojednostavljenog definisanja medijskih aktivnosti i banalizovanja uloge koju tehnološki giganti, poput Fejsbuka i Gugla imaju u medijskom ekosistemu. Stiv Kovač (Steve Kovach),

[127] Andrew, M. (2014). "Digital distributors cannot escape their editorial responsibilities". *Media Policy Blog.* Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/digital-distributors-cannot-escape-their-editorial-responsibilities/ (pristupljeno 06. 03. 2018. godine).

[128] Graham Ruddick. (27 Nov 2017). "Society faces 'tsunami of harms' from lack of online regulation". *The Guardian*. Dostupno na: https://www.theguardian.com/media/2017/nov/27/society-faces-tsunami-of-harms-from-lack-of-online-regulation (pristupljeno 20. 03. 2018. godine).

[129] Ceo intervju koji je operativna direktorka Fejsbuka, Šeril Sendberg, dala za *Axios* dostupan je na linku: https://www.axios.com/exclusive-interview-with-facebooks-sheryl-sandberg-1513306121-64e900b7-55da-4087-afee-92713cbbfa81.html (pristupljeno: 04. 03. 2018. godine).

viši dopisnik *Business Insider*, piše: „Šeril Sendberg i njene kolege u Silikonskoj dolini možda to ne žele da priznaju, ali velike tehnološke kompanije postale su veliki mediji"[130].

Erin Grifit (Erin Griffith, 2017) upućuje rukovodiocima Fejsbuka, putem američkog časopisa *Wired*, ironični vodič kojim želi da dokaže da Fejsbuk zapravo jeste medijska kompanija. Pitanja: „Da li ste najveći izvor vesti u zemlji?" „Da li cenzurišete sadržaj?" „Da li upošljavate kontrolore koji se bave lažnim vestima i prevarama?" „Da li zarađujete od reklamiranja sadržaja?", samo su neka od pitanja napisana kao "podsetnik" Fejsbuku da zaista radi kao medijska kompanija[131].

***

Jakubovič u Rejkjaviku, pre skoro deset godina, kao moguće pravce delovanja u informaciono-komunikacionom okruženju koje uključuje i ne-medijske aktere, istakao je sledeće: sveobuhvatnu analizu načina na koji novi akteri utiču na demokratske procese, razmatranje delovanja novih aktera u oblasti zaštite ljudskih prava u novom okruženju, poseban fokus na analizu uticaja novih aktera na slobodu izražavanja kao osnovno pravo u demokratskim društvima i preispitivanje regulatorne politike koja uključuje nove aktere uz analizu dosega samoregulacije i koreglacije u ovoj oblasti (2009: 37–38). Sve istraživačke oblasti koje je autor izdvojio kao veoma značajne i danas ne gube na značaju. Naprotiv, istraživanja iz ovih oblasti su sve intenzivnija, podstaknuta sve bržim tehnološkim razvojem i inovacijama u oblasti poslovanja ne-medijskih aktera, ali i sve većim uticajem koji ove kompanije ostvaruju; danas, znato više nego 2009. godine.

Jakubovič je tada prepoznao da „u mnogim slučajevima posrednici idu dalje od uloge 'pukog kanala' i obavljaju ulogu vratara" (Jakubowicz, 2009: 24), ali i dodao da „to ne pretvara posrednike u medijske organizacije, ali im omogućava da izvode određene medijske funkcije" (Jakubowicz, 2009: 26). Međutim, sa sve većom ulogom koju posrednici svakodnevno potvrđuju, mogli bismo da zaključimo da je Jakubovičevo predviđanje bilo tačno, ali da bi se njegov stav o odgovornosti novih aktera sada mogao videti kao blag. Ne samo da kompanije, poput Gugla i Fejsbuka, „izvode određene medijske funkcije", već je njihov uticaj u svim oblastima društveno-političke zbilje neslućenih razmera, sa konstantnom tendencijom rasta. Stoga, preporuka kreatorima javnih politika mora ići dalje od samo prepoznavanja njihovog postojanja i opisivanja neutralnim terminima "novih aktera", "posrednika" i slično; i dalje od preporuka o sveobuhvatnim analizama njihove uloge i uticaja. U komparaciji sa stanjem od pre deset godina, novi akteri jesu vidljiviji u regulatornim aktima, preporukama, direktivama, ali još uvek postoji mnogo "sivih zona", kada je reč o njihovom poslovanju i konkretno njihovoj odgovornosti prema javnosti, odnosno javnom interesu.

[130]Kovach, S. (October 12, 2017). "Facebook and the rest of Big Tech are now Big Media, and it's time we start treating them that way". *Business Insider*. Dostupno na: http://www.businessinsider.com/facebook-and-google-are-now-media-companies-2017-10
(pristupljeno 05. 03. 2018. godine).
[131]Griffith, E. (10 December 2017). "Memo to Facebook: How to Tell if You're a Media Company". *Wired*. Dostupno na: https://www.wired.com/story/memo-to-facebook-how-to-tell-if-youre-a-media-company/
(pristupljeno 10. 03. 2018. godine).

4.3. Između komercijalnog i javnog interesa

Uticaj koji internet intermedijatori, na čelu sa Guglom i Fejsbukom, imaju na civilne akcije, opisan je u prethodnom poglavlju (Allcott & Gentzkow, 2017; Bruns, Highfield & Burgess, 2013; Gottfried & Shearer, 2016; Moore, 2016; 2017; Parmelee & Bichard, 2011; Rainie, Anderson & Albright, 2017). Međutim, njihova istrajnost u samopercepciji kao čisto tehnoloških kompanija u nesrazmeri je sa uticajem koji svojim poslovanjem ostvaruju u oblastima izvan pitanja tržišta i inovacija, pre svega u oblastima društveno-političkog delokruga (Miller, 2014; Kovch, 2017; Griffith, 2017; Jakubowicz, 2009).

Dominantni izazovi iz ugla intermedijatora uključuju, očekivano, njihovu konkurentnost, pozicije na tržištu, ekonomski rast i tehnološke inovacije – *ostvarivanje komercijalnog interesa*. Sa druge strane, pitanja, koja se direktno tiču korisnika kao građana, a ne potrošača, jesu pitanja uticaja na oblikovanje društvene, političke, kulturne zbilje, kao i pitanja potencijalnog ugrožavanja ljudskih prava – *ostvarivanje javnog interesa* (Mansell, 2015; Laidlaw, 2008; Thompson, 2015; Pasquale, 2010; De Filippi, 2014).

Komitet Ministara je 2007. godine usvojio *Preporuku državama članicama o merama promovisanja vrednosti javne usluge na internetu*[132], kojom se ističe značaj pristupa internetu, ali i poštovanja ljudskih prava u novom okruženju. Takođe, podstiče se privatni sektor da prepozna značaj svoje uloge u društvenoj koheziji, etičku ulogu i odgovornosti. Preporuka posebno ističe oblasti *demokratije i ljudskih prava, pristupa, otvorenosti, različitosti* i *bezbednosti*, kao oblasti koje zahtevaju dodatnu pažnju na internetu, te poziva države članice i privatni sektor na saradnju u ovim oblastima.

Slično, Mansel (Mansell, 2015) poziva kreatore politika da u regulatorne okvire uključuju i izazove koji se tiču društveno-političkih i kulturnih uticaja, zamerajuću to što je glavni fokus uglavnom na ekonomskim pitanjima i omogućavanju nesmetanog razvoja tržišta. Intermedijatori su postali više od samo komercijalnih kompanija, i uz moć koju imaju u oblasti kreiranja, pa i upravljanja javnom sferom, njihova odgovornost prema zaštiti javnog interesa trebalo bi da zauzme visoku poziciju na listi prioriteta.

Zanemarivanje pitanja javnog interesa i favorizovanje dominantno ekonomskih tema u ovoj oblasti ne opravdava ni Paskal (Pasquale) i ističe da: „Internet intermedijatori upravljaju onlajn-životom" (2010: 105), stoga imaju značajan uticaj i na nekomercijalnu sferu, pre svega na društveno-politički život korisnika. Autor smatra da bi se trebalo okrenuti političkim i društvenim izazovima koje je sa sobom donela komercijalizacija interneta, i koji se ne mogu rešiti u okvirima ekonomskih analiza i jačanja tržišta. U tom kontekstu, pogrešno je posmatrati pretraživače samo kao tržišne igrače, već bi trebalo sagledati i njihovu društvenu, kulturnu i političku ulogu i u skladu sa tim graditi bolji okvir za njihovo poslovanje. Takav okvir bi se bazirao na tržišnim pretpostavkama, ali ne bi zanemarivao ni ne-ekonomski uticaj koji ovi veliki igrači imaju, sa posebnim fokusom na odgovornost prema javnom interesu i zaštiti korisnika (Pasquale, 2010).

[132] *Preporuka* CM/Rec(2007)16 dostupna na linku: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d4a39 (pristupljeno: 03. 05. 2018. godine).

Srž problemskog pitanja, koje analiziramo u ovom potpoglavlju, najbolje opisuje rečenica Emili Lejdlou (Emily Laidlaw, 2008): „Privatna moć, javni interes". Ova kontrastna rečenica sumira niz izazova, svojstvenih onlajn-prostoru i odnosi se na ogromnu moć privatnih kompanija, koje kroje internet pejzaž, i njihovu odgovornost prema nekomercijalnim delatnostima. Izvan njihove uloge isključivo tržišnih aktera, intermedijatorima se pripisuje mnogo značajnija uloga, ona koja se i mimo pravnih stega oslanja prevashodno na etičnost i odgovornost. U tom kontekstu Tomson (Thompson) navodi: „naš pristup odgovornosti intermedijatora trebalo bi da se zasniva na ideji odgovorne komunikacije o pitanjima od javnog interesa" (2015: 843). Međutim, na ovom mestu možemo postaviti i pitanje da li su realna očekivanja da će intermedijatori, tehno-giganti, poštovati interes svojih korisnika kao građana? Da li su kompanije na internetu odgovorne prema javnosti u meri u kojoj su na primer tradicionalne medijske kompanije odgovorne prema javnom interesu, jer „da bismo nametanuli bilo kakve obaveze zaštite javnog interesa poslovanju na internetu, ova preduzeća moraju obavljati aktivnosti koje su važne u funkcionisanju demokratije" (Laidlaw, 2008: 120).

Na ulogu intermedijatora u (pre)oblikovanju društveno-političke sfere ukazano je u prethodnom potpoglavlju kroz brojne primere – od kolektivnih građanskih akcija, kojima su intermedijatori poslužili kao platforma za razmenu informacija i grupisanje, do primera intermedijatora kao vratara, kada regulušu, odnosno uređuju informacije koje su u opticaju.

Kada je reč o pretraživačima postupkom rangiranja ponuđenih infromacija, favorizuju se određene informacije, dok se drugima umanjuje značaj. Na taj način pretraživači dodeljuju određeni status informacijama i utiču na njhovu vrednosnu klasifikaciju. Upravo zbog takvih značenjnskih odrednica uključenih u proces pretrage, koje su daleko od neutralnih tehničko-algoritamskih operacija koje intermedijatori stavljaju u prvi plan, Emili Lejdlou postavlja pitanje: „Zašto pretraživači imaju dužnost prema javnom interesu?" i odgovara: „Zato što oni kontrolišu naše informacijsko iskustvo" (Laidlaw, 2008: 123–137). Intermedijatori direktno oblikuju informaciono okruženje svakog korisnika, stoga je od izuzetnog značaja pitanje značaja promatranja njihovog poslovanja u kontekstu zaštite i promovisanja javnog interesa.

Analizirajući odgovornost internet intermedijatora prema javnom interesu, posebno pretraživača, Lejdlou navodi *četiri prioritetna izazova* u toj oblasti: „relevantne i nepristrasne rezultate pretrage, stepen transparentnosti, poštovanje korisničkog dostojanstva i sprovođenje nezavisnog mehanizma za žalbe" (Laidlaw, 2008: 137–144). Već je bilo reči o mnogobrojnim nepoznanicama koje korisnici imaju u vezi sa načinom rada algoritama uključenih u svaki čin pretrage. Uloga vratara intermedijatora sprovodi se tehnički, ali načini filtiranja i rangiranja nisu strogo neutralni i poseduju vrednosnu dimenziju. U tom kontekstu Lejdlou navodi i poteškoće koje onemogućavaju puno ostvarivanje navedena četiri izazova: prva se odnosi na dizajn algoritama, a druga je manualna manipulacija pretragom.

Kada je reč o kritici algoritamskog dizajna pretrage, ona se najpre odnosi na čin favorizovanja prilikom rangiranja pretrage, na taj način, pretraživači, putem svojih algoritama, kontrolišu protok informacija. Prosečni korisnik, na primer, prilikom pretrage nekog pojma dobije milione rezultata, ali najčešće preglada samo prvorangirane, uz minimalnu verovatnoću da će ikada pogledati one sajtove koji su među poslednjima, pa čak i na desetoj ili dvadesetoj stranici pretrage. Kada je reč o manualnoj manipulaciji, autorka razmatra dva najčešća načina: uklanjanje sadržaja nakon prijave o štetnom sadržaju i uklanjanje sadržaja od strane samog pretraživača – oba se vrlo često sprovode netransparentno.

Pod *manipulacijom* u ovom kontekstu podrazumevamo upravljanje informacijama u smislu uticaja na informacijsko iskustvo korisnika. Ovaj čin ne mora nužno da ima negativnu konotaciju, već može samo da upućuje na namerno upravljanje – na primer, blokiranje ili uklanjanje sadržaja, filtriranje sadržaja, favorizovanje sadržaja, uticaj na rangiranje sadržaja, kao i upošljavanje ljudi koji sprovode ove i slične aktivnosti. Jasno je da upravljanje štetnim sadržajem, odnosno njegovo blokiranje ili filtriranje, ne možemo okarakterisati kao negativnu praksu, ali ukoliko se ta mogućnost zloupotrebi, onda govorimo o upravljanju u negativnom smislu. Ukoliko se pod terminom *manipulacija* podrazumeva isključivo negativna praksa intermedijatora, to će biti jasno naglašeno, uglavnom kroz navođenje primera takvih negativnih praksi. Međutim, ono što je nedvosmisleno jeste da postoji mnogo načina na koje pretraživači dizajniraju rangiranje rezultata pretrage, filtriranje ili blokiranje sadržaja, i time direktno utiču na naše informacijsko iskustvo, što ih postulira kao značajne aktere u novom IKS i povlači sa sobom visok stepen odgovornosti.

Društvene mreže, kao i pretraživači, mogu algoritamski da upravljaju sadržajem koji će se pojavljivati na njihovim stranicama. Fejsbuk, na primer, upravlja rezultatima koji se pojavljuju na početnoj stranici - *NewsFeed* (Abbruzzese, 2014)[133] putem algoritama. Prosečan korisnik uviđa da se informacije na Fejsbuk *NewsFeed* ne pojavljuju hronološki, već na osnovu određene logike za koju se čini da favorizuje, na primer, interakciju sa određenim Fejsbuk prijateljima, ali i sponzorstvom određenih stranica. Na taj način Fejsbuk ima ulogu vratara, koji nam algoritamski nameće, odnosno uskraćuje, određene infromacije, vrednujući ih u odnosu na određeni interes, koji ne mora biti istovetan interesu korisnika.

Napoli izražava zabrinutost zbog „algoritamskog upravljanja javnim interesom" (Napoli, 2015: 756–757), ali i skreće pažnju na pogrešni pristup javnom interesu, kada je reč o intermedijatorima: „Javni interes kod intermedijatora je fokusiran na ono što ne bi trebalo da rade" (Napoli, 2014)[134]. Odnosno, autor smatra da je pristup javnom interesu kod intermedijatora fokusiran na *restrikcije*, a ne na *afirmaciju*. Na taj način, kada se polemiše o odgovornom poslovanju intermedijatora, konstantno se ističu negativne prakse, koje bi trebalo da se potisnu – kao što je narušavanje privatnosti, poštovanje autorskih prava, filtriranje pornografskog sadržaja – a gotovo da nema reči o pozitivnim praksama koje bi trebalo da uključe kako bi se približili ostvarivanju zahteva za javnim interesom, kao što je to, na primer slučaj sa tradicionalnim medijima.

Napoli piše o još jednom pristupu javnom interesu na internetu. Reč je o „individualističkom" pristupu, koji podrazumeva odgovorno korišćenje usluga internet intermedijatora od strane korisnika. To znači da većim delom od korisnika i njihovih aktivnosti zavisi da li će se izboriti za javni interes onlajn, načinom na koji koriste povoljnosti koje intermedijatori pružaju (Napoli, 2014). Ovaj pristup javnom interesu, sa jedne strane, poziva na odgovornost korisnika onlajn-usluga, što se ne može *per se* okarakterisati negativno. Intermedijatori, kao što su Gugl ili Fejsbuk, svojim uslovima korišćenja nameću određena pravila ponašanja korisnicima, ali bilo bi iluzorno očekivati da sami korisnici regulišu komunikaciju na ovim platformama. Individualna odgovornost jeste svakako poželjna, ali ona ne umanjuje odgovornost intermedijatora. Distribucija sadržaja komunikacije, čiji su kreatori korisnici, samo je mali deo usluga, koje pomenuti intermedijatori pružaju, a za koji bismo mogli smatrati

[133] Jason Abbruzzese. (Jul 14, 2014). **"**Seeing More Politics in Your News Feed? Facebook Boosts Partisan Sites". *Mashable*. Dostupno na: https://mashable.com/2014/07/13/facebook-politics-partisan-newsfeed/#b9NVIoG3maql (pristupljeno 05. 04. 2018. godine).

[134] Napoli, P. (2014). "Digital intermediaries and the public interest standard in algorithm governance". *LSE Media Policy Project Blog*. Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2014/11/07/digital-intermediaries-and-the-public-interest-standard-in-algorithm-governance/ (pristupljeno 04. 05. 2018. godine).

odgovornim korisnike. Ostale usluge prevazilaze domen sadržaja, nisu vidljive običnom korisniku, a čine najveći deo informaciono-komunikacione infrastrukture „na mreži“. Intermedijatori najvećim delom upravljaju njome, što ih neupitno čini odgovornim.

Kada je reč o društvenim mrežama, Napoli skreće pažnju na njihovu sve značajniju ulogu u informacionom ekosistemu i poziva na intenzivniji pristup u analizi njihovog uticaja i sprovođenja javnog interesa:

> „Vrlo je moguće (čak i verovatno) da će uloga društvenih mreža u proizvodnji, širenju i konzumiranju vitalnih vesti i informacija nastaviti da dobija na značaju, pa je važno razmotriti potencijalno šire implikacije načina na koji se javni interes oblikuje pri upravljanju društvenim mrežama, u nastojanju da se artikuliše i sprovede model upravljanja društvenim mrežama koji je više proaktivan nego reaktivan u odnosu na sve značajniju ulogu ovih platformi u proizvodnji, diseminaciji i potrošnji vesti i informacija” (Napoli, 2015: 758).

Akumulacija neslućene količine informacija postavlja pretraživače u sam centar informacionog ekosistema, kao posrednika između javnosti i informacionih provajdera. Društvene mreže, kao produkt interaktivnog interneta, *veb* 2.0, sve intenzivnije prodiru u srž procesa globalne diseminacije informacija, koja, kao što je već bilo reči, često može biti izmanipulisana, što direktno može da utiče na oblikovanje javnog stava o gorućim društveno-političkim pitanjima. Postavlja se pitanje: kako bi trebalo pristupiti izgradnji okvira za zaštitu javnog interesa od strane ne-medijskih aktera, s obzirom na njihovu centralnu ulogu u novom informacionom okruženju?

Mansel (Mansell, 2015) opravdava intervencije koje bi dovele do osiguravanja interesa javnosti: „Regulatorni okviri dizajnirani su da osiguraju, kakvu god tržišnu moć imali intermedijatori, da se ona upotrebljava na način koji je u skladu sa interesima potrošača i građana” (Mansell, 2015: 8). Sičnog je mišljenja i Šapiro (Shapiro, 1999):

> „U demokratskom društvu, oni koji kontrolišu pristup informacijama imaju odgovornost da podrže javni interes. S obzirom na njihovu moć nad tako važnim resursom, ovi vratari moraju preuzeti obavezu poverenika za veće dobro. Zaista, osim nekih jasnih naznaka da oni dobrovoljno nose ovaj teret, vlade bi trebalo da im to nametnu” (Laidlaw, 2008: 114, citira Shapiro, 1999).

Sa druge strane, Napoli naglašava neophodnost izgradnje jednog takvog okvira, ali i ostavlja prostor za drugačiji model, koji se ne bi zasnivao isključivo na restrikcijama i tradicionalnom konceptu javnog interesa u medijima:

> „Možda bi za digitalne posrednike mogao (i trebalo) biti izgrađen robusniji, ekspanzivni pojam javnog interesa na temelju utvrđenih principa medijske politike, poput pluralnosti, različitosti i lokalizma. Ili, možda bi trebalo da se pojavi nezavisno na način koji u potpunosti odražava posebne jedinstvene karakteristike interneta kao medijske platforme. U svakom slučaju, okviri upravljanja za ove platforme moraju da se razvijaju u skladu sa načinom na koji su se ove platforme razvile, tako da postoji veća saglasnost

između moći kojom upravljaju i odgovornosti koju bi trebalo da poseduju" (Napoli, 2014)[135].

Bez obzira na razlike u zamisli okvira koji bi trebalo da obezbedi ostvarivanje javnog interesa, da li je reč o restriktivnim merama ili pak o sasvim novom modelu specifičnom za novo okruženje, autori su saglasni da javni interes možemo i moramo tražiti i na internetu. To je naročito slučaj onda kada je reč o kompanijama koje, moglo bi se reći, upravljaju onlajn-životima korisnika, organizujući im informacije prema svom (algoritamskom) nahođenju i kreirajući im svet koji ih okružuje, onlajn i oflajn. Uticaj koji kompanije poput Gugla i Fejsbuka sada već potvrđeno ostvaruju nad milijardama ljudi dovoljan je razlog da se zahteva javni interes u njihovom poslovanju.

Komercijalna priroda neodvojivi je deo ovih giganata i ne bi bilo logično očekivati da će se proglasiti javnim servisima. Ipak, korak ka većoj odgovornosti svakako bi bio razmatranje okvira koji bi pored veće transparentnosti poslovanja uključivao i rad na neutralnijim mehanizmima pretrage i rangiranja sajtova i informacija. Centralni deo takvog okvira mora biti konstantan i intenzivan rad na odgovornosti prema korisnicima, uz prioritetno poštovanje njihovih prava, pre svega, prava na slobodno izražavanja, koje podrazumeva i pluralizam, pravo na informisanje iz različitih izvora, bez manipulativnih tehnika ponude potraživanih informacija. Takođe, pravo na privatnost, kao jedan od najvećih izazova koji se stavlja pred intermedijatore, mora biti poštovano u skladu sa interesima korisnika. Kako De Filipi sažeto konstatuje: „veliki podaci, velika odgovornost" (De Filippi, 2014).

Nakon što se navedenim izazovima pristupi odgovorno, možemo govoriti o pozitivnom pomaku ka izgradnji onlajn-sveta u kojem je javni interes bar podjednako važan koliko i komercijalni. Da bi kompanije dokazale svoju predanost viziji koja podrazumeva sigurniju-onlajn budućnost, moraju najpre da priznaju sebi i drugima da je njihova tehnološka priroda samo njihov hardver, dok njihov softver itekako ima ideološki pogon koji pokreće i kreira čitav jedan (onlajn) svet.

4.4. Samoregulatorna politika internet intermedijatora

Trendovi liberalizacije, deregulacije i privatizacije redefinisali su ulogu vlada i doveli do smene striktne regulacije sve učestalijim samoregulatornim praksama. Sve veća moć privatnih kompanija dovodi do zahteva za uređenjem komercijalnog okruženja na način koji bi uključio i društvenu odgovornost (Haufler, 2013). Samoregulatorni mehanizmi u tom kontekstu mogu se posmatrati kao efikasni način industrija da ostvare korektan odnos sa korisnicima, garantujući im poštovanje njihovih prava. Samoregulacija se može posmatrati i kao „dostizanje društvene reforme kroz promenu korporativnog ponašanja" (Haufler, 2013: 10). Sintagme „korporativna društvena odgovornost", „korporativno građanstvo", „poslovna etika" (Haufler, 2013: 12), „društvena odgovornost" i „moralnost industrije" (Price & Verhulst, 2000: 24) sve češće se koriste kako bi ukazale na nužnost postojanja odgovornosti privatnih kompanija prema korisnicima njihovih usluga i prema javnosti uopšte.

Samoregulacija nije nov vid regulatorne politike, specifičan za internet intermedijatore, ali je svakako dominantan u novom okruženju, počevši od nastanka interneta i insistiranja na isključivo

[135] Ibid.

samoregulatornim mehanizmima. Naime, prvobitni žitelji i kreatori internet prostora verovali su da će potpuno odsustvo regulacije interneta, odnosno prostor koji samoregulišu kreatori i korisnici, biti najbliži ostvarivanju ideala demokratizovanog prostora za otvorene debate i opunomoćavanja korisnika. U međuvremenu je došlo do značajnih promena u ovoj oblasti. Onlajn-prostor nije izbegao različite vidove regulacije i koregulacije, ali je samoregulacija ostala stožer onlajn-okruženja: „Na mnogo načina internet se može smatrati i jednim velikim samoregulatornim sistemom" (de Vey Mestdagh & Rijgersberg, 2010: 386).

Koncept samoregulacije podstiče različite pristupe pri analizi njegove učinkovitosti u stvaranju sigurnijeg internet prostora. Od pozicija sa kojih se samoregulatorna politika smatra jedinom ispravnom, preko zagovoranja istovremenog postojanja regulisanja i samoregulisanja, do ozbiljnih kritika samoregulacije internet intermedijatora, ova oblast nudi višestruke pravce analize (van Kokswijk, 2010; Price & Verhulst, 2000; Ang, 2001; Black, 2001). Kako bismo izbegli čestu zamku, teorijsku dihotomiju na striktnu regulaciju nasuprot samoregulaciji (Sinclair, 1997), u ovom potpoglavlju biće ponuđen osvrt na različite definicije i pristupe samoregulaciji – predočavaćemo i dobre i loše strane, sa posebnim akcentom na samoregulativne mehnanizme dominantne u internet okruženju.

Samoregulacija podrazumeva dobrovoljne prakse uređivanja nekog odnosa, na primer odnosa privatnih kompanija i njihovih korisnika. Iako volontersko, učešće kompanija i korisnika često poprima i formalne oblike kroz različite vidove obavezujućih dokumenata. Danas smo u fazi regulacije industrije koju prepoznajemo kao „korporativnu odgovornost", pod kojom se podrazumeva da nevladini sektor i civilni entiteti vrše pritisak na privatne kompanije kako bi zauzeli odgovoran stav prema društvu u celini (Haufler, 2013).

Haufler (Haufler) razlikuje dva modela samoregulatornog mehanizma industrija. Prvi proističe iz okruženja u kojem kompanije posluju, a koje donosi permanentne izazove kao posledicu globalizacije, transnacionalnog poslovanja, tehnološkog razvoja i slično. Ovi samoregulatorni mehanizmi „namenjeni su za olakšavanje međunarodne razmene dobara i usluga, povećanje ugleda industrije u celini i smanjenje troškova poslovanja" (2013: 9). Drugi model je „stran poslovnom umu", i „zasnovan je na društvenim ili političkim zahtevima izvan poslovne zajednice" (Haufler, 2013: 10).

Kada govorimo o samoregulaciji interneta, prepoznajemo oba navedena modela. Međutim, za našu temu, a kasnije i predmet analize, značajan je drugi model koji se, za razliku od prvog, ne odnosi na ekonomski aspekt poslovanja, već na društvenu odgovornost privatnih kompanija koje posluju na internetu. Drugi model samoregulacije direktno se tiče društvene odgovornosti intermedijatora – odgovornosti prema javnosti u celini – dok u njegovim segmentima, u užem smislu, prepoznajemo i odgovornost prema svakom pojedinačnom korisniku. Intermedijatori se obavezuju na odgovornost prema korisnicima, pre svega, kroz sklapanje elektronskog ugovora – uslovi korišćenja (engl. *Terms of Service*).

Slično Haufleru, Prajs i Verhalst (Price & Verhulst) razlikuju ekonomsku i socijalnu samoregulaciju:

> „Dok se prva odnosi na prilagođavanje tržišta ili druge aspekte ekonomskog života […] socijalna samoregulacija obično podrazumeva mehanizme u kojima preduzeća ili njihova udruženja u obavljanju poslovnih aktivnosti nastoje da osiguraju da se izbegnu neprihvatljive posledice za životnu sredinu, radnu snagu ili potrošače i klijente" (2000: 8).

Međutim, oba tipa samoregulacije međuzavisna su i neodvojiva, jer učinkovita socijalna samoregulacija, u vidu izgradnje klime poverenja, obezbeđuje bolje uslove poslovanja; „samoregulacija se može objasniti kao kolektivna ekonomska odluka, presek maksimiziranja profita i ostvarivanja javnog interesa" (Price & Verhulst, 2000: 7).

Džulija Blek (Julia Black) pod samoregulacijom podrazumeva: „različito meko pravo , kolektivne aranžmane koji mogu biti nepravni i /ili ne podrazumevaju nikakvo učešće vlade , bilateralne aranžmane između preduzeća i vlade , jednostrano usvajanje standarda, uključivanje industrije u formiranje pravila" (2001: 121). Autorka gradira intenzitet samoregulatornih obaveza i u skladu sa tim kriterijumom izdvaja i poseban vid samoregulacije koji se može ostvariti putem posebnih privatnih ugovora, što može značiti „intra-čvrstu regulaciju", dok, sa druge strane, izdvaja i niz praksi koje su nalik samoregulatornim, ali izlaze iz njenih okvira definisanja, kao što su: „koregulacija, kvazi regulacija, kvazi-zakon, meko pravo, volonterizam" (Black, 2001: 121).

Česta je zabluda da samoregulacija predstavlja apsolutno odsustvo regulatornih praksi. Samoregulatorna politika deo je šireg koncepta koji u sebe uključuje odnos sa vladom i oslanja se na formalne načine regulacije, bilo da ih dopunjava ili u nekom specifičnom aspektu menja. Samoregulacija svojim nazivom, isključivim "samo-" može navesti na pogrešan zaključak da je u konstruisanje njenih mehanizama uključena samo industrija; međutim, drugi deo složenice, "regulacija", ipak ukazuje na to da se ona konstituiše u okvirima vladinog delovanja, stoga ne predstavlja neki apstraktni koncept izolovan iz realnosti regulatornog okruženja u okviru kojeg posluju industrije (Black, 2001). Kada je reč o internet okruženju, na primer, samoregulatorni mehanizmi i norme ponašanja privatnih onlajn-kompanija ne proističu iz same industrije, bez učešća država, „norme se razvijaju kroz ono što bi moglo da se nazove 'razgovor' između industrije i vlade" (Price & Verhulst, 2000: 25).

Još jedna srodna i česta zabluda odnosi se upravo na veštački konstruisanu dihotomiju između regulacije i samoregulacije. Sinkler (Sinclair, 1997) ističe da su pogrešne teorijske postavke koje favorizuju ili striktnu ili samoregulaciju, i smatra da postoji bezbroj nijansi između ova dva ekstrema. Autor smatra da su oba vida regulacije pogrešno predstavljena stereotipno; regulacije se posmatra kao „glomazna", „kraj cevi" i „nedelotvorna za stvaranje promena u korporativnoj politici, organizaciji i strategiji koja će dovesti do ekološki održivih industrijskih praksi" i rezultira „kontradiktornim odnosima". Za razliku od toga, samoregulacija je predstavljena kao „prilagođena posebnim okolnostima pojedinih firmi" (Sinclar, 1997: 531).

Regulacija i samoregulacija često su predstavljene u suštinski opozitnom odnosu, uglavnom na način koji je priklonjen samoregulaciji, opisujući pretežno negativnim terminima regulatorne prakse. Ovakvo favorizovanje samoregulacije i otpor prema mešanju vlade u regulisanje poslovanja na internetu ima korene još iz perioda rano razvoja interneta i politike industrije kojom je zagovarana apsolutna sloboda u virtuelnom prostoru.

Međutim, i drugi autori saglasni su sa Sinklerom i smatraju da samoregulatorna politika može biti mnogo bolja i može da prevaziđe trenutnu limitiranost, ali i da joj je u tome neophodna saradnja sa državom, jer samoregulacija nije autonomna u odnosu na druge vrste regulacije, već se one dopunjuju: „samoregulacija nije jedini oblik regulacije i treba je razmatrati u kontekstu suživota sa drugim metodama regulacije" (Cannataci & Bonnici, 2003: 52). Moglo bi se reći da samoregulacija gotovo ne može da postoji bez nekog odnosa prema državi: „Značaj samoregulacije se pomera u zavisnosti od stepena državne prisile ili učešća i od tačne percepcije javnosti o odnosu privatnog sektora i države" (Price & Verhulst, 2000: 3).

Na primeru internet (samo)regulacije očigledni su primeri kada je poželjno, pa čak i neophodno uključivanje vlada u razrešenje dela koja se karakterišu kao krivični prestupi. Upravo zbog toga „samo-samoregulacija onlajn-zajednice nije dovoljna", jer postoje slučajevi kada „ekstremno ponašanje u onlajn-zajednicama često provocira autsajdere da pozivaju na mere vlade. Pa ipak, samoregulacija je prvi i najbolji izbor" (van Kokswijk, 2010: 244).

Kada govorimo uopšteno o mehanizmu samoregulacije, pod njom se podrazumeva proces od izgradnje odgovarajuće politike, kojom se definiše odnos prema drugim licima, preko instrumenata kojima se usvojena politika sprovodi, i na kraju evaluacija uspešnosti, odnosno procena efikasnosti sprovedenih mera. Haufler ovaj proces detaljnije obrazlaže i navodi da samoregulatorne politike uključuju:

> „korporativna pravila ponašanja koja postavljaju društvene obaveze kompanije; menadžment i računovodstveni sistem koji prevode ove obaveze u specifične uloge i odgovornosti unutar organizacije; impelemntaciju programa koja uključuje troškove resursa za postizanje specifičnih ciljeva; monitoring, reviziju, sertifikovanje i označavanje programa koji svedoče o uspešnom postignuću" (Haufler, 2013: 12).

U odnosu na to da li se samoregulatornim mehanizmima kompanije obavezuje u odnosu prema vladama, korisnicima, prema drugim kompanijama ili se pak samoregulišu odnosi zaposlenih možemo razlikovati mnogobrojne instrumente samoregulacije. Prajs i Verhalst (2000) razlikuju kodeks ponašanja, principe, kodove, smernice i preporuke. „Kodeks ponašanja je dizajniran da zaštiti javni imidž organizacije ili industrije i da ga poboljša u određenoj meri, deklarisanjem svojih moralnih standarda" (Price & Verhulst, 2000:34). Kada je reč o kodeksu ponašanja internet intermedijatora, autori navode da se oni uglavnom odnose na „saradnju sa vladinim telima, preuzimanje odgovornosti, zaštitu privatnosti, odnos prema privatnim podacima, zaštitu od štetnih materijala i slično" (Price & Verhulst, 2000: 34–35).

U odnosu na „snagu obaveza koje se nameću industriji", autori gradiraju jačinu ostalih instrumenata samoregulacije od *principa*, koji su najvišeg ranga „bliski nespornim aksiomima koje bi svi članovi industrijskog udruženja trebalo da prihvate kao očigledne"; preko *kodeksa* koji se tiču nekih specifičnih pravila, a „čija kršenja najverovatnije izazivaju neku opomenu ili disciplinsku meru"; do *smernica* i *preporuka* koje su najmanje obavezujuće, „jer su problemi novi, fluidni i/ili teški za jasno opisivanje tako da precizna (ili teška) pravila nisu moguća" (Price & Verhulst, 2000: 36)[136].

Kol (Kohl, 2012) ističe najmanje dva razloga zbog kojih su intermedijatori tako atraktivni akteri u pogledu regulacije sadržaja na internetu: prvo, zbog toga što je vladama lakše da sankcionišu posrednika, nego da u svakom pojedinačnom slučaju lociraju i sankcionišu primarnog krivca. Drugo, kontrola od strane intermedijatora može da se odnosi i na period pre nepravednog postupka, što intermedijatori čine posredstvom različitih mehanizama nadgledanja, a što Kol prepoznaje kao Fukoovo „disciplinovanje društva" stvaranjem „savršenog panoptikona" (2012: 186, 188). Međutim, Mjuler (Mueller) smatra da je došlo do „zablude pomerene kontrole", podrazumevajući pod tim da je politika koja propagira kažnjavanje intermedijatora za nedela počinjena od strane korisnika zapravo

[136] „Iskrenost, pristojnost, pošteno trgovanje i slično su obično podložni ovakvom slabijem tretmanu. U oblasti reklamiranja, samoregulativni sistemi sve više izdaju preporuke, pre nego čvrsta pravila iz straha da previše eksplicitni jezik povećava opasnost da se dobrovoljni kodeksi transformišu u zakone i regulativu"(Price & Verhulst, 2000: 36).

pogrešna, jer „fokusirati se na platformu umesto na aktera promoviše opasnu ideju da vlada treba da reguliše generičke tehnološke mogućnosti a ne loše oblike ponašanja *per se*" (Mueller, 2015: 804).

Samoregulacija kao koncept često je kritikovana, ali najčešći razlog kritike odnosi se na *polaganje poverenja u privatne kompanije da će raditi u skladu sa interesom korisnika*, premda su one primarno komercijalne prirode i prevashodno vođene ostvarenom dobiti: „Smatra se da samoregulacija nikada ne ide protiv interesa (samo-) regulatora" (Ang, 2001: 5). Samoregulacija je najefikasnija onda kada se interes industrije poklapa sa interesom korisnika:

> „Kada postoji značajan jaz između javnog interesa i privatnog interesa industrije, naivno bi bilo osloniti se na asocijaciju industrije koja dobrovoljno preduzima korake u javnom interesu, osim ako ne postoji neki spoljašnji pritisak da se to uradi (obrazloženje šargarepe i štapa). Ovo može da potiče iz različitih izvora, od kojih najvažnije uključuju pretnju direktne vladine intervencije (prisilnu samoregulaciju), širu brigu za održavanje kredibiliteta i legitimiteta (i kao rezultat komercijalnu dobit) i samo tržište" (Price & Verhulst, 2000: 19).

Sledeća kritika samoregulacije upućena je na *račun same prirode onlajn-okruženja, odnosno mnogobrojinih aktera i agenasa koji su u tom prostoru aktivni*. Iako se čini da je to jedan bezgranični pretežno monolitni prostor, samoregulativni mehanizmi ne mogu biti jedinstveni i standardizovani. „Samoregulatorna rešenja verovatno su prikladnije razvijena na nivou sektora" (Price & Verhulst, 2000: 20). Samoregulatorni instrumenti prilagođavaju se i najistnijim segmentima onlajn-okruženja, koje mogu činiti čak i pojedinačni akteri, na primer individualne blog stranice, ali i kompanije enormnih veličina, kakav je, na primer, Gugl. Ukoliko se zadržimo na primeru ove velike kompanije, čak ni ona ne može da jedinstvenim samoregulatornim aktom obuhvati sve oblasti delovanja i sve svoje usluge i servise. Sve to čini samoregulaciju složenom u meri koja otežava ne samo teorijsko razumevanje, već i praktičnu primenu. Upravo na to ukazuje i Ang navodeći sledeće: „Samoregulacija je teža i manje efikasna kada uključuje veliku i heterogenu grupu agensa" (Ang, 2001: 5). Prajs i Verhalst saglasni su sa navedenim poteškoćama: „U slučaju interneta, vrlo decentralizovana priroda i deregulatorna etika koja ga prožima čini posebno teškim da se definiše ko je sam (predmet samoregulacije ili koji je uključen u njegovu nadležnost)" (Price & Verhulst, 2000: 20).

Uprkos navedenim kritikama, samoregulacija ima i mnogobrojne prednosti. Pozivajući se na Drezdena (2004), Van Koksvijk navodi i razloge zbog kojih je samoregulacija u ovoj oblasti učinkovita i jednostavnija od drugih oblika uređivanja. Pre svega, samoregulacija nekada uključuje mnogo više pravila od drugih oblika uređivanja, na primer regulacije, što pogoduje segmentiranom onlajn-okruženju; samoregulacija je delotvorna u kooperaciji sa vladom; „nije nepovezana sa dostupnošću efikasnih pravnih sredstava" i „samoregulacija olakšava zadatke vlade i administrativnih sudova, ali pojačava žalbu građanskim sudovima" (van Kokswijk, 2010: 242).

Samoregulatorna politika je obuhvatnija od zvaničnih politika vlada u ovoj oblasti, uključuje više aktera i može da odgovori interesima svih zainteresovanih ili uključenih strana, u tom smislu deluje kao dopuna ili korektiv. Svakako je nije moguće posmatrati izvan regulatornih tokova i nije samo skup apstraktnih idealizovanih prava i obaveza, već može predviđati i formalno-pravno sankcionisanje, a da opet ne izgubi na fleksibilnosti, koja pogoduje stalno promenljivom okruženju.

Ang ističe: „Industrije koje su brzog razvoja, kao što je internet, manje formalni procesi samoregulacije čine fleksibilnijim i stoga je manje verovatno da će ugušiti inovacije ili preterano ograničiti izbor potrošača" (2001: 5). Ang nizu prednosti dodaje i prednost samoregulisanja struke,

koja je specifična i zahteva znalačke sposobnosti i veštine u domenu tehničkih nauka: „Industrija je ta koja ima najbolju sposobnost da kontroliše kvalitet i prepozna niske standarde", i prednostima dodaje ekonomski aspekt: „pošto industrija snosi troškove regulacije, ona ima podsticaje za smanjenje troškova izvršenja i usklađivanja" (Ang, 2001: 5).

Na kraju, samoregulacija ne doprinosi samo povećanju društvene odgovornosti i zaštiti javnog interesa, ona je u vezi sa izgradnjom boljeg okruženja poslovanja, i svakako je i komercijalno isplativa. Izgradnja bezbednog okruženja i klime poverenja je dugotrajni proces, ali se uspeh kompanija koje pružaju internet usluge meri brojem korisnika, čiji se zahtevi za poštovanjem parava korisnika moraju postaviti kao prioritet, ukoliko kompanija pretenduje da dugoročno posluje profitabilno. Stožer industrija na internetu jeste poverenje korisnika. Jedino što korisnik može da očekuje od kompanija čije usluge koristi jeste da ne iznevere njegovo poverenje u virtuelnom prostoru – ukoliko pak do toga dođe šteta može biti nenadoknadiva.

4.4.1. *Uslovi korišćenja* kao samoregulatorni instrument

Ukoliko samoregulatornu politiku posmatramo samo kroz odnos kompanija prema krajnjim korisnicima, jasno je da bi rukovodioci/vlasnici privatnih kompanija koje pružaju internet usluge, a koje pretenduju da posluju društveno odgovorno, trebalo najpre da imaju izgrađenu svest o svojoj odgovornosti; odnosno, viziju o tome kako da svoj interes uspešno prilagode interesu korisnika i sve to instrumentalizuju kroz samoregulatorne mere. Najčešći oblik takvog vida samoregulacije prepoznajemo u *uslovima korišćenja* kojima internet intermedijatori sklapaju jednu vrsta ugovora između kompanije i korisnika, definišući pravila ponašanja i horizont očekivanja. Pojednostavljeno taj proces možemo opisati na sledeći način:

> „Internet zajednicu kreira provajder ili razvojni programer. Ovaj programer označava granice unutar kojih mogu učestvovati učesnici ovog virtuelnog sveta. Dakle, na početku regulacija onlajn-okruženja sastoji se od okvira koje pruža provajder ili programer, koji se povezuje sa (inter)nacionalnim socijalnim konvencijama putem samoregulacije. U ugovoru 'uslova korišćenja' sa učesnicima virtualnog sveta programer postavlja međusobna prava i obaveze" (van Kokswijk, 2010: 240).

Uslovi korišćenja, „preduslovi unutar kojih se igra igra" (van Kokswijk, 2010: 243), definišu, sa jedne strane, pitanja odgovornosti i obaveza intermedijatora, kao što su poštovanje prava na privatnost, prikupljanje i skladištenje ličnih podataka, ali i njihova prava u pogledu mogućnosti za pristupanje ličnim podacima i njihovo korišćenje u unapred definisane svrhe; sa druge strane, definišu se prava i obaveze korisnika. Korisnicima je uvek predočena mogućnost prihvatanja ili odbijanja uslova, koje ukoliko prihvate imaju snagu svojevrsnog privatnog ugovora dve zainteresovane strane. Upravo to i jeste osnovna ideja i ideal samoregulacije: „da zajednica može stvarati sopstvenu politiku kroz razvoj normi ponašanja, privatnog zakona koji se sprovodi ugovorom, tehnološke arhitekture ili nekom kombinacijom ova tri" (Weiser, 2001: 824).

Međutim, i ovaj vid samoregulacije podložan je kritikama koje se najčešće odnose na razumljivost i transparentnost uslova koji se pred korisnike stavljaju. Naime, čest je slučaj da internet korisnici automatski prihvataju uslove korišćenja bez prethodnog čitanja, što zbog nedostatka vremena

za iščitavanje redova i redova složenih rečeničnih konstrukcija, što zbog nerazumljivosti ponekad krajnje složenih pravnih i tehničkih termina. Upravo na to misli Van Koksvijk (Van Kokswijk) kada uslove korišćenja opisuje sintagmom „ugovori 'koji dave'"(2010: 243). Takođe, autor dodaje da složenost tekstova u ovim neformalnim ugovorima dovodi i do netransparentnih odluka provajdera da pojedince na primer sankcioniše izopštavanjem iz zajednice: „Nerazumni uslovi na osnovu kojih učesnicima može biti uskraćen pristup u onlajn -okruženju bez navođenja razloga ili na osnovu kojih su izrečene sankcije" (van Kokswijk, 2010: 243).

Čest je slučaj da pojedinac bude isključen kao učesnik virtuelne zajednice društvenih mreža, zbog, na primer, prijava drugih korisnika, zbog činjenja dela koja su uslovima korišćenja zabranjena, a sa kojima nije bio upoznat usled nerazumevanja uslova korišćenja. Međutim, na isti način može doći i do zloupotrebe ovog samoregulatornog mehanizma, kada se zbog lažnih prijava korisnik izopštava iz onlajn-zajednice.

Zbog svih navedenih prednosti i mana samoregulacije smatramo da ključ bezbednog (bezbednijeg) internet prostora možemo pronaći u sprezi samoregulacije i regulacije. Samoregulatorne politike internet kompanija usklađuju se sa opštom regulativom kojom se uređuje data oblast. Na primeru Gugla i Fejsbuka, tačnije njihovog odnosa prema pravima svojih korisnika, lako možemo uočiti ovu praksu, koja će u nastavku biti predmet detaljne analize. Naime, samoregulatorna politika ovih kompanija, koja se, kada je reč o odnosu sa korisnicima, ogleda u „uslovima korišćenja", usklađuje se sa opštim regulatornim okvirom regiona u kojima posluju. Regulatorni okvir EU u oblasti poštovanja prava na privatnost ili slobodu izražavanja, na primer, diktira samoregulatornu politiku Gugla i Fejsbuka, a usklađivanje sa njim i njegovo poštovanje uslovljava poslovanje ovih kompanija u datom geografskom područuju – u kontekstu ovog rada reč je o EU zoni.

4.5. Politike Gugla i Fejsbuka u kontekstu evropske regulative

Da bi privatna kompanija poslovala na internetu, ona mora da poštuje regionalni, odnosno nacionalni regulatorni okvir. Intenzitet usaglašavanja poslovanja sa regionalnim, odnosno nacionalnim zahtevima varira u odnosu na to o kojoj kompaniji je reč i o kojoj državi, odnosno o kom regionu je reč. U poređenju sa Sjedinjenim Američkim Državama, na primer, EU ozbiljnije pristupa izazovu osiguravanja prava na privatnost, odnosno zaštiti podataka o ličnosti, naročito u novom tehnološkom dobu. Kada je reč o kompanijama poput Gugla ili Fejsbuka, čija je zemlja matica SAD, a koje posluju van njenih granica, regulativa koja se primenjuje na ove kompanije kada posluju na teritoriji evropskih zemalja jeste zvanična politika EU (Esteve, 2017).

Međutim, postoji razlika u osetljivosti ovih kompanija na nacionalne/regionalne zahteve. Politiku Gugla, na primer, mogli bismo da opišemo sintagmom – *isti za sve*. Gde god na svetu koristite usluge kompanije Gugl, zaštita vaših podataka biće ista: „bez obzira na to gde se obrađuju vaši podaci, primenjujemo iste nivoe zaštite koji su opisani u politici privatnosti" [137]. Međutim, svestan evropske osetljivosti na pitanja privatnosti, Gugl kroz posebne mehanizme svoje poslovanje usklađuje sa EU regulativom. Takođe, kompanija Gugl obavezala se na poštovanje „Štita privatnosti" (*Privacy Shield*) kojim se reguliše prenos podataka između zemalja EU i Švajcarske i SAD:

[137] Gugl, *Pravni okvir za prenos podataka*, dostupno putem linka (pristupljeno 21. 10. 2018. godine).

„EU-SAD i Švajcarska-SAD Okviri za zaštitu privatnosti dizajnirani su od strane Američkog ministarstva trgovine i Evropske komisije i Švajcarske administracije, kako bi se kompanijama sa obe strane Atlantika obezbedio mehanizam za usklađivanje sa zahtevima za zaštitu podataka pri prenosu ličnih podataka iz Evropske unije i Švajcarske u Sjedinjene Američke Države, sa ciljem podrške transatlanskoj trgovini" [138].

Na ovaj način Gugl se obavezuje da će prilikom poslovanja u zemljama EU politiku privatnosti sprovoditi u skladu sa obavezama propisanim regulatornim okvirom EU: „Da bismo prenosili podatke iz Evropskog ekonomskog prostora u druge zemlje, na primer, Sjedinjene Američke Države, pridržavamo se pravnih okvira koji uspostavljaju nivo zaštite ekvivalentan nivou zaštite koji pruža zakon Evropske Unije"[139]. Dakle, politika privatnosti Gugla ista je svuda u svetu, a izgrađena u skladu sa EU propisima.

Sa druge strane, politika kompanije Fejsbuk je *nacionalno fleksibilna*, odnosno osetljivija na nacionalnu regulativu. Bez obzira na opšti regulatorni okvir EU, politika privatnosti Fejsbuka razlikuje se i u zemljama EU, kada su nacionalni zahtevi specifični i nisu predviđeni opštom regulativom. Način na koji Fejsbuk usklađuje svoje poslovanje sa posebnim nacionalnim zahtevima biće detaljno opisan na primeru Nemačke u sledećem poglavlju.

Drugo pravo koje je predmet analize jeste pravo na slobodno izražavanje, koje se, takođe, u novom tehnološkom okruženju usložnjava. Čak i onda kada u nekom zakonskom aktu EU nije eksplicitno naglašeno, ono se podrazumeva i predstavlja temeljno ljudsko pravo. S obzirom na ulogu i uticaj koji Gugl i Fejsbuk imaju u globalnoj diseminaciji informacija, neupitna je njihova povezanost sa ostvarivanjem prava na slobodno izražavanje, odnosno prijemom i širenjem informacija, stoga se drugi deo analize njihovog poslovanja odnosi na mogućnosti ostvarivanja ovog prava.

U nastavku poglavlja biće detaljno analizirani uslovi korišćenja Gugla i Fejsbuka u delu koji se tiče zaštite privatnosti/podataka i uticaja na slobodu izražavanja u kontekstu evropske regulatorne politike. S obzirom da je Guglova politika privatnosti ista svuda u svetu, ona će kao predmet analize biti upoređena sa regulatornim okvirom EU, kako bi se utvrdilo da li je Gugl svojom samoregulatornom politikom odgovorio na zahteve EU. Sa druge strane, kompanija Fejsbuk je specifičnija u pogledu usklađivanja samoregulatorne prakse – uslova korišćenja, sa nacionalnim/regionalnim zahtevima. Da bismo uporedili politiku privatnosti i uticaj na slobodu izražavanja Fejsbuka sa regulatornim okvirom EU, za predmet analize uzeli smo uslove korišćenja preuzete u Austriji. Samoregulatorna politika Fejsbuka u Austriji, kao zemlji članici EU, morala bi da bude usklađena sa EU regulativom, stoga smatramo da ćemo poređenjem EU regulative i politike Fejsbuka u ovoj zemlji, dobiti najobjektivnije rezultate analize. Politika Fesjbuka u Srbiji ne mora nužno da odgovara politikama u zemljama EU, jer Srbija nije članica Evropske unije, zbog toga analiziramo politiku Fejsbuka preuzetu u Austriji, a ne u Srbiji.

Cilj ove analize jeste da se odgovori na postavljeno istraživačko pitanje:

[138] *Privacy Shield*, dostupno na linku: https://www.privacyshield.gov/welcome (pristupljeno 21. 10. 2018. godine).
[139] Gugl, *Pravni okvir za prenos podataka*, dostupno na linku: https://policies.google.com/privacy/frameworks?hl=sr (pristupljeno 21. 10. 2018. godine).

- ***Da li je samoregulatorna politika internet intermedijatora u delu koji se tiče poštovanja prava na privatnost i slobodu izražavanja u skladu sa interesima korisnika?***.

Odnosno da se testira hipoteza:

- *Samoregulatorna politika internet intermedijatora ne garantuje apsolutnu zaštitu prava na privatnost i slobodno izražavanje korisnicima.*

4.5.1. Samoregulatorna politika Gugla

Jedna od najpoznatijih internet kompanija na svetu danas, Gugl, svoju istoriju ispisuje još sredinom devedesetih godina, kada su dva studenta Univerziteta Stenford, Lari Pejdž (Larry Page) i Sergej Brin (Sergey Brin), otpočeli naizgled bezazlenu studentsku saradnju. Gugl je kompanija koja je, moglo bi se reći, ostvarenje američkog sna. Od prvobitnog radnog prostora, garaže, njegovi osnivači svoju kompaniju, koja danas radi u više od 50 zemalja, sa više od 60 hiljada zaposlenih, doveli su do velelepnog kompleksa, Guglpleksa (*Googleplex*)[140].

Gugl je danas mnogo više od internet pretraživača. Iako je najposećeniji sajt u 2018. godini, sa dnevnim posetama 7,89[141], fokus kompanije nije samo internet poslovanje. Gugl poseduje mnoštvo drugih kompanija i ulaže u različite oblasti od robotike do zdravstva[142]. Najpoznatije internet kompanije kojima upravlja Gugl jesu: *YouTube*, *Google Drive*, *Google Maps*, *Android*, *Google Chrome*, *Google Play*[143]. Kompanija Gugl je od 2015. godine pod okriljem kompanije Alfabet (engl. Alphabet)[144], konglomerata koji predvode osnivači Gugla i reprezent je pravog finansijskog i tehno giganta.

S obzirom na neizmerni udeo koji Gugl ima u oblasti globalne komunikacije i informisanja, kao i na već pomenute izazove ostvarivanja javnog interesa i etičkog poslovanja, otvaraju se i nova pitanja odgovornosti, u ovom slučaju prema krajnjim korisnicima. Koliko Gugl vodi računa o svojim korisnicima, da li su njihova sigurnost i prava na listi prioriteta ovog giganta i da li svoje poslovanje usklađuje sa regulatornim okvirom u oblasti prava na privatnost i slobodu izražavanja, pitanja su

[140] Istorijat Gugla dostupan na njihovom sajtu: https://www.google.com/about/our-story/ (pristupljeno 23. 06. 2018. godine).
[141] *Alexa*, dostupno putem linka: https://www.alexa.com/topsites (pristupljeno: 20. 05. 2018. godine).
[142] Biznis insajder navodi listu najznačajnijih Guglovih akvizicija među kojima su i kompanija koja se bavi proizvodnjom energije „Makani Power — Clean energy" , ocenjivanjem restorana „Zagat" , dronovima koji rade na principu solarne energije „Titan Aerospace" , do kompanija koje se bave eksperimentalnim istraživanjem nervnog sistema, po principu eksternog kompjuterskog nadražaja „DNNresearch Inc. " . Dave Smith. (Aug. 12, 2014). „ The 11 Most Important Google Acquisitions Ever". *Business Insider*. Dostupno na: http://www.businessinsider.com/important-google-acquisitions-2014-8 (pristupljeno 23.06.2018. godine).
[143] *Stash Invest*, dostupno putem linka: https://learn.stashinvest.com/companies-brands-owned-google (pristupljeno 23. 06. 2018. godine).
[144] Više o kompaniji videti putem linka: https://abc.xyz/ (pristupljeno 26. 06. 2018. godine).

kojima ćemo se baviti u nastavku. Pravo na privatnost, odnosno zaštita ličnih podataka, i pravo na slobodno izražavanje centralna su tema disertacije, pa shodno tome i analize politike kompanije Gugl.

GDRP, kojim se štite privatnost i lični podaci na internetu, na snazi je od maja 2018. godine, te će analiza poštovanja privatnosti i zaštite ličnih podataka Gugla biti sprovedene u komparaciji sa smernicama koje propisuje regulativa EU, a sa ciljem utvrđivanja stepena poštovanja ovih smernica, budući da je njegovo poslovanje na tlu EU uslovljeno upravo njihovim poštovanjem. GDPR nedvosmisleno ističe da se odnosi na obradu ličnih podataka „nezavisno od toga obavlja li se obrada u Uniji ili ne" (član 3 - ***Teritorijalno područje primene***).

Kada je reč o novinama koje je novi regulatorni okvir za zaštitu privatnih podataka – GDPR doneo, Evropska komisija posebno ističe: *jezik, pristanak, transparentnost, jača prava* i *snažnije primenjivanje tih prava*[145]. Jezik kojim entiteti koji obrađuju podatke o ličnosti pojašnjavaju svoju politiku privatnosti mora biti jednostavan i razumljiv. Mora postojati *afirmativni pristanak,* odnosno korisnici moraju da razumeju na šta pristaju i da to svesno učine. Prenošenje podataka izvan EU mora biti jasno istaknuto i transparentno, kao i način na koji će se prikupljeni podaci koristiti. Posebno značajne dve stavke odnose se na "pravo na pristup" svojim podacima i "pravo na zaborav", odnosno pravo na brisanje podataka. Snažnija primena ovih prava biće omogućena kroz rad posebnih tela za zaštitu podataka, koja su do sada imala malu i ograničenu mogućnost delovanja.

Trebalo je da svi entiteti koji se u nekoj meri bave obradom ličnih podataka do stupanja na snagu regulatornog okvira EU o ličnim podacima (maj, 2018) usklade politike privatnosti sa načelima sadržanim u GDPR. Ovaj zahtev odnosi se i na privatne kompanije na internetu koje sa svojim korisnicima sklapaju tzv. elektronske ugovore, kroz prihvatanje *Uslova korišćenja*, a kojima se definišu prava i obaveze između dve strane (van Kokswijk, 2010; Weiser, 2001).

U okviru Guglovih *Uslova korišćenja*[146] (poslednja izmena 25. oktobra 2017. godine) korisnici su na samom početku upozoreni da moraju poštovati sve smernice i pravila korišćenja. Sledeći i najobimniji segment *Uslova* jeste upravo zaštita privatnosti i ličnih podataka. Kako bi se upoznali sa politikom privatnosti, Gugl korisnike vodi na poseban link posvećen ovom pitanju. Trenutno aktuelna Guglova *Politika privatnosti*[147] stupila je na snagu 25. maja 2018. godine, što znači da bi trebalo da bude u potpunosti usklađena sa novom opštom regulativom EU u ovoj oblasti.

Analiza. Na početku, *Politikom* se poručuje: „Kada koristite naše usluge, poveravate nam svoje informacije. Shvatamo da je to velika odgovornost i stvarno se trudimo da zaštitimo vaše informacije i omogućimo vam kontrolu nad njima."[148] Novi regulatorni okvir EU predviđa snažnije mere upravljanja ličnim podacima i rigoroznije se odnosi prema pružaocima usluga koji obrađuju podatke korisnika. Jedna od najznačajnijih promena u odnosu na *Direktivu 95/46* jeste nedvosmislen zahtev za upoznavanjem korisnika sa informacijama koje se prikupljaju, kao i sa načinom na koji se te informacije dalje obrađuju, prosleđuju trećim licima i na kraju skladište i čuvaju. Transparentnost u

[145] *Evropska komisija*: Nova era zaštite podataka u EU: Šta se menja nakon maja 2018. Videti putem linka: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf (pristupljeno 20. 06. 2018. godine).
[146] Uslovi korišnjenja usluga, Gugl, dostupno putem linka: https://policies.google.com/terms (pristupljeno 23. 06. 2018. godine).
[147] Politika privatnosti, Gugl, dostupno putem linka: https://policies.google.com/privacy (pristupljeno 23. 06. 2018. godine).
[148] Ibid.

pogledu prikupljanja podataka, koji se potom obrađuju, jasno je istaknuta u GDPR (član 5 i Uvodna odredba (39)). Da bi obrada podataka bila zakonita, korisnici moraju nedvosmisleno biti upoznati sa vrstom informacija koje se prikupljaju, i to jednostavnim jezikom, kao i upozoreni na eventualne rizike.

Kada je reč o Guglu, u segmentu *Informacije koje Gugl prikuplja*, nudi se vrlo šturo opšte pojašnjenje:

> „Prikupljamo informacije da bismo svim korisnicima pružili bolje usluge – od otkrivanja nekih osnovnih stvari, kao što je jezik koji govorite, do nekih složenijih, kao što su oglasi koje ćete možda smatrati korisnim, ljudi koji su vam najbitniji onlajn ili Jutjub video snimci koji bi mogli da vam se svide. Informacije koje Gugl prikuplja i način na koji ih koristi zavise od toga kako koristite usluge i kako upravljate kontrolama privatnosti"[149].

U nastavku se velikim boldiranim slovima ističe: „Želimo da razumete tipove informacija koje prikupljamo dok koristite usluge"[150]. Premda Gugl ističe da razume značaj prikupljanja informacija i svoju odgovornost u tom kontekstu, kao i da želi da korisnicima približi i pojasni kako taj sistem funkcioniše, to čini vrlo šturo i jezikom koji nije prilagođen prosečnom korisniku njegovih usluga, iako je, da bi pristanak korisnika bio validan, uslov jednostavnog jezika u GDPR (član 7) istaknut kao jedan od najznačajnijih.

Gugl nudi poseban link ka pojašnjenju ključnih termina[151], što predstavlja pozitivni korak u naporu da korisnicima približi tehničke termine. Međutim, i u ovom segmentu postoje nelogičnosti. Kada, na primer, Gugl navede da čuva podatke i kada korisnik nije prijavljen pomoću posebnih identifikatora, a kada je korisnik prijavljen onda se prikupljaju i čuvaju podaci koje Gugl smatra „ličnim podacima", nije jasno koje su to tačno informacije koje Gugl prikuplja i čuva i smatra „ličnim podacima". Ukoliko korisnik potraži ovaj termin u „ključnim terminima" dolazi do objašnjenja da se pod tim podrazumevaju podaci koje sami korisnici daju poput imena, prezimena, broja telefona, ali i: „informacija za obračun ili drugih podataka koje Gugl osnovano može da poveže sa takvim informacijama, kao što su informacije koje povezujemo sa Gugl nalogom"[152]. Poslednja rečenica kojom se lični podaci određuju kao *informacije koje Gugl može osnovano da povezuje sa nekim drugim informacijama* prilično neodređeno definiše o kojim tačno informacijama je reč, čime se krši član 7, o jednostavnom i jasnom jeziku, ali i član 5, o transparentnosti vrste podataka koji se prikupljaju.

U nastavku *Politike*, u delu „Stvari koje pravite ili nam pružate", jasnije se određuju vrste podataka koje Gugl skladišti i čuva. Međutim, u ovom delu je odgovornost, čini se, već u startu prebačena na korisnika, jer to su stvari koje „vi" pravite i koje „vi", kao korisnik pružate Guglu. Odabir reči „pružati" može da sugeriše da korisnici aktivno učestvuju u procesu prikupljanja informacija i bez zadrške daju svoje informacije i podatke Guglu na raspolaganje. Reč je, pored već navedenih ličnih podataka, o imenu, broju telefona, mejl adresi, i o sadržaju koji korisnici otpremaju ili primaju: „To obuhvata stvari poput imejlova koje pišete i primate, slika i video snimaka koje čuvate, dokumenata i

[149] Ibid.
[150] Politika privatnosti, u delu: Informacije koje Gugl prikuplja, dostupno putem linka: https://policies.google.com/privacy#infocollect (pristupljeno 23. 06. 2018. godine).
[151] Ključni termini, Gugl, dostupno putem linka: https://policies.google.com/privacy/key-terms#toc-terms-personal-info (pristupljeno 23. 06. 2018. godine).
[152] Ibid.

tabela koje pravite i komentara koje ostavljate na Jutjub video snimke".[153] Iz navedenog je jasno da se spisak tu ne završava, jer to su samo neke od stvari, ili stvari poput navedenih. Pored toga što je spisak informacija koje se prikupljaju neodređen i nedovršen, podaci poput mejlova ili komentara mogu se smatrati prekomernom obradom, jer GDPR članom 5 (c) jasno ističe da podaci koji se prikupljaju moraju biti *relevantni*, *ograničeni*, *primereni* u skladu sa svrhom, i sa ciljem *smanjenja količine podataka*.

Pored sadržaja koji kreiraju korisnici i njihovih ličnih podataka, Gugl prikuplja i informacije o uređajima i aplikacijama svojih korisnika, što jasno i navodi kroz sledeći segment „Informacije koje prikupljamo dok koristite usluge". Spisak ovih informacija je dug, ali između ostalog uključuje: „jedinstvene identifikatore, tip i podešavanja pregledača, tip i podešavanja uređaja, operativni sistem, informacije o mobilnoj mreži, uključujući naziv mobilnog operatera i broj mobilnog telefona, i broj verzije aplikacije"[154].

Pored informacija o uređajima i aplikacijama, Gugl prikuplja i informacije o aktivnostima korisnika („Vaše aktivnosti") koje uključuju: „termine koje tražite, video-snimke koje gledate, glasovne i audio informacije kada koristite audio funkcije, […] aktivnosti na sajtovima i u aplikacijama trećih strana koji koriste naše usluge"[155]. Posebno pojašnjena aktivnost koju Gugl prikuplja o svojim korisnicima jeste interakcija sa oglasima. Naime, Gugl posebno prati ovu aktivnost kako bi oglašivačima prosledio informacije o tome da li su i u kojoj meri korisnici pratili dati oglas, da li su pokazali interesovanje za slične oglase, pa čak i: „kako pomerate miš preko oglasa"[156].

Korisnici koji koriste *Google Hangouts* i *Google Voice* dali su dozvolu Guglu da prate sve interakcije ostvarene putem ovih aplikacija, od brojeva telefona do trajanja i datuma poziva i poruka. Zanimljivo pojašnjenje Gugla kojim opravdava potrebu za prikupljanjem svih ovih informacija o aktivnostima korisnika opisano je u jednoj rečenici: „Prikupljamo informacije o vašim aktivnostima u uslugama koje koristimo da bismo vam, na primer, preporučili Jutjub video koji će vam se možda svideti"[157]. Tip prikupljenih informacija više govori u prilog tome da se one zapravo primarno koriste kao povratne informacije oglašivačima i trećim licima, koja koriste usluge Gugla, a sve sa ciljem ostvarivanja komercijalnog interesa – prodaje personalizovanih profila korisnika, radi boljeg plasmana oglasnih sadržaja.

Sledeći tip informacija koje Gugl prikuplja jesu „Informacije o lokaciji". Informacijama o lokaciji korisnik može uspešno da upravlja tako što će isključiti opciju praćenja lokacije uređaja. Međutim, isključivanjem ove opcije, korisniku bivaju uskraćene mnoge druge korisne funkcije, povezane sa lokacijom[158]. Prikupljanje podataka o lokaciji omogućavaju: „GPS, IP adresa, podaci senzora sa uređaja, informacije o stvarima blizu uređaja, poput pristupnih tačaka za Wi-Fi, baznih

[153] Politika privatnosti, *Gugl*, u delu: Stvari koje pravite ili nam pružate, dostupno putem linka: https://policies.google.com/privacy#whycollect (pristupljeno 24. 06. 2018. godine).
[154] Ibid. u delu: Informacije koje prikupljamo dok koristite usluge.
[155] Ibid. u delu: Vaše aktivnosti.
[156] Ibid.
[157] Ibid.
[158] Gugl nalog Pomoć, Upravljajte lokacijom, dostupno putem linka: https://support.google.com/accounts/answer/3467281?p=privpol_location&visit_id=1-636658807163676682-840908512&rd=1 (pristupljeno 23.06.2018. godine).

stanica za mobilnu telefoniju i uređaja sa Bluetooth-om"[159]. Gugl koristi različite vidove tehnologije kako bi prikupljao i skladištio sve ove informacije. Jedan od najpoznatijih načina jeste upotreba tzv. kolačića.

Gugl kolačiće definiše na sledeći način: „Kolačić je mala datoteka koja sadrži niz znakova koji se šalje računaru kada posetite neki veb-sajt. Kada ponovo posetite sajt, kolačić omogućava tom sajtu da prepozna pregledač. Kolačići mogu da skladište korisnička podešavanja i druge informacije."[160] Korisnik može da isključi opciju kolačića, međutim, u tom slučaju mu mogu biti uskraćene neke značajne funkcije određenih veb-sajtova i njihovih usluga. Pored skladištenja podataka, Gugl navodi da koristi kolačiće i: „da bismo zapamtili podešavanja sigurne pretrage, da bismo oglase koje vidite učinili relevantnijim za vas, da bismo izbrojali koliko posetilaca dobija određena stranica, da bismo vam olakšali registrovanje za naše usluge, da bismo zaštitili vaše podatke ili da bismo zapamtili podešavanja oglasa"[161].

Postoje različiti tipovi kolačića. Gugl koristi kolačiće za: *podešavanje*, *bezbednost*, *procese*, *oglašavanje*, *stanje sesije* i *analitiku*[162]. Kolačići za *podešavanja* odnose se na skladištenje osnovnih informacija o korisniku kao što su region, jezik, vremenska zona i slično. Kolačići za *bezbednost* koriste se kako bi se proverila autentičnost korisničkog naloga i sprečila zloupotreba. Kolačići za *procese* odnose se na funkcionalnost pretraživanja, na primer, otvaranje više veb-stranica u isto vreme; „bez ovih kolačića sajt ne može pravilno da funkcioniše"[163]. Kolačiće za *oglašavanje* Gugl koristi kako bi pratio aktivnosti korisnika i u skladu sa tim nudio personalizovane oglase, odnosno oglasne sadržaje koji su u skladu sa interesovanjem korisnika, i da bi, sa druge strane, oglašivačima obezbedio detaljne informacije o interkaciji korisnika sa njihovim oglasima. Kolačići *stanje sesije* odnose se na interakciju korisnika i određenih veb-sajtova, ali: „Ovi kolačići mogu da se koriste i za anonimno merenje efikasnosti plaćanja po kliku i oglašavanja preko promotera"[164]. Poslednja vrsta kolačića odnosi se na Gugl *analitiku*, koja omogućava veb-sajtovima da ostvare uvid u statistički obrađene podatke o, na primer, broju poseta, frekvenciji poseta sajtu i slično. Različite vrste kolačića pomažu Guglu da prati aktivnosti korisnika, analizira ih, skladišti i razvrstava, kako bi ih upotrebio u različite svrhe, od onih koje podrazumevaju poboljšano iskustvo korisnika, do onih koje se tiču poslovanja, odnosno snabevanje poslovnih partnera statistikom neophodnom za uspešno targetiranje i poslovanje.

Gugl svojom *Politikom* ističe da svi prikupljeni podaci, pa i specifični identifikatori, IP adrese, podaci dobijeni putem kolačića, ne mogu otkriti identitet korisnika, te garantuju anonimnost. Međutim, GDPR predviđa da: „mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrebiti za izradu profila pojedinaca i njihovu identifikaciju" (*Uvodna odredba (30)*).

Prvi deo *Politike privatnosti* pokušao je da odgovori na pitanje koje informacije prikuplja i skladišti Gugl, i na koji način to čini. Drugi deo bavi se pitanjem *Zašto Gugl prikuplja podatke*. Prva

[159] Politika privatnosti, *Google*, u delu: Informacije o lokaciji, dostupno putem linka: https://policies.google.com/privacy#whycollect (pristupljeno 23. 06. 2018. godine).
[160] Ibid.
[161] Kako Gugl koristi kolačiće, dostupno putem linka: https://policies.google.com/technologies/cookies (pristupljeno 23. 06. 2018. godine).
[162] Vrste kolačića koje koristi Gugl, dostupno putem linka: https://policies.google.com/technologies/types (pristupljeno 27. 06.2018. godine).
[163] Ibid.
[164] Ibid.

svrha jeste *Pružanje usluga*, kao primer takvih usluga Gugl navodi da IP adresu skladišti da bi omogućio učitavanje videa na Jutjubu ili da slike i video-zapise otpremljene u datoteku Gugl slike skladišti i organizuje na način koji bi korisnicima olakšao njihovo korišćenje ili pravljenje albuma i slično[165]. Druga svrha, koju Gugl navodi jeste *Održavanje i poboljšavanje usluga*, i pod tim podrazumeva praćenje aktivnosti korisnika i uočavanje stvari sa kojima korisnici imaju poteškoće, te rad na njima i njihovom poboljšanju. Slično i treća svrha *Pravljenje novih usluga* odnosi se na praćenje aktivnosti korisnika i analizu i evaluaciju postojećih usluga, kako bi inovacije bile u skladu sa potrebama korisnika.

Pružanje personalizovanih usluga, uključujući sadržaj i oglase sledeća je svrha prikupljanja informacija i podataka o korisnicima. U osnovi reč je o praćenju aktivnosti korisnika kako bi, u skladu sa njihovim preferencijama prilikom pretraga, Gugl ponudio rezultate ili oglase koji će biti u skladu sa prethodno iskazanim interesovanjima. Posebno se ističe da Gugl ne deli lične podatke sa oglašivačima, ukoliko korisnik sam na to ne pristane ili to ne zatraži. Međutim, u ovom delu primećujemo nelogičnost:

> „Ne delimo sa oglašavačima informacije pomoću kojih vas je moguće lično identifikovati, poput imena ili imejla, ako vi to ne zatražite od nas. Na primer, ako vidite oglas za cvećaru u blizini i izaberete dugme 'Dodirnite za poziv', povezaćemo vaš poziv i možda ćemo deliti broj telefona sa cvećarom"[166].

Dakle, u prvom delu Gugl jasno ističe da neće ni u kom slučaju podeliti Vaše podatke sa oglašivačem, dok već u drugom delu pasusa ostavlja prostor za takvu mogućnost, kada navodi da će *možda* ipak podeliti Vaš broj telefona, ukoliko Vi kontaktirate oglašivača.

Merenje učinka je sledeća svrha prikupljanja podataka koja se odnosi na operacije Gugl analitike, a kojima se meri učinkovitost sajtova, proizvoda, aplikacija, ali se i ukrštaju podaci korisnika sa različitih sajtova koji koriste Gugl analitiku kako bi se povećala učinkovitost u oglašavanju. Pored ovoga, *komunikacija sa korisnicima* je jedna od svrha, pod kojom se podrazumeva direktna komunikacija sa korisnicima putem mejl adresa, prilikom slanja različitih obaveštenja[167]. Poslednja svrha u ovom segmentu *Politike privatnosti* odnosi se na bezbednost, odnosno *Zaštitu Gugla, korisnika i javnosti*[168]. Kako je navedeno, svi podaci koji se prate, prikupljaju i skladište, koriste se kako bi se poboljšao kvalitet usluge i kako bi se osigurala bezbedna komunikacija. Gugl prikupljanje podataka i njihovo korišćenje opisuje rečenicom: „Koristimo podatke da bismo napravili bolje usluge"[169].

Premda je nedvosmisleno jasno da praćenje i analiza aktivnosti korisnika obezbeđuje personalizovano iskustvo u pogledu rezultata pretrage i uopšte informacija koje dolaze do krajnjeg korisnika, stiče se utisak da je svaki vid prikupljanja podataka isključivo zarad dobrobiti korisnika, čime se oduzima na značaju komercijalnom interesu kompanije Gugl. Onda kada se i naglasi da je deljenje zbirnih podataka sa oglašivačima deo poslovne prakse, insistira se na tome da je dobit korisnika veća od dobiti oglašivača, odnosno Gugla. Komercijalni interes nije eksplicitno naglašen, kao

---

[165] Politika privatnosti, *Google*, u delu: Zašto Gugl prikuplja podatke, dostupno putem linka: https://policies.google.com/privacy#whycollect (pristupljeno 26. 06. 2018. godine).
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.

što je to slučaj sa interesom korisnika, niti su predviđeni rizici prikupljanja i deljanje tako obimnih podataka.

„Vaše kontrole privatnosti" je treći deo *Politike privatnosti* i odnosi se na mogućnosti pojedinaca da upravljaju svojim podacima i utiču na način njihove primene. Postoji mogućnost isključivanja lokacije ili kolačića, ali ne bez posledica po kvalitet usluge. Dodatna poteškoća Gugl korisnicima jeste i to što svaki Gugl proizvod, *Google Chrome*, *Gmail*, *YouTube*, *Google Maps*, *Google Play*, ima posebna podešavanja privatnosti, što bi značilo da bi korisnik pri instaliciji paketa Guglovih proizvoda i aplikacija, koje su sastavni deo operativnog sistema *Android*, trebalo da se upozna sa politikom svakog Guglovog proizvoda, što dodatno usložnjava već dug i složen proces[170].

Olakšavajuća okolnost je postojanje *Vodiča za privatnost za Guglove proizvode*[171], koji uključuje sve proizvode i posebno istaknuta podešavanja privatnosti, što korisnik može da menja, ali ponovo u meri koja mu neće uskratiti kvalitetno korišćenje svih funkcija. Međutim, GDPR predočava da se pristanak korisnika ne smatra validnim ukoliko korisnik nema *poštene uslove,* odnosno *istinski izbor* (član 7; Uvodna odredba (42)). Kada je posebnim podešavanjima predviđeno isključivanje kolačića, keš memorije, praćenje lokacije i slično, ali je istovremeno naglašeno da će to značajno uticati na pojedine funkcije, te da će neke usluge biti potpuno onemogućene, korisnik je doveden u situaciju nepoštenog izbora između nekvalitetne i nepotpune usluge i prekomerne obrade podataka.

„Kako Gugl deli vaše informacije"[172] sledeći je segment *Politike privatnosti*. U prvoj rečenici ističe se da Gugl ne deli lične informacije svojih korisnika sa drugim licima. Međutim, u nastavku se pojašnjava da Gugl to ipak može da učini zbog nekog od četiri navedena razloga:

1. Ukoliko za to dobije saglasnost korisnika;

2. Ukoliko je korisnik deo *G-Suite*-a, odnosno grupnog poslovnog naloga, pa u tom slučaju administrator ima pristup nalogu, kao i ostali korisnici tog naloga;

3. Za spoljnu obradu, koju Gugl definiše na sledeći način:

> „Lične podatke pružamo našim povezanim licima i drugim pouzdanim pravnim ili fizičkim licima da bi ih u naše ime obradili na osnovu uputstava i u skladu sa politikom privatnosti i sa svim odgovarajućim merama zaštite podataka i bezbednosti. Na primer, koristimo dobavljače usluga za pomoć oko korisničke podrške"[173].

Pod povezanim licima Gugl podrazumeva svoje ispostave u EU[174], međutim, ostaje nejasno koja su druga „pouzdana pravna ili fizička lica", čime se ponovo dovodi u pitanje nivo transparentnosti u pogledu deljenja podataka sa trećim licima (GDPR član 5 (1)).

---

[170] Na primer, autorki je za detaljnu analizu i upoznavanje sa svakom stavkom samo *Politike privatnosti* Gugla trebalo desetak dana.
[171] Vodič za privatnost za Gugl proizvode, dostupno putem linka: https://policies.google.com/technologies/product-privacy (pristupljeno 23. 06. 2018. godine).
[172] Politika privatnosti, *Google*, u delu: Kako Gugl deli vaše informacije, dostupno putem linka: https://policies.google.com/privacy#infochoices (pristupljeno 23. 06. 2018. godine).
[173] Ibid.
[174] Spisak svih afilijacija Gugla u EU dostupan je putem linka: https://privacy.google.com/businesses/affiliates/ (pristupljeno 23. 06. 2018. godine).

Pored navedenih razloga, Gugl informacije o korisnicima može da deli i sa trećim licima, kompanijama sa kojima sarađuje, prevashodno u komercijalne svrhe. Guglovom politikom se naglašava da se ti podaci dele isključivo zbirno, te da je nemoguće ostvariti uvid u pojedinačne informacije o korisnicima. Međutim, kako je već bilo reči *Uvodna odredba (30)* GDPR predviđa mogućnost otkrivanja identiteta, na osnovu prikupljenih ličnih podataka i podataka o uređajima. Gugl informacije najčešće deli sa partnerima oglašivačima:

> „Na primer, dozvoljavamo Jutjub autorima i oglašavačima da sarađuju sa kompanijama za merenje da bi saznali više o publici za svoje Jutjub video snimke ili oglase pomoću kolačića ili sličnih tehnologija. Drugi primer su prodavci na stranicama Kupovine, koji koriste kolačiće da bi utvrdili koliko različitih ljudi vidi njihove unose proizvoda."[175]

Član 6 stavka 1 (f) GDPR nalaže da je „obrada podataka zakonita ako je nužna za legitimne interese voditelja obrade ili treće strane", ukoliko je taj interes veći od interesa da se korisniku zaštite lični podaci. Međutim, član 13 (d,e,f), kojim se predviđaju informacije koje se moraju dostaviti korisnicima čiji se podaci obrađuju, nalaže da se daju jasne informacije o trećim licima, kao i svrha u koju će podaci biti iskorišćeni. Gugl navodi pojedine, kao što su *Jutjub autori*, ali u većeni slučajeva oslovljava ih uopšteno *partnerima, korisnicima* Gugl *usluga, kompanijama* s kojima sarađuje, *oglašivačima* i slično. Na taj način Gugl ne daje tačnu i pouzdanu informaciju o licima kojima se prosleđuju podaci korisnika.

4. Poslednji razlog jesu pravna pitanja. Pored razloga koji uključuju osiguravanje bezbednosti, sprečavanje zloupotrebe, zaštitu pravne svojine i slično, Gugl dobija i zahteve državnih organa za pristup ličnim podacima korisnika u izuzetnim slučajevima. U tom slučaju, pravni tim Gugla pregleda zahteve i odlučuje o tome da li je zahtev opravdan i da li je interes zastupljen zahtevom veći od interesa koji podrazumeva zaštitu korisnika i njegovih ličnih podataka. Gugl objavljuje izveštaje o transparentnosti koji omogućavaju uvid u broj podnetih zahteva po zemlji, kao i konačne brojeve odobrenih, odnosno odbijenih zahteva po godinama[176]. Tri su tipa takvih zahteva: *bezbednost i privatnost, prekidi u pružanju usluga* i *uklanjanje sadržaja*[177]. Kompanija Gugl, sa svojim pravnim timovima, ove zahteve tretira kao posebno osetljive, jer njihova potencijalna neopravdanost može ugroziti kako privatnost korisnika, kada se zahtevi odnose na pružanje informacija o korisnicima, tako i slobodu izažavanja, kada se zahtevi odnose na uklanjanje sadržaja. Najčešći razlozi za takve zahteve jesu kleveta, autorska prava i nacionalna bezbednost. Na primer, u 2017. godini je u prvoj polovini godine, kada se podnosi izveštaj, bilo ukupno 19 176 zahteva za uklanjanjem sadržaja, dok je od juna do decembra 2017. godine bilo još 16 610 takvih zahteva. Od toga je najviše bilo zahteva zbog ugrožavanja nacionalne bezbednosti, u prvoj polovini 2017. godine dve trećine od ukupnog broja zahteva. Najčešći broj zahteva odnosio se na Jutjub 50,3% i veb-pretragu blizu 20%[178]. Kada je reč o Srbiji, najviše zahteva upućeno je u prvoj polovini 2017. godine, a najmanje u drugoj polovini 2017. godine (videti Grafikon 11)

[175] Politika privatnosti, *Google*, dostupno putem linka: https://policies.google.com/privacy#infochoices (pristupljeno 23. 06. 2018. godine).
[176] Guglovi izveštaji o transparentnosti dostupni su putem linka: https://transparencyreport.google.com/user-data/overview (pristupljeno 26. 06. 2018. godine).
[177] Ibid.
[178] Ibid. u delu: Zahtevi vlada za uklanjanje sadržaja

	Период на који се извештај односи	Захтеви за откривање података корисника	Корисници/налози	Проценат захтева за које су пружени неки подаци
▸	јул 2017.–дец 2017.	1	1	0%
▸	јан 2017.–јун 2017.	11	17	36%
▸	јул 2016.–дец 2016.	6	8	17%
▸	јан 2016.–јун 2016.	3	3	0%
▸	јул 2015.–дец 2015.	2	2	0%
▸	јан 2015.–јун 2015.	3	3	33%
▸	јул 2014.–дец 2014.	1	5	0%

Grafikon 11 Zahtevi Srbije za otkrivanjem informacija o korisnicima, Gugl Izveštaj o transparentnosti[179]

Pored mogućnosti da vlade potražuju uklanjanje sadržaja, tu mogućnost imaju i korisnici od maja 2014. godine, kada je *Sud pravde Evropske unije* doneo presudu u korist M. Kostehe Gonzalesa (M. Costeja González), koji je uložio žalbu protiv *Google Spain* i *Google Inc*. sa zahtevom za uklanjanjem njegovih podataka[180]. Pozivajući se na *Direktivu 95/46 o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka*[181], odnosno njene članove 2[182], 4[183], 12[184]. i 14[185], i *Povelju Evropske unije o osnovnim pravima 2007/C 303/01*, odnosno njene članove 7

[179] Izveštaj o Srbiji dostupan je putem linka: https://transparencyreport.google.com/user-data/overview?t=table&user_requests_report_period=series:requests,accounts;authority:NO;time:&lu=user_requests_report_period (pristupljeno 23. 06. 2018. godine).

[180] Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Case C‑131/12. dostupno putem linka: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 (pristupljeno 24. 06. 2018. godine).

[181] engl. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Dostupno putem linka: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046 (pristupljeno 23. 06. 2018. godine).

[182] Član 2 Direktive 95/46: „ budući da su sistemi za obradu podataka osmišljeni da služe čoveku; budući da moraju, bez obzira na nacionalnost ili boravište fizičkih osoba, poštovati njihova temeljna prava i slobode, pravo na privatnost, te doprinositi ekonomskom i socijalnom napretku, širenju trgovine i dobrobiti pojedinaca". Dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[183] Član 4 Direktive 95/46: „budući da se u Zajednici sve više pribegava obradi ličnih podataka u raznim područjima ekonomske i socijalne aktivnosti; budući da napredak ostvaren u računarskoj tehnologiji znatno olakšava obradu i razmenu takvih podataka;" Dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[184] Član 12 Direktive 95/46: „budući da se načela zaštite moraju primenjivati na svaku obradu ličnih podataka koju sprovodi bilo koja osoba čije su aktivnosti uređene pravom Zajednice; budući da je potrebno isključiti obradu podataka koju sprovodi fizička osoba izvršavanjem aktivnosti koje su isključivo lične ili domaće naravi, kao što je dopisivanje i vođenje evidencije adresata;" Dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[185] Član 14 Direktive 95/46: „ budući da se s obzirom na važnost aktualnog razvitka u okviru informacijskog društva, tehnika za prikupljanje, prenos, rukovanje, snimanje, pohranjivanje ili komuniciranje zvučnih ili slikovnih podataka koji se odnose na fizičke osobe, ova Direktiva mora primeniti na obradu koja uključuje takve podatke;" Dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

(Poštovanje privatnog i porodičnog života) i 8 (Zaštita ličnih podataka), *Sud pravde EU* presudio je u korist Gonzalesa, čime mu je omogućio "pravo na zaborav". Zvanično "pravo na zaborav" ulazi u evropsku regulativu usvajanjem GDPR, čiji član 17 posebno predviđa pravo na brisanje, odnosno pravo na zaborav.

U delu o brisanju određenih podataka korisnika ili čitavog Gugl naloga, Gugl informiše svoje korisnike da će neke podatke ipak zadržati na neodređeni vremenski period, u zavisnosti od tipa podataka o kojima je reč:

> „da bismo se uverili da se naše usluge pravilno prikazuju na raznim tipovima uređaja, možemo da zadržimo širinu i dužinu pregledača u periodu do 9 meseci. Preduzimamo i korake da učinimo neke podatke anonimnim u određenim vremenskim periodima. Na primer, podatke o oglašavanju činimo anonimnim u evidencijama servera tako što uklanjamo deo IP adrese posle 9 meseci i informacije kolačića posle 18 meseci[186]".

GDPR posebno ističe značaj što kraćeg perioda zadržavanja ličnih podataka (član 5 (1) (e); *Uvodna uredba* (39)). Da bi se osiguralo da su lični podaci korišćeni isključivo za svrhe koje su bile predviđene, neophodno je period zadržavanja svesti na minimum, a uz to je i značajno da voditelj obrade podataka predvidi razumni rok za brisanje. Gugl ne predviđa tačan rok, navodi periode 9–18 meseci u zavisnosti od tipa podataka, ali ne navodi precizno o kojim podacima je reč.

Kao razloge za zadržavanje određenih podataka navodi: *finansijske podatke, regulatorne uslove, kontinuitet usluga* i sično, i dodaje: „Naše usluge koriste i šifrovan rezervni memorijski prostor kao još jedan sloj zaštite od potencijalnih katastrofa. Podaci mogu da ostanu u ovim sistemima do 6 meseci[187]". Ni u jednom od navedenih stavki nije do kraja jasno koji su podaci koje Gugl zadržava i na koje vreme. Jezik je nejasan, informacije neodređene i uopštene, rokovi brisanja podataka neprecizni.

[186] Kako Gugl zadržava podatke koje prikupljam. Dostupno putem linka: https://policies.google.com/technologies/retention (pristupljeno 23. 06. 2018. godine).
[187] Ibid.

4.5.2. Samoregulatorna politika Fejsbuka

Prema podacima sa zvaničnog sajta kompanije, Fejsbuk ima 2,2 milijarde aktivnih korisnika mesečno, odnosno 1,45 milijardi dnevno aktivnih korisnika, prema proračunu za mart 2018. godine[188]. Fejsbuk je treći najposećeniji sajt u 2018. godini, posle Gugla i Jutjuba, dok je prema vremenu provedenom na sajtu na prvom mestu sa 11,12 minuta po korisniku.[189] Mark Zakerberg (Mark Zuckerberg) je osnivač, predsednik i glavni izvršni direktor kompanije. Rukovodstvo Fejsbuka, pored Zakerberga, čine i Šeril Sandberg (Sheryl Sandberg), operativna direktorka, finansijski direktor, Dejvid Viner (David Wehner), Majk Šroupfer (Mike Schroepfer), glavni direktor tehnologije i Kris Koks (Chris Cox), direktor proizvodnje[190]. Fejsbuk u svom vlasništvu ima i sledeće kompanije: *Facebook Payments Inc*., *Atlas*, *Onavo*, *Moves*, *Oculus*, *Masquerade*, *CrowdTangle*, i među njima najpoznatije: *WhatsApp Inc*. i *Instagram LLC*[191].

Fejsbuk (prvobitno ime *Thefacebook.com*) je 2004. godine počeo kao eksperimentalni projekat perspektivnog studenta Univerziteta Harvard, danas poznatog kao „kralja informacija", Marka Zakerberga. Dejvid Krikpatrik (David Kirkpatrick), objavio je 2011. godine knjigu Efekat *Fejbuka: Insajderska priča kompanije koja povezuje svet*, u kojoj opisuje početak i razvoj ove kompanije, prvobitnu viziju njenog osnivača, ali i put kojim se kretala dok nije postala globalna internet kompanija, danas jedna od najpoznatijih na svetu.

Projekat koji je u osnovi imao viziju o izgradnji boljeg i otvorenijeg društva, koje bi se baziralo na mogućnosti da svako dobije prostor da iskaže sebe i svoje stavove, vremenom je prerastao u tehnološkog giganta, koji, čini se, sve više izneverava inicijalnu ideju na kojoj se prvobitno bazirao. Zakerberg je imao viziju o apsolutno otvorenom i transparentnom društvu. Njegova vizija podrazumevala je da ljudi na Fejbuku nemaju razloga da skrivaju svoje podatke, insistirao je na tačnim ličnim podacima i pravim profilima. Smatrao je da će apsolutna transparentnost stvoriti bolje društvo. Takođe, inicijalna ideja bila je povezana sa konceptom da će tako otvorena zajednica imati moć da vlada, pa će Fejsbuk ostvariti ideal da ljudi vladaju i donose odluke, pokreću akcije. Sve to je u njegovoj zamisli bilo moguće samo kroz iskrenu komunikaciju i iskreno reprezentovanje na mreži. Zakerberg je smatrao da će se čitav svet razvijati u pravcu sve otvorenijeg društva, gde će privatnost izgubiti na značaju, a transparentnost biti centralni koncept (Kirkpatrick, 2011).

Međutim, Krikpatrik je predvideo da će pitanja: „Da li bi trebalo regulisati tako veliki servis? Šta osećamo o potpuno novom obliku komunikacije koji koriste stotine miliona ljudi, koji je u potpunosti kontrolisan od strane jedne kompanije? Da li rizikujemo našu slobodu poveravajući toliko informacija o našem identitetu jednom komercijalnom entitetu?" (2011: 17) biti sve učestalija i intenzivnija sa sve većom popularizacijom Fejsbuka. Bez obzira na želju za izgradnjom potpuno otvorene zajednice, i sam Zakerberg je od početka radio na osiguravanju bezbednog onlajn-prostora, koji neće ugroziti privatnost njegovih korisnika, već će stvoriti klimu poverenja: „Kontrola privatnosti

[188] Facebook, News room, Company Info, dostupno putem linka: https://newsroom.fb.com/company-info/ (pristupljeno 29. 04. 2018. godine).
[189] Podaci dostupnu na sajtu *Alexa*: https://www.alexa.com/topsites (pristupljeno 12. 04. 2018. godine).
[190] Detalji o rukovodiocima kompanije Fejsbuk i dodatni osnovni podaci o kompaniji mogu se videti na njihovom zvaničnom sajtu u delu *Company Info, Leadership*: https://newsroom.fb.com/company-info/ (pristupljeno 04. 05. 2018. godine).
[191] Spisak Fejsbuk preduzeća dostupan je na njihovom sajtu. Videti putem linka: https://www.facebook.com/help/111814505650678?helpref=faq_content (pristupljeno 04. 04. 2018. godine).

bila je deo originalnog dizajna" (Kirkpatrick, 2011: 31). Tome svedoče i podaci koje navodi Krikpatrik, pozivajući se na istraživanja firme *Ponemon Institute and TRUST*, koja se bavi verifikovanjem internet sajtova, i prema kojoj je 2009. godine Fejsbuk bila kompanija kojoj se najviše veruje u pogledu zaštite privatnost korisnika (Kirkpatrick, 2011: 209).

Rubenstin i Gud (Rubenstein & Good, 2013: 53-67) analizirali su incindete Fejsbuka s aspekta ugrožavanja privatnosti i hronološki izdvojili pet koji su, prema njihovom mišljenju, obeležili Fejsbuk od njegovog osnivanja: *News Feed*, *Beacon*, *Fejsbuk aplikacije*, *Deljenje fotografija* i *Promene u podešavanjima privatnosti*. Prvi incident koji autori izdvajaju jeste pokretanje *NewsFeed*-a 2006. godine. Ova promena dovela je do negativnih reakcija korisnika, jer do tada njihove aktivnosti nisu bile dostupne svim njihovim prijateljima. „Najbolniji trenuci kompanije došli su zato što su se preduzimale akcije – poput lansiranja *News Feed*-a - što je iznenada objavilo informacije korisnika na neočekivane načine" (Kirkpatrick, 2011: 200). Međutim, vremenom su se korisnici privikli na ovu promenu, i ko se još seća Fejsbuka bez *NewsFeed*-a? Rubenstin i Gud navode da je incident mogao biti sprečen, ili bar ublažen, da su korisnici unapred dobili obaveštenje o ovoj promeni, da su dobili period privikavanja uz postepene izmene. U ovom slučaju rizik Fejsbuka se na kraju ipak isplatio.

Beacon (doslovni prevod: *Svetionik*) lansiran 2007. godine bila je revolucionarna promena, kada je reč o oglašivačkom targetiranju. Naime, ovaj sistem omogućio je personalizovanu ponudu oglasa korisnicima, na osnovu njihovih individualnih veb-pretraživanja, koja su se potom pojavljivala na *NewsFeed*-u, i bila dostupna svim prijateljima. Zakerberg je verovao da će i ova inovacija biti prihvaćena tokom vremena, međutim, nisu jenjavale žalbe korisnika zbog deljenja njihovih pretraga sa prijateljima sa kojima možda ne žele da ih podele. Fejsbuk je najpre korigovao *Beacon* i učinio ga opcionim, ali je na kraju, 2009. godine ipak isključio ovaj sistem. *Beacon* autori navode kao primer kada je „želja kompanije za inovacijom jača od zaštite privatnosti" (Rubenstein & Good, 2013: 56). Uvođenje Fejsbuk aplikacija je treći takav incindent. Korisnici nisu bili sigurni kojim njihovim podacima mogu pristupiti nove aplikacije. Pitanje ovde pokrenuto izazov je sa kojim se Fejsbuk i danas suočava, a to je pitanje trećih lica i podataka koje sa njima deli Fejsbuk.

Deljenje fotografija, kao četvrti incident, odnosi se na mogućnost označavanja korisnika na fotografijama koje nije sam objavio. Unapređenjem individualnih podešavanja, Fejsbuk je ovaj izazov rešio uvođenjem opcije za odbijanje označavanja, odnosno, označavanja na upit. Poslednji incident, koji ovi autori izdvajaju kao revolucionarni u pogledu privatnosti, jesu promene u politikama i podešavanjima privatnosti. Kritike koje se uglavnom upućuju internet kompanijama, ne samo Fejsbuku, jesu česte promene politika, nerazumljiv jezik i nepotpuna usklađenost sa regulatornim okvirima. Fejsbuk se i danas suočava sa sličnim izazovima kada je reč o politici privatnosti.

Poverenje u kompaniju Fejsbuk varilalo je tokom godina, čemu su doprineli i brojni skandali, kada je reč o pristupu zaštiti podataka korisnika. Afera koja je 2012. godine dovela u pitanje poverenje u Fejsbuk odnosi se na tzv. eksperiment sa osećanjima korisnika. Naime, slučajni uzorak, više od 600 hiljada ljudi, podeljen je u dve grupe. Jednoj grupi je *NewsFeed* bio podešen da prikazuje samo pozitivne objave, dok je druga grupa bila izložena samo negativnim objava (statusima, fotografijama, vestima i slično). U isto vreme praćene su aktivnosti korisnika, koji nisu znali, niti pristali, da budu ispitanici u ovom psihološkom eksperimentu, kako bi se utvrdilo da li će pozitivne/negativne objave

imati uticaj na njihove aktivnosti i ponašanje na ovoj društvenoj mreži (Chambers, 2014)[192]. Olako pristupanje eksperimentisanju ljudi pokrenulo je mnoga pitanja, od etičnosti takvog postupka do neophodnosti eksplicitnog pristanka korisnika, pa sve do neslućenih mogućnosti Fejsbuka da manipuliše rezultatima prikazanim u *NewsFeed*-u, čime direktno utiče na slobodu izražavanja, odnosno nepristrasnog informisanja.

Još jedan skandal, vredan pomena, odnosi se na tužbu Belgije upućenu Fejsbuku 2015. godine. Naime, Belgija je optužila Fejsbuk da je prikupljao podatke građana Belgije i u slučaju kada nisu prihvatili kolačiće, jer se obaveštenja o kolačićima nisu propisno pojavljivala, shodno zakonu EU, ali i u slučajevima kada Belgijanci nisu bili korisnici Fejsbuka. Fejsbuk je pritom koristio druge metode, na primer treća lica sa kojima sarađuje, da bi ilegalno prikupljao podatke građana koji nisu njegovi korisnici. Epilog ove tužbe dobili smo februara 2018. godine, kada je Fejsbuku sudski naloženo da obustavi takvu praksu i obriše sve ilegalno prikupljene podatke. Do dana dok to zvanično i ne uradi, Fejsbuk će morati da plaća kazneni iznos od 250.000 evra dnevno (Gibbs, 2018)[193]. Ovaj slučaj otvara pitanja koja se tiču poverenja u Fejsbuk, odnosno pitanje da li Fejsbuk može ilegalno da prikuplja podatke, iako je to u suprotnosti sa njegovom zvaničnom politikom i regulativom EU, a da korisnici zapravo i ne budu svesni rizika, dok afera, poput slučaja sa Belgijom, ne dobije sudski epilog? Da li korisnicima jedino preostaje da veruju na reč tehno-gigantima da će poštovati njihova prava?

Poslednji skandal u nizu, koji je odjeknuo više od svih prethodnih, jeste slučaj Kembridž analitike (*Cambridge Analytica*), što je doprinelo da poverenje u Fejsbuk opadne za čak 66%[194]. Tom prilikom ugrožena je privatnost podataka više od 50 miliona Fejsbuk korisnika. O tome šta se zapravo desilo piše *Fortune*[195]. Naime, sve počinje još 2014. godine – istraživač Aleksandr Kogan (Aleksandr Kogan)razvio je aplikaciju *Ovo je tvoj digitalni život*, koja je funkcionisala tako što je korisnicima Fejsbuka bilo plaćeno da nakon što instaliraju ovu aplikaciju učestvuju u brojnim anketnim istraživanjima. Aplikacija je ujedno prikupljala i njihove podatke sa Fejsbuka, uglavnom o tome šta su označili sa „sviđa mi se" (engl. *Like*), ali i podatke njihovih prijatelja, kojima je podešavanje na Fejsbuku bilo namešteno tako da aplikacija ima dozvolu za pristup njihovim informacijama. Kogan je imao dozvolu Fejsbuka za takav vid istraživanja, kao i bilo koja druga aplikacija koja sarađuje sa Fejsbukom kao treće lice, sve dok poštuje politiku privatnosti i prikuplja informacije za koje su korisnici, odnosno politika Fejsbuka, dali dozvolu. Do ovog trenutka je sve u skladu sa *Politikom* Fejsbuka.

Međutim, od 2014. godine Kogan počinje saradnju sa kompanijom Kembridž analitika (engl. Cambridge Analytica), kompanijom koja „koristi podatke da bi promenila ponašanje publike", bilo

[192] Chris Chambers (1 Jul 2014). „ Facebook fiasco: was Cornell's study of 'emotional contagion' an ethics breach?". *The Guardian*. Dostupno na: https://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach (pristupljeno 05. 04. 2018. godine).

[193] Samuel Gibbs. (16 Feb 2018). „ Facebook ordered to stop collecting user data by Belgian court". *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court (pristupljeno 06. 05. 2018. godine).

[194] Herb Weisbaum. (Apr.18. 2018). "Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal". *NBCNews*. Dostupno na: https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011 (pristupljeno 04. 05. 2018. godine).

[195] Bloomberg. (10 Apr. 2018). "Facebook Cambridge Analytica Scandal: 10 Questions Answered". *Fortune*. Dostupno na: http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/ (pristupljeno 05.05.2018. godine).

politički ili *komercijalno*, kako i piše na njihovom veb-sajtu[196]. Ova kompanija plaća Koganu za informacije o Fejsbuk korisnicima, naročito o njihovim preferencijama, sa ciljem izgradnje profila korisnika i kasnijeg targetiranja u svrhu političke kampanje Donalda Trampa. Problem koji je nastao tiče se prenosa podataka kompaniji Kembridž analitika, koja ih koristi u političke svrhe, a ne u komercijalne kako je prvobitno bilo predočeno korisnicima. Fejsbuk to saznaje 2015. godine, uklanja Koganovu aplikaciju i zahteva brisanje svih podataka koje su o korisnicima prikupile i njegova aplikacija i kompanije kojima je prosledio podatke. Međutim, u trenutku kada za slučaj saznaje i javnost čelnici Fejsbuka izjavljuju da nisu sigurni šta ove kompanije još uvek imaju od podataka korisnika, odnosno, da li su i u kojoj meri obrisali podatke[197].

Gardijan o ovom skandalu piše:

> „Kompanija za analizu podataka koja je radila s izbornim timom Donalda Trampa i pobedničkom kampanjom Bregzita prikupila je milione Fejsbuk profila američkih birača u jednom od najvećih kršenja podataka tehnološkog giganta ikada i koristila ih za izgradnju snažnog softverskog programa za predviđanje i uticaj na izbore" (Cadwalladr & Graham-Harrison, 2018)[198].

Nekadašnji radnik Kembridž analitike Kritofer Vajli (Christopher Wylie) rekao je tom prilikom da je sistem funkcionisao tako što je pravio individualne profile svakog od potencijalnih glasača, kako bi znao kojim političkim propagandnim materijalom da „gađa" svakog od njih. Vajli je otkrio da je čitav projekat bio usmeren ka stvaranju savršenog sistema političkog oglašavanja, odnosno da su prikupljeni podaci korisnika služili da bi „njima ciljali njihove unutarašnje demone" (Christopher Wylie za *The Gurdian*)[199].

Pitanja pokrenuta ovim slučajem ne tiču se samo narušavanja privatnosti već pokreću pitanja transparentnosti u pogledu poslovanja tehno-giganta, koji ima dozvolu za deljenje ličnih podataka korisnika sa trećim licima, a o kojima korisnici ne znaju gotovo ništa ili ne znaju dovoljno da bi im poverili svoje podatke.

Poslednje izmene *Politike privatnosti* Fejsbuk je učinio 19. aprila 2018. godine. Kao što je to bio slučaj i sa kompanijom Gugl, i analiza *Politike* Fejsbuka biće sprovedena u komparaciji sa opštim regulatornim okvirom EU u ovoj oblasti. *Politika* Fejsbuka koja je ovde predmet analize preuzeta je u Austriji. Austrija je odabrana kao članica EU, stoga se pretpostavlja da bi *Politika* Fejsbuka u Austriji trebalo da bude u skladu sa propisima GDPR.

Analiza. Kada korisnik kreira nalog na Fejsbuku, putem *Uslova korišćenja* on se upoznaje sa svojim pravima. Prihvatanjem *Uslova* on se i obavezuje da će poštovati zahteve koje kompanija nalaže. *Uslovi korišćenja* su najznačajniji samoregulatorni mehanizam Fejsbuka, kojim se uređuje odnos između kompanije i korisnika: „Ovim Uslovima je uređeno vaše korišćenje Fejsbuka i proizvoda,

---

[196] Sajt Kembridž analitike videti putem linka: https://cambridgeanalytica.org/ (pristupljeno 07. 05. 2018. godine).
[197] Bloomberg. (10 Apr. 2018). *Fortune*.
[198] Carole Cadwalladr, Emma Graham-Harrison. (17 Mar. 2018). "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *The Guardian.* Dostupno na: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (pristupljeno 04. 05. 2018. godine).
[199] Ibid.

funkcija, aplikacija, usluga, tehnologija i softvera koje nudimo (Fejsbuk Proizvodi ili Proizvodi), osim kada izričito navedemo da se primenjuju posebni uslovi (a ne ovi)."[200]. *Uslovi korišćenja* Fejsbuka sastoje se iz pet odvojenih delova: *Naše usluge*, *Naša politika o podacima i vaši izbori u pogledu privatnosti*,*Vaše obaveze prema Fejsbuku i našoj zajednici*, *Dodatne odredbe*, *Ostali uslovi i pravila koji se mogu primenjivati na vas*[201].

U delu *Naše usluge* Fejsbuk nudi devet opštih usluga svojim korisnicima. Prvom uslugom kompanija korisnicima obećava "personalizovano iskustvo". Da bi Fejsbuk svojim korisnicima obezbedio takav vid iskustva neophodno je da unapred zna šta određeni korisnik preferira:

> „Vaše iskustvo na Fejsbuku nije kao ičije drugo iskustvo: od objava, priča, događaja, oglasa i drugog sadržaja koje vidite u Novostima ili našoj video platformi do Stranica koje pratite i drugih funkcija koje možda koristite, kao što su Aktuelno, *Marketplace* i pretraga. Koristimo podatke koje imamo – na primer, o vezama koje pravite, izborima i podešavanjima koje birate i šta delite i radite u okviru i van naših Proizvoda – da bismo personalizovali vaše iskustvo."[202]

Već u ovom delu Usluga jasno je naglašeno da Fejsbuk koristi digitalne podatke korisnika u okviru ali i **van** njihovih Proizvoda. U isto vreme naglašena je i individualnost, posebnost svakog korisnika, koju kompanija Fejsbuk vrednuje i ističe. Ono što se zapravo odvija je sledeće: Fejsbuk na osnovu algoritamskog proračuna korisničkih aktivnosti konstruiše profil svakog svog korisnika i u skladu sa preferencijama tog hipotetičkog profila, nudi dodatne aktivnosti, koje bi, prema proračunu, trebalo da budu u skladu sa željama korisnika. Takav postupak je srodan sa postupkom targetiranja ciljnih grupa. Ono što je u slučaju targetiranja na Fejsbuku specifično jeste postupak kojim sam korisnik gradi svoj profil, kroz niz aktivnosti i putem otkrivanja informacija o sebi koje istovremeno kompanija koristi kako bi korisniku ponudila još sličnih informacija ili aktivnosti.

U skladu sa misijom Fejsbuka: „davati ljudima moć izgradnje zajednice i približavanje sveta"[203], druga usluga kao ključnu reč ističe *povezivanje*:

> „Pomažemo vam da pronađete ljude, grupe, kompanije, organizacije i ostalo do čega vam je stalo i povezujemo vas s njima putem Fejsbuk Proizvoda koje koristite. Koristimo podatke koje imamo da bismo napravili predloge za vas i druge – na primer, grupe za učlanjenje, događaje za posećivanje, Stranice za praćenje ili slanje poruka, veb serije za gledanje i ljude s kojima možda želite da postanete prijatelji. Jače veze daju bolje zajednice, a mi verujemo da su naše usluge najkorisnije kada su ljudi povezani s ljudima, grupama i organizacijama do kojih im je stalo". [204]

Obema uslugama Fejsbuk eksplicitno ističe primarnu korist korisnika. Kroz demagoške konstrukcije „mi vas povezujemo", „mi vam pomažemo da pronađete ono što zapravo želite" i slično, stiče se površni utisak da Fejsbuk to radi isključivo za dobrobit korisnika, a da pritom ne ostvaruje i

---

[200] Uslovi korišćenja Fejsbuka u Austriji dostupni su putem linka: https://www.facebook.com/legal/terms/plain_text_terms . Uslovi se često dopunjuju ili menjaju. Datum poslednje revizije aktuelnih Uslova je 19. april 2018. godine. (pristupljeno 07. 02. 2019. godine).
[201] Ibid. (pristupljeno 07. 02. 2019. godine).
[202] Ibid.
[203] Ibid.
[204] Ibid.

sam ličnu korist. Slično je opisana i treća usluga, koja korisnicima „pomaže da se izraze i komuniciraju", što bi apsolutno bilo u skladu sa inicijalnom vizijom Zakerberga o davanju moći ljudima. Međutim, vizija nastala u njegovim studentskim danima i nelagodnost da korisnike obasipa banerima, bledela je i dovela do onoga što se i navodi četvrtom uslugom: „Naši partneri nam plaćaju da vam pokažemo njihov sadržaj, a mi osmišljavamo naše usluge tako da sponzorisani sadržaj koji vidite bude relevantan i koristan za vas kao i sve ostalo što vidite u našim Proizvodima"[205]. Ova usluga nazvana je *Pomažemo vam da otkrijete sadržaj, proizvode i usluge koji vas mogu interesovati*[206]. Svojim nazivom ponovo sugeriše da je predviđena usluga u isključivoj službi korisnika. Međutim, sistem funkcionisanja ove aktivnosti je vrlo jednostavan: Fejsbuk podatke o korisnicima, njihove preferencije, posredno ustupa trećim licima, koja plaćaju Fejsbuku da reklamira njihov sadržaj. Premda čelnici kompanije u *Uslovima* navode da nijedna treća strana nema direktan pristup podacima korisnika, čin korišćenja podataka korisnika u komercijalne svrhe, odnosno pri targetiranju ciljnih grupa za određeni sponzorisani sadržaj, jasno ukazuje na to da Fejsbuk ostvaruje profit korišćenjem podataka svojih korisnika. Upravo je na to mislio i Zakerberg kada je na pitanje kako je Fejsbuk besplatan za korisnike senatoru Orinu Heču (Orrin Hatch) odgovorio da zarađuju od prodaje oglasa[207]. Sa druge strane, Fejsbuk negira da prodaje informacije svojih korisnika (videti sliku 1.), iako se iz prethodno navedenog može zaključiti da su informacije o korisnicima upravo te na osnovu kojih Fejsbuk ostvaruje dobit, u prenesenom značenju: prodaje informacije o korisnicima trećim licima, o čemu svedoči i skandal sa Kembridž analitikom.

Slika 1 Fejsbukov Centar za pomoć[208]

Sledećim uslugama ističe se borba protiv štetnih sadržaja, istraživanje mogućnosti za poboljšanje usluga i slično. Na primer, u okviru usluge *Borimo se protiv štetnog ponašanja i štitimo i podržavamo našu zajednicu* navodi se da kompanija Fejsbuk predano radi na sprečavanju zloupotreba njenih usluga, ali i jasno ističe da tehničkim mehanizmima u toj borbi pomažu i timovi ljudi: „Zapošljavamo posvećene timove širom sveta i razvijamo napredne tehničke sisteme da bismo otkrili zloupotrebu naših Proizvoda, štetno ponašanje prema drugima i situacije u kojima možemo da

[205] Ibid.
[206] Ibid.
[207] Jason Abbruzzese. (April 10 2018). "We run ads". *NBC News*. Dostupno na: https://www.nbcnews.com/card/we-run-ads-n864606 (pristupljeno 04. 05. 2018. godine).
[208] Fejsbukov Centar za pomoć. Dostupno putem linka: https://www.facebook.com/help/207216349317757?helpref=related (pristupljeno 07. 02. 2019. godine).

podržimo ili zaštitimo našu zajednicu"[209]. U ovom delu *Uslova* navodi se i da Fejsbuk konstantno radi na istraživanju ljudskog ponašanja na osnovu podataka kojima raspolažu. Takav tip istraživanja podrazumeva spoj tehničkog i humanističkog pristupa, jer se socijalno ponašanje ljudi analizira na osnovu podataka i algoritmaskih proračuna. Stranica Fejsbuk istraživanja (*Facebook Research*)[210] posvećena je objavljivanju ovih istraživanja.

Drugi deo ugovora odnosi se na *Politiku privatnosti*:

> „Da bismo pružili ove usluge moramo da prikupimo i koristimo vaše lične podatke. Naše prakse su detaljno objašnjene u Politici o podacima na koju morate pristati da biste koristili naše proizvode. Takođe vas savetujemo da pregledate mogućnosti u pogledu privatnosti koje su vam na raspolaganju u vašim podešavanjima".[211]

Politici o podacima posvećena je posebna stranica na kojoj kompanija navodi koje podatke korisnika prikuplja i na koji način ih koristi i deli. Ujedno daje i preporuke korisnicima kako sve mogu da zaštite svoje podatke, odnosno na koji način mogu da upravljaju svojim podacima. U delu u kojem se navode informacije koje kompanija prikuplja od korisnika piše:

> „Da bismo obezbedili Fejsbuk proizvode, moramo da obrađujemo informacije o vama. Vrste informacija koje prikupljamo zavise od toga kako koristite naše proizvode.
>
> [...]
>
> Prikupljamo sadržaj, obaveštenja i druge informacije koje navodite kad koristite naše Proizvode, uključujući prilikom registrovanja za nalog, pravljenja ili deljenja sadržaja, kao i slanja poruka ili komunikacije sa drugim osobama.
>
> […]
>
> To može da uključuje informacije u sadržaju ili o sadržaju koji pružate (kao što su meta podaci), kao što su lokacija fotografije ili datum pravljenja datoteke. Takođe može da uključuje šta vidite kroz funkcije koje nudimo, kao što je naša kamera, kako bismo mogli da preduzimamo aktivnosti kao što su predlaganje maski i filtera koji će vam se možda svideti ili davanje saveta o korišćenju formata na kameri.
>
> […]
>
> Takođe prikupljamo kontakt podatke ako izaberete da ih dodate, sinhronizujete ili uvezete sa nekog uređaja (kao što je imenik ili evidencija poziva ili istorija evidencije poruka) koje koristimo da, na primer, pomognemo vama ili drugima da pronađete osobe koje možda poznajete.
>
> […]

[209] Uslovi korišćenja Fejsbuka (pristupljeno 07.02.2019. godine).
[210] Fejsbuk istraživanja, dotupno na: https://research.fb.com/ (pristupljeno 08. 02. 2019.godine).
[211] Uslovi korišćenja Fejsbuka u Austriji (pristupljeno 07. 02. 2019. godine).

Prikupljamo informacije o tome kako koristite naše Proizvode, kao što su vrste sadržaja koji pregledate ili kojim se bavite; funkcije koje koristite; aktivnosti koje preduzimate; osobe ili nalozi s kojima komunicirate; i vreme, učestalost i trajanje vaših aktivnosti.

[…]

Ako koristite naše Proizvode za kupovinu ili druge finansijske transakcije (npr. kad vršite kupovinu u igri ili dajete donaciju), prikupljamo informacije o toj kupovini ili transakciji. To uključuje podatke o plaćanju, kao što su broj vaše kreditne ili debitne kartice i druge informacije o kartici; druge informacije o nalogu i proveri identiteta; i detalji o naplati, isporuci i kontaktu.

[…]

Takođe primamo i analiziramo sadržaj, obaveštenja i informacije koje druge osobe navode kada koriste naše Proizvode. To može da obuhvata informacije o vama, kao na primer kada drugi dele ili komentarišu fotografiju na kojoj ste vi, šalju vam poruku ili dodaju, sinhronizuju ili uvoze vaše kontakt podatke".[212]

Dakle, iz navedenog se nedvosmisleno može zaključiti da Fejsbuk ima pristup podacima koji se tiču apsolutne komunikacije sa drugima, sadržaju poruka, vrsti kontakta, dalje, ima pristup kameri i imeniku, kao i kontaktima skladištenim na memoriji uređaja. Ovim možemo da zaključimo da je reč o prekomernoj obradi podataka, jer *GDPR* članom 5 (c) propisuje da podaci koji se prikupljaju moraju biti *relevantni*, *ograničeni*, *primereni* u skladu sa svrhom, i sa ciljem *smanjenja količine podataka.* Sadržaj poruka, podaci o kontaktima, podaci skladišteni na internoj memoriji uređaja, očigledno nisu prikupljeni kako bi se omogućila efikasnost usluge, što je osnovna pretpostavka za prikupljanje i obradu podataka, a samim tim i pristanak korisnika na takvu vrstu i obim obrade (član 7 (4)). Takođe, da bi obrada podataka bila legalna korisnici bi morali biti upoznati sa rizikom takve obrade (član 5 i Uvodna odredba (39)), što ni u jednom trenutku nije eksplicitno navedeno.

U posebnom odeljku ovog dela navedeno je kojim informacijama o uređaju ima pristup Fejsbuk:

„Mi prikupljamo informacije o računarima, telefonima, povezanim televizorima i drugim uređajima povezanim preko interneta, koje koristite radi integracije sa našim proizvodima i sjedinjujemo ove informacije širom različitih uređaja koje koristite. Na primer, informacije prikupljene o vašem korišćenju naših proizvoda na vašem telefonu koristimo da bismo bolje personalizovali sadržaj (uključujući reklame) ili funkcije koje vidite kada koristite naše proizvode na nekom drugom uređaju, kao što su laptop ili tablet, ili da bismo procenili da li ste preduzeli neku radnju na drugom uređaju kao odgovor na reklamu koju smo vam prikazali na vašem telefonu".[213]

[212] Fejsbuk, Politika o podacima, u delu: „Koje vrste informacija prikupljamo„, dostupno putem linka: https://www.facebook.com/about/privacy/update/printable (pristupljeno 07. 02. 2019. godine).
[213] Ibid. U delu: „Informacije o uređaju".

Dakle, ukoliko korisnik pristane na Uslove korišćenja Fejsbuka, on je automatski dao dozvolu da Fejsbuk pristupa svim njegovim uređajima povezanim na internet, a sve sa ciljem što učinkovitijeg oglašavanja poslovnih partnera Fejsbuka i merenja efikasnosti reklamiranja.

Između ostalih, informacije koje Fejsbuk prikuplja o uređajima svojih korisnika uključuju:

„Operativni sistem, hardver i verzije softvera, nivo baterije, jačina signala, dostupan prostor za skladištenje, tip pregledača, nazive i vrste aplikacija i datoteka i dodatne komponente.

[…]

Informacije o operacijama i ponašanju na uređaju, kao na primer da li je neki prozor stavljen u prvi plan ili u pozadinu, kao i kretanju miša.

[…]

Jedinstvene identifikatore, ID uređaja i druge identifikatore.

[…]

Informacije koje nam dozvolite da primamo preko uključenih podešavanja uređaja, kao što je pristup GPS lokaciji, kameri i fotografijama.

[…]

Informacije kao što su naziv vašeg mobilnog operatera ili internet provajdera jezik, vremenska zona, broj mobilnog telefona, IP adresa, brzina veze i, u nekim slučajevima, informacije o drugim uređajima koji se nalaze na vašoj mreži ili u njenoj blizini."[214]

Na osnovu navedenih informacija kompanija Fejsbuk u *Politici o podacima* jasno navodi da od svojih korisnika prikuplja gotovo sve informacije, od sadržaja poruka i aktivnosti do tehničkih aspekata njihovih uređaja, bilo da je reč o mobilnim telefonima ili računarima[215]. Premda se ističe da se sve to

[214] Ibid.

[215] Upravo to sugeriše stručnjak za informatičku sigurnost Lucijan Carić, koji za *Al Jazeera Balkans* kaže: „Ono što danas firme poput Fejsbuka i Gugla o vama znaju i prikupljaju, to je ostvarenje najluđih snova najfanatičnijih šefova obaveštajnih službi najtotalitarnijih sistema, a moguće da ni oni u krajnjem ne bi bili toliko inventivni kao ove kompanije – i sve to bez sudskog naloga, bez tajnih uredbi – budući da ste im vi dali pristanak". U tekstu se dalje navodi: „ Zavisno od korisničkih postavki (ali kao što se pokazalo i nevezano za te postavke), aplikacije znaju gde se korisnik trenutno nalazi, koliko se zadržava, kojim smerom i brzinom putuje (znači da li hodate ili se vozite), koga zove telefonom, koliko razgovori traju, mogu snimati te razgovore, mogu snimati zvukove iz okoline telefona kad su uključene, mogu uključiti kameru, mogu videti što korisnik tipka, zapravo mogu sve što može mobilni uređaj ili računar na kojem se aplikacija koristiti, a naravno znaju i podatke o tim uređajima". Mario Pejović (31. mart, 2018). „ Društvene mreže – najbolji špijuni". *Al Jezeera Balkans*. Dostupno na: http://balkans.aljazeera.net/vijesti/drustvene-mreze-najbolji-spijuni (pristupljeno 03. 04. 2018. godine).

čini samo ukoliko korisnik prihvati *Uslove korišćenja*, kojima je obuhvaćena i politika privatnosti, treba istaći da korisnik nema alternativu i ne može selektivno da prihvata uslove – ukoliko želi da kreira nalog, mora da prihvati sve uslove, između ostalog i način na koji će kompanija koristiti njegove podatke. *GDPR* predviđa postojanje poštenog izbora da bi pristanak na *Uslove korišćenja* bio validan (član 7; Uvodna odredba (42)). Korisnik može opciono da utiče na pojedine funkcije, kao što su podešavanja kolačića, ali je, kao i u slučaju Gugla, obavešten o riziku da takva odluka može uticati na kvalitet usluge ili mogućnost usluge uopšte.

Pored samostalnog prikupljanja podataka o korisnicima, Fejsbuk podatke dobija i od svojih partnera „oglašivača, kreatora drugih aplikacija, izdavača", koji Fejsbuku dostavljaju podatke o aktivnostima njihovih korisnika, na primer o tome koju su aplikaciju instalirali na svom uređaju, koje su proizvode kupili i slično. U ovom delu poseban link vodi korisnike na *Facebook Business*[216] alatke i *Centar za pomoć: Na koji način Fejsbuk sarađuje sa dobavljačima podataka?*[217] detaljno objašnjava ovaj proces. U ovom delu *Politike* navodi se da treća lica sa kojima Fejsbuk sarađuje mogu proslediti podatke Fejsbuku, bez obzira da li je pojedinac čiji se podaci prosleđuju korisnik Fejsbuka ili ne. Naglašava se da Fejsbuk zahteva da treća lica takvu radnju sprovode legalno. Takođe, Fejsbuk upućuje svoje dobavljače podataka na obrasce kojima se dobija odobrenje za takvu aktivnost, odnosno daje mogućnosti korisnicima da odbiju takvu vrstu prikupljanja podataka[218]. Iako je evidentan napredak da se korisnicima približi delatnost dobavljača podataka i njihova saradnja sa Fejsbukom, zamerke upućene ovom delu *Politike* odnose se na kompleksnost jezika[219] (član 7 (2)) i nedovoljne transparentnosti (*GDPR,* član 5 (1)) u pogledu identifikovanja trećih lica, koja se najčešće nazivaju *dobavljačima, partnerima* i slično.

Drugi deo *Politike o podacima* govori o načinu na koji Fejsbuk koristi prikupljene podatke. U prvom delu istaknute su pogodnosti za korisnike, odnosno korišćenje njihovih podataka za izgradnju personalizovanih ponuda stranica koje su u skladu sa njihovim interesovanjima, pronalaženje osoba sa kojima bi verovatno želeli da postanu prijatelji, ali i reklama, koje bi odgovorile njihovim interesovanjima – akcenat je stavljen i na to da se prikupljeni podaci koriste za poboljšanje korisničkog iskustva, tehnološke inovacije, pa i za "dobrobit društva" u celini. U nastavku se zatim detaljnije obrazlažu načini korišćenja lokacije, i posebno dodaju načini na koje se Fejsbuk proizvodi međusobno snabdevaju informacijama:

> „Na primer, možemo da predložimo da se pridružite nekoj grupi na Fejsbuku koja uključuje ljude koje pratite na Instagramu ili s kojima komunicirate na Mesindžeru (*Messenger*). Takođe možemo da učinimo da vaš doživljaj bude nesmetan, na primer,

[216] *Facebook Business* alatke dostupno putem linka: https://www.facebook.com/help/331509497253087 (pristupljeno 07. 02. 2019. godine).
[217] Fejsbuk. Centar za pomoć. (pristupljeno 07. 02. 2019. godine).
[218] Ibid.
[219] Na primer: „*Facebook Business* alatke predstavljaju tehnologije koje pruža *Facebook* Inc. i *Facebook Ireland Limited* koje pomažu vlasnicima veb lokacija i izdavačima, programerima aplikacija i poslovnim partnerima, uključujući oglašivače i druge da izvrše integraciju sa uslugom Facebook, da razumeju i mere proizvode i usluge i da lakše stignu do ljudi koji koriste njihove proizvode i usluge ili su zainteresovani za njih. Ove alatke obuhvataju API-ije i SDK, *Facebook piksel, Facebook* društvene dodatne komponente poput dugmeta 'Sviđa mi se' i 'Podeli', *Facebook* prijavu i *Account Kit,* kao i druge integracije platforme, dodatne komponente, kod, specifikacije, dokumentaciju, tehnologiju i usluge". *Facebook Business* alatke: https://www.facebook.com/help/331509497253087 (pristupljeno 23. 06. 2018. godine).

automatski popunjavajući informacije potrebne za registraciju (kao što je broj telefona) iz jednog Fejsbuk proizvoda kada se registrujete za nalog u nekom drugom proizvodu"[220].

Primetan je napor da se viškom informacija i detaljnijim objašnjenjima korisnicima približi *Politika*, međutim, obim podataka koji se obrađuje i dalje ostaje upitan, kao i to da ni u celom ovom odeljku nisu predočeni rizici takvog masovnog prikupljanja i korišćenja podataka korisnika (član 5 i Uvodna odredba (39)).

Treći deo *Politike o podacima* posvećen je načinu na koji se prikupljeni podaci dele. Najznačajnije odredbe GDPR u ovoj oblasti tiču se transparentnosti u pogledu lica sa kojima se podaci korisnika dele (član 5; Uvodna odredba (39); član 13 (d,e,f)), pa će u skladu sa tim biti analiziran ovaj deo *Politike*. Naime, korisnici delimično sami odlučuju o tome sa kim će deliti informacije, posredstvom podešavanja privatnosti na svom nalogu. U tom smislu, korisnik može da odluči da li će njegove objave na ovoj društvenoj mreži biti vidljive za sve, samo za prijatelje ili čak samo za određene prijatelje. Ovakav postupak individualnog podešavanja privatnosti može se primeniti na sve objave na Fejsbuku, fotografije, statuse, video-zapise, podeljene linkove i slično.

Kada je reč o deljenju informacija sa trećim stranama, na primer korišćenje aplikacije neke igrice preko Fejsbuka, nije tako ograničeno. Naime, programeri tih aplikacija mogu, takođe, da prikupljaju podatke o korisnicima, ali i o njihovim prijateljima. Njihovo korišćenje podataka nije obuhvaćeno *Politikom o podacima* Fejsbuka, već podleže njihovim politikama, što bi značilo da ukoliko je Fejsbuk korisnik ujedno i korisnik neke igrice trećeg lica koje je partner sa kompanijom Fejsbuk, podaci korisnika sa Fejsbuka nisu zaštićeni od strane Fejsbuka, već podležu politici o podacima trećeg lica – na primer, programerima određene aplikacije. Prosečan korisnik bi u tom smislu morao da poznaje obe politike o podacima, pri čemu ne može siguran kako njegove aktivnosti na Fejsbuku koristi treće lice, a sam Fejsbuk u tom kontekstu ima ograničenu odgovornost.

U nastavku se navode *spoljni partneri* sa kojima Fejsbuk deli informacije o korisnicima. Na početku Fejsbuk obaveštava korisnike da je takav vid deljenja podataka neophodan, jer on omogućava pružanje besplatne usluge korišćenja Fejsbuka. Odnosno, Fejsbuk naplaćuje svoje usluge spoljnim partnerima, stoga Fejsbuk korisnici *besplatno* koriste usluge Fejsbuka. Ovakva tvrdnja može da dovede u zabludu da je korišćenje Fejsbuka zaista besplatno. Međutim, kako piše Radojković: „sve više je jasno da se upotreba popularnih društvenih mreža koje su besplatne ipak plaća – ličnim podacima" (Radojković, 2017: 23). Svakako, Fejsbuk svoje usluge ne naplaćuje novčano, ali da bi nam bilo jasnije kako Fejsbuk ipak naplaćuje usluge krajnjim korisnicima, moramo da razumemo da su „lični podaci postali novi izvor ekonomije vrednosti", odnosno da su kompanije poput Gugla i Fejsbuka „izgrađene na ekonomiji ličnih podataka" (Esteve, 2017: 36).

Primeri trećih lica sa kojima Fejsbuk deli informacije jesu: oglašivači, kompanije, odnosno njihovi analitičari i statističari, prodavci proizvoda i usluga, istraživači i organi reda, kada imaju sudski nalog za takav zahtev. Ono što je istaknuto jeste da kompanija Fejsbuk komercijalnim partnerima ne ustupa pojedinačne informacije korisnika već generisane, koje zatim spoljni partneri koriste za targetiranje ciljnih grupa ili evaluaciju svoje učinkovitosti. Na primeru oglašivača pojašnjeno je da Fejsbuk ne ustupa podatke koji mogu da identifikuju pojedinca, kao što su ime ili mejl adresa. Međutim, već je bilo reči o tome da nova regulativa predviđa mogućnost re-identifikacija putem IP adresa ili drugih sprecifičnih identifikatora (*GDPR*, Uvodna odredba (30)), stoga je jedan od primarnih uslova obaveštavanje korisnika o takvim i sličnim rizicima prilikom obrade podataka (član 5 i Uvodna odredba (39)), što ni u ovom delu *Politike* nije predočeno.

[220] Fejsbuk, Politika o podacima (pristupljeno 22. 06. 2018. godine).

Jedna od stavki u ovom delu odnosi se na novog vlasnika, odnosno na pitanje šta se dešava sa podacima korisnika ukoliko se promeni vlasništvo cele kompanije ili nekog njenog dela. Naime, u takvoj situaciji Fejsbuk prenosi sve ili deo skladištenih podataka o korisnicima novom vlasniku. S obzirom na to da su korisnici prihvatanjem *Uslova korišćenja* sklopili ugovor sa komapanijom Fejsbuk na čelu sa Markom Zakerbergom, opravdano se može postaviti pitanje da li bi korisnici pristali na iste uslove da je vlasnik bila kompanija koja promoviše vrednosti koje nisu u skladu sa njihovim. Da li bi u situaciji promene vlasnika bilo opravdanije sklapanje novog ugovora, čime bi se korisnicima dala mogućnost izbora u odnosu na to ko može raspolagati njihovim ličnim podacima.

U posebnom odeljku objašnjava se način na koji Fejsbuk kompanije sarađuju. Pojašnjenje je šturo, u jednom pasusu opisno se konstatuje da Fejsbuk kompanije poput Vacapa (*WhatsApp*) i Instagrama dele infrastrukturu i tehnologiju, stoga međusobno sarađuju kako bi obezbedili bolje iskustvo i inovirali sisteme – međutim, izostaje deo gde bi pojasnili na koji način ove kompanije dele podatke o korisnicima.

Kada je reč o brisanju podataka, u *Politici* se navodi da korisnik u svakom trenutku može da izbriše podatke koje je sam podelio, ali kada je reč o podacima koji su prikupljeni preko, na primer, veb-pretrage ili kolačića, nije takav slučaj: „Na primer, kada pretražujete nešto na Fejsbuku možete da pristupite tom upitu i da ga izbrišete iz svoje istorije pretrage u svakom trenutku, ali se evidencija o toj pretrazi briše nakon 6 meseci"[221].

U *Politici* se, kao što je to slučaj sa Guglovom *Politikom*, ne navodi eksplicitno „pravo na zaborav" (*GDPR*, član 17). Fejsbuk ne daje jasan odgovor o zadržavanju podataka: „Ovo se utvrđuje od slučaja do slučaja što zavisi od stvari kao što je priroda podataka, zašto su prikupljani i obrađivani, kao i relevantnih pravnih ili operativnih potreba za čuvanjem".[222] Navedeno je i da se evidencije o pretrazi brišu nakon šest meseci, podaci prikupljeni od kolačića se čine anonimnim ili brišu u roku od 90 dana. Navedena obrazloženje podložna su različitim interpretacijama i ne daju korisnicima jasnu sliku o tome koliko se dugo zadržavaju njihovi podaci, iako GDPR jasno zahteva transparentnost u pogledu zadržavanja podataka i skraćeno vreme zadržavanja (član 5 (1) (e); Uvodna uredba (39).

Sledeći deo *Politike* pojašnjava kako Fejsbuk odgovara na pravne zahteve i sprečava nastanak štete. U ovom delu navodi se da Fejsbuk deli podatke korisnika sa regulatornim telima i organima reda:

> „Kao odgovor na pravni zahtev (kao što je nalog za pretragu, sudski nalog ili sudski poziv) ako u dobroj nameri verujemo da se to od nas zahteva zakonom. To može da obuhvata odgovor na pravne zahteve iz jurisdikcija izvan Sjedinjenih Američkih Država kada u dobroj nameri verujemo da je odgovor neophodan na osnovu prava u toj jurisdikciji, da utiče na korisnike u toj jurisdikciji i da je u skladu sa međunarodno priznatim standardima"[223].

Dalje, *Poltikom* se pojašnjava da je globalni prenos podataka korisnika neophodan i da se Fejsbuk oslanja na preporuke Evropske komisije kada je reč o zaštiti podataka, te da sami korisnici pristajanjem na uslove daju svoj pristanak za prenos podataka u SAD i druge zemlje.

[221] Ibid. u delu: Na koji način mogu da upravljam o informacijama o sebi ili da ih izbrišem?
[222] Ibid. U delu: „Na koji način mogu da upravljam podacima o sebi ili da ih izbrišem?"
[223] Ibid. U delu: „Na koji način odgovaramo na pravne zahteve ili sprečavamo nastanak štete?"

Na kraju *Politike privatnosti* Fejsbuk obaveštava korisnike o načinu na koji mogu da kontaktiraju kompaniju, ukoliko imaju dodatna pitanja. Takođe, upućuju korisnike na kompaniju *TrustArc*[224], posredstvom koje mogu da rešavaju sporove koje imaju sa kompanijom Fejsbuk, a koji su u vezi sa zaštitom podataka.

Politika privatnosti bila je najkompleksniji deo *Uslova korišćenja*. Treći deo *Uslova korišćenja* odnosi se na obaveze korisnika prema Fejsbuku. U skladu sa inicijalnom vizijom Fejsbuka i insistiranju na transparentnosti i iskrenosti, prvi uslov koji se stavlja pred korisnike jeste tačnost navedenih podataka i ističe se značaj akcija usmerenih protiv lažnih profila na ovoj društvenoj mreži. Takođe, korisnici se pozivaju da poštuju prava drugih, ali i da sami prijavljuju neželjen sadržaj i tako pomognu izgradnji bezbednijeg okruženja.

U ovom delu *Uslova* se između ostalog, korisnici eksplicitno obaveštavaju da prihvatanjem *Uslova* daju dozvolu za korišćenje njihovih sadržaja:

> „Preciznije, kada delite, objavljujete ili dodajete sadržaj koji je obuhvaćen pravima intelektualne svojine (kao što su fotografije ili video zapisi) u okviru naših Proizvoda ili u vezi sa njima, dajete nam neisključivu, prenosivu, širom sveta primenjivu licencu, bez naknade, sa pravom podlicenciranja, da hostujemo, koristimo, distribuiramo, menjamo, pokrećemo, kopiramo, javno izvodimo ili prikazujemo, prevodimo i od vašeg sadržaja stvaramo dela prerade (u skladu sa vašim podešavanjima za privatnost i aplikacije). To znači da, na primer, ako podelite neku fotografiju na Fejsbuku, nama dajete dozvolu da je čuvamo, kopiramo i delimo s drugima (da ponovimo, prema vašim podešavanjima), kao što su pružaoci usluga koji podržavaju našu uslugu ili druge Fejsbuk proizvode koje koristite"[225].

Korisnici ovim ugovorom daju svoj pristanak na apsolutno raspolaganje sadržajem koji dele na ovoj mreži. Premda se čelnici kompanije pozivaju na posebna podešavanja, ona se uglavnom odnose na deljenje sa prijateljima na Fejsbuku.Kontrola deljenja sadržaja koja se odvija između Fejsbuka i trećih lica koja Fejsbuku plaćaju usluge nije kontrolisana od strane korisnika, osim u delu gde korisnik pristaje na *Uslove*, jer je alternativa brisanje profila. I sledeći deo *Uslova* govori upravo o tome da su korisnici dali svoju dozvolu za deljenje podataka sa sponzorisanim stranama:

> „Dajete nam dozvolu da koristimo vaše ime i sliku na profilu i informacije o aktivnostima koje ste preduzeli na Fejsbuku pored ili u vezi sa reklamama, ponudama i drugim sponzorisanim sadržajem koji smo prikazali širom naših proizvoda, bez naknade za vas. Na primer, možemo da prikažemo vašim prijateljima da ste zainteresovani za oglašeni događaj ili da vam se sviđa stranica koju je napravio brend koji nam je platio da prikažemo njihove reklame na Fejsbuku"[226].

Kompanija u nastavku navodi da je svaki korisnik slobodan da u bilo kom trenutku izbriše svoj nalog ukoliko nije saglasan sa navedenim uslovima. Na osnovu svih informacija o ličnim podacima koji se prikupljaju, obrađuju i dele sa trećim licima, jasno je da je reč o prekomernoj obradi podataka koja nije nužna sa ispunjavanje svrhe usluge koju Fejsbuk pruža (članom 5 (c), član 7 (4)).

---

[224] *TrustArc*. Dostupno putem linka: https://feedback-form.truste.com/watchdog/request (pristupljeno 07. 02. 2019. godine).
[225] Uslovi korišćenja Fejsbuka u Austriji (pristupljeno 07. 02. 2019. godine).
[226] Ibid.

Ostale obaveze oslanjaju se na poštovanje *Standarda zajednice*[227]. *Standardi* obuhvataju tri široka polja: *Bezbednost*, *Glas* i *Pravičnost*. Kada je reč o bezbednosti, Fejsbuk je razvio posebne mehanizme uklanjanja štetnog sadržaja sa svoje mreže. Pod štetnim sadržajem uglavnom se podrazumeva govor mržnje, nasilnički sadržaji, različiti vidovi zlostavljanja i slično. U ovom delu *Uslova* susrećemo se sa pitanjem cenzurisanja sadržaja, odnosno sa ***pravom na slobodno izražavanje***. Fejsbuk sebe opisuje kao neutralnu platformu, bez uređivačke politike, bar kada je reč o tradicionalnom načinu uređivanja u koja su uključeni ljudi. Odsustvo uređivačkog procesa bilo je glavni argument čelnicima Fejsbuka da tvrde kako oni nisu medijska organizacija, te nemaju odgovornost koju sa sobom nosi medijska aktivnost, između ostalog i značajan udeo u pravu na izražavanje. Međutim, Natali Helberger i Damijan Triling (Damian Trilling) 2016. godine navode:

> „Otkriveno je. Fejsbuk nije neka magična crna kutija mašina za vesti. Koristi urednike. [...] Fejsbuk sada ima više ciljeve. Želi da obavesti ljude o tome šta zavređuje da bude vest i šta je vredno znati. Fejsbuk više nije jednostavna 'platforma za sve ideje'. [...] sada je jasno da je Fejsbuk prešao liniju koja razlikuje hostovanje sadržaja od urednika sadržaja, a biti urednik donosi i pravne i etičke odgovornosti. [...] Sada kada je Fejsbuk prešao liniju, vreme je da se mediji i akademici probude i bliže sagledaju šta je to što Fejsbuk smatra vestima i koju ulogu želi da igra u industriji vesti"[228].

Maja 2016. godine procurio je dokument koji dokazuje da Fejsbuk koristi urednike kako bi odredio koje su vesti značajne[229]. Drugim rečima, Fejsbuk učestvuje u kreiranju agende vesti, premda su čelnici ove kompanije oduvek tvrdili da se Fejsbuk ne može smatrati medijskom organizacijom, jer algoritmi odlučuju o tome koje su vesti u fokusu, bez učešća ljudskog faktora. Interni dokument Fejsbuka „Trending Review Guidelines"[230] nedvosmisleno je upućen timovima ljudi koji su zaduženi za opšte uređivačke procese. Teme koje su u fokusu i rangiranje sadržaja su sledeće:

> „**Urednički tim** je odgovoran za prihvatanje svih naslova koji reflektuju događaje u realnom svetu. Mi obezbeđujemo kontekst kako bismo pomogli ljudima da razumeju trend i obezbeđujemo metapodatke kako bismo informisali algoritme da targetiraju trendove.
>
> **Tim za otkrivanje tema** odgovoran je za podizanje na površinu tema koje su na čekanju i njihovo rangiranje nakon što su prihvaćene.
>
> **Tim za rangiranje sadržaja** odgovoran je za isporuku visokog kvaliteta" (*Trending Review Guidelines*)[231].

Kasnije, nakon brojnih kritika upućenih na algoritamsko upravljanje osetljivim pitanjima, ali i sve češće postavljano pitanje o učešću ljudi u uređivanju informacija koje će se širiti mrežom, Fejsbuk je i zvanično uposlio veliki broj ljudi (prema podacima koje je 2017. godine objavio QUARTZ blizu

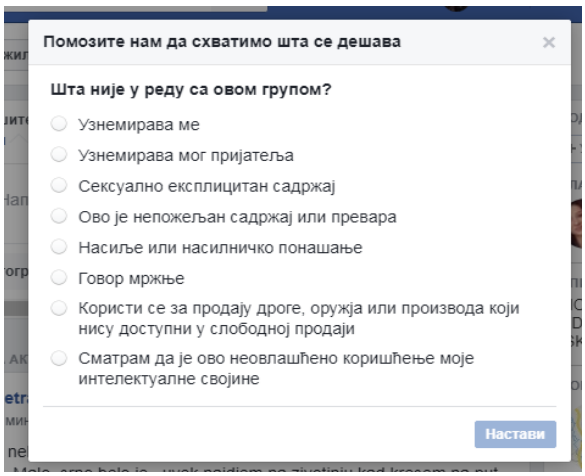
[227] Standardi zajednice na Fejsbuku, dostupno putem linka: https://www.facebook.com/communitystandards/ (pristupljeno 07. 02. 2019. godine).
[228] Helberger, N.,Trilling, D., (2016). *LSE blog*.
[229]Thielman, S. (12 May 2017). „ Facebook news selection is in hands of editors not algorithms, documents show". *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2016/may/12/facebook-trending-news-leaked-documents-editor-guidelines (pristupljeno 04. 03. 2018. godine).
[230] Trending Review Guidelines, dostupno putem linka: https://fbnewsroomus.files.wordpress.com/2016/05/full-trending-review-guidelines.pdf (pristupljeno 04. 03. 2019. godine).
[231] Ibid.

9000 ljudi)[232] koji moderiraju takav sadržaj. Već je bilo reči o primerima gde je Fejsbuk manipulisao objavama koje će se pojavljivati u *News Feed*-u, čime direktno daje na značaju određenim informacijima, odnosno uskraćuje važnost drugim. Svakako da neke od odrednica značaja mogu biti i aktuelnost objava ili faktori personalizovanog interesovanja korisnika. Međutim, ukoliko se *News Feed*-om manipuliše u eksperimentalne svrhe, o čemu svedoči primer iz 2014. godine, jasno je da se može manipulisati i u komercijalne, pa i političke.

Pod principom *Glas*, Fejsbuk podrazumeva zaštitu slobode govora i iznošenje različitih mišljenja i stavova. Naime, u ovom delu se navodi:

> „Uvek ćemo pre odabrati da dozvolimo sadržaj, čak i ako ga neko smatra problematičnim, osim ukoliko bi uklanjanje tog sadržaja sprečilo određenu štetu. Štaviše, ponekad ćemo dozvoliti sadržaj koji je važan, koji predstavlja vest ili je od javnog značaja – čak i ako u drugim okolnostima krši naše standarde. To radimo nakon procene vrednosti javnog značaja sadržaja u odnosu na rizik od štete koju može naneti u stvarnom svetu."[233]

Treći princip *Pravičnost* je svojevrsna dopuna prethodnom principu kojim se promoviše sloboda izražavanja. Ovim principom ističu se poteškoće kompanije da uvek reaguje u skladu sa navedenim smrenicama, ističući značaj konteksta pojedinačnih situacija, kada kompanija reaguje „u duhu smernica, a ne na osnovu doslovnog teksta smernica"[234]. Takođe, u ovom delu *Smernica* članovi Fejsbuk zajednice, odnosno korisnici, pozivaju se na aktivno učestvovanje u izgradnji bezbedne platforme, pri čemu se eksplicitno navodi da je to odgovornost svih. Korisnici se pozivaju da prijave štetne sadržaje kada ih uoče, a mere koje Fejsbuk u tom slučaju sprovodi u rasponu su od opomene do suspendovanje profila. Aktivnost korisnika koja podrazumeva prijavu drugih korisnika zbog deljenja štetnog sadržaja podložan je manipulaciji. Korisnik može da prijavi određeni profil ili stranicu ili konkretnu objavu kao štetnu (videti sliku 2.). Sistem funkcioniše tako da Fejsbuk dobija obaveštenje da je određeni sadržaj prijavljen kao štetan.



Slika 2 Postupak prijave štetnog sadržaja na Fejsbuku

[232] Dave Gershgorn & Mike Murphy (October 12, 2017). „Facebook is hiring more people to moderate content than Twitter has at its entire company". *QUARTZ*. https://qz.com/1101455/facebook-fb-is-hiring-more-people-to-moderate-content-than-twitter-twtr-has-at-its-entire-company/ (pristupljeno 04. 04. 2018. godine).
[233] *Standardi zajednice* na Fejsbuku, u delu *Glas* (pristupljeno 07. 02. 2019. godine).
[234] Ibid. u delu *Pravičnost*.

Samoregulatorni mehanizam koji podrazmeva aktivnost „uoči i ukloni", takođe, otvara brojna pitanja o mogućnostima manipulisanja. Jasno je da postoje nedvosmisleno štetni sadržji, poput pornografije, prikazivanja scena nasilja i slično, međutim, ono što je sporno odnosi se na način na koji korisnici „uočavaju", a Fejsbuk „uklanja" takav sadržaj. Ovaj sistem ostavlja prostor za manipulaciju prijavljivanjem sadržaja koji nije štetan u domenu ponuđenih kategorija. Moguće je, na primer, organizovanje grupe ljudi koji će istog dana prijaviti određeni profil, nakon čega administratori Fejsbuka suspenduju profil, dok ne ustanove da li je reč o stvarnom kršenju pravila ponašanja na Fejsbuku. Međutim, dok analiza prijave traje, korisnik ostaje uskraćen za korišćenje svog profila, čime mu se uskraćuje pravo na slobodu izražavanja, naročito ukoliko se uzmu u obzir primeri prijavljivanja političkih neistomišljenika. Radmilo Marković (2016) u svom članku navodi:

> „U poslednjih nekoliko nedelja korisnici društvenih mreža u Srbiji mogli su da primete da se povećava broj onih koji tvrde da su blokirani na Fejsbuku (FB), najpopularnijoj društvenoj mreži na svetu […] Većina njih svoje neugodno iskustvo privremenog ili trajnog isključenja sa FB dovodi u vezu sa vladajućim SNS-om i njegovim liderom"[235].

Autor teksta navodi iskustva više opozicionih lidera kojima je Fejsbuk blokirao nalog nakon objavljivanja kritika na račun aktuelne vlasti. Jedan od primera u tekstu je i Ljubiša Preletačević Beli, kome je Fejsbuk suspendovao nalog, bez upozorenja, sat vremena nakon što je objavio tekst kojim kritikuje svoje političke oponente. Onizražava sumnju da je verovatno organizovano upućen veliki broj prijava na koje je Fejsbuk reagovao suspenzijom profila[236].

Najznačajniji deo *Uslova* dolazi na kraju, gde se kompanija vrlo jasno ograđuje od bilo kakve odgovornosti za bilo kakvu potencijalnu štetu korisnika:

> „Naporno radimo da obezbedimo što bolje proizvode i damo jasne smernice svima koji ih koriste. Naši proizvodi su međutim obezbeđeni 'u viđenom stanju' i ne dajemo nikakve garancije da će uvek biti bezbedni, sigurni i bez grešaka niti da će funkcionisati bez prekida, kašnjenja ili nedostataka. U meri dozvoljenoj zakonom, takođe ODRIČEMO SE SVIH GARANCIJA, IZRIČITIH ILI PODRAZUMEVANIH, UKLjUČUJUĆI PODRAZUMEVANE GARANCIJE O PODESNOSTI ZA PRODAJU, POGODNOSTI ZA ODREĐENU NAMENU, PRAVU VLASNIŠTVA I NEKRŠENjU. Ne kontrolišemo niti upravljamo onime što ljudi čine ili govore i nismo odgovorni za njihove radnje ili ponašanje (bilo na mreži ili van mreže) niti bilo koji sadržaj koji dele (uključujući sadržaj koji je uvredljiv, neprikladan, nepristojan, nezakonit ili na neki drugi način nepoželjan).
>
> Ne možemo da predvidimo kada može doći do problema s našim proizvodima. Shodno tome, naša odgovornost je ograničena u najvećem obimu dozvoljenom primenjivim pravom i nećemo biti odgovorni prema vama za bilo koji gubitak profita, prihoda, informacija ili podataka niti za posledične, posebne, posredne, kaznene ili direktne

[235] Radmilo Marković (27. oktobar 2016. godine). "Javi Đuri da blokira Fejsbuk". *Vreme*. dostupno putem linka: https://www.vreme.com/cms/view.php?id=1438089&print=yes (pristupljeno 05. 05. 2017. godine).
[236] Ibid.

posledične odštete koje proističu iz ovih Uslova korišćenja ili proizvoda kompanije Fejsbuk ili se na njih odnose, čak i ako smo bili upozoreni o mogućnosti takve odštete"[237].

Iz navedenog može se zaključiti da garancije koje Fejsbuk obećava svojim korisnicima u svim prethodnim delovima *Uslova* zapravo nikada i nisu na snazi, jer nakon svih detaljnih uveravanja u bezbednost korisnika, u samo jednom pasusu se Fejsbuk poziva na ograničenu odgovornost, čime ugovor postaje ništavan.

***

Analizom samoregulatorne politike u oblasti poštovanja prava na slobodno izražavanje i privatnost korisnika, potvrdili smo i drugu hipotezu: *Samoregulatorna politika internet intermedijatora ne garantuje apsolutnu zaštitu prava na privatnost i slobodno izražavanje korisnicima.* Osnovne primedbe koje se tiču novih *Politika privatnosti* Gugla i Fejsbuka, i njihove usklađenosti sa novom EU regulativom mogle bi se odrediti na sledeći način:

(a) ***izostanak „afirmativnog" pristanka korisnika***;
(b) ***netransparetnost u pogledu informacija koje se prikupljaju i u pogledu lica sa kojima se informacije dele*** i
(c) ***netransparentnost u pogledu brisanja i zadržavanja podataka***.

(a) Da bi pristanak korisnika bio dobrovoljan i validan neophodno je da korisnik nedvosmisleno razume *Uslove korišćenja* i da ima pošten izbor koji ne podrazumeva uslov: pristani ili odustani. *GDPR* jasno ističe da uslovi pristanka podrazumevaju *jednostavan jezik* (član 7 (2)), koji je razumljiv prosečnom korisniku, kao i to da se dobrovoljnost pristanka određuje na osnovu toga da li je „pružanje usluge bilo uslovljeno prihvatanjem uslova koji se odnose na obradu podataka, a koja nije bila nužna" (član 7 (4)), odnosno da li je prekomerna obrada podataka ujedno i uslov korišćenja usluge. Takođe, Uvodna odredba (32) samo *aktivni* pristanak[238], koji podrazumeva *informisanog* korisnika, smatra dobrovoljnim i validnim. Kako Estiv (Estive) ističe: „Informisani pristanak leži u srcu prava za zaštitu ličnih podataka" (2017: 42). U slučaju *Politike* Gugla, i pored dodatnog napora za pojašnjenjem stručnih izraza, u delu „ključnih termina", jezik ostaje pretežno tehnički neprilagođen prosečnom korisniku. Njegovo razumevanje zahteva bar osnovno znanje iz tehničko-tehnološke oblasti. S pravom se možemo zapitati da li korisnici „prihvataju politiku privatnosti zato što moraju" (Esteve, 2017: 41).

Trebalo bi pohvaliti i domišljati vizuelni pristup Gugla u rešavanju ovog problema. Putem atraktivnih kratkih animiranih klipova, ne dužih od minut, Gugl je pojedine stavke iz *Politike privatnosti* pojasnio na kreativan i jednostavan način. Ukoliko korisnik nema vremena ili dovoljno predznanja da se upusti u iščitavanje redova i redova suvoparnog

[237] Uslovi korišćenja, u delu *Ograničenje odgovornosti*.
[238] Na primer, Francusko regulatorno telo za zaštitu podataka je 2012. godine, nakon što je Gugl ažurirao politiku privatnosti, tražilo je od kompanije Gugl da im dostave tačan broj korisnika koji su posetili sajt kako bi se upoznali sa novom politikom i utvrdili efektivnost njihovog pristanka. Gugl je to odbio (Esteve, 2017: 41).

teksta, najosnovnije informacije može da dobije na zanimljiv i jednostavan način, putem video-prezentacije[239](videti sliku 3).

Slika 3 Isečci iz promo-klipova Politike privatnosti Gugla (YouTube)[240]

Međutim, trebalo bi imati u vidu da su ovi kratki klipovi svojevrsni promo-materijal, koji ističe samo pozitivne strane Guglove politike. Animirani likovi, koji su sa svojim kućnim ljubimcima, koji sa prijateljima sede u kafiću, ili se vraćaju iz kupovine, dok uz pomoć Guglovih alatki pretražuju obližnje restorane ili destinacije za putovanje, nisu slučajno u tim ulogama. Ovi klipovi mogu sublimalno delovati na korisnike, ostavljajući razdragane animirane likove kao najjači utisak, dok se primarna svrha video-prezentacije podsvesno zanemaruje.

Kada je reč o *Politici* Fejsbuka, jezik je dosta jednostavniji i primereniji prosečnom korisniku, međutim, ne postoji dodatno pojašnjenje u vidu „ključnih termina", kao što je to slučaj sa Guglom. Fejsbuk nudi vizuelnu prezentaciju, koja se može oceniti kao dodatni napor da se korisnicima na jednostavniji način približi politika privatnosti.

Pored nerazumljivog jezika ključno je i pitanje opširnosti *Politika*. Koliko je zapravo prosečnom korisniku potrebno vremena da se upozna sa svim stavkama politika privatnosti, ne samo Gugla ili Fejsbuka, već i njihovih podkompanija, ali i svih ostalih sajtova i aplikacija koje redovno koristi? MekDonald i Krenor (McDonland & Cranor, 2008) sprovele su zanimljivo istraživanje kojim su procenile da je korisniku potreban približno 201 sat godišnje da bi pročitao politike privatnosti sajtova koje koristi. Pored kompleksnosti

[239] Politika privatnosti, *Google*, ili putem Jutjuba: https://www.youtube.com/watch?time_continue=57&v=YlmVKT3Zvhw (pristupljeno 23. 06. 2018. godine).
[240]Isečci iz promo klipova Politike privatnosti Gugla, dostupno na putem linka: https://www.youtube.com/watch?time_continue=44&v=48l-xdS4pXg (pristupljeno 23. 06. 2018. godine).

jezika, opširnost se nameće kao drugi problem. Davanje dodatnih informacija zaista može pozitivno uticati na transparentnost, ali sa druge strane nije „od praktične koristi" (Wagner, 2013: 565), jer korisnicima dodatno otežava upoznavanje sa *Uslovima korišćenja*.

Obe *Politike* su preopširne, zahtevaju višednevno iščitavanje. Proces čitanja dodatno usložnjavaju posebni linkovi koji korisnika vode na nove stranice, pa u nekom trenutku možete otvoriti i preko deset stranica da biste se detaljno upoznali sa samo jednim odeljkom *Politike*.

(b) Transparentnost je, pored odgovornosti, druga ključna reč u novom regulatornom okviru EU. Korisnici moraju biti nedvosmisleno upoznati sa informacijama koje se od njih prikupljaju i sa načinom na koji se one dele sa trećim licima (*GDPR* član 5 i Uvodna odredba (39)). Takođe, korisnici moraju znati koja su to treća lica sa kojima Gugl može podeliti njihove lične podatke (*GDPR*, član 13 (d,e,f)). Analiza novih *Politka* Gugla i Fejsbuka pokazala je da korisnici nisu do kraja upoznati sa ovim informacijama. Poznato je da postoje najmanje dva načina na koja ove kompanije prikupljaju podatke. Jedan od načina podrazumeva lične informacije koje sam korisnik deli, potrebne, na primer, da bi otvorio Gugl nalog ili Fejsbuk profil – i u tom smislu je korisniku jasno koje su to tačno informacije. Drugi način podrazumeva prikupljanje podataka od strane kompanija na načine koji nisu do kraja transparentni. Takvi podaci mogu se prikupljati na osnovu uređaja korisnika, na primer IP adresa, uz pomoć posebnih identifikatora, lokacija i slično, ali mogu se prikupljati i na osnovu pretrage korisnika (Gugl) ili interakcije u vidu „sviđanja" (putem opcije *Like*). Kompanije koriste takav tip informacija kako bi korisniku *obezbedili personalizovano iskustvo*, drugim rečima, kako bi ih prosledili trećim licima, uglavnom oglašivačima, koji onda na osnovu tih informacija uspešno targetiraju svoje ciljne grupe. Problem koji se u ovom procesu javlja jeste netransparentnost u pogledu informacija koje se prikupljaju. Čak i onda kada postoji opis pojedinih podataka koji se na taj način prikupljaju, lista nije konačna i uglavnom se podaci definišu rečima: *poput* ovih podataka, kao *na primer* ovaj podatak i *slični* podaci.

Sledeći problem jeste nepreciznost kada je reč o definisanju trećih lica sa kojima se takav tip podataka deli. Gugl se koristi frazama kao što su *poslovni partneri*, *kompanije koje koriste naše usluge* i slično, dok korisniku ostaje nejasno o kojim kompanijama je zapravo reč. S pravom se možemo zapitati da li korisnik može da prepozna da je njegova privatnost ugrožena, ukoliko ne prepoznaje ni tip podataka koje deli, ni kompanije kojima ih Gugl prosleđuje (Wagner, 2013). Kada je reč o Fejsbuku, *Politikom* su detaljnije opisana treća lica sa kojima se informacije dele. Međutim, u mnogim delovima ostaje nejasno da li odgovornost nad prikupljenim podacima ima Fejsbuk ili kompanija sa kojom sarađuje, na primer kompanija za igrice na Fejsbuku.

(c) Sledeći izazov, koji je novim okvirom EU trebalo uspešno prevazići, jeste pitanje brisanja (*GDPR*, član 17), odnosno zadržavanja podataka o ličnosti (član 5 (1) (e); Uvodna uredba (39)). Guglova *Politika* predviđa brisanje podataka na zahtev, pozivajući se na „pravo na zaborav", čime čini pozitivni pomak ka usklađivanju sa aktuelnom *Uredbom*, Ipak, period zadržavanja podataka i dalje je neprecizno određen. *Politikom* je predviđeno da se pojedini podaci mogu čuvati 6–18 meseci, što ne predstavlja ni *precizan*, ni *razuman* rok, kako to regulativa predlaže. Takođe, ostaje nejasno koji su to podaci koji se zadržavaju, jer

ih Gugl definiše kao *pojedine podatke* – nejasno je i iz kojih razloga su baš oni zadržani, jer su navedeni vrlo opšte i neprecizno.

Kada je reč o Fejsbuku, predviđena je opcija brisanja podataka i naloga, ali se ne spominje „pravo na zaborav" eksplicitno, kao što je to slučaj sa Guglom. Takođe, period zadržavanja podataka nije precizno naveden, kao ni tip podataka koji se zadržavaju na, na primer 30 dana, ili šest meseci.

Izazovima sa kojima se pravo na slobodno izražavanje susreće u oblasti poslovanja internet pretraživača i društvenih mreža, posebno Gugla i Fejsbuka, možemo pristupiti iz najmanje dva ugla:

(a) izazovi koji potiču od industrije i
(b) izazovi koji proističu iz regulative.

(a) Ukoliko pitanju prava na slobodno izražavanje pristupimo sveobuhvatno i pod njim podrazumevamo i pravo da pojedinac širi, ali i dobija informacije iz različitih izvora, te da mu se ne uskraćuje informisanje iz pojedinih izvora, onda odnos rezultata pretrage putem Gugla i slobodnog izražavanja postaje jasan. Sa jedne strane, Gugl ima obavezu prema krajnjim korisnicima da ponuda rezultata bude nepristrasna., Sa druge strane, pak, ima obavezu prema onima koji nude sadržaje, da njihove veb-stranice ne budu diskriminisane, izuzev u slučajevima kada je reč o štetnom sadržaju[241].

Pretraga putem pretraživača Gugl sastoji se od četiri integralna dela: *pre pretraživanja, pretraga, rangiranje* i *rezultat*[242]. Naime, dok korisnik još ne pristupi pretrazi Gugl indeksira dostupne veb-sajtove. Gugl to radi pomoću „veb-popisivača" (*Googlebot*)[243], tako što elektronski „popisuje" veb-sajtove koje vodi nazad do Guglovih servera. U trenutku pretrage, Guglov algoritam traži informacije koje odgovaraju potraživanom pojmu, i uz pomoć „tragova", koji povezuju potraživani pojam sa ponuđenim sadržajima indeksiranih veb-stranica, nudi rezultat pretrage. Ključni deo pretraživanja odnosi se na rangiranje stranica, odnosno na način na koji Guglovi algoritmi rangiraju rezultate. Na njihovom sajtu navodi se da *Gugl ne koristi plaćanje stranica kako bi ih češće popisivao*, odnosno kako bi ih bolje rangirao. Rangiranje stranice (*PageRank*), ili kako je Pejdž i Brin definišu: „objektivna mera značaja citatnosti koja dobro korespondira sa ljudskom subjektivnom idejom o važnosti"[244], najbolji je način davanja prioriteta stranici, smatraju osnivači Gugla. Međutim, neutralnost, zasnovana na algoritamskom uređenju pretraživanja često je dovođena u pitanje (Van Ejik, 2006; Introna & Nissenbaum, 2000; Musiani et al., 2016;

[241] Gugl, Borba protiv nepoželjnog sadržaja, dostupno putem linka: https://www.google.com/intl/sr/insidesearch/howsearchworks/fighting-spam.html (pristupljeno 23. 06. 2018. godine).
[242]Gugl, Infografika, Kako pretraživanje funkcioniše, dostupno putem linka: https://static.googleusercontent.com/media/www.google.com/en/intl/sr/insidesearch/howsearchworks/assets/searchInfographic.pdf (pristupljeno 23. 06. 2018. godine).
[243] Gugl, Popisivanje i indeksiranje, dostupno putem linka: https://www.google.com/intl/sr/insidesearch/howsearchworks/crawling-indexing.html (pristupljeno 23. 06.2018. godine).
[244] Sergey Brin and Lawrence Page. The Anatomy of a Large-Scale Hypertextual Web Search Engine. Dostupno putem linka: http://infolab.stanford.edu/~backrub/google.html (pristupljeno 23. 06. 2018. godine).

Musiani, 2013; Kohl, 2013). Poslednje izmene[245] u pogledu načina pretraživanja, koje Gugl naziva *kvalitativnim poboljšanjima pretrage*, takođe su naišle na kritiku. Naime, poslednje izmene predviđaju jaču kontrolu veb-ponude, te će sajtovi koje Gugl oceni kvalitetnim, odnosno *merodavnim,* imati bolju poziciju pri rangiranju, dok će oni drugi, sa *niskokvalitetnim sadržajem*, biti manje vidljivi. Ovakav način rangiranja, u skladu sa određivanjem nivoa kvaliteta, ostavlja prostor za manipulacije. Jedna od poslednjih primedbi došla je od strane levičara u Americi, koji navode da je stranicama sa njihovim sadržajem opalo rangiranje za 45%, od primene novih izmena[246].

Društvene mreže, među njima i Fejsbuk, mogu biti predmet cenzure ili mogu same cenzurisati određeni sadržaj. U prvom slučaju, pritisak dolazi spolja, u drugom, od same industrije (Jackson, 2014). Brojne su autoritarne vlade koje blokiraju pristup Fejsbuku ili vrše pritisak na Fejsbuk da uklanja određen sadržaj. Sa druge strane, društvene mreže generalno, mogu da filtriraju sadržaj iz različitih razloga, Džekson navodi neke od njih: „ukoliko smeta njihovim poslovnim interesima", ukoliko „veruju da može pogrešno da se odrazi na samu društvenu mrežu", „da bi promovisale specifične političke agende ili kao odgovor na pritisak određenih grupa korisnika" (2014: 130–131). Ukoliko do toga i ne dođe, činjenica da Fejsbuk može tako nešto učiniti ostavlja korisnicima jedino mogućnost da veruju da to neće i učiniti u nekom trenutku. Na kraju, metode kojima se to može sprovesti nisu bliske ni razumljive prosečnom korisniku, pa on za njih saznaje tek onda kada informacije o tome dospeju u javnost, ili ne saznaje uopšte.

Takođe, mogućnost manipulacije objavama u *News Feed*-u (Chambers, 2014; Abbruzzese, 2014) otvara prostor za nametanje tema od društvenog značaja, čime se direktno utiče na slobodu izražavanja korisnika koji se informišu putem ove platforme. Takva manipulacija može biti ekperimentalna, komercijalna, ali i krajnje politička.

(b) Kada je reč o izazovima koji proističu iz regulative, preciznije iz novog regulatornog okvira EU, na meti kritika našao se član 17, *Uredbe* iz 2016. godine, odnosno „pravo na zaborav". Uvođenje ovog člana daje korisnicima veći pristup i kontrolu nad informacijama u novom internet okruženju. Naime, korisnik ima pravo da potražuje brisanje informacija ukoliko one više nisu potrebe za svrhu za koju su primarno prikupljene, ukoliko nisu tačne ili su nezakonito prikupljene. Stav 3, člana 17, navodi izuzetke od ovog člana i to u slučajevima kada tako nešto *ugrožava slobodu izražavanja ili informisanja*, kada *nije u skladu sa javnim interesom,* kada je potrebno zbog *naučnih, istorijskih* ili *statističkih* svrha i slično. Međutim, ovo pravo naišlo je i na negativne kritike kojima se, sumirano, sugeriše da može ugroziti slobodu izražavanja (Fazlioglu, 2013; Singleton, 2015; Kaye, 2017; Nielsen, 2014). Fazlioglu (2013) ističe pozitivne namere nove regulative i davanje veće moći pojedincima u upravljanju i pristupu sopstvenim podacima na internetu, ali i kritikuje primenu člana 17 u kontekstu mogućeg konflikta između prava na zaborav i prava na slobodno izražavanje. Druga kritika odnosi se na neosetljivost primene ovog člana prema nacionalnim razlikama, pa kao primer navodi SAD, gde je slobodno izražavanje gotovo bezuslovno zaštićeno, i neusaglašenost ovog člana sa Prvim amandmanom. Singltonova (Singleton, 2015) analizirajući primer *Google Spain* ističe kritične tačke primene „prava na

[245] *Google,* „ Our latest quality improvements for Search", dostupno putem linka: https://blog.google/products/search/our-latest-quality-improvements-search/ (pristupljeno 23. 06. 2018. godine).
[246] Matthew Sheffield (October 18, 2017) „ 'Fake news' or free speech: Is Google cracking down on left media?". (pristupljeno 24. 06. 2018. godine).

zaborav". Sud pravde Evropske unije je u slučaju *Google Spain* postavio određeni standard na koji bi se mogli pozivati svi kasniji slični slučajevi. Autorka navodi insistiranje Suda na upotrebi *testa balansiranja*, odnosno procene u svakom pojedinačnom slučaju da li će prevagnuti pravo na slobodno izražavanje ili pravo na zaborav, i zaključuje da takav pristup može biti problematičan: „s obzirom na to da jedno pravo ne može uvek da nadmaši drugo, ovo takmičarsko opravdanje nužno rezultira tenzijom između prava na zaborav i prava na slobodno izražavanje" (Singleton, 2015: 180)[247].

Slučaj *Google Spain* izazva je burne i oprečne reakcije i ministara EU. Britanski ministar pravde upozorava na stvaranje prava koja ne mogu biti izvodiva u praksi; Poljski ministar pravde navodi da bi se ovakav presedan mogao negativno odraziti na pravo na slobodno izražavanje u budućnosti; Francuski ministar, takođe, ostaje rezervisan i izražava zabrinutost za ugrožavanjem prava na slobodno izražavanje, dok Španija tvrdi da pravo na zaborav nije neusaglašeno sa pravom na izražavanje (Nielsen, 2014)[248]. Član 17 u Stavu 3 (1) navodi da se ovo pravo neće primenjivati onda kada ugrožava slobodu izražavanja i informisanja, međutim, sporan je način na koji će se u pojedinačnim slučajevima odlučivati o tome da li pozivanje na brisanje podataka, zapravo ugrožava drugo pravo. *Balansiranje* između ova dva prava preporuka je Suda, ali je u krajnjem reč o subjektivnoj proceni, pre svega zbog opšteg određenja prava na slobodno izražavanje, ali i njegovog drugačijeg interpretiranja u okvirima različitih nacionalnih zakonodavstava (primer SAD u odnosu na EU).

4.6. Redefinisanje odgovornosti internet intermedijatora

Internet intermedijatori, kao jedni od centralnih aktera u novom informaciono-komunikacionom okruženju, imaju značajnu ulogu u diseminaciji informacija, i u mnogim oblastima života savremenih korisnika predstavljaju glavni izvor informisanja. Pretraživači i društvene mreže, kao intermedijatori koji su u najneposrednijoj vezi sa krajnjim korisnicima, pružaju neslućene mogućnosti participacije i pozivanja na akcije, i kristališu se kao potporni stubovi u informacionom društvu. Mogućnosti koje novi akteri pružaju korisnicima, ali i njihova moć zaokružena terminom *tehno-giganti,* donosi sa sobom i pitanja njihove odgovornosti, prema krajnjim korisnicima i društvu u celini.

Oni posluju u okvirima pravila ponašanja privatnih kompanija, pa često može biti zamagljen pogled na obaveze koje imaju prema javnom interesu, ali njihov „posao" ne može se posmatrati isključivo u dihotomiji ponuda : potražnja, već u jednom širem okviru koji u sebe uključuje i obaveze i odgovornosti. Upravljanje informacijama ne može se izjednačiti sa upravljanjem bilo kojom drugom

[247] Ukoliko političar traži uklanjanje informacija o tome da je nekada bio član neke nepopularne političke opcije, lako je doneti sud o tome da je pravo javnosti da zna tu informaciju o javnoj ličnosti jače od prava na zaborav. Ukoliko žena koja aplicira za posao traži uklanjanje informacija o svom pijanstvu u vreme studentskih dana jer je to prvi rezultat pretrage njenog imena i svakako se odražava na odluku poslodavca, prilično je jasno da njen studentski život nije od javnog interesa (Singleton, 2015: 181). Međutim, postoje brojni slučajevi kada jedno pravo ne može tako nedvosmisleno da prevagne nad drugim i vodi stvaranju konflikta između ova dva prava.

[248] Nikolaj Nielsen. (10. Oct, 2014) "Freedom of expression complicates EU law on 'right to be forgotten'". *Euobserver*. Dostupno na: https://euobserver.com/justice/126011 (pristupljeno 28. 06. 2018. godine).

robom. Organizovanje i ponuda informacija najvećem delu razvijenog sveta u direktnoj je vezi sa kreiranjem pogleda na svet i dešavanja u njemu, dok omogućavanje pristupa i kreiranja informacija od strane korisnika direktno utiče na učešće korisnika/građana, ostvarivanje njihovih osnovnih prava i, na kraju,na razvoj demokratije u celini.

Privatne kompanije koje „gospodare internetom", među kojima su i Gugl i Fejsbuk, ne negiraju svoju odgovornost u pogledu zaštite ljudskih prava, štaviše u njihovim *Uslovima korišćenja* posebno se insistira na poštovanju slobode izražavanja i zaštiti privatnosti. Međutim, netransparentnost njihovog poslovanja i česti slučajevi kršenja ovih prava pokazuju da svoju odgovornost ne shvataju previše ozbiljno i da onda kada se interes korisnika sukobi sa komercijalnim interesom prevagne drugi. Misleći o tome, Estiv navodi: „Ono što Gugl i Fejsbuk opisuju u svojim politikama privatnosti ne bi se trebalo smatrati njihovim istinskim praksama" (2017: 39). Njihova moć u upravljanju komunikacionim krajolikom na internetu je ogromna, a njihov cilj je jasan: akumulirati što veću količinu podataka. Ove kompanije su izgrađene na ličnim podacima korisnika; Kako piše Nisenbaum: „Lični podaci su 'zlato' nove kategorije kompanija" (2004: 121). Zakerberg, Pejdž i Brin raspolažu neslućenom količinom ličnih podataka, a njihove apetite možda najbolje opisuje Kripatrik koji o Zakerbergu navodi: „On želi da vlada ne samo Fejsbukom, već u nekom smislu komunikacijskom infrastrukturom planete" (2011: 319).

Prepoznajući moć i ulogu intermedijatora, kao i potencijalne opasnosti po bezbednost korisnika, evropski regulatorni okvir predviđa brojne obaveze i preporučuje regulatorne i samoregulatorne mere u vezi sa intermedijatorima. *Preporuka (CM/Rec(2011)7) Komiteta Ministara državama članicama u vezi sa novim poimanjem medija* prepoznaje nove aktere kao izuzetno značajne u novom medijskom ekosistemu, pa u skladu sa tim insistira na njihovoj odgovornosti. *Preporuka* nove aktere razlikuje od medija u tradicionalnom smislu, ali kod njih prepoznaje funkcije koje su istovetne medijskim – ima slučajeva kada ih i nadmašuju, na primer kada govorimo o globalnoj dostupnosti ili participaciji. *Preporuka* posebno ističe njihovu ulogu u *kontroli* i *nadzoru* nad informacijama. Prepoznajući i njihove uređivačke funkcije, ona poziva kreatore politika da posebnu pažnju obrate na poštovanje osnovnih ljudskih prava u okvirima poslovanja internet intermedijatora.

Preporuka (CM/Rec(2014)6) komiteta ministara državama članicama o vodiču o ljudskim pravima za korisnike interneta[249] poziva države članice Saveta Evrope da obezbede svojim građanima poštovanje njihovih prava i na internetu. *Preporukom* se ističe da su ljudska prava *univerzalna i nedeljiva*, te da uvek imaju prednost u odnosu na pravila koja korisnicima nameću privatne internet kompanije. Posebno izdvojena prava su pored *prava na pristup*, *okupljanje*, *udruživanje i učestvovanje*, *obrazovanje i pismenost* i prava koja su predmet analize disertacije: *sloboda izražavanja* i *privatnost i zaštita podataka.* Kreatori *Preporuke* napominju da ova prava nisu nova, niti posebno osmišljena za internet okruženje, već predstavljaju osnovna ljudska prava koja se moraju poštovati bez obzira na medijum i okruženje u kom se ostvaruju.

[249] Preporuka dostupna putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f4d (pristupljeno 20. 06. 2018. godine).

Preporuka (CM/Rec(2018)2) Komiteta Ministara državama članicama o ulogama i odgovornosti internet intermedijatora[250] usvojena je 7. marta 2018. godine. Ovom *Preporukom* posebno se tretiraju pravo na slobodno izražavanje i zaštita ličnih podataka. U delu o slobodi izražavanja navodi se: „Povećanjem sposobnosti javnosti da traži, prima i prenosi informacije bez uplitanja i bez obzira na granice, internet igra posebnu ulogu u pogledu prava na slobodu izražavanja" (CM/Rec(2018)2, Uvodna odredba (2)). *Preporukom* se državama članicama predočava da država ne može uskraćivati pravo na slobodno izražavanje pojedinaca vršenjem pritiska na intermedijatora, osim kada je reč o krivičnom delu, takođe, država je obavezna da zaštiti građane ukoliko privatne kompanije ugrožavaju pravo na slobodno izražavanje njenim građanima, te mora da sarađuje sa intermedijatorima u izgradnji politike kojom će ovo pravo biti garantovano, kooperacijom regulatornih i samoregulatornih mehanizama (CM/Rec(2018)2: 1.3). Pravo na privatnost *Preporuka* tretira kao *osnovu za uživanje i ostvarivanje većine drugih prava i sloboda* (CM/Rec(2018)2, Uvodna odredba (3)).

Komitet Ministara dvema Preporukama posebno predviđa poštovanja ljudskih prava u odnosu prema pretraživačima, odnosno društvenim mrežama, i ističe njihovu odgovornost u tom pogledu. Naime, *Preporuka (CM/Rec(2012)3) Komiteta Ministara državama članicama o zaštiti ljudskih prava u odnosu na pretraživače*[251] tretira pretraživače kao značajne aktere u demokratskim praksama i procesima i posebno ističe mogućnost ugrožavanja ljudskih prava pri poslovanju pretraživača:

> „Akcija pretraživača može uticati na slobodu izražavanja […] na pravo na privatni život i zaštitu ličnih podataka. Takvi izazovi mogu proizaći, između ostalog, iz dizajna algoritama, deindeksiranja i/ili parcijalnog tretmana ili pristranih rezultata, koncentracije tržišta i nedostatka transparentnosti oko procesa odabira i rangiranja rezultata" (CM/Rec(2012)3, član 4).

Kada je reč o slobodnom izražavanju *Preporukom* se pretraživači postuliraju kao jedni od najznačajnijih aktera u pogledu ostvarivanja ovog prava u novom informaciono-komunikacionom okruženju:

> „Pretraživači imaju ključnu ulogu, kao jedna od prvih tačaka kontakta na internetu, u ostvarivanju prava traženja i pristupa informacijama, mišljenjima, činjenicama i idejama, kao i ostalim sadržajima, uključujući i zabavu. Takav pristup informacijama bitan je za izgradnju nečijeg ličnog mišljenja i učestvovanja u društvenom, političkom, kulturnom i ekonomskom životu. Pretraživači su takođe važan portal pristupa građana masovnim medijima, uključujući elektronske novine i audiovizualne medijske usluge" ((CM/Rec(2012)3).

Kada je reč o najčešćem načinu na koji se ugrožava ovo pravo, *Preporuka* prepoznaje netransparentnost u pogledu rangiranja rezultata pretrage: „Većina pretraživača pruža vrlo malo ili samo opšte informacije o tim pitanjima, a posebno o kriterijumima koji se koriste za kvalifikovanje

---

[250] Engl. *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14 (pristupljeno 23. 06. 2018. godine).

[251] engl. *Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines*, dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87 (pristupljeno 24. 06. 2018. godine).

određenog rezultata kao 'najboljeg' odgovora na određeni upit" ((CM/Rec(2012)3. Analiza pretraživača Gugl potvrdila je opasnost za slobodu izražavanja, koje pretpostavlja i ova *Preporuka*.

Kada je reč o zaštiti privatnosti, *Preporuka* upozorava na ogromne količine informacija koje pretraživači prikupljaju od svojih korisnika, a da korisnici nisu do kraja upoznati sa vrstom podataka, ni načinom dalje obrade, što smo potvrdili i na primeru Gugla. Stoga, *Preporuka* posebno ističe značaj: *povećanja transparentnosti* u pogledu načina odabira informacija, odnosno način *rangiranja*, da bi se obezbedio pluralizam i različitost, *povećanja transparentnosti pri obradi ličnih podataka*, pristup ličnim podacima i mogućnost brisanja, kako bi se osiguralo pravo na privatni život i zaštita ličnih podataka.

Preporuka (CM/Rec(2012)4) Komiteta Ministara državama članicama o zaštiti ljudskih prava u odnosu prema društvenim mrežama[252] posebno tretira pitanja uloge i značaja društvenih mreža, ali i potencijalne opasnosti po ljudska prava, posebno slobodu izražavanja i pravo na privatnost. Naime, *Preporukom* se društvene mreže definišu kao veoma značajne u procesu širenja i primanja informacija, te značajne u pogledu oblikovanja javnog mišljenja i učestvovanju u političkom, društvenom i ekonomskom životu. Društvenim mrežama se upućuje zahtev za *zaštititom korisnika bez narušavanja prava na slobodno izražavanje* i na *transparentnost u pogledu prikupljanja i deljenja ličnih podataka*.

Komitet Minisatara je 2016. godine usvojio i *Preporuku (CM/Rec(2016)3) državama članicama o ljudskim pravima i poslovanju*[253]. „Prepoznajući da su poslovna preduzeća odgovorna za poštovanje ljudskih prava", ova *Preporuka* se obraća državama članicama sa ciljem da preuzmu sve potrebne mere kako bi osigurale poštovanje ljudskih prava pri poslovanju privatnih kompanija. Slično, Ujedinjene nacije „Vodećim principima o poslovanju i ljudskim pravima"[254] daju smernice državama i privatnim preduzećima kako da zaštite ljudska prava u poslovnom okruženju, odnosno da komercijalni interes ne nadjača interes građana/korisnika.

Opšti regulatorni okvir EU koji se odnosi na zaštitu podataka o ličnosti poslednji je korak u nizu kojim se daje na značaju zaštiti ljudskih prava pri poslovanju privatnih kompanija. Ključne reči ovog okvira jesu *odgovornost* i *transparentnost*. Čini se da su to dva najveća izazova kada je reč o (samo)regulisanju poslovnog okruženja, odnosno zaštiti ljudskih prava u takvim uslovima. U svim navedenim aktima odgovornost privatnih aktera, u našem slučaju intermedijatora, implicitno je ili eksplicitno naglašena. Njihova odgovornost implicitno se ističe prilikom navođenja njihovih uloga i ogromnog značaja za demokratske procese i društvo u celini – svaki entitet koji u toj meri raspolaže informacijama i podacima, pritom imajući mehanizme da aktivno utiče na njihov nadzor i kontrolu, mora imati i proporcionalnu odgovornost, bez obzira na privatni okvir poslovanja. Sa druge strane,

[252] engl. *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member State on the protection of human rights with regard to social networking services* . Dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b (pristupljeno 25. 06. 2018. godine).
[253] Engl. *Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and busines* . Dostupno putem linka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1ad4 (pristupljeno 27. 06. 2018. godine).
[254] engl. *Guiding Principles on Business and Human Rights* (2011). Dostupno putem linka: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (pristupljeno 27. 06. 2018. godine).

eksplicitno su navedene smernice koje bi trebalo da prate privatni akteri, kako ne bi ugrozili prava svojih korisnika.

Regulatorni okvir EU stalno radi na dopunjavanju i poboljšanju smernica i preporuka kada je reč o navedenim izazovima, insistirajući na pravima, obavezama i odgovornostima. Gugl i Fejsbuk su, između ostalih, kompanije na koje su primenljiva sva navedena akta. Analizom njihovih *Uslova korišćenja,* ali i javnim istupanjem njihovih rukovodioca, videli smo da one često ne prihvataju u potpunosti svoju odgovornost prema javnosti i javnom interesu, te su česta i kršenja prava na slobodno izražavanje i privatnost korisnika.

Novousvojeni EU okvir ocenjuje se kao jedan od najpotpunijih do sada. Propusti koji su se ticali netransparentnosti, manjka odgovornosti, nejasnih *Uslova korišćenja* i slično, trebalo bi da budu poboljšani primenom novog okvira. Odgovornost intermedijatora svakako je redefinisana u smislu pojačane kontrole nad njihovim poslovanjem, preporukama koje sve manje ostavljaju prostora za slobodnu interpretaciju, insistiranjem na poslovanju u skladu sa regulativom. Međutim, na primeru Gugla i Fejsbuka videli smo da *Uslovi korišćenja* nisu u potpunosti u skladu sa novim okvirom, iako ažurirani nakon usvajanja nove regulative. S obzirom na to da su novim okvirom predviđena i nadzorna tela i stalno praćenje rada privatnih aktera, te sankcije pri kršenju zagarantovanih prava, ostaje da vidimo da li će redefinisana odgovornost ostati samo u formi pravnog dokumenta ili će zaživeti i u praksi i primorati intermedijatore da, pored ubiranja plodova više nego unosnog poslovanja, istupe i kao društveno-odgovorne kompanije.

5. Perspektiva internet korisnika

Domen regulacije i samoregulacije u značajnoj meri obuhvata mnogobrojne probleme i izazove u novom okruženju, nudi smernice, pretpostavlja zaštitu, pa ipak, opšti utisak je da imamo mnogobrojne razloge za zabrinutost kada je o sigurnosti „na mreži" reč. Država i privatni akteri ne samo da ne koriste uvek svoje ingerencije u pozitivnom smeru, već često i same predstavljaju opasnost po pravo na slobodno izražavanje i privatnost na internetu.

U prethodnim poglavljima bilo je reči o tome koliko su prava internet korisnika zaštićena u onlajn-prostoru, tačnije njihovo pravo na slobodno izražavanje i privatnost, i u kojoj meri država i privatni akteri čine sve što je u njihovoj moći da korisnicima obezbede sigurno okruženje. Treći aspekt istraživanja u ovoj disertaciji predstavljaju internet korisnici. Poslednji u sadržaju, ali ne i najmanje značajni, upravo su krajnji korisnici ti koji donose konačan sud o tome da li se i u kojoj meri osećaju bezbedno dok krstare nepreglednim prostranstvima internet pejzaža. Na kraju, učinak regulatornih i samoregulatornih mehanizama ocenjuju internet korisnici.

Mnogobrojni autori bavili su se upravo ovim aspektom, analizirajući stavove korisnika o poštovanju njihovih prava onlajn (Govani & Pashley, 2005; Gross & Acquisti, 2005; Acquisti & Gross, 2006; et al., 2010; Liu et al., 2011; Beresforda et al., 2012; Pitkänen & Tuunainen, 2012; Morando et al., 2014; Goggin et al., 2017; Olmstead & Smith, 2017a; Olmstead & Smith, 2017b). Sumirano, gotovo sva istraživanja stavova internet korisnika, bez obzira na nacionalni okvir, pokazuju negativan stav o onlajn-bezbednosti.

Pitanja koja se nameću, a na neka od njih nastojaćemo da damo odgovor i kroz istraživanje stavova internet korisnika u Srbiji, jesu: da li korisnici unapred odustaju od privatnosti, jer je smatraju nemogućom na internetu; da li imaju vremena da čitaju opširne i suvoparne uslove korišćenja; da li i onda kada ih zaista pročitaju razumeju pročitano, s obzirom na kompleksnost jezika, kako smo izneli u prethodnom poglavlju; da li su korisnici dovoljno upoznati sa opasnostima i izazovima korišćenja onlajn-usluga; i na kraju, da li je uopšte moguće da korisnici zaštite svoja prava na internetu, jer uslovi korišćenja nemaju alternativu, dok ih posebna podešavanja štite uglavnom od drugih korisnika, ali ne i od korporacija i države?

5.1. Sigurna „mreža" ili razlog za zabrinutost: prethodna istraživanja

Poznavanje prostora u kojem se odvija komunikacija, njegovih pravila ponašanja, ali i obaveza, preduslov je za preduzimanje koraka koji bi vodili bezbednijem komunikacionom okruženju. Insistiranja na *individualnoj odgovornosti* internet korisnika, koja podrazumeva savesno korišćenje onlajn-usluga (Napoli, 2014; CM/Rec(2012)4), uključuje korisnike kao važnu kariku u zaštiti prava (svojih i tuđih) na internetu. Svest o rizicima, aktivno korišćenje mehanizama zaštite, poznavanje okruženja u kojem se ostvaruje interakcija, upoznavanje sa politikama privatnosti i uslovima korišćenja, samo su neki od zahteva koji se stavljaju pred savremenog korisnika internet usluga. Sumirano, prethodna istraživanja ukazuju na sledeće izazove kada je reč o individualnoj odgovornosti korisnika:

a) Korisnici nisu dovoljno upoznati sa potencijalnim opasnostima, stoga nemaju dovoljno izgrađenu svest o riziku.

Jedno od istraživanja, koje su sproveli Olmsted i Smit (Olmstead & Smith, 2017a) upravo je imalo za cilj da utvrdi koliko su ispitanici/internet korisnici u Americi (njih 1055) svesni sajber sigurnosti i koliko su upoznati sa problemima i terminima u ovoj oblasti. Nalazi do kojih su došli ukazuju da većina internet korisnika može da odgovori na nešto više od 50% pitanja koja se tiču sajber sigurnosti. Samo 1% dao je tačan odgovor na sva postavljena pitanja. Ovi rezultati govore u prilog već istaknutom izazovu koji se tiče nerazumljivih tehničkih termina i kompleksnosti jezika. Međutim, razlika u odgovorima značajno se razlikuje kada se uporedi sa stepenom obrazovanja ispitanika – procenat tačnih odgovora smanjuje se sa smanjenjem stepena obrazovanja. Takođe, razlika u odgovorima na pojedina pitanja primetna je i kada je reč o starosnoj dobi ispitanika. Naime, u određenim oblastima, uglavnom kada je reč o tehničkim i manje poznatim terminima, grupa 18–29 godina zabeležila je bolji rezultat u odnosu na starosnu grupu preko 65 godina.

Tou i saradnici (Tow et al., 2010) sproveli su opsežno eksploratorno istraživanje koje je obuhvatalo tri integralna dela: učestvovanje jednog od autora u jednoj Fejsbuk zajednici, upitnik i intervjue sa korisnicima. Rezultati do kojih su autori došli pokazali su da korisnici ne prepoznaju opasnosti prilikom iznošenja privatnih informacija o sebi. Generalni zaključak je da korisnici nisu informisani o tim pitanjima, te danemaju svest o rizicima. Autori upućuju preporuke kreatorima

komunikacionih politika koje se odnose na neophodnost organizovanja kampanja, kako od strane država tako i privatnih aktera koji posluju na internetu, a čiji bi fokus bio skretanje pažnje korisnicima na potencijalne opasnosti po njihovu bezbednost u onlajn-prostoru.

b) Čak i kada su svesni rizika ili su lično doživeli povredu privatnosti, korisnici ne ulažu dodatni napor da se zaštite.

Akvisti i Gros (Acquisti & Gross, 2006) poredili su odnos prema privatnosti ispitanika koji su korisnici Fejsbuka i onih koji nisu. Uključili su i brojne druge varijable, poput pola, godina starosti i slično. Nalazi do kojih su došli pokazali su da je generalni stav o značaju zaštitite privatnosti slab pokazatelj da li će osoba imati ili neće imati Fejsbuk nalog. Ispitanici koji su bili svesni rizika po privatnost svejedno su otvarali naloge na ovoj društvenoj mreži. Većina ispitanika smatrala je da može da kontroliše lične podatke podeljene na ovoj mreži. Takođe, „nerazumevanje ili ignorisanje načina na koji Fejsbuk (kompanija) tretira lične podatke veoma je rasprostranjeno" (Acquisti & Gross, 2006: 15).

Olmsted i Smit su, u okviru Istraživačkog centra Pju, sproveli istraživanje kojim su želeli da utvrde kakva je percepcija građana Amerike o bezbednosti ličnih podataka na internetu (Olmstead & Smith, 2017b). Rezultati su pokazali da je većina ispitivanih Amerikanaca lično doživela povredu sigurnosti ličnih podataka, čak 64%. Od toga je skoro polovina povreda u vezi sa prevarama koje se odnose na kreditne kartice, ali je njih 16% doživelo preuzimanje mejl naloga, a 13% preuzimanje njihovih profila na društvenim mrežama. Skoro polovina ispitanika (48%) osećala se manje bezbedno u odnosu na period od pre pet godina, a većina je iskazala namanje poverenje prema federalnoj vladi i društvenim mrežama, kada je reč o zaštiti njihovih podataka:

> „Oko 28% Amerikanaca uopšte nije uvereno da savezna vlada može održati njihove lične podatke sigurnim i bezbednim od neovlašćenog korišćenja, dok 24% korisnika društvenih mreža nema poverenje u veb stranice kada je reč o zaštititi njihovih podataka. Nasuprot tome, samo 12% Amerikanaca (i 9% korisnika društvenih mreža) ima vrlo visok nivo poverenja da ti entiteti mogu održati njihove lične podatke sigurnim i bezbednim" (Olmstead & Smith, 2017b: 3–4).

Međutim, iako se većina Amerikanaca oseća ugroženo u sajber prostoru ili su i sami doživeli povredu ličnih podataka, čini se da nisu posebno zabrinuti za svoju sigurnost onlajn. Skoro 70% ispitanika ne brine o tome koliko je njihov pasvord zaštićen, čak i Amerikanci koji su lično doživeli povredu ličnih podataka nisu obazriviji od prosečnog korisnika, kada je reč o sigurnosti njihovih lozinki. Rezultati ovog istraživanja govore u prilog odsustvu individualne odgovornosti korisnika koji, i onda kada su motivisani i svesni rizika, ne čine dovoljno da se zaštite pri korišćenju onlajn-usluga. Upravo na to misle Morando i saradnici (Morando et al., 2014) kada govore o sukobu između *deklarisanih* i *otkrivenih* preferencija. Naime, autori pod prvom preferencijom podrazumevaju podatke do kojih istraživači dolaze kada istražuju generalne stavove korisnika o bezbednosti na internetu, dok pod drugim, otkrivenim preferencijama, podrazumevaju realne korake koje korisnici preduzimaju kada koriste internet usluge. Odnosno,:

> „ Potrošači izražavaju zabrinutost u vezi sa zloupotrebom ličnih podataka, na primer, sebe opisuju kao zabrinute i daju visoku ocenu ličnim podacima i privatnosti, kao odgovor na različite vrste upitnika zasnovanih na anketama. Ipak, oni i dalje pružaju lične podatke na društvenim mrežama, pri onlajn-kupovini i na drugim sajtovima" (Morando et al., 2014: 3).

Dakle, i kada visoko ocene pitanje privatnosti i bezbednosti, i svesni su rizika (*deklarisane* preferencije), korisnici ne iskazuju visok stepen odgovornosti dok koriste internet usluge, pa se, i pored svesti o rizicima, korisnici odlučuju da prekomerno dele svoje podatke „na mreži" (*otkrivene* preferencije).

c) Nedovoljna motivacija i nezainteresovanost korisnika da čitaju uslove korišćenja.

Ignorisanje je jedan od ključnih termina kada je reč o politikama privatnosti i uopšte uslovima korišćenja. Obar i Hirš-Uldorf (Obar & Hirsch-Oeldorf, 2016) sproveli su zanimljivo istraživanje kako bi ispitali da li korisnici društvenih mreža uopšte čitaju politike privatnosti i uslove korišćenja pre nego što ih prihvate. Naime, autori su osmislili fiktivnu društvenu mrežu *NameDrop* i analizirali ponašanje 543 korisnika pri pristupanju ovoj društvenoj mreži. Rezultati do kojih su došli su, sa aspekta zaštite privatnosti, poražavajući. Više od 70% korisnika nije ni pročitalo politiku privatnosti, već su automatski prihvatili uslove. Prosečno vreme čitanja bilo je manje od minuta, dok je 98% onih koji su pročitali uslove korišćenja previdelo klauzulu, koja je zapravo bila „zamka" – onapredviđa da korisnici plate pristup društvenoj mreži prvorođenim detetom, odnosno da ga dodele mreži *NameDrop*. Autori su izdvojili tri faktora koji utiču na odluku korisnika da ne čitaju politiku privatnosti i uslove korišćenja: preopširnost, osećaj da nemaju šta da skrivaju i nerazumevanje tehničkih termina (Obar & Hirsch-Oeldorf, 2016: 18).

Zanimljive su i okolnosti pod kojima su ispitanici pristali na testiranje nove univerzitetske društvene mreže. Naime, niko od njihovih prijatelja, kolega, ni porodice nije mogao da koristi ovu fiktivnu mrežu, tako da oni nisu mogli da dobiju preporuku ili garanciju o njenoj bezbednosti; takođe, ni u jednom trenutku nije rečeno da će njihovi podaci nakon testiranja mreže biti uklonjeni, niti je iko od ispatanika to doveo u pitanje, pa ipak, gotovo svi učesnici u ovom testiranju odlučili su da veruju novoj društvenoj mreži, bez čitanja njenih uslova korišćenja.

Pored nedostatka motivacije, uzrok nečitanja uslova korišćenja jeste i preopširnost i kompleksan tehnički jezik kojim uslovi korišćenja obiluju, te zahtevaju dosta vremena i predznanja (Van Kokswijk, 2010; McDonland & Cranor, 2008)[255].

d) Korisnici u zamenu za sitne ustupke pristaju na prekomerno deljenje ličnih podataka.

Još jedan problem, kada je reč o privatnosti korisnika na internetu jeste to što se korisnici internet usluga odriču dela svoje privatnosti zarad nekih drugih pogodnosti. U prethodnom poglavlju ukazali smo na slučaj kada korisnici prihvate „ kolačiće", kako bi dobili kvalitetniju i sveobuhvatnu uslugu. Autori u Nemačkoj (Beresforda et al., 2012) sproveli su zanimljiv eksperiment kako bi utvrdili da li je internet korisnicima faktor čuvanja ličnih podataka značajan i koje su situacije u kojima ga se

[255] Ovakvi i slični rezultati istraživanja rezultirali su pokretanjem veb stranice „Uslove korišćenja, Nisam pročitao" (engl. *Terms of Service, Didn't read – ToS;DR*) . Naime, kreatori ove veb stranice tvrde da je rečenica: „ 'Pročitao sam i slažem se sa Uslovima', najveća laž na internetu", dok je, kako se navodi na stranici, njihov cilj da to poprave. *ToS;DR,* kao interaktivni sajt, osnovan 2012. godine i namenjem korisnicima internet usluga, pruža mogućnost ocenjivanja poltika privatnosti sajtova od veoma dobrog (*Class A*), do veoma lošeg (*Class E*) i na taj način omogućava razmenu korisničkog iskustva. Ključni problem, kako ocenjuju kreatori ToS;DR, jeste preopširnost uslova korišćenja, što odovodi do toga da korisnici prihvataju uslove iako ih nisu pročitali. Dostupno na: https://tosdr.org/

odriču zarad nekih drugih pogodnosti. Naime, korisnici podvrgnuti eksperimentu imali su zadatak da obave onlajn-kupovinu DVD-a. Ispitanicima su bile ponuđene različite opcije, odnosno nekoliko firmi sa različitim zahtevima kada je reč o odavanju ličnih podataka. Jedna od fiktivnih podfirmi Amazona nudila je popust od jednog evra u zamenu za odavanje mesečnog prihoda i datuma rođenja. Rezultati su pokazali da se većina učesnika u eksperimentu, koji su se odlučili za onlajn-kupovinu, opredelila za firmu koja je manje senzibilna prema ličnim podacima u zamenu za popust u iznosu od jednog evra. Rezultati ovog istraživanja ukazuju da korisnici nisu preterano zainteresovani za zaštitu ličnih podataka, naročito onda kada u zamenu za njih dobiju neku pogodnost, u ovom slučaju novčanu.

Međutim, drugi deo eksperimenta pokazao je da i kada nije bilo popusta, samo se polovina učesnika opredelila za firmu sa boljom zaštititom ličnih podataka. Ovakav odnos prema ličnim podacima autori delom tumače kao opštu nezainteresovanost za zaštitu ličnih podataka, iako je većina učesnika koji su otkrili svoje podatke bila nezadovoljna tretmanom njihovih podataka, što je takođe utvrđeno istraživanjem.

e) Veliki broj korisnika jednostavno automatski pristaje na uslove zbog već navedenih razloga, ali je čest slučaj da korisnici odaju informacije i kojima nije uslovljen pristup i usluga, jer smatraju da nemaju šta da kriju ili da mogu da kontrolišu svoju bezbednost.

Gros i Akvisti (Gross & Acquisti, 2005) analizirali su ponašanje na Fejsbuku 4000 studenata Karnegi Melon Univerziteta (*Carnegie Mellon University*) u Pitsburgu. Fokus istraživanja odnosio se na procenu količine ličnih informacija koju studenti otkrivaju o sebi i uopšte njihov odnos prema podešavanjima u vezi sa privatnosti. Rezultati su pokazali da studenti otkrivaju zapanjujuće ogromanu količinu ličnih podataka. Najčešće je reč o fotografijama (90,8%), datumu rođenja (87,8%), skoro 40% otkriva svoj broj telefona, a polovina mesto stanovanja. Premda Fesjbuk nudi posebna podešavanja privatnosti, zanemarljiv broj studenata koristio je ove alatke, te je većina ispitanika svoje profile automatski stavila na uvid svima. Gotovo identične rezultate dobili su i Đovani i Pašli (Govani & Pashley, 2005).

Pitkajnen i Dunajnen (Pitkänen & Tuunainen, 2012) istraživali su dva tipa ponašanja koja su u vezi sa privatnosti: otkrivanje ličnih podataka i zaštitu privatnosti. Ispitanici su bili finski studenti, ujedno i Fejsbuk korisnici, njih 160. Zajedničko gotovo svim ispitanicima bili su razlozi kreiranja profila na Fejsbuku: *umrežavanje* i *komunikacija.* Kada je reč o količini podeljenih informacija, ali i o poznavanju osnova politike privatnosti, autori su došli do zanimljivih rezultata. Naime, skoro svi ispitanici imali su pravo ime i prezime i svoju profilnu sliku, dok je više od 80% ispitanika objavilo svoj rodni grad, podatke o obrazovanju, mejl adrese. Zanimljivo je da je preko 30% ispitanika objavilo svoj broj telefona, dok je 18% navelo tačan naziv i broj ulice u kojoj stanuju.

Jasno je da je većina ispitanika objavila prekomernu količinu podataka o sebi, međutim, Fejsbuk nudi opciju deljenja takvih informacija sa svima, samo sa prijateljima, samo sa određenim prijateljima ili ni sa kim. Istraživanje je pokazalo da je većina podelila te informacije samo sa prijateljima, ali je veliki procenat (34%) navedene podatke stavio na uvid apsolutno svim korisnicima Fejsbuka, odnosno, odabrao opciju *javno*.

Drugi deo ovog istraživanja bavio se zaštititom privatnosti, odnosno stavom ispitanika o značaju zaštite ličnih podataka. U ovom delu autori zaključuju da ne postoji velika bojazan ispitivanih korisnika od narušavanja njihove privatnosti, kada je reč o Fejsbuku: „ispitanici su čini se bili više

zabrinuti za pitanja privatnosti povezana sa internetom generalno, nego za one povezena sa konkretno Fejsbukom. Ovo se može objasniti time što je internet viđen kao 'velika nepoznanica' [...] dok je Fejsbuk platforma koja se deli sa prijateljima" (Pitkänen & Tuunainen, 2012: 17). U prilog tome govori i činjenica da je veliki broj ispitanika (75%) bio siguran da zna ko sve može da vidi njihove profile.

Iako samouvereni kada je reč o kontrolisanju svoje privatnosti na Fejsbuku, ispitanici nisu bili tako sigurni ko i na koji način može imati pristup njihovim informacijama – čak 73% ispitanika nije bilo svesno toga da Fejsbuk može da deli njihove podatke sa trećim licima. Takođe, samo 21% korisnika pročitao je politiku privatnosti, a samo 15% uslove korišćenja. Zanimljiv podatak je i taj da više od polovine ispitanika koji su tvrdili da su pročitali uslove korišćenja nisu znali da Fejsbuk može proslediti njihove podatke trećim licima. Ovo neslaganje može se objasniti ili davanjem društveno poželjnih odgovora, ili nerazumevanjem pročitanog, ili pak letimičnim čitanjem uslova, percipiranim kao da su dovoljni za upoznavanje sa pravima i obavezama.

f) I kada je korisnik informisan i svestan rizika, nije zadovoljan ponuđenim uslovima korišćenja.

Ukoliko i pođemo od pretpostavke da su Fejsbuk korisnici svesni rizika i dovoljno upoznati sa izazovima, možemo da postavimo pitanje koliko su zapravo zadovoljni alatkama za zaštitu privatnosti koje im se nude? U jednom takvom istraživanju autori (Liu et al., 2011) su analizirali u kojoj meri se razlikuju realna podešavanja privatnosti na Fejsbuku od željenih. Kako bi ispitali ovu razliku, autori su anketirali 200 Fejsbuk korisnika, ali su pored toga analizirali i njhove objave na Fejsbuku (uglavnom fotografije) kako bi utvrdili da li i u kojoj meri korisnici koriste indivudialna podešavanja privatnosti. Njihovi rezultati pokazuju da trenutni mehanizmi zaštitite privatnosti na ovoj društvenoj mreži odgovaraju željenim sa samo 37%. Zanimljiv nalaz je da kada individualno podese privatnost na određenim objavama, čak i tada podešavanja odgovaraju sa samo 39% u odnosu na njihova očekivanja, „što ukazuje na to da čak i korisnici koji su savesniji kada je reč o privatnosti imaju poteškoće da ispravno upravljaju postavkama privatnosti i održavaju ih" (Liu et al., 2011: 62). Dakle, informisan korisnik, onaj koji zna šta želi od politike privatnosti i zna kako da njome upravlja, nije dovoljan preduslov za sigurnu zaštitu. Individualnom faktoru odgovornosti mora se dodati i korporativni.

g) Čak i kada nisu zadovoljni ponuđenim mehanizmima zaštite, korisnici nisu sigurni na koji način bi oni mogli da se unaprede, što govori o potrebi za organizovanjem javnih debata o ovim izazovima, koje bi intenzivnije uključivale i internet korisnike.

Gogin i saradnici (Goggin et al., 2017) sproveli su kompleksno istraživanje o digitalnim pravima u Australiji kroz anketiranje 1600 Australijanaca, fokus grupe i analizu nacionalne komunikacione politike, uz reprezentativne studije slučaja. Istraživanje je bilo fokusirano na pitanja privatnosti, uloge vlade i nadzora, poslovnog okruženja i prava na slobodno izražavanje. Rezultati anketiranja pokazali su da su Australijanci zabrinuti za zaštitu ličnih podataka onlajn, i da samo 38% ispitanika veruje da može da kontroliše privatnost onlajn. Autori su ukazali na to da je pol značajna varijabla: žene su obazrivije kada je reč o zaštiti privatnosti, te češće (63% naspram 58%) od muškaraca individualno podešavaju privatnost na društvenim mrežama, ali se gotovo podjednako osećaju nesigurno (39% naspram 38%). Entiteti prema kojima je iskazano najveće nepoverenje jesu: privatne korporacije (57%), zatim vlada (47%) i drugi korisnici (47%). Ovaj nalaz je značajan jer su *drugi korisnici* kao potencijalna opasnost na trećem mestu, dok, paradoksalno, internet kompanije

najglasnije promovišu mogućnosti individualnih podešavanja privatnosti kojima korisnici štite svoje podatke uglavnom od drugih korisnika (na primer, ko od prijatelja može da vidi objave na Fejsbuku). Sa druge strane, na prvom mestu su privatne korporacije, a obrazloženje za takav rezultat delimično leži i u tome što je značajna većina ispitanika u Australiji istakla da želi da zna kako društvene mreže raspolažu njihovim ličnim podacima (78%). Dakle, netransparentnost u pogledu deljenja ličnih podataka sa trećim licima stvara nepoverenje u rad privatnih korporacija.

Zadržavanje podataka jedan je od značajnih indikatora poštovanja prava na privatnost i zaštite ličnih podataka. U pomenutom istraživanju je čak 79% ispitanika smatralo da je zadržavanje ličnih podataka o telefonskim pozivima narušavanje privatnosti, dok se 58% ispitanika protivi zadržavanju informacija o internet komunikaciji od strane vlade i njenih agencija. Međutim, zanimljivo je da ovi procenti opadaju kada je kontekst doveden u vezu sa antiterorističkim strategijima. Tada čak 57% ispitanika podržava prikupljanje ličnih podataka od strane države.

Kada je reč o slobodnom izražavaju, autori istraživanja ističu da Australijanci nisu u toj meri posvećeni apsolutnom ostvarivanju ovog prava, kakav je slučaj sa Amerikancima, što rezultati ankete i potvrđuju. Nešto više od trećine ispitanika bilo je saglasno sa stavom da svako ima pravo da kaže i radi šta poželi onlajn, dok se trećina ispitanika tome protivila, a preostala trećina bila je neodlučna po ovom pitanju. I ovde autori primećuju značaj pola ispitanika, pa su muškarci ti koji više daju na značaju slobodnom izražavanju od žena, što autori objašnjavaju generalno većim učešćem muškaraca u javnom životu oflajn i onlajn.

Više od trećine (36%) ispitanika nije bilo sigurno kako odgovoriti na sledeće pitanje: šta je to što bi društvene mreže trebalo da urade kako bi osigurale svoj prostor i učinile ga bezbednijim za korisnike,. Autori su ovaj nalaz istakli kao veoma značajan jer govori u prilog opštoj neinformisanosti korisnika, zbog čega pozivaju na češće javne debate o ulozi i značaju društvenih mreža, kao prostora za socijalnu interakciju sa širokim implikacijama (Goggin et al. 2017: 47).

5.2. Iz ugla internet korisnika u Srbiji

Prema podacima Republičkog zavoda za statistiku (RZS) za 2018. godinu, 72,9 % domaćinstva u Srbiji poseduje internet prikuljučak (RZS, 2018: 14). Zanimljiv podatak je da građani u Srbiji koji nemaju internet priključak u preko 70% slučajeva kao razlog navode *odsustvo potrebe za internetom,* ostali kao razloge uglavnom navode *nedovoljnu osposobljenost za korišćenje novih tehnologija, skup pristup* ili *tehničke probleme,* dok samo 0,2 % navodi kao razlog *zaštitu bezbednosti i privatnosti*.

I pored procentualnog porasta u odnosu na prethodnu godinu, u Srbiji čak 22,8% pojedinaca nikada nije koristilo računar. Udeo korisnika zavisi od nivoa obrazovanja, mesta prebivališta (urbana/seoska sredina), ali i od radnog statusa; svi studenti (100%) su u poslednja tri meseca koristili računar, zatim zaposlena, nezaposlena lica i na kraju ostale grupe (44%), koje između ostalih uključuju i penzionere.

Kada je reč o upotrebi interneta, u Srbiji je 73,4% lica koristilo internet u poslednja tri meseca, što je povećanje od 1,4% u odnosu na 2017. godinu (RZS, 2018: 23). Internet najčešće koriste ljudi sa

sa višim i visokim obrazovanjem (90,8%), studenti (100%), češće muškarci (76,8%) u odnosu na žene (70,1%).

Kada je reč o načinu na koji građani Srbije koriste internet, odnosno u koje svrhe, u istraživanju RZS navodi se da su tri najčešća razloga: *traženje informacija o robi i uslugama* (76,8%), *gledanje video sadržaja* (76,3) i *učešće u društvenim mrežama* (70,3%) (RZS, 2018: 26). Mali procenat internet korisnika u Srbiji preduzeo je neke aktivnosti kako bi poboljšao svoje veštine u vezi sa upotrebom interneta (12% besplatna obuka, 4,1% plaćena obuka). Oblasti koje se tiču preduzetih aktivnosti jesu: *korišćenje računara*, *softver* (37,3%), *analiza podataka* (24,2%), ali i *društvene mreže* (18%) i *bezbednost* i *privatnost* (6,7%) (RZS, 2018: 34-35).

Cilj ovog poglavlja jeste da odgovori na istraživačko pitanje: **Kakav je stav internet korisnika u Srbiji o zaštiti njihovih prava u onlajn-prostoru?**, odnosno da se testiraju postavljene hipoteze:

- H3: **Internet korisnici u Srbiji osećaju se nesigurno prilikom deljenja ličnih podataka na internetu.**

- *H3a. Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožava država.*

- *H3b. Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožavaju privatni akteri (Gugl i Fejsbuk).*

- H4: **Internet korisnici u Srbiji ne veruju u odgovornost internet intermedijatora i pravne mogućnosti države, kada je reč o zaštiti njihovog prava na slobodno izražavanje u onlajn-prostoru.**

- *H4a. Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožava država*
.
- *H4b. Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožavaju privatni akteri (Gugl i Fejsbuk).*

- **H5. Internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti kada je o zaštiti njihovih prava na internetu reč.**

H5a: *Internet korisnici u Srbiji ne čine dovoljno da zaštite svoju privatnost, iako su svesni rizika od zloupotrebe ličnih podataka*.

- H5b: *Internet korisnici u Srbiji nisu u dovoljnoj meri upoznati sa Uslovima korišćenja kompanija čije usluge koriste***.**

Za potrebe ovog istraživanja odabrana je elektronska anketa, koja podrazumeva upitnik dizajniran onlajn i namenjen internet korisnicima.

5.2.1. Veb-anketa

Veb-anketa suočava se sa mnogobrojnim kritikama, pa ipak, u skladu sa osnovnim ciljem istraživanja i predviđenim hipotezama, odabrana je kao najpogodniji metod. Naime, osnovna zamerka upućena ovom vidu ispitivanja odnosi se na nemogućnost postizanja reprezentativnog uzorka. Kako isticu Kuper i Miler, „okviri internet korisnika u obliku prikladnom za uzorkovanje ne postoje – i verovatno neće postojati" (Couper & Miller, 2008: 832). Međutim, onda kada osnovni cilj istraživanja nije generalizovanje dobijenih rezultata na čitavu populaciju, kao što je slučaj i sa ovim istaživanjem, već ispitivanje stavova aktivnih internet korisnika o određenoj temi, ova metoda se čini ne samo pogodnom već i daleko isplativijom u smislu uštede vremena. Navedenomožemo okarakterisati kao „prednost brzih ciklusa distribucije i odgovora" (Andrews et al., 2003: 186). Odnosno, veb-anketa pruža mogućnost da se dosegne do ispitanika bez ličnog prisustva istraživača, jednostavnim slanjem linka putem mejla i deljenjem upitnika putem veb-stranica ili društvenih mreža (*brza distribucija*). Na isti način, povratna informacija u vidu *odgovora* ispitanika – popunjen upitnik – stiže nazad do istraživača i automatski se dodaje bazi. Sa druge strane, pored uštede vremena, značajna je i ušteda novca, jer ovakva metoda isključuje štampanje upitnika.

Takođe, ukoliko je cilj istraživanja ispitati aktivne internet korisnike, onda se elektronska anketa čini najpraktičnijom. Populaciji internet korisnika u Srbiji, a posebno onima koji su korisnici usluga konkretnih kompanija, praktičnije je pristupiti putem interneta, negoli tradicionalnim metodama istraživanja.

Istraživači koji se koriste veb-anketom suočavaju se i sa izazovima koji se tiču stope odgovora, odnosno responzivnosti, namernim pogrešnim odgovorima, višestrukim popunjavanjem ankete i slično. Ovi nedostaci mogu se ublažiti beleženjem IP adrese korisnika pri odgovoru, kontrolnim pitanjima (Ninković-Slavnić, 2016: 158), usklađivanjem teme sa interesovanjima ispitanika, garantovanjem privatnosti, višestrukim kontaktiranjem ispitanika, predviđenim vremenom za popunjavanje upitnika i slično (Andrews et al., 2003: 192).Ipak, ni onda se ne garantuje da do ovih anomalija neće doći. Međutim, ni klasično anketiranje ne garantuje stoprocentno upotrebljive upitnike, niti može da u potpunosti spreči neodgovaranje na sva pitanja, namerno davanje pogrešnih odgovora i slične propuste, koji se pripisuju veb-anketi.

Kuper i Miler (Couper & Miller, 2008) kao jednu od osnovnih karakteristika veb-ankete navode raznovrsnost, stoga predočavaju da je neophodno što detaljnije pojasniti proces istraživanja. Postoje određene *metodološke komponente* kojima se može uticati na uspešnost sprovedene veb-ankete, ali koje ujedno mogu da posluže i u procesu pojašnjenja konkretnih koraka od kreiranja do prikupljanja rezultata putem veb-ankete. Andrjus i saradnici (Andrews et al.) predstavljaju pet takvih komponenti: *dizajn, privatnost* i *tajnost, uzorkovanje* i *selekcija učesnika*, *menadžment distribucije* i *odgovora*, i *pilot istraživanje* (2003: 186). Kada je reč o dizajnu upitnika, autori sumiraju mnogobrojne studije i navode „kriterijume za kvalitetan dizajn elektronskog anketiranja" (Andrews et al., 2003: 187) prikazane u Tabeli 1.

Podržava različite platforme i pregledače / *e-mail* (Iun & Trumbo, 2000)
Kontrole za podešavanja pretraživača (Iun & Trumbo, 2000)
Detektovanje više podnesaka automatski (Iun & Trumbo, 2000)
Pruža pitanja na logičan ili adaptivan način , na primer, omogućava kontrolu kada i kako su postavljena pitanja (Kehoe & Pitkov, 1996; Norman, Friedman, Norman, Stevenson, 2001)
Omogućava čuvanje odgovora pre završetka (Smith, 1997)
Prikuplja odgovore otvorenog ili opcionog tipa (Bachmann & Elfrink, 1996; Kiesler & Sproull, 1986; Loke & Gilbert, 1995; Schaefer & Dillman, 1998; Iun i Trumbo, 2000)
Pruža automatske povratne informacije sa završetkom (Smith, 1997)
Koristi principe dizajna upitnika na papiru (Dillman, 2000; Oppenheim, 1992; Preece, Rogers & Sharp, 2002; Vitmer, Colman i Katzman, 1999)
Pruža automatski prenos odgovora na bazu podataka (Kehoe & Pitkov, 1996; McCoi & Marks, 2001;Smith, 1997)
Sprečava izmenu ankete (Vitmer et al., 1999)
Pruža kontrolu odgovora i ekonomične prikaze (Preece et al., 2002; Stanton, 1998)
Omogućava vezu sa definicijama , menijima, kvadratićima za opcije, animacijom, zvukom, grafikom i tako dalje (Preece et al., 2002; Iun & Trumbo, 2000)
Ne zahteva poznavanje softvera za prezentaciju istraživanja (Sheehan & Hoi, 1999)
Displej se brzo pojavi učesniku (Couper, Traugott, & Lamias, 2001)
Prati izvor neuspešnih odgovora (Paolo, Bonamino, Gibson, Patridge, & Kallail, 2000).

Tabela 1 Kriterijumi kvaliteta za dizajn istraživanja (Andrews et al., 2003: 187)

U ovom istraživanju korišćen je upitnik dizajniran putem Guglovih usluga – Gugl upitnici. Gugl upitnik, kada je reč o kriterijumima kvalitetnog dizajna, odgovara svim navedenim pretpostavkama, čime omogućava uspešnu kontrolu i sprovođenje istraživačkog postupka. Naime, Guglov upitnik sproveden u ovom istraživanju je multiplatformski, odnosno nije tehnički ograničen na način koji bi podrazumevao pristupanje pomoću jedne određene platforme. Konkretno za naše istraživanje, upitnik je deljen putem mejla i društvenih mreža, a moglo mu se pristupiti sa računara, tableta ili pametnog telefona, pri čemu se ne gubi na vizuelnom ni na tehničkom dizajnu upitnika.

Odgovori se automatski detektuju i čuvaju na Guglovom serveru, dok ispitanici dobijaju povratnu informaciju da je upitnik uspešno popunjen. Odmah po popunjavanju upitnika memorišu se rezultati pojedinačnih upitnika, ali se i statistički generišu, odnosno dodaju bazi podataka. Upitnik je dizajniran tako da onemogućava izmene od strane ispitanika i ne zahteva poznavanje softvera za popunjavanje upitnika. Vizuelni prikaz odgovara dizajnu upitnika na papiru, omogućava opcione

odgovore, podržava pitanja otvorenog i zatvorenog tipa, poseduje mogućnost grafičkih i vizuelnih prikaza i dodatnih pojašnjenja.

S obzirom na kompleksni cilj ovog istraživanja koji podrazumeva ispitivanje stavova korisnika o tri različita, ali logički povezana aktera: državu, Gugl i Fejsbuk i njihovu ulogu u zaštiti prava na slobodno izražavanje i privatnost na internetu, procenjeno je da bi dizajn koji uključuje više stranica podeljenih po logičkim celinama bio učinkovitiji. Shodno tome, upitnik se sastoji od četiri grupe, odnosno baterije pitanja. Prva grupa pitanja odnosi se na opšti lični stav ispitanika o dvama navedenim pravima i izazovima sa kojima se susreću u onlajn-okruženju (*Odnos prema privatnosti i slobodi izražavanja na internetu*). Druga grupa pitanja odnosi se na stav ispitanika o kompaniji Fejsbuk kada je reč o zaštiti prava na slobodno izražavanje i prava na privatnosti (*Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja*), dok treća baterija pitanja ima isti cilj ali drugog aktera: kompaniju Gugl (*Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja*). Četvrta baterija pitanja, uključuje poslednjeg značajnog aktera, državu (*Odnos prema Republici Srbiji (RS) kada je reč o privatnosti i slobodi izražavanja*).

Iako je za većinu istraživanja pogodniji dizajn koji između ostalog podrazumeva preglednost, koja uključuje jednu stranicu, specifikum ovog upitnika višestruki predmeti istraživanja, zahtevao je specifični dizajn, kojim se ispitanicima olakšava praćenje pitanja, a koja su logički grupisana i podeljena po posebnim stranicama . Na kraju, „kraći upitnici ne moraju nužno proizvesti veće stope odgovora" (Andrews et al., 2003: 191) od broja pitanja, i značajniji je logični dizajn sa logičnim sledom pitanja.

Druga metodološka komponenta, *privatnost i tajnost*, takođe je zagarantovana. Pristupanje upitniku ne zahteva odavanje identiteta, niti se to čini naknadno. Rezultati se prikupljaju i generišu bez ikakvih naznaka o identitetu ispitanika.

Uzorkovanje i selekcija ispitanika treća je komponenta neophodna za uspešno sprovedeno istraživanje. Kao što je već istaknuto „nema 'garantovanog' načina onlajn-uzorkovanja" (Andrews et al., 2003: 189). Zbog toga je neophodno jasno naglasiti da se „rezultati za onlajn-populaciju ne mogu generalizovati i na oflajn populaciju" (Andrews et al., 2003: 189). U ovom konkretnom istraživanju ne pretenduje se na reprezentativnost uzorka, već se on selektuje na osnovu specifične aktivnosti – aktivno korišćenje usluga Gugla i Fejsbuka. Odnosno, ciljna grupa jesu korisnici Guglovih usluga i usluga kompanije Fejsbuk. Shodno tome, upitnik je deljen tehnikom grudve (komponenta *distribucije*), koja podrazumeva da istraživač pošalje ili podeli link koji vodi ka upitniku osobama koje su mu dostupne, a da zatim primarni ispitanici dalje prosleđuju upitnik svojim kontaktima, sekundarni ispitanici svojim kontaktima, čineći uzorak većim sa svakim sledećim deljenjem, poput grudve. Upitnik je u ovom slučaju podeljen putem mejla (*Gmail*) i društvene mreže Fejsbuk, jer su ispitanici selektovani na osnovu korišćenja usluga ovih privatnih kompanija, čime se unapred ograničava uzorak na ciljanu populaciju internet korisnika.

Ovakva selekcija ispitanika nije bez ograničenja, jer ne možemo da pretpostavimo da li će svako od kontaktiranih ispitanika biti korisnik usluga obe kompanije[256]. Upravo iz tog razloga, i pretpostavke da će veći broj ispitanika koristiti Guglove usluge, te da će biti onih koji ne koriste Fejsbuk, upitnik je dizajniran tako da ispitanici koji ne koriste Fejsbuk nakon što odgovore negativno na to pitanje automatski prelaze na deo upitnika koji se tiče Guglovih usluga.

[256] Međutim, trebalo bi imati na umu da svako ko koristi telefon sa operativnim sistemom *Android* automatski jeste korisnik Guglovih usluga.

Pilot istraživanje kao poslednja metodološka komponenta, o kojoj piše Andrjus, ima za cilj da proveri instrument ”upitnik, pre nego se sa istraživanjem i zvanično počne, te da reši eventualne propuste. Ova komponenta je jedna od najznačajnijih, jer omogućava ispravku prethodnih komponenti (*dizajn*, *distribucija*, *privatnost*) pre sprovođenja istraživanja, te istraživaču umnogome olakšava kasniji proces istraživanja.

U ovom slučaju, pilot istraživanje podrazumevalo je slanje upitnika osobama koje su iz različitih profesionalnih oblasti, sa različitim nivoom znanja iz oblasti koja se istražuje. Ispitanici u pilot istraživanju bili su pozvani da ukažu na sve nelogičnosti, na pitanja koja su neprecizno ili kompleksno formulisana, odnosno na sve eventualne poteškoće sa kojima su se susreli prilikom popunjavanja upitnika. Tokom ovog procesa autorka je dobila dve sugestije slične prirode. Jedna od sugestija odnosila se na ujednačenu upotrebu transkribovanih i doslovno prevedenih reči sa engleskog jezika. Druga sugestija odnosila se na konkretan set pitanja, u delu o Fejsbuku, gde je ispitanik u pilot istraživanju ukazao na to da je *News Feed* termin poznat svim korisnicima Fejsbuka, te da termin „ početna strana”, koji je prvobitno bio upotrebljen, može da dovede do zabune, jer nije tako učestao u upotrebi. Autorka je prihvatila obe sugestije.

5.3. Rezultati istraživanja: demografski podaci

Anketa dizajnirana putem Guglove usluge – Gugl upitnici bila je aktivna, odnosno dostupna za popunjavanje, tačno mesec dana: od 16. oktobra do 16. novembra 2018. godine. U tom periodu anketu je popunilo 783 ispitanika – internet korisnika. Dobijeni podaci obrađeni su pomoću statističkog softvera SPSS.

S obzirom da je već naglašeno da uzorak ne teži reprezentativnosti, odnosno da je tehnika za koju smo se opredelili usmerena ka targetiranju ispitanika prema unapred određenim karakteristikama – aktivnom korišćenju usluga Gugla i Fejsbuka – i u skladu sa postavljenim ciljevima istraživanja, demografski podaci (prikazani u Tabelama 2 i 3) opisnog su karaktera.

Pol ispitanika		
	Broj ispitanika	**%**
muški	211	26.9
ženski	572	73.1
Total	783	100.0

Tabela 2 Pol ispitanika

U istraživanju je učestvovalo 211 muških i 572 ženska ispitanika (Tabela 2). Najviše ispitanika, 82%, starosti je do 38 godina, a najmanje, svega njih 10, starosti je preko 60 godina (Tabela 3). Ovakav odnos bio je očekivan, s obzirom na to da je generacija milenijalaca (rođenih nakon 1980. godine) generacija koja je najviše upućena na internet komunikaciju.

Godine starosti ispitanika		
	Broj ispitanika	**%**
18-38	642	82.0
39-59	131	16.7
60+	10	1.3
Total	783	100.0

Tabela 3 Godine starosti ispitanika

Kada je reč o mestu stanovanja, zanemarljiv procenat ispitanika boravi u ruralnoj sredini, svega 10% od ukupnog broja (Tabela 4). Međutim, ovaj podatak bi trebalo uzeti s rezervom, jer je pitanje formulisano tako da isključuje mesto rođenja i upućuje isključivo na mesto trenutnog boravišta. Verujemo da bi drugačije koncipirano pitanje donelo i drugačije rezultate, naročito ukoliko uzmemo u obzir migracije stanovništa ka gradovima, zbog studiranja, posla i slično.

Mesto stanovanja ispitanika		
	Broj ispitanika	**%**
ruralna sredina	78	10.0
urbana sredina	705	90.0
Total	783	100.0

Tabela 4 Mesto stanovanja ispitanika

Poslednje dve karakteristike ispitanika tiču se nivoa obrazovanja (Tabela 5) i profesionalnog usmerenja (Tabela 6). Društveno okruženje autorke imalo je uticaj na obe. Naime, najveći broj ispitanika, njih 52,02% ima visokoškolsko obrazovanje, dok 26, 4% ispitanika ima postdiplomsko obrazovanje.

Obrazovanje ispitanika		
	Broj ispitanika	**%**
osnovnoškolsko	2	.3
srednjoškolsko	165	21.1
visokoškolsko	409	52.2
postdiplomsko	207	26.4
Total	783	100.0

Tabela 5 Obrazovanje ispitanika

Takođe, zbog profesionalnog okruženja autorke, očekivano je bilo da će najveći broj ispitanika imati društveno-humanističko profesionalno usmerenje: 74,5% ispitanika je iz društveno-humanističke oblasti, zatim sledi pravno-ekonomska oblast (10,9%), tehničko-tehnološka oblast sa 9,6%, i najmanje ispitanika je iz oblasti prirodnih nauka, svega 5,1%, odnosno 40 ispitanika.

Profesionalno usmerenje		
	Broj ispitanika	**%**
društveno-humanistička oblast	583	74.5
oblast prirodnih nauka	40	5.1
pravno-ekonomska oblast	85	10.9
tehničko-tehnološka oblast	75	9.6
Total	783	100.0

Tabela 6 Profesionalno usmerenje ispitanika

Bez obzira na dominantne procente ispitanika iz društveno-humanističke oblasti, i onih sa visokoškolskim i postdiplomskim obrazovanjem, autorka nije izuzela nijednog ispitanika, jer, kao što je već istaknuto, cilj ovog upitnika nije formiranje demografski reprezentativnog uzorka. Ono što ispitanike kvalifikuje kao odgovarajuće za ovo istraživanje odnosi se samo na njihove internet aktivnosti. Iako ćemo ukazati i na pojedine korelacije između demografskih odlika i odgovora na pojedina pitanja, karakter ovih korelacija biće isključivo opisan, važiće samo za testirani uzorak, bez pretenzije da se tumači kao validan za opštu populaciju internet korisnika u Srbiji. Hipoteze koje ćemo testirati ne uključuju specifične demografske odlike ispitanika, već se njima testiraju svi ispitanici – internet korisnici bez obzira na pol, godine, mesto stanovanja i slično.

Opštim hipotezama, u ovom delu rada, pretpostavljamo da se internet korisnici u Srbiji ne osećaju sigurno prilikom deljanja ličnih podataka na internetu, te da ne veruju u apsolutno ostvarivanje prava na slobodno izražavanje onlajn. Takođe, pretpostavili smo da internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti, iako su svesni rizika po njihova prava onlajn. Najpre smo ispitivali opšti stav ispitanika o zaštiti navedena dva prava na internetu, a zatim smo kroz setove pitanja uveli državu i privatne kompanije Gugl i Fejsbuk, kao aktere koji ova prava mogu zaštiti ili zloupotrebiti, te smo u skladu sa tim pretpostavkama testirali stavove korisnika. Pitanja kojima se testira individualna odgovornost predstavljaju ujedno i kontrolna pitanja, i inkorporirana su u setove pitanja o privatnim kompanijama.

Rezultate istraživanja prikazaćemo sledeći redosled poglavlja u disertaciji, odnosno, najpre će biti prikazani rezultati koji se tiču odnosa korisnika prema zaštiti prava na privatnost i slobodi izražavanja uopšte, zatim njihovi stavovi prema ulozi države, kada je o pravima koja su predmet istraživanja reč, a zatim odnos korisnika prema ulozi intermedijatora – Gugla i Fejsbuka, u kontekstu navedena dva prava. Upitnik je bio koncipiran tako da su ispitanici najpre odgovarali na set pitanja o privatnim kompanijama, a zatim na pitanja o državi. Međutim, odlučili smo se za prikazivanje rezultata redosledom koji prati strukturu disertacije: država – privatni akteri. Na kraju ćemo prikazati rezultate do kojih smo došli analizom kontrolnih pitanja, sa ciljem testiranja hipoteze o individualnoj odgovornosti korisnika.

5.3.1. Rezultati istraživanja: Odnos prema slobodi izražavanja i privatnosti na internetu

Cilj ovog seta pitanja bio je da se ustanovi da li se internet korisnici u Srbiji osećaju sigurno prilikom deljanja ličnih podataka na internetu, odnosno da li veruju u zaštitu svoje privatnosti onlajn, i da li veruju da je na internetu moguće apsolutno ostvarivanje prava na slobodno izražavanje. Dve opšte hipoteze u tom kontekstu su sledeće:

- H3: ***Internet korisnici u Srbiji osećaju se nesigurno prilikom deljenja ličnih podataka na internetu.***

- H4: ***Internet korisnici u Srbiji ne veruju u apsolutno ostavarivanje prava na slobodno izražavanje na internetu.***

Za potvrdu treće hipoteze posebno su značajna pitanja, odnosno dve tvrdnje, koje od ispitanika zahtevaju iznošenje stava koji se direktno tiče zaštite podataka na internetu. Na prvu tvrdnju: ***Smatram da su moji podaci koje delim na internetu zaštićeni***, ispitanici su većinski odgovorili negativno (52,1 %), nešto više od 40 procenata nije bilo sigurno u ovu tvrdnju, dok je svega 7,5%, odnosno 58 ispitanika, smatralo da su njihovi podaci na internetu zaštićeni (Tabela 7).

Smatram da su moji podaci koje delim na internetu zaštićeni.		
	Broj ispitanika	**%**
Ne	401	52.1
Nisam siguran	310	40.3
Da	58	7.5
Total	769	100.0

Tabela 7 Prvo pitanje u delu: ***Odnos prema privatnosti i slobodi izražavanja na internetu***

Druga tvrdnja u ovom kontekstu: ***Smatram da je moguće zaštititi privatnost na internetu***, donosi nešto drugačije procente. Dok je za prvu tvrdnju svega 7,5% ispitanika smatralo da su njihovi podaci na internetu zaštićeni, sada 20,6% ispitanika smatra da je moguće zaštiti privatnost na internetu, dok skoro 80% smatra da to nije moguće ili nije sigurno u takvu mogućnost (Tabela 8).

Smatram da je moguće zaštititi privatnost na internetu.		
	Broj ispitanika	**%**
Ne	353	45.7
Nisam siguran	261	33.7
Da	159	20.6
Total	773	100,0

Tabela 8 Drugo pitanje u delu: Odnos prema privatnosti i slobodi izražavanja na internetu

Rezultati idu u prilog prvoj opštoj hipotezi. S obzirom na to da svega 7,5% ispitanika smatra da njihovi podaci jesu zaštićeni, te da samo petina veruje da uopšte postoji mogućnost zaštite privatnosti onlajn, možemo da zaključimo da su ispitanici nesigurni prilikom deljenja podataka na internetu.

Kada je reč o slobodi izražavanja na internetu, mišljenje je podeljeno. Gotovo isti broj ispitanika smatra da mu jeste, odnosno nije, zagarantovana sloboda izražavanja na internetu, dok 36% ispitanika nije sigurno u navedenu tvrdnju (Tabela 9).

Smatram da mi je sloboda izražavanja na internetu zagarantovana.		
	Broj ispitanika	**%**
Ne	261	34.0
Nisam siguran	276	36.0
Da	230	30.0
Total	767	100.0

Tabela 9 Pitanje 2. u delu: ***Odnos prema privatnosti i slobodi izražavanja na internetu***

Sa druge strane, gotovo polovina ispitanika (47,4%) ne oseća se slobodno da objavljuje svoje stavove onlajn (Tabela 10).

Osećam se slobodno da objavljujem sve svoje stavove onlajn.		
	Broj ispitanika	**%**
Ne	367	47.4
Nisam siguran	191	24.6
Da	217	28.0
Total	775	100.0

Tabela 10 Pitanje 4. u delu: ***Odnos prema privatnosti i slobodi izražavanja na internetu***

Na osnovu dobijenih rezultata, gde svega 30% ispitanika smatra da je sloboda izražavanja na internetu zagarantovana, dok se skoro polovina ne oseća slobodno da objavljuje svoje stavove, možemo da zaključimo da internet korisnici u Srbiji ne veruju u apsolutno ostvarivanje prava na slobodno izražavanje na internetu.

Na osnovu opštih hipoteza postavljene su i pomoćne hipoteze kojima se država i privatne kompanije uvode kao značajni akteri kada je reč o ostvarivanju dvaju navedenih prava. Posebnim setovima pitanja ispitivani su stavovi internet korisnika o ovim akterima i njihovoj ulozi u zaštiti, ili zloupotrebi, navedenih prava. Odnos ispitanika prema državi i privatnim akterima u ovom kontekstu značajan je za potvrdu opštih hipoteza, jer se njime dodatno pojašnjava zbog čega se internet korisnici u Srbiji ne osećaju sigurno da iskazuju svoje stavove onlajn, kao i zbog čega veruju da je njihova privatnost na internetu ugrožena.

5.3.2. Rezultati istraživanja: Odnos internet korisnika u Srbiji prema državi

Odnos internet korisnika prema državi, kada je reč o pravu na privatnost i slobodi izražavanja na internetu u Srbiji, pretpostavili smo dvema pomoćnim hipotezama:

- H3a: ***Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožava država***.

- H4a: ***Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožava država.***

Da bismo testirali ove hipoteze, upitnikom smo ispitanicima ponudili više različitih tvrdnji o kojima su se izjašnjavali sa *Da*, *Nisam siguran* i *Ne*. Sa prvom takvom tvrdnjom: ***Smatram da Vlada Republike Srbije narušava privatnost internet korisnika***, skoro 40% ispitanika je saglasno, skoro polovina ispitanika (47%) nije sigurna, dok svega 14,6% ispitanika smatra da država ne narušava privatnost internet korisnika u Srbiji (Tabela 11).

Smatram da Vlada RS narušava privatnost internet korisnika.		
	Broj ispitanika	**%**
Ne	114	14.6
Nisam siguran	368	47.0
Da	301	38.4
Total	783	100.0

Tabela 11 Pitanje 32. u delu: ***Odnos Republike Srbije (RS) prema internet korisnicima***

Kako bismo konkretizovali mogućnosti države da ugrozi pravo na privatnost internet korisnika, sledeća tvrdnja je eksplicitnija: ***Smatram da Vlada RS i njene agencije prate aktivnosti internet korisnika u Srbiji***. Ova tvrdnja donosi drugačije procente u odgovorima. Naime, povećava se broj ispitanika koji smatraju da Vlada RS prati aktivnosti korisnika (65,6%), dok se procenat onih koji nisu sigurni u tvrdnju ili nisu saglasni sa njom smanjuje (29,4%, odnosno 5%) (Tabela 12).

Smatram da Vlada RS i njene agencije prate aktivnosti internet korisnika u Srbiji.		
	Broj ispitanika	**%**
Ne	39	5.0
Nisam siguran	230	29.4
Da	514	65.6
Total	783	100.0

Tabela 12 Pitanje 33. u delu: ***Odnos Republike Srbije (RS) prema internet korisnicima***

Iz predočenih rezultata naslućuje se potvrda prve pomoćne hipoteze. Međutim, poređenjem odgovora na dva pitanja (Tabela 13 i Tabela 14) uočena je promena odnosa internet korisnika prema državi u kontekstu zaštite privatnosti onlajn. Naime, ispitanici u značajnom procentu (čak 87,7%) smatraju da neovlašćeno presretanje njihove onlajn-komunikacije narušava njihovu privatnost (Tabela 13).

Kada bih znao da Vlada RS može da pristupi sadržajima koje delim na internetu, bez sudskog naloga, čak i kada su te objave privatne, putem mejla ili direktnih poruka na društvenim mrežama, osećao/osećala bih: [da vlada ugrožava moju privatnost]		
	Broj ispitanika	**%**
Ne	26	3.3
Nisam siguran	70	8.9
Da	687	87.7
Total	783	100.0

Tabela 13 Pitanje 36a, u delu: *Odnos Republike Srbije (RS) prema internet korisnicima*

Međutim, kada smo ovoj tvrdnji dodali pitanje bezbednosti, odnosno da li bi neovlašćen pristup podacima korisnika od strane države značio i zaštitu bezbednosti svih građana, procenti su se značajno promenili: gotovo polovina ispitanika (Da – 17% i Nisam siguran – 30,3%) opravdava takav vid intervencije države ili nisu sigurni u navedenu tvrdnju. Ukoliko uporedimo sa prethodnom tvrdnjom, gde se gotovo 90% ispitanika izjasnilo da neovlašćeni pristup podacima od strane države smatraju narušavanjem privatnosti, možemo da zaključimo da je uvođenje termina *bezbednost* u kontekst uticalo da značajan broj ispitanika promeni stav o neovlašćenom presretanju onlajn-komunikacije od strane države (Tabela 14).

Kada bih znao da Vlada RS može da pristupi sadržajima koje delim na internetu, bez sudskog naloga, čak i kada su te objave privatne, putem mejla ili direktnih poruka na društvenim mrežama, osećao/osećala bih: [da vlada štiti bezbednost svih građana]		
	Broj ispitanika	**%**
Ne	413	52.7
Nisam siguran	237	30.3
Da	133	17.0
Total	783	100.0

Tabela 14 Pitanje 36c, u delu: *Odnos Republike Srbije (RS) prema internet korisnicima*

Do sličnih rezultata došli su i Gogin i saradnici (2017) pri ispitvanju stavova internet korisnika u Australiji[257]. Da podsetimo, kada su autori uključili *antiterorističku strategiju* kao razlog neovlašćenog praćenja internet korisnika, procenat Australijanaca koji je opravdao nadzor u te svrhe bio je znatno veći nego kada je reč o pitanju koje je pretpostavljalo nadzor građana, bez uključenog elementa bezbednosti.

Set tvrdnji postavljen pod okriljem 37. pitanja, imao je za cilj da proveri da li ispitanici smatraju da država ipak može da ih zaštiti ukoliko bi neka privatna kompanija zloupotrebila njihove podatke, i koji bi način zaštite u tom kontekstu bio najefikasniji (Tabela 15).

[257] Istraživanje je detaljno opisano u potpoglavlju: Prethodna istraživanja.

	Smatram da bi Vlada RS mogla da me zaštiti ukoliko bi neka privatna kompanija zloupotrebila moje podatke deljene onlajn kroz:				
	[jasno zakonodavstvo]	[nacionalna tela oformljena specijalno u srvhu monitoringa rada privatnih kompanija na internetu]	[zakonom predviđeno sankcionisanje privatnih internet kompanija]	[veću saradnju sa privatnim kompanijama na internetu]	[veće učešće u regulisanju internet prostora]
Ne	146	151	128	185	173
Nisam siguran	207	262	207	337	273
Da	430	370	448	261	337
Total	783	783	783	783	783

Tabela 15 Pitanje 37a, b, c, d, e. u delu: *Odnos Republike Srbije (RS) prema internet korisnicima*

U Tabeli 15 mogu se očitati nelogičnosti u odgovorima ispitanika. Naime, najveći broj ispitanika saglasio se sa tim da su sankcionisanje privatnih kompanija i jasno zakonodavstvo najefikasniji načini kojima bi država mogla da zaštiti korisnike od zloupotrebe koju bi nanele strane privatne kompanije. Međutim, ispitanici ujedno, pored saradnje sa privatnim kompanijama, najveći procenat neslaganja iskazuju prema stavu da bi država trebalo da uzme veće učešće u regulisanju internet prostora.

S obzirom na to da svega 14,6% ispitanika smatra da država ne ugrožava privatnost internet korisnicima u Srbiji, te da se samo 5% ispitanika nije saglasilo sa tvrdnjom da Vlada RS i njene agencije prate aktivnosti internet korisnika u Srbiji, hipoteza kojom se pretpostavlja da internet korisnici u Srbiji smatraju da država predstavlja opasnost po njihovu privatnost na internetu je potvrđena.

Sledeća pomoćna hipoteza, koja se tiče odnosa ispitanika prema državi, dovodi se u vezu sa slobodom izražavanja na internetu i njome se pretpostavlja da internet korisnici u Srbiji smatraju da njihovu slobodom izražavanja ugrožava država. Kako bismo testirali ovu hipotezu, ispitanicima smo kroz upitnik postavili niz tvrdnji o kojima su se izjašnjavali. Prvom takvom tvrdnjom želeli smo da dobijemo odgovor na pitanje da li se ispitanici osećaju zabrinuto ili nesigurno kada kritikuju Vladu Srbije u onlajn-komunikaciji (Tabela 16).

Osećam se nesigurno ili zabrinuto pri onlajn deljenju stavova koji kritikuju Vladu RS.		
	Broj ispitanika	**%**
Ne	244	31.2
Nisam siguran	178	22.7
Da	361	46.1
Total	783	100.0

Tabela 16 Pitanje 34. u delu: ***Odnos Republike Srbije (RS) prema internet korisnicima***

Na osnovu rezultata prikazanih u Tabeli 16, zaključujemo da se skoro polovina ispitanika, odnosno 46,1%, oseća zabrinuto ili nesigurno kada kritikuje Vladu RS onlajn, skoro 28% bilo je neodlučno, dok se trećina ispitanika ne oseća zabrinuto. Dakle, dve trećine ispitanika ima bojazan, ili nije sigurno kako se oseća, kada je reč o upućivanju otvorenih kritika svojoj Vladi. Ovakvi nalazi govore u prilog hipotezi i implicitno ukazuju na to da strah od javne kritike može imati uticaj na slobodno iznošenje političkog mišljenja internet korisnika.

Sledeća tvrdnja u ovoj bateriji pitanja imala je za cilj da svojom eksplicitnošću iznudi direktniji stav ispitanika, te da ujedno proveri stepen saglasnosti sa prethodnom tvrdnjom (Tabela 17).

Smatram da Vlada RS i njene agencije ugrožavaju slobodu izražavanja internet korisnika u Srbiji.		
	Broj ispitanika	**%**
Ne	117	14.9
Nisam siguran	246	31.4
Da	420	53.6
Total	783	100.0

Tabela 17 Pitanje 35. u delu: ***Odnos Republike Srbije (RS) prema internet korisnicima***

Rezultati prikazani u Tabeli 17 pokazuju drugačiju sliku. Naime, 46,1% ispitanika iskazalo je saglasnost sa prethodnom tvrdnjom i potvrdilo da se oseća zabrinuto pri onlajn kritici Vlade RS; sada je 53,6% ispitanika saglasno sa tvrdnjom da Vlada RS ugrožava slobodu izražavanja internet korisnicima u Srbiji. Razliku u procentima možemo tumačiti na sledeći način: to što više od polovine ispitanika smatra da Vlada ugrožava slobodu izražavanja ne znači nužno da će se internet korisnici osećati nelagodno pri iznošenju političkog stava i kritike. Sa druge strane, značajnija je razlika u procentima kojima se kvanitifikuje neodlučnost; neodlučnost ispitanika kada je reč o tome da li smatraju da Vlada RS ugrožava slobodu izražavanja internet korisnicima povećana je za skoro 8%.

I u ovom delu istraživanja, kada je reč o slobodi izražavanja, želeli smo da proverimo da li će postojati razlika u odgovorima ispitanika ukoliko uključimo termin *bezbednost*. Naime, 649 ispitanika, odnosno skoro 83%, okarakterisalo je neovlašćeno praćenje i pristup onlajn-komunikaciji internet korisnika u Srbiji , kao opasnost po slobodu izražavanja (Tabela 18).

	Kada bih znao da Vlada RS može da pristupi sadržajima koje delim na internetu, bez sudskog naloga, čak i kada su te objave privatne, putem mejla ili direktnih poruka na društvenim mrežama, osećao/osećala bih:	
	[da vlada ugrožava moju slobodu izražavanja.]	[da vlada štiti bezbednost svih građana]
Ne	51	413
Nisam sigurar	83	237
Da	649	133
Total	783	783

Tabela 18 Pitanje 36b, c. u delu: ***Odnos Republike Srbije (RS) prema internet korisnicima***

Međutim, kada smo kroz jednu od tvrdnji dodali pitanje bezbednosti građana, procenat se značajno promenio. Dok je svega 6,5% (51 ispitanik) smatralo da takav vid nadzora ne ugrožava slobodu izražavanja, sada skoro 18% (133 ispitanika) veruje da je takav vid nadzora opravdan ukoliko posredi pitanje bezbednosti. Najveća razlika je u procentima neodlučnih ispitanika: svega 83 ispitanika nije bilo sigurno da li takav vid praćenja i presretanja onaljn podataka i komunikacije preti da ugrozi slobodu izražavanja, dok sada čak 237 ispitanika nije sigurno da li bi takav neovlašćeni nadzor bio u službi zaštite bezbednosti građana.

Na osnovu dobijenih rezultata, prema kojima se skoro polovina ispitanika ne oseća sigurno da kritikuje Vladu RS na internetu, dok nešto više od polovine smatra da Vlada RS ugrožava slobodu izražavanja internet korisnicima u Srbiji, možemo da zaključimo da je i druga pomoćna hipoteza potvrđena.

5.3.3. Rezultati istraživanja: Odnos internet korisnika u Srbiji prema privatnim akterima

Setom pitanja i tvrdnji, podeljenim u dve baterije, posebno za Fejbuk i Gugl, imali smo za cilj da testiramo stav ispitanika prema privatnim kompanijama, kada je reč o zaštititi privatnosti i slobodnom izražavanju. Pretpostavili smo da su korisnici podjednako nepoverljivi i prema privatnim akterima, kao i prema državi. U skladu sa tim, postavili smo dve pomoćne hipoteze koje se tiču odgovornosti privatnih kompanija:

- H3b: ***Internet korisnici u Srbiji smatraju da njihovu privatnost ugrožavaju privatni akteri (Gugl i Fejsbuk).***

- H4b: ***Internet korisnici u Srbiji smatraju da njihovu slobodu izražavanja ugrožavaju privatni akteri (Gugl i Fejsbuk).***

Neophodno je napomenuti da je upitnik bio dizajniran tako da negativan odgovor na pitanje: *Da li imate profil na društvenoj mreži Fejsbuk*? ispitanike automatski vodi na set pitanja o Guglu. Zbog toga je broj ispitanika koji su odgovarali na pitanja o Fejsbuku 735, dok je ukupan broj ispitanika 783.

Kao što je prikazano u Tabelama 19 i 20, ispitanici su gotovo jednako nepoverljivi prema Fejsbuku i Guglu, kada je reč o zaštiti njihove privatnosti, a prilikom korišćenja usluga ovih kompanija.

Zadovoljan sam načinom na koji Fejsbuk štiti moju privatnost.		
	Broj ispitanika	**%**
Ne	270	36.7
Nisam siguran	378	51.4
Da	87	11.8
Total	735	100.0

Tabela 19 Pitanje 19. u delu: ***Odnos prema kompanije Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Naime, 11,8% ispitanika zadovoljno je načinom na koji Fejsbuk štiti njihovu privatnost (Tabela 19), dok je nešto više korisnika, 13%, zadovoljno Guglom u tom kontekstu (Tabela 20). Sa druge strane, veći je procenat onih koji nisu sigurni da li Fejsbuk u dovoljnoj meri štiti njihove podatke, 51,4%, naspram 44,6% za Gugl. Samim tim je veći procenat onih koji nisu zadovoljni zaštitom privatnosti od strane kompanije Gugl (42,4%), u poređenju sa Fejsbukom u tom kontekstu (36,7%).

Smatram da Gugl i aplikacije povezane sa njim, štite moju privatnost i lične podatke.		
	Broj ispitanika	**%**
Ne	332	42.4
Nisam siguran	349	44.6
Da	102	13.0
Total	783	100.0

Tabela 20 Pitanje 23. u delu: ***Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja***

Zbog načina fukcionisanja društvene mreže Fejsbuk, koja svakako pretpostavlja veće i učestalije deljenje ličnih podataka korisnika nego što je to slučaj sa pretraživačima, u ovom slučaju kompanijom Gugl, naredni set pitanja fokusiran je na odnos korisnika prema zaštiti privatnosti i ličnih podataka od strane društvene mreže Fejsbuk.

Sa ciljem da ispitamo koga ispitanici – Fejsbuk korisnici, smatraju najvećom pretnjom po svoja prava prilikom korišćenja usluga ove društvene mreže, ponudili smo najčešće pretpostavljene aktere. Naši rezultati pokazuju sledeće: korisnici najveću pretnju vide u trećim licima sa kojima Fejsbuk deli podatke svojih korisnika (40,7%), zatim vide gotovo podjednaku pretnju u poslovanju same kompanije i aktivnostima drugih korisnika (27,2% naspram 22,2%), dok je država poslednja na njihovoj listi opasnosti po prava internet korisnika, sa svega 9,9% (Tabela 21).

Prava internet korisnika na Fejsbuku najviše su ugrožena od:		
	Broj ispitanika	**%**
drugih Fejsbuk korisnika	163	22.2
Države	73	9.9
kompanije Fejsbuk	200	27.2
trećih lica kao što su reklamne agencije, agencije za statistikui slično	299	40.7
Total	735	100.0

Tabela 21 Pitanje 22. u delu: ***Odnos prema kompanije Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

U ovim rezultatima očitavamo i određene nelogičnosti. Naime, ispitanici su, kao što smo mogli videti pri razmatranju i testiranju prethodne hipoteze, iskazali veliko nepoverenje u državu kada je reč o zaštiti njihovih podataka. Ipak, državu smatraju najmanjom pretnjom od svim navedenih aktera. Uzrok tome možemo potražiti i u redosledu pitanja, odnosno u samoj bateriji pitanja. Kao što je već navedeno, pregled rezultata prati strukturu rada, te je set pitanja o državi, i hipoteze koje se odnose na državu, prvi predstavljen. Međutim, upitnik je bio koncipiran tako da su ispitanici najpre odgovarali na set pitanja o privatnim akterima, pa tek onda o državi. Možemo da pretpostavimo da su u trenutku odgovaranja na ovu tvrdnju ispitanici bili fokusirani na zloupotrebe od strane privatnih kompanija, dok je fokus na državi bio tek u narednom setu pitanja. U prilog našoj interpretaciji govori i odgovor na poslednje pitanje u upitniku: *Ukoliko bih morao/morala da biram, moje podatke koje delim onlajn prepustio/prepustila bih na čuvanje: državi ili privatnim kompanijama?* (Tabela 22).

Ukoliko bih morao/morala da biram, moje podatke koje delim onlajn prepustio/prepustila bih na čuvanje:		
	Broj ispitanika	**%**
Državi	284	36.3
privatnim kompanijama (Fejsbuku, Guglu)	499	63.7
Total	783	100.0

Tabela 22 Pitanje 41.

Kao što je prikazano u Tabeli 22, 63,7% ispitanika bi svoje podatake poverilo privatnim kompanijama, nasuprot 36,3% korisnika koji bi se ipak opredelili za državu. Dakle, iako su na ponuđenoj listi aktera, koji su pretpostavljena pretnja privatnosti Fejsbuk korisnika, privatni akteri i kompanije koje sarađuju sa njima na vrhu, a država na začelju, ispitanici ipak veruju da bi privatne kompanije odgovornije postupale sa njihovim ličnim podacima.

Zabrinutost korisnika kada je reč o deljenju podataka sa trećim licima potvrđen je i kroz naredne tvrdnje. Više od polovine ispitanika smatra da bi Fejbuk trebalo da bude transparentniji u pogledu deljenja podataka sa trećim licima (Tabela 23).

Smatram da bi Fejsbuk trebalo da bude transparentniji u pogledu deljenja podataka svojih korisnika sa trećim licima, drugim kompanijama.		
	Broj ispitanika	**%**
Ne	176	23.9
Nisam siguran	166	22.6
Da	393	53.5
Total	735	100.0

Tabela 23 Pitanje 17. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Čak 95% ispitanika saglasno je sa još konkretnijom tvrdnjom kojom se ističe da korisnik ima pravo da nedvosmisleno zna kojim licima i kojim povodom Fejsbuk prosleđuje njihove podatke (Tabela 24).

Smatram da imam pravo da nedvosmisleno znam kojim licima i kojim povodom je Fejsbuk prosledio moje podatke.		
	Broj ispitanika	**%**
Ne	15	2.0
Nisam siguran	22	3.0
Da	698	95.0
Total	735	100.0

Tabela 24 Pitanje 18. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

S obzirom na to da je svega 11,8% ispitivanih korisnika zadovoljno načinom na koji Fejsbuk štiti njihovu privatnost, dok je Guglovom zaštitom privatnosti zadovoljno samo 13% ispitanika, možemo da zaključimo da je pomoćna hipoteza kojom pretpostavljamo da internet korisnici smatraju da ove privatne kompanije predstavljaju opasnost po njihovu privatnost potvrđena.

Pitanje odnosa slobode izražavanja i privatnih kompanja kompleksnije je i manje očigledno od pitanja privatnosti na internetu. Set pitanja kojima smo želeli da testiramo hipotezu kojom se pretpostavlja da internet korisnici u Srbiji nemaju poverenje u privatne aktere, Gugl i Fejsbuk, kada je reč o apsolutnom ostvarivanju prava na slobodno izražavanje, koncipiran je tako da bude blizak prosečnom korisniku, a da opet svojim odgovorima doprinese testiranju hipoteze. Prve tvrdnje bile su direktne i eksplicitno su potraživale odgovore na pitanja da li ispitanici smatraju da Fejsbuk, odnosno Gugl, mogu imati uticaj na njihovu slobodu izražavanja (Tabele 25 i 26).

Smatram da kompanija Fejsbuk može da mi uskrati slobodu izražavanja.		
	Broj ispitanika	**%**
Ne	226	30.7
Nisam siguran	188	25.6
Da	321	43.7
Total	735	100.0

Tabela 25 Pitanje 19. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Kako je prikazano u Tabeli 25, trećina ispitanika smatra da Fejsbuk ne može imati uticaj na njihovu slobodu izražavanja, 25,6% nije sigurno u tvrdnju, dok 43,7% smatra da Fejsbuk može da uskrati slobodu izražavanja. Međutim, kada je reč o kompaniji Gugl, procenti su znatno drugačiji (Tabela 26).

Smatram da Gugl može imati uticaj na moju slobodu izražavanja.		
	Broj ispitanika	**%**
Ne	265	33.8
Nisam siguran	253	32.3
Da	265	33.8
Total	783	100.0

Tabela 26 Pitanje 28. u delu: ***Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja***

Naime, ispitanici su procentualno gledano gotovo ujednačeni kada je reč o kompaniji Gugl. Isti broj ispitanika smatra tvrdnju tačnom, odnosno netačnom, po 265, dok nešto manji broj, 253 ispitanika, nije siguran u navedenu tvrdnju. Ovakvi rezultati bili su i očekivani zbog prirode poslovanja ove dve kompanije. Fejsbuk je, kao društvena mreža, internet prostor u koji su korisnici znatno upućeniji u smislu prisustva, samoprezentacije, participacije, deljenja ličnih podataka, iznošenja ličnih stavova i slično. Pretpostavljamo da prilikom korišćenja pretraživača prosečni korisnik ne može lako da uoči načine na koje pretraživač može da utiče na slobodu izražavanja, kao što je to slučaj sa društvenim mrežama.

Kako bismo testirali da li su korisnici upoznati sa načinom na koji se uređuje opticaj informacija na društvenim mrežama, odnosno rangiranje pretrage, postavili smo set tvrdnji o kojima su se ispitanici izjašnjavali. Kako rezultati pokazuju, 69% ispitanika saglasno je sa tvrdnjom da Fejsbuk manipuliše objavama koje se pojavljuju na početnoj stranici (engl. *News Feed*) (Tabela 27).

Smatram da Fejsbuk manipuliše objavama koje se pojavljuju na početnoj stranici (News Feed).		
	Broj ispitanika	**%**
Ne	47	6.4
Nisam siguran	181	24.6
Da	507	69.0
Total	735	100.0

Tabela 27 Pitanje 20. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Dakle, više od dve trećine ispitanika zna da se informacije i objave na početnoj stranici Fejsbuka ne objavljuju bez učešća algoritma, odnosno bez prethodnog upravljanja, ili kako smo mi to nazvali – manipulisanja. U ovom kontekstu pod manipulisanjem podrazumevamo upravljanje bez vrednosnog određenja, odnosno ne podrazumevamo nužno negativnu praksu.

S obzirom na to da je veći broj ispitanika upoznat sa tim da se početnom stranicom upravlja mimo njihove volje, zanimalo nas je da li su korisnici svesni načina na koji algoritam funkcioniše. U skladu sa tim postavili smo četiri odrednice značaja: aktuelnost, hornologiju, interesovanja korisnika i sponzorstvo (Tabela 28).

	Smatram da se objave na početnoj stranici (News Feed) pojavljuju po:			
	[aktuelnosti]	[hronologiji]	[interesovanjima korisnika]	[sponzorstvima]
Ne	137	277	98	59
Nisam siguran	233	270	202	176
Da	365	188	435	500
Total	735	735	735	735

Tabela 28 Pitanje 21a, b, c, d. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi***

Na osnovu dobijenih rezultata možemo da zaključimo da ispitanici prepoznaju značaj navedenih odrednica. Najveća saglasnost odnosi se na sponzorstva, odnosno ispitanici su u najvećoj meri saglasni sa tvrdnjom da se objave na početnoj stranici Fejsbuka pojavljuju na osnovu ove odrednice (68% ispitanika je saglasno). Sa druge strane, ispitanici su u najvećoj meri neodlučni kada je reč o tome da li akutelnost i hronologija imaju uticaj na objave koje se pojavljuju na početnoj strani.

Isti set pitanja postavljen je i za pretraživač Gugl. Cilj ovih tvrdnji bio je da se ispita da li su i u kojoj meri ispitanici upoznati sa načinom rangiranja pretraživanih pojmova. Skoro dve trećine ispitanika saglasno je sa tim da Gugl manipuliše rezultatima pretrage (Tabela 29), odnosno za 10% manje nego što je to bio slučaj sa Fejsbukom.

Smatram da pretraživač Gugl manipuliše rezultatima pretrage.		
	Broj ispitanika	**%**
Ne	103	13.2
Nisam siguran	214	27.3
Da	466	59.5
Total	783	100.0

Tabela 29 Pitanje 29. u delu: ***Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja***

Kada je reč o odrednicama na osnovu kojih Gugl rangira pretraživane pojmove, ispitanici su, takođe, u najvećoj meri bili saglasni sa tim da na pretragu utiču sponzorstva, njih 64% (Tabela 30) – za samo 4% manje nego što je to bio slučaj sa Fejsbukom.

	Prilikom pretrage putem Gugla, informacije koje dobijem kao rezulatat pretrage rangiraju se prema:			
	[interesovanjima korisnika]	[aktuelnosti]	[hronologiji]	[sponzorstvima]
Ne	93	85	242	59
Nisam siguran	209	217	334	224
Da	481	481	207	500
Total	783	783	783	783

Tabela 30 Pitanje 30a, b, c, d. u delu: ***Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja***

Identičan broj ispitanika, 481, odnosno nešto više od 60%, smatra da su aktuelnost i interesovanja korisnika značajne odrednice pri rangiranju, dok je najmanja saglasnost (nešto više od 26%) iskazana kada je reč o hronologiji kao kriterijumu za rangiranje.

Na kraju, ispitanicima smo dali nekoliko predloga/preporuka, a koje se tiču onoga što bi ove kompanije mogle da urade kako bi se korisnici osećali bezbednije pri korišćenju njihovih usluga (Tabela 31).

	Šta je prema vašem mišljenju to što bi kompanije, poput Gugla i Fejsbuka, trebalo da urade da biste se osećali sigurnije kada koristite njihove usluge			
	[da budu transparentiji u pogledu deljenja mojih podataka]	[da poboljšaju politiku privatnosti]	[da odlučnije preuzmu odgovornost za svoje poslovanje]	[da na jednostavniji način upoznaju korisnike sa načinom poslovanja]
Ne	101	26	31	25
Nisam siguran	141	95	114	63
Da	541	662	638	695
Total	783	783	783	783

Tabela 31 Pitanje 31.

Ispitanici su u većinski bili saglasni sa svim predlozima. Kako rezultati pokazuju,najveća saglasnost, preciznije, 695 ispitanika, tiče se preporuke da kompanije pronađu jednostavniji način, primereniji korisnicima, kako bi ih upoznali sa načinom poslovanja, . Ovaj podatak govori u prilog rezultatima analize uslova korišćenja, kojima se sugeriše da su nerazumljiv jezik i kompleksnost politika jedne od najvećih prepreka za postizanje afirmativnog pristanka korisnika.

Pomoćnu hipotezu kojom se pretpostavlja da internet korisnici u Srbiji smatraju da privatne kompanije ugrožavaju njihovo pravo na slobodno izražavanje potvrđuje sledeće: 1) trećina ispitivanih korisnika (33,8%) smatra da Gugl može ugroziti slobodu izražavanja korisnika, dok 43,7% veruje da to može i Fejsbuk, 2) najveći broj ispitanika saglasan je sa tvrdnjom da su sponzorstva prva na listi odrednica značaja, a na osnovu kojih se nude ili rangiraju određene informacije.

5.3.4. Rezultati istraživanja: individualna odgovornost korisnika

Hipoteze koje su razmatrane u prethodnom delu ticale su se odgovornosti kompanija kada je reč o zaštiti podataka korisnika. Međutim, česta tema istraživanja jeste i individualna odgovornost korisnika, odnosno radnje koje sami korisnici preduzimaju kako bi se zaštitili od zloupotreba na internetu, naročito prilikom korišćenja društvenih mreža. Pitanje individualne odgovornosti korisnika formulisano je kroz sledeće hipoteze:

- **H5. Internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti kada je o zaštiti njihovih prava na internetu reč.**

- H5a: *Internet korisnici u Srbiji ne čine dovoljno da zaštite svoju privatnost, iako su svesni rizika od zloupotrebe ličnih podataka*.

- H5b: *Internet korisnici u Srbiji nisu u dovoljnoj meri upoznati sa Uslovima korišćenja kompanija čije usluge koriste***.**

S obzirom na to da je svest korisnika o rizicima potvrđena, odnosno da korisnici u najvećem procentu ne veruju u zaštitu podataka na internetu, te da nemaju poverenje u privatne aktere kada je reč o zaštiti njihove privatnosti, smatrali smo da je set pitanja o tome kako se ispitanici odnose prema zaštiti svojih podataka značajan, jer implicitno ukazuje na to koliko ispitanici zapravo ulažu u zaštitu svojih podataka. U prilog ovome idu i rezultati koji pokazuju da su ispitanici nepoverljivi prema državnim i privatnim akterima, te da se većina njih oseća nesigurno ili zabrinuto.

Kako bismo testirali pomoćnu hipotezu (H5a), ispitanicima smo postavili nekoliko tvrdnji o njihovom angažovanju koje se tiče manualnog podešavanja privatnosti na društvenoj mreži Fejsbuk. Zanimljivo je da, kako je i prikazano u Tabeli 32, gotovo svi ispitanici, njih 93,6%, smatraju da bi svako trebalo da vodi računa o svojoj privatnosti na Fejsbuku.

Smatram da bi svako trebalo da vodi računa o svojoj privatnosti na Fejsbuku.		
	Broj ispitanika	**%**
Ne	16	2.2
Nisam siguran	31	4.2
Da	688	93.6
Total	735	100.0

Tabela 32 Pitanje 8. u delu: ***Odnos prema kompaniji Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Iako ispitanici evidentno smatraju da je individualna odgovornost prema sopstvenim podacima veoma značajna, procenat onih kojih su promenili podešavanja privatnosti na Fejsbuku kako bi se dodatno zaštitili nije istovetan; 75,1% ispitanika odgovorio je potvrdno, dok 10,9% ispitanika nije sigurno, a 14% ispitanika nije promenilo podešavanja privatnosti (Tabela 33).

Promenio/la sam podrazumevana podešavanja na Fejsbuku koja se odnose na privatnost i na taj način dodatno zaštitio/la svoju privatnost.		
	Broj ispitanika	**%**
Ne	103	14.0
Nisam siguran	80	10.9
Da	552	75.1
Total	735	100.0

Tabela 33 Pitanje 9. u delu: ***Odnos prema kompanije Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Dakle, procenat ispitanika koji su promenili podešavanja i time dodatno zaštitili svoju privatnost je za skoro 20% manja (93,6% naspram 75,1%) od procenta onih koji smatraju da je zaštita privatnosti i lična odgovornost korisnika. Dodatnu nelogičnost donose i rezultati odgovora na kontrolno pitanje da li većinu objava na Fejsbuku mogu da vide i oni koji nisu Fejsbuk prijatelji ispitanika: 81% odgovara odrično, 14,3% potvrdno, dok 4,5% ispitanika nije sigurno (Tabela 34).

Većinu mojih objava na Fejsbuku mogu da vide i oni koji mi nisu prijatelji.		
	Broj ispitanika	**%**
Ne	597	81.2
Nisam siguran	33	4.5
Da	105	14.3
Total	735	100.0

Tabela 34 Pitanje 10. u delu: ***Odnos prema kompanije Fejsbuk kada je reč o privatnosti i slobodi izražavanja***

Ukoliko ove procente uporedimo sa prethodnim, videćemo da je 75,1% ispitanika sigurno da je promenilo podešavanja na Fejsbuku, dok je sada 81% ispitanika sigurno da njihove objave ne mogu videti oni korisnici koji im nisu Fejsbuk prijatelji. Razlika u procentima može se tumačiti kao česta zabluda Fejsbuk korisnika da je automatska postavka privatnosti zapravo koncipirana tako da štiti njihovu privatnost, čak iako nisu manualno promenili podešavanja o privatnosti.

S obzirom na to da samo 7,5% ispitanika smatra da su podaci na internetu zaštićeni, potvrđeno je da su internet korisnici svesni rizika po njihovu privatnost onlajn. Takođe, pošto 25% ispitanika nije manualno promenilo podešavanja na Fesjbuku ili nisu sigurni da li su to učinili, evidentno je da ispitanici ne čine sve što je u njihovoj moći da dodatno zaštite svoju privatnost onlajn.

Da bismo testirali pomoćnu hipotezu: *Internet korisnici u Srbiji nisu u dovoljnoj meri upoznati sa Uslovima korišćenja usluga kompanija Fejsbuk i Gugl*, korisnike smo najpre, na samom početku upitnika, pitali da li čitaju Uslove korišćenja kompanija čije usluge koriste. Iznenađujući procenat ispitanika, čak 32,6%, odgovorio je potvrdno (Tabela 35).

Čitam *Uslove korišćenja* (Fejsbuka, Gugla) pre nego što ih prihvatim.		
	Broj ispitanika	**%**
Ne	461	59.2
Nisam siguran	64	8.2
Da	254	32.6
Total	779	100.0

Tabela 35 Pitanje broj 5. u delu: *Odnos prema privatnosti i slobodi izražavanja na internetu*

Kako bismo testirali njihovo poznavanje Uslova korišćenja kompanija Fejsbuk i Gugl, postavili smo niz kontrolnih pitanja. Pitanja su formulisana tako da je odgovor *Da* zapravo tačan odgovor na navedenu tvrdnju, jer su tvrdnje preuzete iz važećih Uslova korišćenja i politika privatnosti kompanija Gugl i Fejsbuk. Ukrštanjem odgovora na pitanje da li ispitanici čitaju uslove korišćenja sa odgovorima na kontrolna pitanja, želeli smo da testiramo njihovo realno poznavanje uslova. Kontrolna pitanja postavljena su posebno za obe navedene kompanije.

Kada je reč o kompaniji Fejsbuk, rezultati ukrštanja pokazali su da korisnici koji su tvrdili da čitaju Uslove korišćenja ne poznaju Uslove više od korisnika koji su na to pitanje odgovorili negativno, čak su u pojedinim slučajevima pokazali manje poznavanje Uslova korišćenja (Tabela 36).

	Čitam Uslove korišćenja (Fejsbuka, Gugla) pre nego što ih prihvatim.			Total	chi sq	sig
	Ne	Nisam	Da			

			siguran				
Fejsbuk ima moju dozvolu da koristi podatke sa mog uređaja, računara ili mobilnog telefona.	Ne	132	15	134	281	51.829	<0.001
	Nisam siguran	166	23	45	234		
	Da	140	18	58	216		
Fejsbuk ima moju dozvolu da pristupi zvučniku i kameri na mom uređaju, računaru ili mobilnom telefonu.	Ne	123	15	130	268	50.887	<0.001
	Nisam siguran	141	21	46	208		
	Da	174	20	61	255		
Fejsbuk ima moju dozvolu da pristupi mojim mejl i telefonskim kontaktima.	Ne	200	23	153	376	27.153	<0.001
	Nisam siguran	149	24	48	221		
	Da	89	9	36	134		
Fejsbuk ima moju dozvolu da pristupi mojoj galeriji, slikama sačuvanim na memoriji uređaja.	Ne	108	10	108	226	38.001	<0.001
	Nisam siguran	126	20	43	189		
	Da	204	26	86	316		
Fejsbuk ima moju dozvolu da moje podatke ustupa trećim licima, kompanijama sa kojima sarađuje.	Ne	200	20	170	390	55.103	<0.001
	Nisam siguran	199	30	46	275		

	Da	39	6	21	66		

Tabela 36 Ukrštanje odgovora na 5. pitanje sa odgovorima na kontrolna pitanja o Fejsbuku.

Broj Fejsbuk korisnika koji je potvrdio da čita Uslove korišćenja je 237. Na prvo kontrolno pitanje – *Fesjbuk ima moju dozvolu da koristi podatke sa mog uređaja, računara ili mobilnog telefona* – više od polovine ispitanika koji su tvrdili da su pročitali Uslove korišćenja odgovorili su negativno. Sa druge strane, od 438 ispitanika koji su tvrdili da ne čitaju Uslove korišćenja, svega 30% nije tačno odgovorilo na prvo kontrolno pitanje. Gotovo identični rezultati dobijeni su i na drugom kontrolnom pitanju – *Fejsbuk ima moju dozvolu da pristupi zvučniku i kameri na mom uređaju, računaru ili mobilnom telefonu*.

Kod kontrolnog pitanja: *Fejsbuk ima moju dozvolu da pristupi mojoj galeriji, slikama sačuvanim na memoriji uređaja*, uočava se najveći procenat tačnih odgovora u odnosu na ostala kontrolna pitanja (36,2%). Pretpostavljamo da je ovaj vid dozvole najočigledniji, jer je korisnicima jasno predočeno pre svakog deljenja fotografija na Fejsbuku da daju dozvolu da kompanija pristupi njihovoj galeriji na telefonu ili računaru.

Kontrolna tvrdnja: *Fejsbuk ima moju dozvolu da moje podatke ustupa trećim licima, kompanijama sa kojima sarađuje*, donela je poražavajuće rezultate sa aspekta poznavanja uslova korišćenja. Naime, svega 8,9% ispitanika koji su tvrdili da su pročitali Uslove korišćenja dali su tačan odgovor na ovo pitanje. Od ukupnog broja ispitanika – Fejsbuk korisnika (731), svega 66 njih, odnosno manje od 8%, zna da Fesjbuk ima dozvolu korisnika da njihove podatke deli sa trećim licima.

Set kontrolnih tvrdnji postavljen je i za kompaniju Gugl (Tabela 37). Takođe, odgovor na pitanje da li ispitanici čitaju Uslove korišćenja ukršten je sa odgovorima na kontrolna pitanja čiji je tačan odgovor *Da*. Rezultati su, kao što je to bio slučaj i sa kontrolnim tvrdnjama za Fejsbuk, pokazali da većina korisnika ne poznaje uslove korišćenja, što je naročito izraženo kod ispitanika koji su tvrdili da su ih pročitali.

	Čitam Uslove korišćenja (Fejsbuka, Gugla) pre nego što ih prihvatim.				chi sq	sig
	Ne	Nisam siguran	Da	Total		

Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe podacima sa mog uređaja: mobilnog telefona, tableta, računara i slično.	Ne	92	16	106	214	41.293	<0.001
	Nisam siguran	130	20	45	195		
	Da	239	28	103	370		
Gugl i aplikacije povezane sa njim imaju moju dozvolu da prate moje aktivnosti na internetu.	Ne	104	16	105	225	28.924	<0.001
	Nisam siguran	165	24	71	260		
	Da	192	24	78	294		
Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe mojim kontaktima na mejlu.	Ne	145	20	129	294	27.997	<0.001
	Nisam siguran	141	17	53	211		
	Da	175	27	72	274		
Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe sadržaju mojih mejlova.	Ne	170	21	147	338	33.022	<0.001
	Nisam siguran	190	26	69	285		
	Da	101	17	38	156		

Tabela 37 Ukršten odgovor na 5. pitanje sa odgovorima na kontolna pitanja za Gugl

Na prvu kontrolnu tvrdnju *Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe podacima sa mog uređaja: mobilnog telefona, tableta, računara i slično* skoro 42% ispitanika, koji su tvrdili da su pročitali Uslove korišćenja, nije odgovorilo tačno, odnosno nije se saglasilo sa navedenom tvrdnjom. U gotovo identičnom broju (106 naspram 105 ispitanika), ispitanici su negativno odgovorili i

na drugo kontrolno pitanje: *Gugl i aplikacije povezane sa njim imaju moju dozvolu da prate moje aktivnosti na internetu*.

Stepen neslaganja je rastao sa preostale dve kontrolne tvrdnje. Sa tvrdnjom: *Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe mojim kontaktima na mejlu* nije saglasno 50,8%, dok sa tvrdnjom: *Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe sadržaju mojih mejlova* nije saglasno čak 57,9% onih ispitanika koji su tvrdili da su pročitali Uslove korišćenja Gugla.

Na osnovu navedenih rezultata možemo da zaključimo da čak i oni korisnici koji tvrde da su pročitali Uslove korišćenja kompanija Gugl i Fejsbuk većinski nisu upoznati sa dozvolama koje su prilikom prihvatanja uslova korišćenja dali ovim kompanijama. Takve rezultate možemo da interpretiramo na više načina: ili su ispitanici dali društveno poželjan odgvor na pitanje da li čitaju Uslove korišćenja, ili su delimično pročitali Uslove, smatrajući da je to dovoljno za njihovo razumevanje, ili su, pak, pročitali Uslove korišćenja, ali ih nisu razumeli na adekvatan način zbog njihove kompleksnosti.

Na osnovu dobijenih rezultata zaključujemo da je potvrđena i hipoteza: *Internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti kada je o zaštiti njihovih prava na internetu reč*. Testiranjem pomoćnih hipoteza potvrdili smo da ispitanici ne ulažu dovoljno u zaštitu svojih podataka kroz, na primer, individualna podešavanja privatnosti, niti su u dovoljnoj meri upoznati sa Uslovima korišćenja usluga kompanija čiji su aktivni korisnici.

5.3.5. Rezultati istraživanja: uticaj varijabli

S obzirom na to da uzorak korišćen u ovom istraživanju ne pretenduje na reprezentativnost, rezultati analize koji uključuju uticaj varijabli pola, godina starosti, mesta stanovanja i profesionalnog usmerenja odnose se isključivo na uzorak testiran upitnikom, i ne odnose se na opštu populaciju. Zbog navedenog, ove varijable nisu pretpostavljene hipotezama, već će biti isključivo opisnog karaktera.

Prilikom analize, nijedna od varijabli nije pokazala statističku značajnost osim pola ispitanika. Da bi se proverila povezanost pola i nesigurnosti kada je reč o slobodnom izražavanju na internetu, upotrebljen je hi kvadrat – test za ispitivanje zavisnosti dva obeležja (Tabela 38).

-

		pol1		Total	chi sq	sig
		muški	ženski			
Osećam se slobodno da objavljujem sve svoje stavove onlajn.	Ne	86	281	367	7.102	0.029
	Nisam siguran	47	144	191		
	Da	72	145	217		

Tabela 38 Uticaj pola ispitanika na slobodno izražavanje na internetu.

Kako je prikazano u Tabeli 38, kada je reč o slobodi ispitanika da iskazuju svoje stavove onlajn, za 10% je veći procenat muškaraca koji se osećaju slobodno da iznose svoje mišljenje na internetu u odnosu na ispitanike ženskog pola (35% naspram 25%). Pol kao značajnu varijablu, kada je reč o slobodi izražavanja na internetu, potvrđuje i istraživanje Gogina i saradnika (2017), koji su takođe došli do rezultata da je muškarcima značajnije pravo na slobodno izražavanje na internetu. Autori ovo povezuju sa većim učešćem muškaraca i u tradicionalnoj javnoj sferi.

***

Sprovedeno istraživanje potvrdilo je sve hipoteze koje se odnose na internet korisnike i njihov odnos prema slobodi izražavanja i zaštiti podataka na internetu. Dobijeni podaci govore u prilog tome da su internet korisnici u Srbiji nepoverljivi prema državi, ali i prema privatnim akterima kada je reč o zaštiti njihovih prava onlajn. Međutim, potvrđeno je i da sami korisnici ne čine dovoljno kako bi se zaštitili onlajn. Najznačajnije nalaze možemo da sumiramo kroz sledeće teze:

- Više od polovine ispitanika smatra da podaci koje dele na internetu nisu zaštićeni, dok svega petina njih smatra da je moguće zaštiti privatnost na internetu.

- Nešto manje od trećine ispitanika smatra da je sloboda izražavanja na internetu zagarantovana, dok se gotovo identičan broj ispitanika ne oseća slobodno da objavljuje svoje stavove onlajn.

- Svega šestina ispitanika smatra da Vlada RS ne narušava privatnost internet korisnika u Srbiji, dok svega 5% njih veruje da Vlada RS ne prati aktivnosti internet korisnika.

- Neovlašćeno praćenje komunikacije na internetu samo 26 od 783 ispitanika ne doživljava kao ugrožavanje privatnosti od strane Vlade RS; međutim, ukoliko je reč o zaštiti bezbednosti građana, 133 ispitanika smatra takav vid nadzora opravdanim.

- Najveća saglasnost ispitanika, kada je reč o akcijama kojima država može da zaštiti građane od privatnih korporacija, odnosi se na sankcionisanje privatnih aktera i jasno zakonodavstvo – međutim, ispitanici nisu u istoj meri saglasni sa tim da bi država trebalo da uzme veće učešće u regulisanju internet prostora.

- Skoro polovina ispitanika oseća se nesigurno ili zabinuto kada kritikuje Vladu RS onlajn – u skladu sa tim, nešto više od polovine smatra da Vlada ugrožava slobodu izražavanja internet korisnicima u Srbiji.

- Svega 11,8% ispitanika zadovoljno je načinom na koji Fejsbuk štiti njihovu privatnost, dok je 13% zadovoljno načinom na koji to čini kompanija Gugl.

- Najveću pretnju po svoja prava na Fejsbuku korisnici vide u trećim licima, a najmanju u državi – međutim, u krajnjem se ipak dve trećine ispitanika odlučuje da svoje podatke poveri na čuvanje privatnim kompanijama pre nego državi.

- Polovina ispitanika smatra da bi Fejsbuk trebalo da bude transparentniji u pogledu deljenja podataka korisnika sa trećim licima, dok 95% njih veruje da bi nedvosmisleno trebalo da znaju ko su kompanije sa kojima Fejsbuk deli podatke.

- Nešto manje od polovine ispitanika smatra da Fejsbuk može da ugrozi slobodu izražavanja korisnicima, dok trećina veruje da to može i Gugl.

- Ispitanici su u dovoljnoj meri upoznati sa načinom rangiranja objava na početnoj stranici Fejsbuka i načinom rangiranja prilikom pretraživanja putem Gugla. Najveća saglasnost ispitanika, za obe kompanije, uočena je kod odrednice sponzorstva, kao značajne pri rangiranju objava, odnosno pretraživanih pojmova.

- Kada je reč o preporukama za bolje poslovanje i bezbednije okruženje pri korišćenju usluga Fejsbuka i Gugla, ispitanici su se u najvećoj meri saglasili sa tim da bi ove kompanije trebalo da na jednostavniji i razumljiviji način upoznaju korisnike sa načinom poslovanja, zatim da odlučnije preuzmu odgovornost i da poboljšaju svoje politike privatnosti.

- Internet korisnici ne čine dovoljno da se dodatno zaštitite prilikom korišćenja usluga privatnih kompanija na internetu; 25% ispitanika nije promenilo ili nije sigurno da li je promenilo individualna podešavanja privatnosti na Fejsbuku.

- Trećina ispitanika tvrdi da je pročitala Uslove korišćenja Gugla i Fejsbuka, a prosečno polovina njih nije upućena u osnove uslova korišćenja na koje su pristali i nije dala tačne odgovore na kontrolna pitanja.

- Svega 8,9% ispitanika, koji su tvrdili da su pročitali Uslove korišćenja, znaju da kompanija Fejsbuk deli njihove podatke sa trećim licima.

Na osnovu dobijenih podataka možemo da zaključimo da pored toga što su korisnici nepoverljivi prema državi i privatnim akterima, oni nisu dovoljno upoznati sa načinom poslovanja kompanija čije usluge svakodnevno koriste, ostavljajući za sobom nemerljive količine digitalnih otisaka. Ispitanici jesu svesni rizika po svoja prava onlajn, ocenjuju ga visokom ocenom, ali ih to ne motiviše da dostupnim mehanizmima zaštite svoje podatke, ili da se informišu o načinima na koje kompanije koriste njihove podatke. Takav nalaz je u saglasnosti sa istraživanjem Moranda i saradnika (Morando et al., 2014) – bez obzira na nedvosmislenu zabrinutost za bezbednost u onaljn-sferi (*deklarisane* preferenicije), koja je potvrđena i u ovom istraživanju, internet korisnici pokazuju nizak nivo poznavanja uslova korišćenja i ne čine dovoljno da se dodatno zaštite (*otkrivene* preferencije).

Nepoznavanje načina poslovanja privatnih kompanija delom se može pripisati nedovoljnoj individualnoj odgovornosti korisnika. Međutim, odgovornost možemo da potražimo i u korporacijama i u državi. Naime, ispitanici su se većinski saglasili sa tim da postoji potreba da kompanije na jednostavniji način upoznaju svoje korisnike sa načinom poslovanja. Jasan jezik politika, pojašnjenje tehničkih i stručnih termina, redukovanje preopširnih elektronskih ugovora, moglo bi da motiviše korisnike da pročitaju uslove pre nego da ih samo automatski prihvate. Sa druge strane, češće javne debate, organizovanje javnih rasprava i foruma na temu onlajn-prava i bezbednosti, u kojima bi učestvovali i građani, o čemu pišu i Gogin i saradnici (2017), moglo bi da doprinese približavanju kompleksnih tema prosečnim internet korisnicima.

6. Upravljanje internetom: komparativna perspektiva

Internet, koji je u svom začetku delovao monolitno i neukrotivo od strane pojedinačnih regiona i država, postao je prostor koji nije imun na državnu jursdikciju, odnosno na nacionalne zakone i pravila ponašanja. Danas, internet više ne prepoznajemo kao nesagledivo i apsolutno neregulisano prostranstvo – iako postoje zone koje izmiču regulaciji – već kao biznis prostor, sastavljen od mnogobrojnih privatnih korporacija koje moraju poslovati ne samo legalno već i etički.

Regulisanje rada privatnih kompanija „na mreži" predmet je mnogobrojnih pravnih dokumenata, na regionalnom nivou, kao što je to slučaj sa EU, ali i na nacionalnom nivou, kao što će u nastavku ovog poglavlja biti detaljno prikazano. Uređenje države diktira odnos prema internet slobodama, u ovom radu posmatranih kroz slobodu izražavanja i pravo na privatnost internet korisnika. Na nekim od ranijih primera, pokazano je da autoritarne zemlje imaju tehničku mogućnost infrastrukturnog blokiranja pristupa pojedinim delovima veba ili pak čitavom vebu. Takođe, na ovim primerima demonstrirana je i mogućnost konstantnog neovlašćenog nadzora i sankcionisanja građana – internet korisnika. Dakle, tehničke mogućnosti za sprovođenje kontrole postoje. One su dostupne i demokratskim zemljama, ali bi njihova primena podrazumevala odstupanje od demokratskih načela, kao i izvesno nepoštovanje osnovnih ljudskih prava. Međutim, primeri demokratskih zemalja analiziranih u nastavku pokazaće da ni demokratsko uređenje ne garantuje apsolutnu zaštitu prava internet korisnika.

Oslanjajući se na izveštaje organizacije Fridom haus iz 2018. godine o internet slobodi, kao i na sekundarna istraživanja o zemljama koje će biti predmet analize, u ovom poglavlju razmatraju se razlike između različitih država u oblasti upravljanja internet prostorom. Izveštaji oraginizacije Fridom haus predstavljaju polaznu osnovu analize koja se nadograđuje pregledom radova u kojima je razmatrano stanje u određenim državama u kontekstu internet sloboda generalno, i odnosa država prema građanima – internet korisnicima, i njihovim onlajn-pravima.

Zemlje koje su odabrane za komparativnu perspektivu su sledeće: SAD, Nemačka, Francuska i Rusija. Ovakva selekcija izvršena je tako da uključi različite tipove informaciono-komunikacionih sistema sledeći klasifikaciju Halina i Manćinija (2004): SAD je predstavnik liberalnog modela, Nemačka demokratsko-korporativnog, a Francuska predstavlja mediteranski model. Rusija je zbog svog specifičnog uređenja odabrana kao zemlja za koju se može pretpostaviti da će se umnogome razlikovati od ponuđenih modela, te da će pružiti uvid u to kako se postsovjetske zemlje, koje još uvek nisu izgradile čvrste demokratske temelje, odnose prema internet slobodama.

Cilj ovakvog odabira jeste da ukaže na uticaj istorije i političkog uređenja na izgradnju različitih odnosa prema internet slobodama. U tom smislu, SAD je predstavnik liberalnog sistema u kojem je sloboda izražavanja neupitno i najznačajnije pravo, zagarantovano Prvim amandmanom, za koji se može pretpostaviti da će takve tendencije iskazati i kada je reč o slobodnom izražavanju na internetu. Takođe, pretpostavlja se da će odnos prema nadzoru i privatnosti biti specifičan u ovoj zemlji zbog događaja u skorijoj istoriji – sa jedne strane, zbog terorističkih napada i pitanja bezbednosti, i sa druge strane, zbog Snoudenovih otkrića i pitanja neovlašćenog nadzora.

Nemačka je istorijski osetljiva po pitanju nacističke propagande i teži sprečavanju govora mržnje po cenu ugrožavanja slobode izražavanja, što je opozit logici regulative u SAD. Pored ovoga, osnovana je pretpostavka da će se istorijski jaka uloga države odraziti na uređivanje onlajn-prostora kroz uspostavljanje jače regulacije, ali sa ciljem efikasnije komunikacije.

Francuska je takođe osetljiva na pitanja nacističke propagande, ali i istrajna u nameri da internet učini bezbednijim mestom – ponekad žrtvujući slobodu izražavanja i pravo na privatnost internet korisnika. Na uređenje onlajn-komunikacije u Francuskoj, koje pokazuje tendenciju ka jačoj regulativi, mogli bi uticati skoriji događaji koje su pokrenuli teroristički napadi od 2015. godine, te istorijski jaka uloga države i politički paralelizam.

Rusija, kao postsovjetska zemlja, autoritarnog tipa, pružiće uvid u to kako se pretežno nedemokratske zemlje odnose prema internet slobodama. Pretpostavka je da istorijski jaka uloga autoritarne države rezultira negativnim odnosom prema internet slobodama, a što se ogleda u kontroli, nadzoru, cenzuri i sankcijama.

Na osnovu analize različitih nacionalnih pristupa internet slobodama, u radu će biti predstavljena četiri ***modela državnog upravljanja internetom***. Ovi modeli ne pretenduju da budu važeći za sve zemlje sličnog tipa i uređenja, već je cilj da se ponude smernice za identifikaciju različitih modela upravljanja internetom.

Na kraju, kroz sagledavanje i evaluaciju postojećih praksi, u radu se apstrahuje novi, ideal-tipski model upravljanja internetom – ***model cirkularne odgovornosti***, kojim se koncept *odgovornosti* pozicionira kao centralni i najznačajniji. Varijacije ideal-tipskog modela biće definisane i prikazane u odnosu na to koji od aktera – država, privatni akteri ili korisnici – zauzima dominantnu poziciju pri upravljanju internet prostorom:

a) ***etatistički model upravljanja internetom*** – kada je država dominantni akter,

b) ***komercijalni model upravljanja internetom*** – kada su privatni akteri dominantni akteri, i

c) ***model apsolutne slobode / anarhični model*** – kada su korisnici dominantni akteri.

6.1. Liberalni model: Sjedinjenje Američke Države

Prema klasifikaciji Halina i Manćinija (2004), Sjedinjene Američke Države spadaju u liberalni model medijskog sistema. Liberalni model, prema ovim autorima, karakterišu srednji nivo cirkulacije štampe i rani razvoj masovne cirkulacije komercijalne štampe, koja je još u svom povoju bila namenjena masovnoj čitalačkoj publici, odnosno bila je komercijalne prirode. Okrenutost ka tržištu i potražnji, usađena još u začetku razvoja masovnih medija, kasnije je rezultirala slabim državnim intervencijama koje su do danas ostale zanemarljive. Sa druge strane, južnoevropska štampa, na primer, koja je u svom začetku bila usko usmerena, namenjena elitnoj publici, nije bila komercijalno isplativa, već se razvijala kao politička štampa, zavisna od partija i države.

Za liberalni model karakteristično je postojanje internog pluralizma u medijima koji podrazumeva pluralizam na strukturnom i sadržinskom nivou, odnosno karakterističan je za medije koji

teže da održe neutralnost u uređivačkoj politici i izveštavanju, te da izbegnu veze sa političkim grupama. U skladu sa tim, politički paralelizam u ovom modelu je nizak, što se odražava i na upravljanje radiodifuzijom – za nju je karakterističan profesionalni model upravljanja, odnosno emitovanje koje je izolovano od političkih uticaja i kontrole, vođeno medijskim profesionalcima. Novinare u ovom medijskom sistemu odlikuje izraženi profesionalizam – autonomija praćena poštovanjem profesionalnih standarda i etičkih normi (Hallin & Mancini, 2004: 198-248).

Amerika je „očigledno najčistiji primer liberalnog modela. […] Liberalne zemlje su, po definiciji, one u kojima je društvena uloga države relativno ograničena, a uloga tržišta i privatnog sektora relativno velika", ali, kako ističu Halin i Manćini, "uloga države ne može da se ignoriše" (Hallin & Mancini, 2004: 228), premda je ona znatno slabija nego u zemljama demokratsko-korporativnog i mediteranskog modela. Kada je reč o upravljanju internetom i odnosu prema internet slobodama, pretpostavljamo da će izrazito liberalni model upravljanja tradicionalnim komunikacionim sistemom imati uticaj i na onlajn-sferu, te da će Amerika i u odnosu prema internet komunikaciji imati dominatno liberalni stav.

U skladu sa liberalnom usmerenošću, upravljanje internetom u SAD pretežno se odvija kroz samoregulaciju – odnosno privatni sektor ima dominantnu poziciju u kreiranju politike upravljanja internetom u odnosu na javni sektor, dok vlada reaguje onda kada je potrebno regulisati sadržaj koji je opšteprihvaćen kao štetan.

Moglo bi se reći da je: „pisanje istorije interneta, na mnogo načina slično pisanju istorije američke mreže" (Wagner, 2016: 66). Liberalna priroda interneta, karakteristična pre svega za njegov začetak, umnogome je posledica njegovog nastajanja na tlu Amerike. Iako ni kao *američki proizvod* nije izbegao regulaciju, internet suštinski teži oslobađanju od svakog vida kontrolnih stega, pa se može pretpostaviti da će u mestu njegovog rođenja biti najbliži ostvarenju te težnje.

Prvi amandman je ono što američki medijski sistem najviše razlikuje od evropskih. Halin i Manćini pojašnjavaju da dok evropski pristup slobodi izražavanja podrazumeva uravnoteženost sa ostalim pravima, kao što je pravo na privatnost, zaštitu dostojanstva i slično, u Americi se ovom pravu pristupa gotovo apsolutistički, i u skladu sa takvim pristupom se sloboda izražavanja tretira kao najviši princip ostvarenja demokratije (Hallin & Mancini, 2004: 229). Prvim amandmanom slobodno izražavanje je još 1791. godine postavljeno na pijedestal: „Kongres ne može da donosi nikakav zakon o ustanovljenju državne religije, kao ni zakon koji zabranjuje slobodno ispovedanje vere, a ni zakon koji ograničava slobodu govora ili štampe ili pravo naroda na mirne zborove i na upućivanje peticije vladi za ispravljanje nepravdi" (Ustav SAD, Amandan 1.)[258].

Očekivano, pravo na gotovo apsolutno ostvarivanje slobode izražavanja u tradicionalnoj sferi odrazilo se i na onlajn-sferu. Najznačajniji događaj u tom kontekstu odnosi se na 1997. godinu, kada je Vrhovni sud u slučaju *Reno vs American Liberty Civic Union*[259] potvrdio da i onlajn-sloboda izražavanja uživa najviši nivo ustavne zaštite, odnosno da je zaštićena Prvim amandmanom.

[258] Ustav SAD na srpskom jeziku dostupan je na: http://www.prafak.ni.ac.rs/files/nast_mat/Ustav_SAD_sprski.pdf (pristupljeno 02. 03. 2019. godine).
[259] Detaljnije o slučaju na: https://supreme.justia.com/cases/federal/us/521/844/ (pristupljeno 02. 03. 2019. godine).

Prema izveštaju organizacije Fridom haus o slobodi na internetu 2018. godine, SAD spada u red slobodnih zemalja sa 22 od 100 negativnih poena (Izveštaj organizacije Fridom haus, 2018)[260]. Pri analizi internet sloboda Fridom haus kao identifikatore uključuje: *prepreke za pristup internetu, ograničavanje sadržaja* i *povrede prava korisnika*. Mogućnost pristupa internetu ocenjena je sa 4 od 25 negativnih poena, što pokazuje da je pristup internetu u Americi na zadovoljavajućem nivou. Naime, kritike u ovom delu izveštaja upućene su na račun i dalje visokih cena internet paketa u poređenju sa zemljama koje imaju isti nivo penetracije interneta, kao i na činjenicu da je starijim Amerikancima i onima koji žive u ruralnim sredinama pristup i upotrebljivost interneta delimično ograničen.

Kada je reč o ograničavanju povezivanja na internet, u Izveštaju se navodi da Amerikanci gotovo da nemaju problem sa restrikcijama vlade kojima bi se korisnicima uskratio pristup sadržaju na internetu. Takođe, „Sjedinjene Države imaju brojne tačke povezivanja , što bi gotovo onemogućilo isključivanje cele zemlje sa interneta" (Izveštaj organizacije Fridom haus, 2018).

Međutim, SAD ima zakonski predviđenu mogućnost ometanja internet konekcije. Reč je o protokolu poznatijem kao Standardni operativni postupak (SOP) 303, koji je ustanovljen 2006. godine nakon terorističkog napada na metro u Londonu. SOP 303 predviđa restriktivne mere u slučaju „nacionalne krize" ali, „šta predstavlja 'nacionalnu krizu' i koje zaštitne mere postoje protiv zloupotrebe ostaju u velikoj meri nepoznate , budući da puna dokumentacija SOP 303 nikada nije bila objavljena javno" (Izveštaj organizacije Fridom haus, 2018).

Kada je reč o regulatornim telima, ne postoji telo koje reguliše internet u Americi. Federalna komisija za komunikacije (FKK) zadužena je za brojna pitanja povezena sa internetom, međutim, ukidanje net neutralnosti, decembra 2017. godine, smanjilo je mogućnost FKK da upravlja pitanjima u vezi sa internetom (Izveštaj organizacije Fridom haus, 2018).

Kada je reč o *ograničavanju sadržaja:* „Generalno, vlada SAD ne primorava internet servis provajdere ili hostove sadržaja da blokiraju ili filtriraju sadržaj na mreži" (Izveštaj organizacije Fridom haus, 2018). Međutim, zakon kojim se predviđa uklanjanje štetnog sadržaja na mreži, usvojen marta 2018. godine, kritikovan je zbog povećanja odgovornosti internet servisa za ilegalni sadržaj. Reč je o zakonu koji se odnosi na sprečavanje seksualnog iskorišćavanja i trgovine ljudima onlajn, poznatijeg kao SESTA/FOSTA[261]. Prema ovom zakonu, legalnu odgovornost imaju internet servisi koji: „promovišu ili olakšaju prostituciju pet ili više osoba, ili […] postupaju nepromišljeno zanemarivajući ponašanje koje doprinosi seksualnoj trgovini" (Izveštaj organizacije Fridom haus, 2018). Do usvajanja ovog zakona, prema Zakonu o pristojnoj komunikaciji, takvi internet servisi nisu bili zakonski odgovorni za sadržaj ukoliko nisu obavešteni da se on nalazi na njihovom servisu. Ovakav vid pooštravanja odgovornosti dovodi do preventivnog uklanjanja sadržaja, što vodi autocenzuri i odražava se na slobodu izražavanja onlajn, smatraju kritičari ovog zakona. I zaista, u izveštaju organizacije Fridom haus navode se primeri autocenzure, koji su nastupili ubrzo nakon usvajanja FOSTA.

[260] Izveštaj organizacije Fridom haus za Ameriku dostupan je na: https://freedomhouse.org/report/freedom-net/2018/united-states (pristupljeno 02. 03. 2019. godine).
[261] Originalni naziv zakona - „Allow States and Victims to Fight Online Sex Trafficking Act of 2017", poznat i kao: SESTA/FOSTA.

Kongres je usvajanjem ovog zakona cenzurisao internet, smatra Harmon i dodaje da ućutkivanje internet korisnika ne čini internet sigurnijim mestom (Harmon, 2018)[262]. Sa druge strane, usvajanje ovog zakona dovodi u pitanje član 230 Zakona o pristojnosti u komunikaciji, a on je, kako se navodi na stranici *Electronic Frontier Foundation*: „najznačajniji akt koji zakonski štiti slobodu govora na internetu"[263]. Naime, u članu 230 navodi se da nijedan provajder niti korisnik neće biti odgovoran za informacije, to jest za sadržaj koji obezbeđuje neki drugi provajder informacija. Odnosno:

> „Onlajn posrednici koji hostuju ili objavljuju govor zaštićeni su od niza zakona koji bi se inače mogli koristiti da bi se zakonski smatrali odgovornim za ono što drugi kažu i rade. Zaštićeni posrednici uključuju ne samo internet servis provajdere (ISP), već i čitav niz 'pružalaca usluga interaktivnih računara', uključujući u osnovi bilo koju onlajn-uslugu koja objavljuje sadržaj trećih strana" (*Electronic Frontier Foundation*)[264].

Iako su se internet libertarijanci isprva protivili Zakonu o pristojnosti komunikacije, njegov član 230 postaje osnova za odbranu interneta od cenzure. Upravo zbog ovoga je novousvojeni zakon FOSTA toliko kritikovan – on otvara prostor za autocenturu, zbog straha od pravnih sankcija. FOSTA je, moglo bi se reći, atipičan zakon za liberalni pristup internetu i slobodi izražavanja onlajn, koje Amerika slavi. Zbog toga je i vredan pomena, kao primer promene kursa, ka „ne-američkom" poimanju ograničavanja slobode izražavanja na internetu.

Kada govorimo o raznovrsnosti i manipulaciji sadržajem na internetu, Fridom haus u izveštaju ističe da je onlajn medijsko okruženje u Americi raznoliko, ali da se poslednjih godina uviđaju prakse širenja dezinformacija i dominacija partijskih medija (Izveštaj organizacije Fridom haus, 2018). Debate o širenju dezinformacija, odnosno lažnih vesti na internetu, te njihov uticaj na političke odluke, obeležile su predsedničke izbore 2016. godine, ali su imale uticaj i u godinama koje su usledile. Godinu dana kasnije, 2017. godine, čelnici najuticajnijih društvenih mreža pozvani su da svedoče pred Kongresom zbog sumnji da su dezinformacije fabrikovane u Rusiji imale uticaj na političke izbore 2016. godine. Čelnici su potvrdili prisustvo takvog sadržaja na mreži, mada ostaje nejasno da li su i koliki uticaj takve dezinformacije imale na konačni ishod izbora. Sa druge strane, društvene mreže, kojima se širio ovakav sadržaj, preduzele su određene mere kako bi utvrdile njihovo poreklo i sprečile dalju diseminaciju lažnih vesti. Međutim, društvene mreže ostale su prostor koji pogoduje korisnicima u širenju neuravnoteženih informacija, navodi se u izveštaju (Izveštaj organizacije Fridom haus, 2018).

Sa druge strane, pretnje po slobodno izražavanje ne dolaze samo iz inostranstva. Predsednica upravnog odbora Komiteta za zaštitu novinara (KZN), Sandra Mims Rou (Sandra Mims Rowe) optužila je predsednika Trampa za gušenje slobode štampe:

> „Donald Tramp, kroz svoje reči i postupke kao kandidat za predsednika Sjedinjenih Država, konstantno izdaje vrednosti Prvog amandmana. Odbor direktora KZN-a je 6. oktobra usvojio rezoluciju kojom se Tramp proglašava neviđenom pretnjom pravima novinara i sposobnosti KZN-a da se zalaže za slobodu medija širom sveta. […] Tokom svoje kampanje, Tramp je rutinski donosio nejasne predloge kako bi ograničio osnovne

[262] Elliot Harmon (March 21, 2018). How Congress Censored the Internet. Electronic Frontier Foundation. Dostupno na: https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet (pristupljeno: 02. 03. 2019. godine).
[263] Electronic Frontier Foundation. CDA 230. *The Most Important Law Protecting Internet Speech*. Dostupno na: https://www.eff.org/issues/cda230 (pristupljeno: 02. 03. 2019. godine).
[264] Ibid.

elemente slobode štampe i slobode interneta. […] Iz tog razloga, KZN sada preduzima korak bez presedana. Ovde nije reč o izboru strane na izborima. Već o prepoznavanju da Trampovo predsedavanje predstavlja pretnju slobodi štampe kakva nije viđena u modernoj istoriji" (Committee to Protect Journalists, 2016)[265].

Ove negativne prakse predsednika Trampa nastavljene su i u narednim godinama. Pored ograničavanja slobode štampe, Tramp je jasno pokazao pretenzije i ka upravljanju onlajn-sferom. Naime, savezni sudija je za Trampov postupak na Tviteru gde je blokirao korisnike koji ga kritikuju smatrao da je protivustavan, te da krši Prvi amandman, te da krši Prvi amandman. Tviter je u ovom kontekstu prepoznat kao onlajn-forum za razmenu mišljenja, a blokiranjem korisnika Tramp građanima direktno uskraćuje učešće u javnoj debati i ugrožava slobodu izražavanja (Herrman&Savage, 2018)[266].

Fridom haus dodelio je 14 od 40 negativnih poena za narušavanje prava korisnika u Americi. Ovaj identifikator procenjivan je na osnovu: *pravnog okruženja*, *krivičnih gonjenja internet aktivista*, *nadzora*, *privatnosti i anonimnosti*, *zastrašivanja i nasilja* i *tehničkih (sjaber) napada*.

Zakon o kompjuterskim prevarama i zloupotrebama (*Computer Fraud and Abuse Act – CFAA*) iz 1986. godine, kojim se predviđa da niko nema pravo na pristup kompjuteru bez odobrenja u okviru CFAA, kritikovan je zbog ostavljenog prostora sudovima da sami interpetiraju šta se podrazumeva pod terminom „bez odobrenja" (Izveštaj organizacije Fridom haus, 2018). Primena ovog spornog zakona dovela je 2011. godine do samoubistva internet aktiviste Arona Švarca (Aaron Swartz), koji je protivno CFAA preuzeo milione datoteka akademskih članaka. Zbog kazne, koja je mogla dostići i 35 godina zatvora, Švarc je izvršio samoubistvo i nije dočekao suđenje (Izveštaj organizacije Fridom haus, 2018).

Nakon Švarcove smrti, pokrenuta je inicijativa za usvajanje „Aronovog zakona", odnosno izmene postojećeg CFAA. Reforma zakona bi, između ostalog, ukinula zatvorske kazne za kršenje uslova korišćenja, štitila istraživače, inovatore, prilagodila kaznu zločinu itd[267]. Predlog izmene zakona nije dobio dovoljnu podršku, te nije usvojen.

Sa druge strane, retki su slučajevi krivičnog gonjenja onlajn-aktivista, prvenstveno zbog zaštite koju im pruža Prvi amandman. Slučajevi koji su u periodu pisanja Izveštaja privukli pažnju javnosti jesu privođenje Kristofera Danijelsa (Christopher Daniels)[268] zbog navodnog pozivanja na nasilje nad policijom putem Fejsbuka i privođenje novinara, Manuela Djurana (Manuel Duran)[269] zbog izveštavanja o protestu migranata. Obe optužbe su odbačene nakon saslušanja (Izveštaj organizacije Fridom haus, 2018).

---

[265] Committee to Protect Journalists. (October 13, 2016). *CPJ chairman says Trump is threat to press freedom*. Dostupno na: https://cpj.org/2016/10/cpj-chairman-says-trump-is-threat-to-press-freedom.php (pristupljeno: 02. 03. 2019. godine).

[266] Herrman J. and Savage C. (May 23, 2018). *Trump's Blocking of Twitter Users Is Unconstitutional, Judge Says*. The New York Times. Dostupno na: https://www.nytimes.com/2018/05/23/business/media/trump-twitter-block.html (pristupljeno 02. 03. 2019. godine).

[267] Electronic Frointer Fondation. *Computer Fraud And Abuse Act Reform*. Dostupno na: https://www.eff.org/issues/cfaa (pristupljeno: 03. 03. 2019. godine).

[268] Više o slučaju: Martin de Bourmont. (January 30, 2018). Is a Court Case in Texas the First Prosecution of a 'Black Identity Extremist'?. *Foreign Policy*. https://foreignpolicy.com/2018/01/30/is-a-court-case-in-texas-the-first-prosecution-of-a-black-identity-extremist/ (pristupljeno: 03. 03. 2019. godine).

[269] Više o slučaju: US Press Freedom Tracker. (April 5, 2018). Journalist Manuel Duran, arrested while covering immigration protest, could be deported by ICE. https://pressfreedomtracker.us/all-incidents/journalist-manuel-duran-arrested-while-covering-immigration-protest-could-be-deported-ice/ (pristupljeno 03. 03. 2019. godine).

Kada je reč o nadzoru i privatnosti korisnika interneta u Americi, proteklih godina usvojeni su zakoni koji mogu negativno da utiču na prava korisnika. Naime, korisnički podaci američkih građana zaštićeni su članom 5 Zakona o Federalnoj trgovinskoj komisiji (*Federal Trade Commission Act – FTCA*)[270], kojim se zabranjuje obmana korisnika u pogledu korišćenja njihovih podataka. Takođe, član 222 Zakona o telekomunikacija (*Telecommuniciations Act*)[271] propisuje da telekomunikacioni operateri ne smeju da dele podatke korisnika bez njihove saglasnosti.

Reafirmisanje odeljka 702, čime se Zakonom o nadzoru u inostranstvu (*Foreign Intelligence Surveillance Act* – FISA) omogućava nadzor i sakupljanje metapodataka građana SAD do 2024. godine, jedan je od akata , kojima se dovodi u pitanje zaštita podataka korisnika i pokreće pitanje nadzora. Takođe, Akt o pojašnjenju zakonitog korišćenja podataka u inostranstvu (*Clarifying Lawful Overseas Use of Data Act* – CLOUD), usvojen marta 2018, proširuje ovlašćenje pravosudnim organima, kada je reč o pristupu podacima internet korisnika (Izveštaj organizacije Fridom haus, 2018).

Uopšteno, nadzor i ograničavanje privatnosti građana SAD obuhvaćeni su *Patriotskim aktom*, zakonom koji je stupio na snagu nakon terorističkog napada na zgrade bliznakinje, 2001. godine (Izveštaj organizacije Fridom haus, 2018). Osnovni cilj ovog zakona jeste: „Očuvanje života i slobode: Ujedinjavanje i jačanje Amerike pružanjem odgovarajućih sredstava potrebnih za presretanje i ometanje terorizma"[272]. Odnosno, ovaj akt predviđa ograničavanje privatnosti građana Amerike u zamenu za bezbednost, odnosno borbu protiv terorizma. Ovako široko postavljena ovlašćenja mogu lako dovesti i do zloupotrebe u primeni zakona, što se ispostavilo kao istinito nakon Snoudenovog otkrića o masovnom nadzoru građana Amerike od strane NSA[273]. Patriotski akt je, između ostalog, predviđao primenu programa PRISM, kojim su građani Amerike bili masovno praćeni od strane njihove Vlade.

Barak Obama je 2015. godine, sa namerom da revidira sporne odeljke Patriotskog akta, potpisao *Akt Slobode*. Izmena, koja se može tumačiti kao pozitivni pomak, jeste ukidanje mogućnosti nadzora elektronske komunikacije građana bez naloga. Naime, novi Akt predviđa da praćenje i nadzor telefonskih poziva i elektronske komunikacije građana Amerike nije zakonito bez „osnovane sumnje" da imaju veze sa terorizmom, što se dokazuje pred FISA sudom. Međutim, FISA sud je u poslednjih tridesetak godina skoro stoprocentno odobravao ovakve zahteve, te je pitanje koliko će efikasno štiti privatnost Amerikanaca (Kapocsi, 2018)[274].

U Izveštaju se dakle jasno dovodi u sumnju namera američke Vlade kada je reč o nadzoru građana, ali i o pohranjivanju njihovih ličnih podataka:

> „Pod okriljem seta složenih zakona, američke agencije za sprovođenje zakona i obaveštajne službe mogu da prate sadržaj i zapise komunikacije, ili metapodatke, pod

[270] *Article 5 Federal Trade Commission Act:* https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf (pristupljeno 02. 03. 2019. godine).
[271] *Section 222 Telecommunications Act:* https://www.law.cornell.edu/uscode/text/47/222 (pristupljeno 02. 03. 2019. godine).
[272] The USA PATRIOT Act, dostupno na: https://www.justice.gov/archive/ll/highlights.htm (pristupljeno 03. 03. 2019. godine).
[273] Glenn Greenwald. (Jun 6 2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Dostupno na: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (pristupljeno 03. 03. 2019. godine).
[274] Cody Kapocsi. (September 14 2018). What is the USA FREEDOM Act? What's So Free About It?. *Cloudwards.* Dostupno na: https://www.cloudwards.net/freedom-act/ (pristupljeno 03. 03. 2019. godine).

različitim stepenima nadzora kao deo krivičnih ili nacionalnih bezbednosnih istraga. Vlada može da zahteva da kompanije pohranjuju takve podatke do 180 dana u skladu sa Zakonom o pohranjenim komunikacijama, ali kako će oni prikupljati i čuvati komunikacijski sadržaj i zapise razlikuje se od kompanije do kompanije" (Izveštaj organizacije Fridom haus, 2018).

Zakon CLOUD, kojim se reguliše prekomorsko deljenje podataka, usvojen marta 2018. godine, proširio je mogućnosti odavanja podataka korisnika od strane privatnih kompanija i kada oni nisu pohranjeni na teritoriji SAD, dok se prethodni zakon o pohranjivanju podatka odnosio samo na podatke pohranjene u Americi. Kritičari ovog zakona smatraju da je njegovo usvajanje samo još jedan način da se kompanije primoraju da predaju podatke svojih korisnika (Izveštaj organizacije Fridom haus, 2018).

Zanimljivo je da je policija u SAD 2016. godine sprovodila nadzor društvenih mreža, odnosno korisnika koje je sumnjičila za kriminalne aktivnosti sa namerom praćenja komunikacije na društvenim mrežama, koristeći alat *Geofeedia*. Nakon saznanja o tome, Fejsbuk, Tviter i Instagram blokirali su pristup ove aplikacije njihovim podacima (Izveštaj organizacije Fridom haus, 2018).

Takođe, Izveštajem se ističu i pokušaji Vlade da se uvede Zakon o enkripciji, kojim bi se organima reda olakšalo dešifrovanje poruka korisnika onda kada Vlada ima osnovanu sumnju da su korisnici povezani sa nekim kriminalnim delom. Međutim, ovakav zakon nije usvojen, dok postojeći zakon *Communications Assistance for Law Enforcement Act* – CALEA predviđa da operateri dizajniraju svoje usluge tako da vladinim organima olakšaju presretanje komunikacija onda kada to zakon predviđa (Izveštaj organizacije Fridom haus, 2018).

***

Trend regulacije internet prostora nije zaobišao ni kolevku slobodnog internet prostora – Ameriku. SAD su zadržale liberalni odnos prema internet komunikacijama, s tim što je primetan napor da se komunikacijama na internetu u većoj meri upravlja. Kao najznačajniji događaji u 2018. godini, koji se tiču internet sloboda u Americi, u izveštaju organizacije Fridom haus ističu se:

- ukidanje pravila o net neutralnosti decembra 2017. godine;
- širenje štetnih sadržaja i lažnih vesti;
- usvajanje zakona o onlajn-trgovini ljudima u seksualne svrhe, koji je povećao odgovornost intermedijatora;
- svedočenja direktora Fejsbuka, Jutjuba i Tvitera pred Kongresom u vezi sa uticajem Rusije na izbore u Americi (oktobar 2017. godine);
- svedočenje Marka Zakerberga u vezi sa „Kembridž Analitika aferom";
- ponovno odobrenje amandmana, uključujući i odeljak 702, kojima se zakonom o nadzoru u inostranstvu (*Foreign Intelligence Surveillance Act* – FISA) omogućava nadzor i skupljanje metapodataka Amerikanaca;

- usvajanje Akta o pojašnjenju zakonitog korišćenja podataka u inostranstvu (*Clarifying Lawful Overseas Use of Data Act* – CLOUD), marta 2018. godine, kojim se proširuju mogućnosti pristupa korisničkim podacima od strane pravosudnih organa.

Većina navedenih akata ide u prilog ograničavanju prava na privatnost, odnosno, povećanju nadzora građana Amerike. Premda bi trebalo istaći da je u osnovi svih akata zapravo povećanje bezbednosti onlajn-komunikacije i antiteroristička strategija.

Nesumnjivo je da je borba protiv terorizma imala udela u gotovo svim novousvojenim ili reafirmisanim zakonskim merama, pa bismo mogli da zaključimo da je odnos Amerike prema internet komunikaciji u značajnoj meri izgrađen pod uticajem terorističkih pretnji ili skorašnjih događaja. Sa druge strane, saslušanjima čelnika tehnoloških giganata u vezi sa narušavanjem prava na zaštitu ličnih podataka i uticajem lažnih vesti na izbore u Americi, američka vlada pozvala je na odgovornost i privatne kompanije, čime je potvrdila da je u oblasti upravljanja internetom uloga države nekada dominantna i neopodna, koliko god sistem bio libaralan.

6.2. Evropske zemlje razvijene demokratije – demokratsko korporativni model: Nemačka

Medijski sistem Savezne Republike Nemačke, prema klasifikaciji Halina i Manćinija (2004), spada u demokratsko-korporativne medijske sisteme. Ovaj model karakterističan je za zemlje centralne i severne Evrope (Austrija, Belgija, Švedska, Finska) i odlikuje ga visoka stopa cirkulacije štampe, eksterni pluralizam u medijima, pod kojim se podrazumeva postojanje suživota medija različitih usmerenja i uređivačkih politika. Radiodifuzija uključuje politiku, odnosno političke okolnosti imaju uticaj na radiodifuziju, ali ima i značajnu autonomiju. Takođe, prisutan je visok stepen profesionalizma medijskih radnika, što u krajnjem i doprinosi pozitivnom odnosu prema slobodi medija. Jaka uloga države karakteristična je za ovaj model, ali ona, za razliku od mediteranskog modela, pospešuje slobodu štampe. Odnosno, državna intervencija i regulacija uglavnom su usmerene ka obezbeđivanju pluralizma, fer tržišta, zaštiti prava i slično (Hallin & Mancini, 2004: 143-197). Ovaj okvir značajan je za analizu odnosa prema internet komunikaciji, jer se može pretpostaviti da će on imati uticaj i na odnos prema internet slobodama.

Da bi se razumeo generalni odnos Republike Nemačke prema pravu na slobodno izražavanje, neophodno je uzeti u obzir i istorijski kontekst. Naime, nakon neslavne nacističke istorije, Republika Nemačka, posebno osetljiva na pitanja manjina i govor mržnje, poštovanje ljudskog dostojanstva ističe kao najznačajnije pravo i polaznu osnovu za poštovanje svih ostalih ljudskih prava. Ljudsko dostojanstvo je zagarantovano članom 1 Ustava Republike Nemačke[275] i definisano kao nepovredivo pravo.

U skladu sa navedenim, može se pretpostaviti da će jaka uloga države i regulacija biti primetne, te da će borba protiv govora mržnje i isticanje nepovredivosti ljudskog odstojanstva biti značajni elementi u izgradnji odnosa prema internet komunikaciji, ali da će internet sloboda ipak biti u najvećoj

[275] Ustav Republike Nemačke dostupan je na: https://www.btg-bestellservice.de/pdf/80201000.pdf (pristupljeno: 01. 02. 2019. godine).

meri ostvarena. U prilog tome govori i izveštaj organizacije Fridom haus iz 2018. godine, koji Nemačku pozicionira u red zemalja koje karakteriše slobodan internet prostor (Izveštaj organizacije Fridom haus, 2018)[276]. Nemačka je dobila 19 od 100 negativnih poena, što je, prema Izveštaju, čini najslobodnijom od ostalih zemalja analiziranih u ovom poglavlju.

Da bi se razumeo kontekst u kojem se razvijala politika u vezi sa komunikacijom na internetu u Nemačkoj, najpre se mora pojasniti njeno državno uređenje. Naime, Savezna Federativna Republika Nemačka sastoji se od 16 saveznih država i svaka od njih ima izraženu autonomiju. Nakon Drugog svetskog rata, komunikaciona politika Nemačke razvijala se u pravcu decentralizovanog regulatornog okvira, odnosno postoji suživot brojnih regulatornih tela na nivou federacije, ali i pojedinačnih nemačkih država. Takav okvir značajnim delom osmišljen je zbog bojazni da bi mediji, i uopšte sredstava masovne komunikacije i informisanja, mogli ponovo da postanu predmet zloupotrebe od strane države, te da ponovo budu propagandno (zlo)upotrebljeni (Wagner, 2014; 2016).

Kako Vagner (Wagner, 2014; 2016) navodi, sličan model pratio je krajem osamdesetih godina razvoj privatnih medija, a kasnije i regulisanje internet prostora. Autor ističe izraženu borbu između federalne vlade i saveznih država za prevlast nad regulisanjem interneta još u njegovom povoju, devedesetih godina. Međutim, kada je federalna vlada izuzela pitanje regulacije internet sadržaja iz Telekomunikacijskog akta 1996. godine, savezne države dobile su zeleno svetlo za autonomno regulisanje ove oblasti. U skladu sa tim, u godinama koje su usledile oformljena su mnogobrojna tela za (samo)regulaciju neželjenog onlajn-sadržaja[277], sa različitim uticajem, ali i poimanjem regulisanja i neželjenog sadržaja. Upravo zbog toga, Vagner režim regulisanja interneta u Nemačkoj naziva "krpežom" (2014: 64).

Poslednji akt u nizu, koji izaziva velike kontroverze, kada je reč o internet slobodi u Nemačkoj, jeste zakon o društvenim mrežama – *Network Enforcement Act* (nem. *Netzdurchsetzunggesetz*, skraćeno NetzDG)[278], čija je inicijalna svrha borba protiv govora mržnje i lažnih vesti na društvenim mrežama. Naime, nemački Budenstag je 30. juna 2017. godine usvojio NetzDG, kojim se bliže uređuje poslovanje društvenih mreža koje svoje usluge pružaju na teritoriji Republike Nemačke. Ovaj Zakon stupio je na snagu 1. oktobra 2017. godine, a primenjuje se na: "provajdere telemedijskih usluga koji, u profitne svrhe, obezbeđuju internet platforme koje su dizajnirane da omoguće korisnicima da dele bilo kakav sadržaj sa drugim korisnicima ili da takav sadržaj učine dostupnim javnosti (društvene mreže)" (NetzDG, član 1(1)).

NetzDG isključuje provajdere onlajn-medija i platforme namenjene ličnoj komunikaciji korisnika, kao što su mejlovi ili privatne onlajn-poruke. Takođe, ne odnosi se na društvene mreže koje imaju manje od dva miliona korisnika registrovanih na teritoriji Nemačke. S obzirom na to da, prema internet statistici[279], oko 30 miliona Nemaca ima profil na društvenoj mreži Fejsbuk, NetzDG primenjuje se na Fejsbuk, ali i na Jutjub, Tviter itd.

[276] Izveštaj organizacije Fridom haus „Internet sloboda 2018" za Nemačku dostupan je na: https://freedomhouse.org/report/freedom-net/2018/germany (pristupljeno 01. 02. 2019. godine).
[277] Najznačajnija samoregulatorna tela koja se bave neželjenim sadržajem na interentu u Nemačkoj jesu: *Jugendschutz.Net, German Internet Industry Association ('eco'), Internet Content Task Force (ICTF), Internet hotline for memebers ISPs* (Wagner, 2014: 63-67).
[278] NetzDG dostupan na: https://germanlawarchive.iuscomp.org/?p=1245 (pristupljeno 02. 02. 2019. godine).
[279] *Internet World Stats*, dostupno na: https://www.internetworldstats.com/stats4.htm (pristupljeno 02. 02. 2019. godine).

NetzDG propisuje da je društvena mreža koja primi više od 100 pritužbi u toku jedne godine obavezna da napiše izveštaj koji će objaviti u *Federalnoj Gazeti* i na svom sajtu, početnoj stranici, najkasnije mesec dana nakon isteka perioda od pola godine. Izveštaj bi trebalo da sadrži, između ostalog, detaljan opis kako se društvena mreža nosi sa pritužbama, detaljno pojašnjenje mehanizama kojima se služi kako bi odgovorila na pritužbe i ispitala prijavljene slučajeve, broj pritužbi koje je dobila, njihov opis i razrešenje, spisak stručnjaka koji su zaduženi za analizu pritužbi itd (NetzDG, član 1(2)).

Stavom 3, prvog člana NetzDG, društvenim mrežama nalaže se sledeće: 1) da obezbede korisnicima jednostavan, lako uočljiv i transparentan način prijavljivanja nezakonitog sadržaja; 2) uklanjanje evidentno nezakonitog sadržaja u roku od 24 časa od trenutka prijavljivanja, odnosno u periodu od sedam dana ukoliko je potrebna dodatna istraga – period od sedam dana može da se produži jedino ukoliko društvena mreža angažuje spoljnu agenciju, koja bi se bavila određenom prijavom, a koja bi bila prepoznata kao *Agencija za regulisanu samoregulaciju*.

Članom 4 društvenim mrežama nalaže se da imenuju domaćeg agenta, odnosno da ovlaste osobu na teritoriji Republike Nemačke koja će biti odgovorna za sprovođenje mera koje NetzDG predviđa. Ukoliko se o ovaj stav ogluše ili ne reaguju na prijave, kazna za individualnu odgovornost može dostići i 5 miliona evra, a za provajdere društvenih mreža kazne mogu biti i do 50 miliona evra (Gesely, 2017)[280].

Usvajanje NetzDG izazvalo je oprečna mišljenja stručne javnosti. Tvorek (Tworek, 2017) ovaj potez Nemačke prepoznaje kao najodlučniju akciju koju je jedna demokratska zemlja preduzela u borbi protiv nelegalnog sadržaja na društvenim mrežama, ali istovremeno smatra da je posredi i nešto više. O usvajanju NetzDG-a Tvorek piše:

> „Njegova glavna meta su američki tehnološki giganti, provajderi glavnih društvenih mreža u Nemačkoj. Sukob između američkih društvenih mreža i nemačke vlade je više od brisanja onlajn-komentara mržnje. To je borba o tome koliko slobode govora demokratija može da podnese" (Tworek, 2017).[281]

NetzDG poznat je i kao *Zakon o Fejsbuku*. U stručnim debatama zaista jeste primetna dominacija tema kojima se ovaj vid regulacije dovodi, pre svega, u vezu sa Fejsbukom. Čelnici Fejsbuka usvajanje i primenu ovog Zakona ocenjuju negativno i smatraju da propisi NetzDG nisu u skladu sa Ustavom Nemačke, kao i da nisu u saglasnosti sa zakonima Evropske unije. Njihove kritike usmerene su i ka restriktivnim merama koje ovaj Zakon predviđa. Naime, kako čelnici Fejsbuka smatraju, Zakon može imati negativan uticaj na slobodu izražavanja, jer postoji mogućnost da provajderi društvenih mreža uklanjaju sadržaj za koji nisu sigurni, ili nisu u potpunosti sigurni da je ilegalan prema NetzDG, kako bi izbegli ogromne finansijske kazne (do 50 miliona evra). Takođe, ovaj vid regulisanja ilegalnog sadržaja na društvenim mrežama iz Fejsbuka ocenjuju kao prebacivanje

[280] Jenny Gesley (July 11, 2017). Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act". *The Law Library of Congress*. Dostupno na: http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/ (pristupljeno 03. 02. 2019. godine).

[281] Heidi Towerk (May 16, 2017). How Germany Is Tackling Hate Speech. *Foreign Affairs*. Dostupno na: https://www.foreignaffairs.com/articles/germany/2017-05-16/how-germany-tackling-hate-speech (pristupljeno 03. 02. 2019. godine).

odgovornosti za kompleksna pravna pitanja sa javnih vlasti na privatne aktere (Shead, 2017)[282]. Kada je reč o građanima Nemačke, dve trećine njih smatra usvajanje NetzDG opravdanim, dok 26% Nemaca veruje da ove mere mogu imati negativni uticaj na slobodu izražavanja (Inhoffen, 2017)[283].

U ovom trenutku prepoznaje se napor Nemačke da se i u onlajn-komunikaciji izbori za poštovanje dostojanstva i anulira govor mržnje: „Zakon o Fejsbuku je pokušaj da se vidi da li ljudsko dostojanstvo može da preživi internet – a njegov uspeh ili neuspeh mogao bi vrlo dobro za ostatak sveta da odredi šta znači biti čovek, i biti onlajn" (Kinstler, 2017)[284].

Pored sprečavanja govora mržnje, jedan od razloga usvajanja NetzDG bila je i borba sa lažnim vestima na društvenim mrežama i njhovim uticajem na političke izbore. O tome da li su društvene mreže, odnosno lažne vesti i automatizovani botovi imali uticaj na federalne izbore u Nemačkoj, septembra 2017. godine, postoje različita mišljenja (Kinstler, 2017). Politički eksperti i zvaničnici vlade tvrde da su ti uticaji bili mali i nisu mogli da budu presudni za krajnji ishod izbora (Shalal &Auchard, 2017). U izveštaju je navedeno: „eksperti su zaključili da nijedna dezinformativna kampanja nije imala vidljiv uticaj na izborne rezultate" (Izveštaj organizacije Fridom haus, 2018).

Takođe, Zakerberg se oglasio tim povodom u toku trajanja izbora i otkrio da aktivno učestvuje u sprečavanju uticaja na izbore u Nemačkoj:

> „Mi radimo na obezbeđivanju integriteta nemačkih izbora ovog vikenda, od preduzimanja akcija protiv hiljada lažnih naloga do partnerstva sa javnim vlastima kao što je Savezna kancelarija za bezbednost informacija, i do deljenja bezbednosnih praksi sa kandidatima i strankama" (Zuckerberg, 2017)[285].

Sa druge strane, istraživanje ProPublike (*ProPublica*) pokazuje da je Fejsbuk ostao nem na brojne prijave protiv političkih oglasa koji su bili usmereni protiv Zelene partije, a čijem poreklu nije moglo da se uđe u trag (Dodt, Larson & Angwin, 2018)[286].

Uslovi koji se NetzDG propisuju nisu novina u nemačkom zakonodavstvu, i mogu se tumačiti kao apsolutni sklad sa nemačkim stavom i ustavnim propisima o slobodi izražavanja, naročito sa Krivičnim zakonikom. Sa druge strane:

---

[282] Shead, S. (May 30, 2017). Facebook said Germany's plan to tackle fake news would make social media companies delete legal content. *Business Insider*. Dostupno na: https://www.businessinsider.com/facebook-says-germany-fake-news-plans-comply-with-eu-law-2017-5?r=UK&IR=T (pristupljeno: 02. 02. 2019. godine).

[283] Istraživanje *YouGov*-a, sprovedeno je na reprezentativnom uzorku 1036 građana Nemačke, od 7. do 11. aprila 2017. godine. Dostupno na: https://yougov.de/news/2017/04/15/mehrheit-der-deutschen-findet-gesetzentwurf-gegen-/ (pristupljeno 01. 02. 2019. godine).

[284] Kinstler, L. (Nov 2, 2017). Can Germany Fix Facebook? *The Atlantic*. Dostupno na: https://www.theatlantic.com/international/archive/2017/11/germany-facebook/543258/ (pristupljeno: 02. 02. 2019. godine).

[285] Link ka objavi Marka Zakerberga: https://www.facebook.com/zuck/posts/10104052907253171 (pristupljeno 02. 02. 2019. godine).

[286] Dodt, S., Larson, J. & Angwin, J. (Oct. 18, 2017). Facebook Allowed Questionable Ads in German Election Despite Warnings. *ProPublica*. Dostupno na: https://www.propublica.org/article/facebook-allowed-questionable-ads-in-german-election-despite-warnings?utm_source=pardot&utm_medium=email&utm_campaign=dailynewsletter (pristupljeno 02. 02. 2019. godine).

„Ono što je jasno vidljivo u NetzDG je, međutim, da velike društvene mreže moraju biti u skladu sa nemačkim zakonom. Očigledna spremnost velikih kompanija društvenih mreža da prihvate premisu da moraju da poštuju nacionalno zakonodavstvo (a ne samo standarde društvenih mreža) trebalo bi da se računa kao velika koncesija" (Jayakumar, 2018)[287].

Drugim rečima, da bi kompanija Fejsbuk, ili neka druga društvena mreža, mogla da posluje na teritorije Nemačke, ona mora da poštuje nacionalni zakonodavni okvir, u suprotnom joj prete ogromne finansijske sankcije. Fejsbuk, kao nacionalno fleksibilan, uskladio je svoje uslove korišćenja sa novim zakonom, NetzDG. Shodno tome, uslovi korišćenja Fejsbuka u Nemačkoj drugačiji su od uslova korišćenja u drugim zemljama EU. Za korisnike Fejsbuka u Nemačkoj postoji posebna stranica *Centar za pomoć za NetzDG* namenjena upoznavanju sa novim zakonom i njegovom primenom (Slika__). To je ujedno i prva stavka u okviru uslova korišćenja Fejsbuka u Nemačkoj.

Slika 4 Primena NetzDG na Fejsbuku u Nemačkoj[288]

Kada je reč o mogućnosti pristupa internetu, kao preduslovu za ostvarivanje svih ostalih prava onlajn, organizacije Fridom haus u izveštaju o internet slobodama u Nemačkoj za 2018. godinu navodi da je mogućnost pristupa internetu na zadovoljavajućem nivou. Naime, izveštajem se pristup analizira na nekoliko nivoa, pre svega internet penetracijom, koja se u Nemačkoj, s obzirom na to da prelazi prosečne vrednosti na nivou zemalja EU, izveštajem ocenjuje visokom ocenom. Drugi faktori kojima se procenjuje mogućnost pristupa internetu podrazumevaju potencijalne restrikcije kada je reč o internet konekciji, tržište i regulatorna tela. U ovom delu izveštaja navodi se da, premda su u skorijoj

[287] Shashi Jayakumar. (March 13, 2018). Germany's NetzDG: Template for Dealing with Fake News?. *RSIS Commentary. No. 41.* Dostupno na: https://www.rsis.edu.sg/wp-content/uploads/2018/03/CO18041.pdf (pristupljeno: 02. 02. 2019. godine).

[288] U Nemačkoj je, usled primene NetzDG-a, Fejsbuk imenovao osobu zaduženu za sprovođenje ovog zakona (Procesni agent za upravne postupke i građanske sudske postupke u smislu člana 5(1) NetzDG-a: Freshfields Bruckhaus Deringer LLP (Berlin), Potsdamer Platz 1, Berlin 10785). Uslovi korišćenja upotrebljeni za analizu preuzeti su u Nemačkoj.

prošlosti postojale kritike upućene regulatornom telu zaduženom za pitanja pristupa (*Bundesnetzagentur* – BNetzA), a koje su se odnosile na favorizovanje bivšeg državnog monopoliste, Telekoma, analize nisu zabeležile restrikcije pristupa za ovaj period, kao ni favorizovanje tržišnih igrača, te je sada nemačko IKT tržište decentralizovano i uključuje stotine provajdera (Izveštaj organizacije Fridom haus, 2018).

Drugi identifikator, *ograničavanje sadržaja*, procenjuje se kroz analizu blokiranja i filtriranja sadržaja, uklanjanje sadržaja, manipulaciju sadržajem. Generalni zaključak izveštaja jeste da je onlajn-komunikacija u Nemačkoj slobodna, te da se država retko kada uključuje u blokiranje sadržaja. Međutim, novousvojeni NetzDG ukazao je na neke sporne situacije. Reč je o uklanjanju sadržaja sa društvenih mreža koji su bili satirične prirode, ali su ishitreno okarakterisani kao štetni. U tom kontekstu u izveštaju se navodi: „Mnogi tvitovi, postovi ili druge izjave na društvenim mrežama mogu izgledati kao da spadaju u opseg odredbi o govoru mržnje ako su istgnuti iz konteksta" (Izveštaj organizacije Fridom haus, 2018).

Treći identifikator, *povrede prava korisnika*, poslednjih godina najčešće je dovođen u vezu sa migrantskom krizom, odnosno sa širenjem govora mržnje usmerenog na migrante. Međutim, kako se u izveštaju navodi, primetan je i napor nemačke vlade da kroz regulatorne mehanizme učvrsti kontrolu nad internet prostorom, što je dovelo i do sporadičnih kontroverznih slučajeva narušavanja prava korisnika. Naime, ovaj identifikator obuhvata nekoliko kategorija: *zakonsko okruženje, procesuiranje i kažnjavanje onlajn aktivista, nadzor, privatnost* i *anonimnost, zastrašivanje i nasilje* i *tehničke napade*.

Kada je reč o zakonskom okruženju, u izveštaju se navodi da je NetzDG doneo najveće promene u ovoj oblasti, te se ponovo ističu granični slučajevi, oni između satire i sadržaja, koji bi se izvan konteksta mogao protumačiti kao govor mržnje. Pored ovoga, ukazuje se na slabost potupne primene ovog zakona, što bi često moglo da dovede do kršenja prava na slobodno izražavanje. U izveštaju se navodi da je tokom 2017. godine policija sprovela pretrese (racije) 36 korisnika društvenih mreža zbog navodnog govora mržnje.

Zakon koji je usvojen krajem 2016. godine, i koji se, prema izveštaju organizacije Fridom haus, u trenutku pisanja izveštaja još uvek razmatra, jeste novi zakon o Federalnoj obaveštajnoj službi, kojim se znatno proširuju mogućnosti nadzora internet komunikacije u Nemačkoj. Naime, nakon Snoudenovog otkrića o praćenju komunikacije nemačkih zvaničnika od strane američke Agencije za nacionalnu bezbednost (NSA) u Nemačkoj, oformljena je komisija zadužena za ispitivanje ovog slučaja. Analiza je pokazala da nema nezakonitog nadzora i presretanja komunikacije, dok su opozicioni lideri imali drugači stav. Uprkos tome, novousvojeni zakon o nadzoru proširio je mogućnosti praćenja internet komunikacije. Iako je ovaj Zakon prevashodno namenjen za praćenje komunikacije stranih državaljana, stručna javnost kritikuje njegovu primenu i smatra da se tako nešto ne može sprovesti bez uticaja na internet komunikaciju građana Nemačke. Pored toga, „pošto Nemačka savezna obaveštajna služba prema novom zakonu ima eksplicitnu dozvolu da nadgleda domaći internet saobraćaj sve dok cilja na strane državljane, grupe za slobodu medija tvrde da zakon ugrožava ustavom zaštićeni rad stranih novinara koji izveštavaju u Nemačkoj" (Izveštaj organizacije Fridom haus, 2018).

Još jedna sporna primena zakona koja se u izveštaju detaljno obrazlaže jeste proširivanje popisa kaznenih dela koja omogućavaju Saveznoj kriminalističkoj policiji da instalira špijunski softver na uređaje (telefon, tablet, kompjuter) osumnjičenih. Kritičari primene ovog zakona tvrde da je spisak kaznenih dela peopširan, da policiji daje prevelika ovlašćenja kada je reč o nadzoru, te da potencijalno može da ugrozi pravo na privatnost i slobodno izražavanje građana. Ove sumnje dodatno su učvršćene kada je otkriveno da kriminalistička policija radi na tome da te „federalne trojance" iskoristi i za

praćenje komunikacije na aplikacijama koje su široko primenjene u svakodnevnoj komunikaciji građana, kao što je Vacap (*WatsApp)* (Izveštaj organizacije Fridom haus, 2018).

Takođe, jedan od zakona kritikovan u Izveštaju jeste i zakon kojim se reguliše zadržavanje podataka, usvojen 2015. godine. Ovaj zakon ocenjen je kao zakon koji je u suprotnosti sa odlukom Evropskog suda pravde o čuvanju podataka. Naime, sporna primena ovog zakona odnosi se na zahteve da različite vrste korisničkih podataka budu sačuvane na serverima 10 nedelja. Pored ovoga, u Izveštaju se navodi i sledeće:

> „Provajderi moraju da zadrže brojeve, datume vreme telefonskih poziva i tekstualnih poruka. Internet servis provajderi takođe moraju zadržati IP adrese svih korisnika, kao i datume i vreme povezivanja. Podaci o lokaciji mobilnih telefonskih veza moraju biti čuvani četiri nedelje. Zahtevi isključuju veb-lokacije kojima se pristupa, metapodatke o prometu putem e-pošte i sadržaj komunikacija" (Izveštaj organizacije Fridom haus, 2018).

Međutim, to nije bio jedini zakon koji je izazvao nepoverenje u odlučnost Vlade Nemačke da zaštiti podatke svojih građana. Naime, 2017. godine usvojen je zakon o elektronskoj identifikaciji koji je omogućio svim saveznim državama, policiji i službama da ostvare pristup bazi podataka sa fotografijom iz pasoša svih građana Nemačke. Kao odgovor na ove mere javila se bojazan da bi, u kombinaciji sa drugim spornim zakonima o nadzoru, to omogućilo neometano praćenje kretanja svih građana Nemačke (Izveštaj organizacije Fridom haus, 2018).

Sa druge strane, u toku analiziranog perioda nije zabeležen nijedan slučaj direktnog fizičkog nasilja nad onlajn novinarima ili korisnicima informaciono-komunikacionih sistema u Nemačkoj. Takođe, nevladine organizacije i digitalni aktivisti retko su mete sajber napada, dok je češći slučaj sajber napada na vladu i njene agencije.

Najmanje negativnih poena Nemačka je dobila za identifikator *prepreke za pristup internetu* – 3 od 25, zatim za *ograničenje sadržaja* – 5 od 35, dok je izuzetno loš rezultat ostvarila za identifikator *povrede prava korisnika* – 11 od 40. Uzevši sve u obzir, Fridom haus ocenjuje internet prostor u Nemačkoj kao slobodan.

***

Na osnovu svega navedenog, moglo bi se zaključiti da je odnos Federativne Republike Nemačke prema internet komunikaciji i slobodama umnogome oblikovan nacionalnim i istorijskim specifičnostima, te da se, kako Vagner navodi: „može razumeti samo u specifičnom istorijskom kontekstu, kao evolucija regulatornih praksi i normi dozvoljenog govora" (2014: 58). Istorijski žig nacizma vidljiv je i pri upravljanju onlajn-prostorom. Očuvanje ljudskog dostojanstva i sprečavanje govora mržnje ostaje fokus i u internet komunikaciji. Za razliku od SAD, sloboda izražavanja u Nemačkoj nije nepovredivo pravo, naročito ukoliko je na drugom tasu odbrana dostojanstva. Takav odnos prema normama slobodnog izražavanja direktna je posledica istorijskog nasleđa.

Filtriranje štetnog sadržaja i uključivanje privatnih kompanija u zajedničko upravljanje onlajn-komunikacijom kako bi se stvorilo bezbednije okruženje za korisnike, sada je već svakodnevna praksa gotovo svih liberalnih demokratija. Međutim, Nemačka, bliža demokratsko-korporativnom modelu koga karakteriše istorijski jaka uloga države i regulacije, primer je demokratske države, članice EU,

koja insistira na poštovanju, pre svega, nacionalnih zakona, a oni, kako je izvestio Fridom haus, često i nisu u potpunoj saglasnosti sa zakonima EU.

Pokušaj nacionalizacije internet prostora, ma kako on bio slabog intenziteta, može se, sa jedne strane, tumačiti kao zaštita građana od globalnih privatnih kompanija. Međutim, prekomerna upotreba i stalno proširivanje primene pojedinih zakonskih odredbi može voditi ugrožavanju drugih prava građana, kao što su privatnost koja je potencijalno ugrožena zbog prekomernog nadzora ili zadržavanja podataka, te sloboda izražavanja potencijalno ugrožena praksama filtriranja i blokiranja. Možda je najbolja rečenica kojom bi se opisala stalna potraga za balansom između ovih prava – *hodanje po tankom ledu*.

6.3. Evropske zemlje razvijene demokratije – mediteranski model: Francuska

Medijski sistem Francuske, prema klasifikaciji Halina i Manćinija (2004), pripada mediteranskom, odnosno pluralističko-polarizivanom modelu. Međutim, odmah na početku bi trebalo ukazati na to da je Francuska zapravo granični slučaj, jer je pozicionirana negde između demokratsko-korporativnog i mediteranskog modela, ali je autori ipak, zajedno sa Italijom, Portugalijom, Španijom, Grčkom, svrstavaju u mediteranski tip.

Mediteranski tip medijskog sistema karakteriše niska stopa cirkulacije štampe, koja je ujedno i elitna, politički orjentisana. Visok nivo političkog paralelizma još jedna je od odlika ovog tipa medijskog sistema, a sa izraženim političkim paralelizmom dolazi i eksterni pluralizam, primetan u zemljama mediteranskog tipa. Novinarstvo je generalno komentatorski nastrojeno, dok novinari iskazuju nizak nivo profesionalizma. Politika je u mediteranskom modelu iznad radiodifuzije i dominantan je vladin model radiodifuzije. Ovaj model odlikuje i izražena instrumentalizacija, kao i jaka uloga države kroz državne intervencije – državne subvencije za štampu, na primer, u Francuskoj i Italiji najviše su u odnosu na sve ostale zemlje Evrope. U zemljama ovog tipa u prošlosti bili su dominantni periodi cenzure, dok se privatizacija medijskog sistema sprovodila bez jasnog regulatornog okvira i u teoriji je poznata kao „divlja deregulacija", što, na primer, nije bio slučaj u Francuskoj (Hallin & Mancini, 2004: 89-142).

Autori ističu da medijski sistem Francuske nije najreprezentativniji primer mediteranskog tipa, pre svega zbog toga što Francuska, pa i Italija imaju mnogo dužu istoriju demokratske politike od, na primer, Španije ili Portugalije u čijim se medijskim sistemima mnogo jasnije očitavaju navedene karakteristike polarizovanog tipa (Hallin & Mancini, 2004: 70).

U tom kontekstu Halin i Manćini navode:

> „Francuska je izuzetak na značajan način, svakako se karakteriše polarizovanim pluralizmom, snažnom ulogom države i istorijom snažnog političkog paralelizma u medijima, ali i snažnijom industrijalizacijom i snažnijim razvojem masovne cirkulacije tiražne štampe i racionalno-pravne vlasti" (2004: 74).

Iako drugačija od ostalih mediteranskih zemalja, autori se iz nekoliko razloga opredeljuju da je, ipak, odrede kao najbližu mediteranskom tipu. Na ovakav postupak odlučuju se, pre svega, zbog: 1) izrazite „tendencije da mediji dominiraju političkom sferom“, što je čini dosta udaljenom od liberalnog i demokratsko-korporativnog tipa, 2) jake veze između francuskih medija i drugih južnoevropskih zemalja, između ostalog, usled Napoleonove invazije (2004: 90); pored ovoga 3) „francuska istorija karakteriše se oštrijim konfliktom između tradicije i modernosti” (2004: 128) nego što je to slučaj sa zemljama u preostala dva modela.

Francuska je, kao reprezent mediteranskog tipa, odabrana za analizu zbog toga što izveštaj koji daje Fridom haus za 2018. godinu nije uključio zemlje bliže ovom modelu (Portugaliju, Španiju, Grčku), već samo Francusku i Italiju[289]. S obzirom na to da su obe zemlje dobile isti broj poena, 25 od 100 negativnih poena, što ih svrstava u red zemalja sa slobodnim internetom, na odluku da Francuska bude predstavljena uticali su aktuelni događaji u oblasti internet upravljanja u Francuskoj.

Naime, izbori u Francuskoj 2017. godine stavili su pitanje uticaja „lažnih vesti” u žižu interesovanja i pokrenuli lavinu debata o jačoj regulaciji interneta u ovoj oblasti. Pored ovoga, teroristički napadi koji su se proteklih nekoliko godina desili u Francuskoj rezultirali su jačom regulacijom kada je o onlajn-podsticanju na terorizam reč. I na kraju, predsednik Francuske Emanuel Makron (Emmanuel Macron) govorio je na Forumu o upravljanju internetom 2018. godine (*Internet Governance Forum*, 2018), gde je predstavio svoju vizuju upravljanja internetom, koja se bazira na jačoj regulaciji.

Zbog svega navedenog, Francuska, pored toga što je predstavnik mediteranskog tipa, pogodna je i za ukazivanje na to kako se odgovara na aktuelne izazove u oblasti upravljanja internetom, u jednoj evropskoj, demokratskoj zemlji.

U govoru na Forumu o upravljanju internetom, 2018. godine, francuski predsednik Makron je, o aktuelnim izazovima upravljanja internetom, rekao sledeće:

> „Duboko verujem da je regulacija potrebna. To je uslov za uspeh slobodnog, otvorenog i bezbednog internet – vizije osnivača. […] To je takođe uslov da demokratski izabrane vlade poštuju vladavinu prava kako bi zaštitile svoj narod. […] ako ne regulišemo internet, postoji rizik da će se temelji demokratije uzdrmati ; ako ne regulišemo odnose prema podacima i pravima naših građana nad njihovim podacima – pristup podacima i deljenje podataka – kakvo je onda značenje demokratski izabranih vlada? Ali ko može bolje od ovih vlada da uspostavi zakon? To znači da implicitno prihvatamo da bi igrači, na osnovu ekonomske dominacije, ili sistema koji nikada nije bio predmet praktične rasprave, bili legitimniji od vlade u odnosu prema svojim građanima” (Macron, 2018)[290].

Iz govora predsednika Makrona jasno je da je zvanični stav Francuske pooštrenje regulatornih mehanizama, kada je o internetu reč. Međutim, kako je kasnije u obraćanju Makron i obrazložio, njegova težnja za većom kontrolom nije neosnovana. Najmanje je dva razloga koja u poslednjih nekoliko godina idu u prilog tezi o jačoj regulaciji interneta u Francuskoj: *lažne vesti* i njihov moguć

[289] Pregled svih zemalja koje je Fridom haus uključio u analizu dostupan na: https://freedomhouse.org/report/countries-net-freedom-2018 (pristupljeno 05.03.2019. godine).
[290] Internet Governance Forum 2018; Speech by French President Emmanuel Macron: https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron (pristupljeno 11. 03. 2019. godine).

uticaj na političke odluke i *terorizam*, odnosno sprečavanje terorističkih aktivnosti i organizovanja onlajn.

U izveštaju organizacije Fridom haus, kojim se analiziraju internet slobode u Francuskoj, navodi se da se Francuska „generalno ne upušta u politički motivisano blokiranje veb stranica", te da društvene mreže, blogovi i ostale usluge funkcionišu slobodno i bez ometanja. Međutim, nakon napada na Šarli Ebdo (*Charlie Hebdo*), februara 2015. godine, i terorističkog napada novembra iste godine u Parizu, vlada Francuske objavila je da će „ograničavanje osnovnih prava građana služiti javnoj sigurnosti, a sadržaj terorizma biti podložan cenzuri" (Izveštaj organizacije Fridom haus, 2018)[291]. Generalno, to je najavilo set zakonskih izmena kojima će se internet sadržaj u Francuskoj strože kontrolisati, a sa ciljem sprovođenja antiterorističkih mera.

Mesec dana nakon terorističkog napada na redakciju satiričnog časopisa Šarli Ebdo, izdata je uredba kojom se predviđaju mere za blokiranje veb stranica putem kojih se terorizam veliča, podržava ili inicira. Upravni organ koji je zadužen za sprovođenje ovih mera, odnosno za sastavljanje crnih lista sajtova i blokiranje, jeste Centralna kancelarija za borbu protiv kriminala povezanog sa informacijskom i komunikacijskom tehnologijom (fr. *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* – OCLCTIC). Centralna kancelarija može od urednika ili domaćina (*host*) da zatraži uklanjanje sadržaja, a da nakon 24 sata zatraži od internet servis provajdera i blokiranje sajta.

Međutim, kako se u Izveštaju navodi, ubrzo nakon usvajanja ovog dekreta, došlo je do blokiranja pet veb stranica bez sudskog naloga i uvida javnosti zbog sumnje da su povezane sa terorizmom. Netransparetnost u sprovođenju ovih mera dovodi se u pitanje sa stanovišta legaliteta: „Nedostatak pravosudnog nadzora u blokiranju veb stranica koje podstiču ili promovišu teroristička dela ostaje glavna briga" (Izveštaj organizacije Fridom haus, 2018). U tom kontekstu, postoji vrsta mehanizma koji se može prepoznati kao unutrašnja kontrola. Naime, Nacionalna komisija za informatiku i slobodu (fr. *Commission nationale de l'informatique et des libertés- CNIL*), upravno regulatorno telo koje bi trebalo da korisnicima osigura zaštitu njihovih podataka, može uputiti žalbu upravnom sudu u vezi sa preduzetim akcijama OCLCTIC, ukoliko ih smatra pogrešnim. Međutim, kako se u izveštaju navodi, javnost je nezadovoljna radom CNIL: „iako je CNIL osnovan da zaštiti slobode na internetu, sada nadgleda ograničavanje tih istih prava" (Izveštaj organizacije Fridom haus, 2018).

Novi Zakon o jačanju unutrašnje sigurnosti i borbi protiv terorizma iz oktobra 2017. godine izazvao je kritike boraca za građanska prava. Dok francuska vlada tvrdu da: „Njegove odredbe imaju za cilj sprečavanje terorističkih akata uz očuvanje individualnih sloboda"[292], postoji bojazan da nove odbredbe zakona daju „široka ovlašćenja snagama sigurnosti sa ograničenim sudskim ovlašćenjima" (Izveštaj organizacije Fridom haus, 2018).

Međutim, i pre terorističkih napada 2015. godine, u Francuskoj su na snazi bili rigorozni zakoni protiv terorizma, kako onlajn tako i oflajn. Na primer, :

[291] Izveštaj organizacije Fridom haus za Francusku dostupan na: https://freedomhouse.org/report/freedom-net/2018/france (pristupljeno 20. 03. 2019. godine).
[292] Gouvernement.fr. *Reinforcing internal security and the fight against terrorism*. https://www.gouvernement.fr/en/reinforcing-internal-security-and-the-fight-against-terrorism (pristupljeno 23. 04. 2019. godine).

„Zakon o suzbijanju terorizma usvojen u novembru 2014. godine kažnjava govor na internetu koji se smatra 'izvinjenjem za terorizam' (*apologie du terrorisme*) sa do sedam godina zatvora i novčanom kaznom od 100.000 evra (100.000 USD). Onlajn-kazne su oštrije od oflajn-kazni, koje predviđaju pet godina zatvora i 75.000 evra kazne" (Izveštaj organizacije Fridom haus, 2018).

Borba protiv terorizma imala je uticaj i na povećanje hapšenja internet korisnika pod sumnjom da su njihove aktivnosti na internetu u vezi sa teorizmom, odnosno da „slave ili podstiču terorizam na internetu"; dok se, sa druge strane, „nijedan građanin nije suočio sa politički motivisanim hapšenjima ili krivičnim gonjenjem" (Izveštaj organizacije Fridom haus, 2018).

Sporna pravna terminologija kojom se određena dela dovode u vezu sa terorističkim aktima, takođe, često je kritikovana. Pojmovi poput „podsticanja" i „veličanja" terorizma, na primer, ne mogu da se odrede jednoznačno i nedvosmisleno. U izveštaju se u tom kontekstu navode dva primera primene ovih terminoloških odrednica u praksi, što je rezultiralo zatvorskom, odnosno uslovnom kaznom:

„U martu 2018. godine, nakon terorističkog napada na supermarket u Trebesu, bivši član francuske političke stranke 'La France Insoumise' ismevao je na Tviteru žandarma koji je umro u zamenu za taoca tokom terorističkog napada. Bivši političar dobio je kaznu zatvora u trajanju od jedne godine. Povodom istog događaja, veganskoj aktivistkinji izrečena je uslovna kazna od sedam meseci jer je na društvenoj mreži objavila komentar koji kaže da je imala 'nula sažaljenja' za mesara koji je umro za vreme napada i upitala je: 'Da li vas šokira to što je ubicu ubio terorista? Mene ne...'" (Izveštaj organizacije Fridom haus, 2018).

Ova dva primera možda i najbolje ilistruju koliko je francuska vlada ozbiljna u nameri da sankcioniše „podsticanje" i „veličanje" terorizma na internetu. Pitanje je da li ujedno i guši slobodu izražavanja, koliko god se ona nekada koristila za iznošenje kontroverznih stavova i mišljenja pojedinaca kao što je to bio slučaj sa bivšim političarem i aktivistkinjom.

Pored svega navedenog, antiterorističke mere podrazumevaju i pojačan nadzor onlajn-komunikacije koji je u Francuskoj dobio legalitet kroz razne zakone. Navedeno se može ilustrovati sledećim navodom iz Izveštaja:

„Zakon o obaveštajnoj delatnosti, omogućava obaveštajnim agencijama da sprovedu elektronski nadzor bez sudskog naloga i zahteva od internet servis provajdera da instaliraju takozvane 'crne kutije', algoritme koji analiziraju metapodatke korisnika sa 'sumnjivim' ponašanjem u realnom vremenu. […] U julu 2016. godine, amandmanom je odobreno prikupljanje metapodataka pojedinaca u realnom vremenu i to ne samo onih koji su 'identifikovani kao teroristička pretnja' već i onih 'koji će verovatno biti povezani' sa terorističkom pretnjom, ili sa onima koji pripadaju 'pratnji' 'dotične osobe'" (Izveštaj organizacije Fridom haus, 2018).

Kako se u izveštaju navodi, Ustavni sud Francuske pojedine odredbe ovog zakona proglasio je neustavnim još ranije, međutim, nakon niza terorističkih napada mnogobrojni sporni amandmani uvojeni su u svrhu „odbrane i promovisanja osnovnih interesa zemlje".

Kada je reč o zaštiti podataka korisnika na internetu, Zakon o digitalnoj republici usvojen u oktobru 2016. godine ocenjuje se kao pozitivan u tom kontekstu jer se njime nastoji da se poboljšaju prava pojedinaca kada je reč o korišćenju njihovih ličnih podataka. Generalno, CNIL je regulatorno telo čija nadležnost jeste upravo zaštita privatnosti, odnosno podataka korisnika. Dva su skorija slučaja u kojima je CNIL imao učešće a reč je o kršenju prava korisnika od strane privatnih kompanija. Prvo, kao deo šire evropske istrage, CNIL je kaznio Fejsbuk zbog prikupljanja ličnih podataka građana koji nisu Fejsbuk korisnici. Naime, Fejsbuk je prikupljao podatke internet korisnika preko trećih lica, sa kojima sarađuje, a da korisnici o tome nisu bili obavešteni i nisu dali svoj pristanak. Zbog toga je maja 2017. godine CNIL kaznio Fejsbuk sa 150.000 evra (Kar-Gupta & Rosemain, 2017)[293]. Takođe, „CNIL je 18. decembra zatražio i od Vacapa da ispravi svoju praksu prenosa ličnih podataka na Fesjbuk bez pristanka krajnjeg korisnika" (Izveštaj organizacije Fridom haus, 2018).

Posebno sporno pravo, oko koga se vodi dosta polemika u Francuskoj, jeste pravo na zaborav. Naime, neslaganje u vezi sa poimanjem sprovođenja ovog prava između Francuske i privatnih kompanija eksaliralo je na primeru Gugla. CNIL je zahtevao od kompanije Gugl da odluke o pravu na zaborav sprovodi sveobuhvatno, odnosno da ukloni sadržaj i sa domena *Google.com*, a ne samo sa domena u Francuskoj – *Google.fr*. Ipak, čelnici kompanije Gugl smatraju da bi ovakav presedan iskoristile autoritarne vlade koje bi onda od Gugla zahtevale da i njihove „nacionalne zakone primeni izvanteritorijalno" (Izveštaj organizacije Fridom haus, 2018), kao i: „da će to ometati pravo javnosti na informisanje i da će biti oblik cenzure" (CNIL, 2015)[294].

Međutim, „francuski regulatori privatnosti, između ostalog, zahtevali su da kompanija primeni 'pravo na zaborav' na svoje globalne domene kako bi se uskladila sa strogim pravilima zaštite podataka u Evropi koja štite privatnost pojedinca kao osnovno ljudsko pravo" (Scott, 2016)[295]. Kompanija Gugl kažnjena je sa 112.000 dolara zbog toga što nije primenila evropsku regulativu i uklonila sadržaje sa globalnih domena.

***

Francuska je dobila 25 od 100 negativnih poena u analizi organizacije Fridom haus i time je svrstana u red zemalja sa slobodnim internetom. Najveći broj negativnih poena dobila je za narušavanje prava korisnika (16 od 40), što se može objasniti konstantnom borbom za održavanjem balansa između prava korisnika i očuvanja bezbedne komunikacije na internetu.

Kao netipična mediteranska zemlja, Francuska nije pokazala znatno veću ulogu države od primera demokratsko-korporativne zemalje. Moglo bi se uopšteno zaključiti da Francuska teži jačoj regulaciji internet prostora, o čemu je i predsednik Makron otvoreno govorio. Međutim, težnja za većim učešćem u upravljanju internetom u Francuskoj javlja se odgovor na aktuelne izazove u onlajn-

[293] Kar-Gupta & Rosemain. (May 16 2017). Facebook fined 150,000 euros by French data watchdog. *Reuters*. https://uk.reuters.com/article/us-facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUKKCN18C10C (pristupljeno 23. 04. 2019. godine).
[294] CNIL. (Sep 21 2015). Right to delisting: Google informal appeal rejected. https://www.cnil.fr/fr/node/15814 (pristupljeno: 22. 04. 2019. godine).
[295] Scott, M. (March 24 2016). Google Fined by French Privacy Regulator. *The New York Times*. https://www.nytimes.com/2016/03/25/technology/google-fined-by-french-privacy-regulator.html?_r=0 (pristupljeno 22. 04. 2019. godine).

prostoru, pre svega na terorizam i lažne vesti. Mere francuske vlade u ovoj oblasti mogle bi se onda sagledati kao akcije koje idu u prilog očuvanju bezbedne i slobodne komunikacije.

Kao što je pokazano na primeru Nemačke, balans između slobodne i bezbedne internet komunikacije jedan je od najvećih izazova demokratskim zemljama. Slični napori prepoznaju se i u primerima iz Francuske.

6.4. Postsovjetske zemlje: Rusija

Kako bi se odredio tip odnosa Rusije prema internet slobodama, u radu se polazi od tipa medijskog sistema u Rusiji, kao što je bio slučaj i sa prethodno analiziranim zemljama. Pretpostavka je da će istorijat razvoja medijskog sistema u Rusiji, te odnos države prema medijskim slobodama imati dominantan uticaj i na njen odnos prema komunikaciji na internetu i internet slobodama uopšte. Dakle, kakav je medijski sistem Rusije danas? Da li je bliži zapadnim modelima i da li ga možemo svrstati u neki od tipova koje nude Halin i Manćini (2004)? Upravo ovim pitanjem bavila se Elena Vartanova (Elena Vartanova u Hallin & Mancini, 2012) u radu koji je deo knjige Halina i Manćinija *Poređenje medijskih sistema izvan Zapadnog sveta* (engl. *Comparing media systems beyond the Western world,* 2012).

Vartanova smatra da je Rusija zemlja kontradiktornosti, a da je takvom uređenju doprinela njena duga i iscrpna tranziciona istorija. Naime, dok devedestih godina 20. veka nije ušla u poslednju tranziciju ka liberalizaciji i uspostavljanju zapadnog modela demokratije, Rusija je u poslednja dva veka imala više tranzicionih perioda: od agrarnog društva u ranom 19. veku, ka neujednačenom rastu kapitalizma u drugoj polovini 19. veka, te ka kratkotrajnoj višestranačkoj demokratiji (oktobar, 1917. godine), i ka socijalističkoj revoluciji i uspostavljanju Komunističke partije, nakon čega su usledile godine ekonomske recesije i političke propagande, što je rezultiralo raspadom SSSR i na kraju do transformacije po modelu zapadnih liberalnih demokratija devedestih godina (Vartanova, 2012: 119-120).

Društveno-politička transformacija devedesetih podrazumevala je i transformaciju medijskog sistema Rusije, koji je, sledeći model zapadnih demokratija, trebalo da ukine cenzuru, ojača medijske slobode, te da ide put profesionalizacije i privatizacije, i ograniči ulogu države. Međutim, Vartanova smatra da je ovakva putanja transformacije bila uglavnom retorička, te da je tako zamaskirala složenost postsovjetskih društava koja nisu bila spremna da na adekvatan način prekopiraju zapadni model, niti da ga prilagode sopstvenim potrebama – „Stoga se transformacija postsovjetskih medijskih sistema ne može objasniti kao linearno i univerzalno kretanje prema imaginarnom i nekritički shvaćenom idealnom zapadnom medijskom modelu" (Vartanova, 2012: 121).

Medijski sistem Rusije ostao je pod jakim uticajem države sve do danas: „Tradicionalni paternalistički karakter odnosa medija i države u kojem mediji još uvijek igraju ulogu nevinog i poslušnog deteta ostaje središnji deo ruskog sistema" (Vartanova, 2012: 142). Jakubovič i Sukosd (Jakubowicz&Sükösd, 2008) smatraju da su postsovjetske zemlje najbliže mediteranskom tipu Halina i Manćinija i tu im pronalaze „mesto na mapi". Međutim, Vartanova ističe odnos države i medija kao ključnu karakteristiku kojom se ruski medijski sistem razlikuje od mediteranskog, odnosno polarizovanog sistema: „Ruski mediji razlikuju se od njega u jednoj ključnoj dimenziji, a to je odnos

države i medija , uključujući ulogu države i državnih agencija u oblikovanje medijskih struktura , politike i novinarske prakse" (Vartanova, 2012: 142). Naime, autorka ističe da je uloga države u postsovjetskim zemljama ključna, te da nije istovetna ulozi države u mediteranskim sistemima – država je uključena u svaku poru medijskog sistema Rusije, ona nije samo značajan akter već moglo bi se reći i centralni.

Kako se onda može odrediti medijski sistem Rusije, ukoliko se za okvir uzme klasifikacija Halina i Mančinija? Vartanova smatra da ruski model delimično preuzima liberalni okvir, u smislu otvorenog tržišta, koje se prevashodno odnosi na komercijalnu potražnju, zanemarujući društvene potrebe i potražnju. Sa druge strane, ogromna uloga države i neprepoznavanje medija kao stuba demokratije približava ruski model mediteranskom, pa ipak, nijedan od ova dva modela ne bi mogao da obuhvati kontradiktore karakteristike ruskog modela. Zbog toga Vartanova ruski model naziva *etatističko komercijalizovani model* – tržišno orjentisan model u kojem država i dalje ima dominantnu ulogu i značaj (Vartanova, 2012: 142).

Pri analizi odnosa Rusije prema internet slobodama, u ovom radu polazi se od teze zasnovane na analizi Vartanove, i pretpostavlja da su ruska burna tranziciona istorija, ali i nikada iskorenjen etatizam glavni uzrok njenog odnosa prema internetu danas. U prilog ovoj tezi govori i izveštaj organizacije Fridom haus o internet slobodama 2018. godine, koji Rusiju svrstava u red neslobodnih zemalja, sa 67 od 100 negativnih poena (Izveštaj organizacije Fridom haus, 2018)[296]. Negativni poeni u izveštaju dodeljeni su pretežno zbog restriktivnih zakona kojima se uređuje internet prostor, nelegalnog cenzurisanja i blokiranja veb sadržaja i narušavanja osnovnih prava internet korisnika, što je u saglasnosti sa pretpostavkom da će jaka uloga države imati dominantni uticaj na odnos Rusije prema internet slobodama.

Nacionalizacija internet prostora u Rusiji može se najpre uočiti na primeru dominantne upotrebe ruskog nacionalnog pretraživača *Yandex.ru* i ruske društvene mreže *VKontakte*. Naime, nacionalni pretraživač je češće upotrebljen nego Gugl i nalazi se na drugom mestu najposećenijih sajtova u Rusiji, dok je Gugl na četvrtom. Na trećem mestu je nacionalna društvena mreža – *VKontakte*, dok je, poređenja radi, Fejsbuk tek na četrnaestom mestu[297]. Ovakva pozicija nacionalnih internet kompanija već nagoveštava etatistički odnos prema internet prostoru u Rusiji.

Međutim, autoritarni odnos prema internet komunikaciji najpreciznije se može identifikovati na nivou regulacije, odnosno tela i zakona kojima se upravlja internetom u Rusiji. Regulatorno telo nadležno za mnogobrojne zakone kojima se reguliše internet u Rusiji je Roskomnadzor (rus. *Роскомнадзор*), odnosno Federalna služba za nadzor komunikacije, informacionih tehnologija i masovnih medija (rus. *Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций*). Roskomnadzor je zaslužan za usvajanje mnogobrojnih spornih zakona kojima se reguliše internet komunikacija, među kojima su Zakon o blogerima, Zakon o lokalizaciji podataka, i, najkontrverzniji među njima, set antiterorističkih amandmana usvojen 2016. godine, poznat pod nazivom Jarovaja zakon (engl. *Yarovaya law)* (Izveštaj organizacije Fridom haus, 2018).

[296] Izveštaj organizacije Fridom haus za Rusiju, 2018, dostupan na: https://freedomhouse.org/report/freedom-net/2018/russia. (pristupljeno 02. 03. 2019. godine).
[297] *Alexa. Top sites in Russia*. Dostupno na: https://www.alexa.com/topsites/countries/RU (pristupljeno 02. 03. 2019. godine).

Kontroverzni Zakon o blogerima iz 2014. godine predviđa da se blogeri koji imaju više od 3000 poseta dnevno regustruju kod državnog regulatora – Roskomnadzor, i imaju isti nivo odgovornosti kao i masovni mediji – „Takva registracija znači da blogeri više ne mogu ostati anonimni i da su pravno odgovorni za sadržaj objavljen na njihovom sajtu , uključujući komentare trećih lica" (Izveštaj organizacije Fridom haus, 2018). Ovaj zakon pretrpeo je brojne kritike blogera, organizacija civilnog sektora, ali i zapadnih zemalja. Svi oni ukazali su da restriktivan zakon, kao što je Zakon o blogerima, nužno vodi autocenzuri i ugrožavanju slobode izražavanja (Birnbaum, 2014)[298].

Nakon otkrića Edvarda Snoudena o prisluškivanju NSA, pojavio se još veći pritisak za jačom kontrolom interneta u Rusiji. Pod utiskom ovog otkrića: „Nekoliko članova oba doma parlamenta predložilo je da svi serveri na kojima se čuvaju lični podaci ruskih građana treba da budu smešteni u Rusiji […] ili da zahtevaju da budu dostupni u Rusiji pod domenom *.ru*, ili da se obavežu da budu hostovani na ruskoj teritoriji" (Nocetti, 2015: 114). Naime, ruske vlasti smatraju da su politike privatnosti transnacionalnih kompanija, kao što su Gugl, Fejsbuk, Tviter, zapravo „pretnja digitalnom suverenitetu Rusije – a time i nacionalnoj sigurnosti" (Nocetti, 2015: 114).

Prethodno komentarisano rezultiralo je usvajanjem Zakona o lokalizaciji podataka 2014. godine, koji je stupio na snagu septembra 2015. godine, a kojim se predviđa da kompanije koje posluju u Rusiji skladište podatke na serverima fizički lociranim u Rusiji (Savelyev, 2016). Primena ovog zakona dovela je do mnogobrojnih kontroverznih postupaka Rusije prema internet kompanijama koje posluju u okvirima njenih granica.

Prvi sporni primer primene ovog zakona odnosi se na slučaj iz novembra 2016. godine, kada je društvena mreža *LinkedIn* blokirana u Rusiji. Naime, *LinkedIn* je bio blokiran od strane lokalnih internet servis provajdera, a na naređenje telekom regulatora Roskomnadzora. Tako je *LinkedIn* "postao prva velika međunarodna platforma koja je blokirana u Rusiji zbog neusklađenosti sa zahtevima za lokalizaciju podataka" (Izveštaj organizacije Fridom haus, 2018).

Premda postoje spekulacije da je primena ovog zakona prevashodno u službi cenzure i kontrole internet korisnika[299], pojedine svetske kompanije su u skladu sa zakonom preselile neke svoje servere u Rusiju – među njima su *Uber* i *Viber*, ali i *Apple*[300] i Gugl[301]. Sa druge strane, kompanijama koje se nisu povinovale zakonu o lokalizaciji podataka, ruske vlasti prete blokiranjem i sudskim tužbama.

Roskomnadzor je januara 2019. godine objavio da tuži Fejsbuk i Tviter zbog nepoštovanja zakona o lokalizaciji podataka. Postojeća regulativa ne predviđa rigorozne novčane kazne za nepoštovanje zakona, ali predviđa obavezu usklađivanja sa zakonom u ograničenom vremenskom roku,

[298] Michael Birnbaum. (July 31, 2014). Russian blogger law puts new restrictions on Internet freedoms. *The Washington Post*. Dostupno na: https://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html?utm_term=.e6f6cd636416 (pristupljeno 02. 03. 2019. godine).
[299] BBC. (Nov 17 2016). LinkedIn blocked by Russian authorities. Dostupno na: https://www.bbc.com/news/technology-38014501 (pristupljeno 02. 03. 2019. godine).
[300] Liam Tung. (September 11, 2015). Apple reportedly takes up Moscow datacentre to comply with Russia's personal data law. *ZDNet*. Dostupno na: https://www.zdnet.com/article/apple-reportedly-takes-up-moscow-datacentre-to-comply-with-russias-personal-data-law/ . (pristupljeno 03. 03. 2019. godine).
[301] Olga Razumovskaya. *(*April 10 2015). Google Moves Some Servers to Russian Data Centers. *The Wall Street Journal*. dostupno na: https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491 (pristupljeno 03. 03. 2019. godine).

najviše godinu dana od stupanja na snagu, te ruski regulator preti blokiranjem ukoliko ove kompanije ne usklade svoje poslovanje sa nacionalnim zakonom o lokalizaciji (Meyer, 2019)[302].

Najkontroverzniji set zakona stupio je na snagu jula 2018. godine – *Jarovaja zakon*. Ovaj set zakonskih izmena ime je dobio po jednoj od njegovoj najznačajnijih kreatorki, zamenici predsedavajućeg Državne dume, Irini Jarovajevoj (Irina Yarovaya). *Jarovaja zakon* zapravo predstavlja set amandmana kojima se menja desetak zakona koji se u značajnoj meri odnose i na internet slobode. Dok vlast ovaj zakon vidi kao anti-terorističku meru, sa ciljem povećanja bezbednosti korisnika, internet aktivisti oštro su kritikovali donošenje zakona i prozvali ga *Ruski zakon'Veliki brat'* (engl. *Russia's 'Big Brother' Law*)[303].

U izveštaju organizacije Fridom haus sumiraju se najznačajnije izmene koje je ovaj set zakona doneo: pooštravanje zatvorskih kazni za dela podsticanja i pozivanja na onlajn-terorizam (do sedam godina zatvora), kao i za ekstremizam i separatizam (do pet godina zatvora), i podsticanje na mržnju (do šest godina zatvora). Pored toga, ukoliko se neko lice sumnjiči za neko od navedenih krivičnih dela, čak i ukoliko se ispostavi da je nevino, može dospeti na listu ekstremista, i u skladu sa tim bi se moglo postupati sa tim licem, odnosno mogli bi mu biti zamrznuti bankovni računi, uskraćeno bavljenje određenim profesijama, bez obzira na to što nije osuđeno za delo za koje se teretilo. U izveštaju se posebno ističe da: „Oštre kazne i široka formulacija prekršaja otvaraju vrata zloupotrebama, odnosno kriminalizaciji legitimnog, nenasilnog izražavanja na internetu" (Izveštaj organizacije Fridom haus, 2018).

Sa druge strane, ovaj set zakona povećava i mogućnost nadzora, odnosno, „prisiljava mobilne i internet kompanije da registruju tekstualne poruke, telefonske razgovore i čet aktivnosti korisnika na šest meseci i da ih pruže sigurnosnim službama u slučaju sudskog naloga."[304] Zakon predviđa i još restriktivnije mere, nalažući onlajn-uslugama koje nude enkripciju da Federalnoj bezbedonosnoj agenciji pomažu da dešifruje šifrovane podatke. Iako je to čak i tehnički neizvodljivo za mnoge kompanije, kazna koja im preti ukoliko odbiju saradnju može dostići 15.000 dolara (Izveštaj organizacije Fridom haus, 2018).

Aplikacija za razmenu poruka *Telegram*[305] blokirana je u aprilu 2018. godine upravo zbog odbijanja da Federalnoj bezbedonosnoj agenciji obezbedi ključ za dešifrovanje enkriptovanih korisničkih poruka (Izveštaj organizacije Fridom haus, 2018). Dok je Federalna agencija takav zahtev pravdala borbom protiv terorizma i bezbednošću građana Rusije, *Telegram* je odbio zahtev uz obrazloženje da će narušiti pravo na privatnost korisnika (Kiselyova & Stubbs, 2018)[306]. Osnivač *Telegrama*, Dumov, smatra da bi: „zabrana oštetila kvalitet života 15 miliona Rusa i ne bi učinila ništa

[302] David Meyer. (January 21, 2019). Russia: We're suing Facebook, Twitter for snubbing law on storing users' data locally. ZDNet. dostupno na: https://www.zdnet.com/article/russia-were-suing-facebook-twitter-for-snubbing-law-on-storing-users-data-locally/ (pristupljeno 03. 03. 2019. godine).
[303] The Moscow Times. (July 1, 2018). Russia's 'Big Brother' Law Enters Into Force. Dostupno na: https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066 (pristupljeno 03. 03. 2019. godine).
[304] Ibid.
[305] *Telegram* je popularna platforma u Rusiji, sa preko 10 miliona korisnika, čiji je osnivač Rus Pavel Durov, a sedište kompanije je u Velikoj Britaniji.
[306] Maria Kiselyova & Jack Stubbs. (April 16, 2018). Russia starts blocking Telegram messenger. *Reuters*. Dostupno na: https://www.reuters.com/article/us-russia-telegram-blocking/russia-starts-blocking-telegram-messenger-idUSKBN1HN13J (pristupljeno 04. 03. 2019. godine).

da poboljša bezbednost Rusije. […] Smatramo da je odluka o blokiranju protvustavna i nastavićemo da branimo pravo Rusa na tajnu prepisku" (Dumov za *Reuters*, 2018)[307].

Januara 2018. godine na snagu je stupio i amandman na Zakon o informacijama, informacionim tehnologijama i informacionoj sigurnosti, kojim se društvenim mrežama i komunikacijskim platformama zabranjuje da štite anonimnost svojih korisnika: „Platforme moraju da povežu korisničke naloge sa njihovim telefonskim brojevima, efikasno povezujući aktivnosti na mreži sa njihovim pravim identitetom" (Izveštaj organizacije Fridom haus, 2018). Pored ovoga, prema važećem zakonodavstvu u Rusiji, da bi internet servis provajderi dobili dozvolu za rad u Rusiji oni moraju da ispune *SORM*[308] *sistemske zahteve*, odnosno "obavezni su da instaliraju tehnologiju koja omogućava sigurnosnim službama da prate internet saobraćaj" (Izveštaj organizacije Fridom haus, 2018).

Pored nadzora internet sadržaja, ruske vlasti imaju i široko diskreciono pravo na blokiranje veb sadržaja. Kako je navedeno u Izveštaju, u periodu od 2012. do 2013. godine amandmanima je, pored Roskomnadzora, uvedeno još nekoliko agencija – Kancelarija glavnog tužioca, Federalna služba za nadzor nad pravima potrošača i dobrobit ljudi (Rospotrebnadzor) – koje imaju ovlašćenja za blokrianje veb stranica i sadržaja bez sudskog naloga. Reč je o sadržajima koji su prepoznati kao dečja pornografija, informacije u vezi sa samoubistvom, drogama, kršenje autorskih prava, ali i o sadržaju koji je prepoznat kao ekstremistički, ili kao poziv na nedozvoljeni javni skup ili akciju (Izveštaj organizacije Fridom haus, 2018). Sporno je to što ove agencije često ne daju jasna objašnjenja zbog čega su neke sadržaje blokirali, što potvrđuje i široko definisanje protivzakonitih sadržaja koje se može lako zloupotrebiti od strane vladinih agencija.

Proces uklanjanja internet sadržaja u Rusiji uglavnom se odvija tako što vladini organi izdaju nalog Raskomnadzoru da ukloni identifikovan ilegalan sadržaj, odnosno da naloži provajderu da izda upozorenje veb stranici na kojoj je objavljen sporan sadržaj:

> „Vlasnici veb stranica imaju pravo da ulože žalbu sudu , ali im se često daje kratak vremenski interval u kojem to mogu učiniti . Kao rezultat toga , većina vlasnika brzo briše zabranjene informacije kako ne bi rizikovala blokiranje čitavog sajta. Ako se sadržaj ne ukloni, stranica se nalazi na crnoj listi, a internet servis provajderi moraju da je blokiraju u roku od 24 sata od prijema upozorenja od strane Roskomnadzora ili da se suoče sa kaznama" (Izveštaj organizacije Fridom haus, 2018).

Regulator ima ovlašćenje da sajtove koji nisu ispunili neku od zakonskih obaveza, na primer uklanjanje sadržaja nakon upozorenja, stavi na tzv. *crnu listu*. Međutim, u Izveštaju se navodi i da je nejasno u kojoj meri regulator zaista sprovodi ove restriktivne mere blokiranja sajtova jer je većina sajtova koji su na *crnoj listi* aktivna.

Zanimljivo je da je Rusija, po ugledu na nemački NetzDG, aprila 2018. godine usvojila zakon o sprečavanju širenja *lažnih vesti.* Zakonom se predviđa da veb stranice, uključujući i društvene mreže sa više od 100.000 dnevnih poseta, uklone sadržaje sa netačnim informacijama u roku od 24 sata. Ukoliko to ne učine mogu da se suoče sa kaznom od 800.000 dolara. Takođe, istovetno NetzDG propisu, i ruski

[307] Ibid.

[308] SORM je *sistem za operativne istražne mere*, koje ruska vlada koristi za svoje aktivnosti onlajn-nadzora. Trenutno koristi SORM-3 tehnologiju koja joj omogućava dubinsko praćenje paketa na svim telekomunikacionim mrežama u Rusiji (Freedom House. *Freedom on the Net 2018. Russia*).

zakon predviđa da onlajn tehnološke kompanije imenuju pravno lice na teritoriji Rusije koje će biti odgovorno za sprovođenje zakona (Izveštaj organizacije Fridom haus, 2018).

Kopiranje nemačkog zakona u Rusiji može se protumačiti i kao svojevrsan paradoks. *Reporteri bez granica* tako smatraju da je restriktivni zakon jedne demokratske zemlje poslužio kao opravdanje za zakon kojim će se cenzurisati sadržaj u nedemokratskim zemljama: „Ruski zakon pokazuje da kada vodeće demokratije osmišljavaju drakonske zakone , one represivnim režimima daju ideje" (*Reporters Without Boders*, 2017)[309]. Slično kritikama nemačke stručne javnosti, kritike upućene ruskoj verziji NetzDG odnose se na rigorozne kaznene mere, koje mogu voditi autocenzuri, te na nejasno definisanje načina na koji se utvrđuje *netačnost* sadržaja, i s tim u vezi široke mogućnosti zloupotrebe.

Zbog navedenih autoritarnih zakona, predviđenih rigoroznih kaznenih mera, ali i sprovođenja praksi koje krše prava internet korisnika u Rusiji, Fridom haus je ruski internet prostor ocenio kao neslobodan. Rusija je dobila 67 od 100 negativnih poena, pri čemu je najviše negativnih poena, 31 od 40, dobila zbog narušavanja prava korisnika, odnosno zbog gušenja prava na slobodno izražavanje onlajn, uklanjanja korisničkog sadržaja, te neovlašćenog nadzora korisnika.

***

Internet je, čini se od njegovog začetka, dominantno posmatran kao američka tvorevina, odnosno kao prostor koji je stvoren od strane SAD, i samim tim prostor u kojem vladaju pretežno liberalna pravila i vrednosti. Kako to Majer (Mayer) konstatuje: „internet je američka stvar" (2000: 149). Međutim, ne pokušavaju samo evropske zemlje, kako smo videli na primeru Nemačke, da internet skroje po svojoj meri. Nezapadne zemlje su u toj nameri još odlučnije.

Džulijen Noceti (Julien Nocetti, 2015) smatra da postoji jasna tendencija nezapadnih zemalja da postave nove temelje upravljanja sajber prostorom. Sa jedne strane, demografski podaci nezapadnih zemalja idu u prilog ovoj nameri – prema podacima Svetske internet statistike, u martu 2019. godine 50, 4% ukupnog broja internet korisnika na svetu je iz Azije, i 10, 9% iz Afrike, dok Evropljani imaju udeo od 16,5%, a korisnici iz Severne Amerike svega 7,5%[310]. Sa druge strane, postoje i duboko politički razlozi za takvu nameru "osvajanja interneta" od strane nezapadnih zemalja: „sve veći broj vlada više nije zadovoljan sadašnjim sistemom upravljanja internetom i nastoje da izazovu istorijsku dominaciju Sjedinjenih Američkih Država u sajber domenu" (Nocetti, 2015: 111-112).

Uzrok postojećeg odnosa Rusije prema internetu mogao bi se potražiti u obrazloženoj tendenciji za osvajanjem internet prostora i želji da se Rusija nametne kao dominantna u upravljanju internetom. Ova pasivna borba, između Amerike i Rusije, za prevlast u sajber prostoru može se opisati i kao *politika hladnog onlajn-rata* u 21. veku (Nocetti, 2015: 127).

Međutim, za pretežno autoritaran odnos prema internetu, Noceti navodi još dva moguća razloga. Sa jedne strane, autor to povezuje sa „inherentno autoritarnom prirodom ruskog režima" i

[309] Reporters Without Boders. (July 19, 2017). Russian bill is copy-and-paste of Germany's hate speech law. Dostupno na: https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law (pristupljeno 04. 03. 2019. godine).
[310] Internet World Stats. https://www.internetworldstats.com/stats.htm (pristupljeno 02. 04. 2019. godine).

“nastavljanjem vekovne navike blokiranja disidentskih glasova bilo kojim sredstvom koje je trenutno dostupno” (Nocetti, 2015: 115). Sa druge strane, „strategija se može pripisati činjenici da je Rusija relativno mlada nacionalna država još uvek nesigurna u pogledu svog suvereniteta, te stoga snažnije posvećena suverenom pristupu upravljanja internetom” (2015: 115).

Prvi razlog Noceti obrazlaže željom za državnom kontrolom novih komunikacionih kanala onako kako država to čini sa tradicionalnim medijskim sistemom, i nelagodom koju izazivaju novi načini informisanja, a koji sistemom disintermedijacije zaobilaze tradicionalne kanale i prkose kontroli i cenzuri. Potonji razlog Noceti (Nocetti, 2015) objašnjava tradicionalnim odnosom Rusije prema kategorijama suverenosti. Naime, ruska država svoju percepciju suverenosti preliva i u sajber prostor i, iscrtavajući virtuelne nacionalne granice, zahteva isti nivo kontrole i suverenosti kao što je to slučaj sa fizičkim svetom.

6.5. Modeli državnog upravljanja internet prostorom

Zadatak ovog poglavlja jeste predstavljanje mogućih modela državnog upravljanja internetom, definisanih na osnovu pregleda istraživanja u oblasti internet slobode pojedinih zemalja. Okvir za klasifikaciju modela kreiran je na osnovu sekundarne analize podataka za četiri zemlje zastupnice različitih medijskih sistema, te se ne može smatrati sveoubuhvatnim i celovitim. Pored ovoga, on može predstavljati osnovu za dalje analize upravljanja internetom u različitim sistemima i za izradu sveobuhvatnijih teorijskih ili empirijskih klasifikacija.

U ovom delu rada korišćeni su prevashodno rezultati istraživanja koje je sproveo Fridom haus, a koji je kao nevladina organizacija analizirao zemlje sa aspekta internet sloboda, odnosno ocenjivao njihov odnos prema internet pravima i slobodi. Njihova analiza odabrana je jer je, sa jedne strane, u trenutku pisanja ovog rada bila najnovija, sprovedena 2018. godine, i sa druge strane, obuhvata slične kriterijume koji su bili upotrebljeni i pri analizi Srbije u tom kontekstu (analiza reglatornog okvira, analiza kontkretnih primera primena zakona, analiza primera iz prakse, narušavanje prava korisnika i slično).

Kada je reč o zemljama odabranim za analizu, odabir je pratio klasifikaciju medijskih sistema Halina i Manćinija, odnosno uključena je po jedna zemlja za svaki od njihovih modela: liberalni (SAD), demokratsko-korporativni (Nemačka) i mediteranski model (Francuska), pri čemu je pretpostavljeno da će odnos prema internet komunikaciji pratiti odnos prema tradicionalnim medijskim sistemima. Pretpostavljeno je sledeće: 1) da će liberalna zemlja biti najotvorenija prema internetu komunikaciji i negovati slobodu izražavanja onlajn; 2) da će u zemlji demokratsko-korporativnog modela biti uočena jaka uloga države u vidu regulacije, ali i dominacija internet slobode; 3) da će primer mediteranske zemlje pokazati da se jaka uloga države i negativne posledice po slobodnu komunikaciju i informisanje u tradicionalnom medijskom sistemu odražavaju i na internet prostor. Prateći argument da će pristup internetu u postsovjetskoj zemlji dati dobar okvir za poređenje sa odnosom prema internet slobodama u razvijenim demokratijama, u analizu je uključena i Rusija.

Nakon završenog pregleda odabranih zemalja, pojedine pretpostavke pokazale su se većinski istinitim – pre svega, utvrđeno je da će odnos prema tradicionalnom medijskom sistemu imati jak uticaj na odnos države prema internet komunikaciji, ili, da će istorijski i društveno-politički kontekst analizirane zemlje imati presudan uticaj na internet slobodu. Međutim, postoje i brojni primeri iz analiziranih zemalja koji izlaze iz unapred ustaljenih obrazaca i navode na dodatno promišljanje o pitanju: Šta je to što definiše odnos prema internetu u nekoj zemlji? Da li je *put zavisnosti* zaista toliko važan (North, 1990, prema Hallin & Manicini, 2004: 12), ili se pak internet politike instant oblikuju, kao i da li su one vođene impulsima trenutnih izazova, poput terorizma, bezbednosti ili lažnih vesti?

U ovom potpoglavlju ponuđen je okvir za klasifikaciju modela državnog upravljanja internetom a ne kruta klasifikacija, delimično zato što je u stalno promenljivom svetu gotovo nemoguće pojedinačnim modelom obuhvatiti prirodu nekog sistema, a delimično zbog ograničenosti analize koja je obuhvatila sekundarnu istraživačku građu.

Pokušaj da se različiti pristupi pri upravljanju internetom obuhvate krutim klasifikacijama predstavlja izazov iz nekoliko razloga. Prvo, zbog prirode internet prostora, koji je nesaglediv i uključuje brojne izazove; drugo, zbog nemogućnosti da se bilo kojim mehanizmom obuhvate svi izazovi na internetu; treće, zbog mogućnosti svake države da gradi sopstvene mehanizme koji ne moraju biti slični čak ni onima u državama istog tipa; četvrto, jer svaki mehanizam koji funkcioniše danas već sutra može da bude zastareo i neprimenljiv.

Pri klasifikaciji modela, takođe, može se polaziti od brojnih i raznovrsnih kriterijuma. Ukoliko se, na primer, za kriterijum uzme generalni ***odnos prema internet slobodama***, koji isključuje senzitivne razlike i nacionalne specifičnosti, moglo bi se upasti u zamku hladnoratovskih podela, pri čemu bi se pristupi u upravljanju internetom mogli odrediti kao *autoritarni* ili *liberalni*. U tom slučaju, demokratske zemlje Zapadne Evrope i SAD bile bi okarakterisane kao liberalne, dok bi, na primer, Rusija, bila nedvosmileno ocenjena kao autoritarni model.

Iako je analiza zemalja predstavljena u prethodnom poglavlju obuhvatila namerni uzorak, jasno je da se i zemlje koje bi se mogle okarakterisati kao liberalni model, umnogome razlikuju kada je reč o odnosu prema internetu. Takođe, zemlje koje prepoznajemo kao autoritarne prema tipu vladanja primenjuju različite metode pri upravljanju svojim internet prostorom, te se ne mogu sve istovetno i jednostavno odrediti rečju – autoritarni. Bilo je reči o klasifikaciji Dajberta i Rohozinskog (2010), koji su prilikom analize odnosa prema internet slobodama kao merilo uzimali *vrstu kontrole nad sajber prostorom* koju države koriste (kontrola prve, druge i treće generacije). Autori su, u skladu sa primenom ovog identifikatora, autoritarne zemlje gradirali od onih koje koriste ogoljenu cenzuru (Turkmenistan) do onih koji koriste kombinaciju kontrola, na primer kombinaciju druge i treće generacije kontrole – perfidna kontrola, putem zastrašivanja i indukovanja autocenzorski mera (Rusija). Iako slične po uređenju, analizirane države su pokazale različite pristupe u kontroli internet prostora.

Dakle, jasno je da jednostavna podela na autoritarne i liberalne zemlje nije primenljiva kada je reč o odnosu država prema internetu, odnosno o državnom upravljanju internetom. Zemlje pretežno autoritarne prirode ili tipa vladanja međusobno se razlikuju u odnosu na mehanizme koje primenjuju pri upravljanju internet prostorom, a to neretko prelazi i u strogu kontrolu. Sa druge strane, ni demokratske zemlje ne možemo odrediti kao liberalne samo na osnovu njihovog opšteg odnosa prema slobodi izražavanja i pravima na internetu uopšte. Takođe, vredi istaći da ni demokratske zemlje nisu ostale imune na različite mehanizme kojima kontrolišu svoj internet prostor. Kako Radojković, Stojković i Vranješ primećuju: „SAD i Velika Britanija imaju alat uz pomoć kog mogu da stanu rame

uz rame sa Kinom, kada je reč o narušavanju ljudskih prava i sloboda u sajber prostoru" (Radojković, Stojković, Vranješ, 2015: 149).

Nacionalne države, bile one pretežno autoritarne ili demokratske, raspolažu istim mehanizmima pri upravljanju *svojim* internet prostorom – pitanje je jedino da li postoje razlike u razlozima i načinima primene. *Svoj internet prostor* je sintagma koja je možda bila nezamisliva u periodu ranog razvoja interneta i, sa ove vremenske distance moglo bi se reći, nezamisliva u pogledu iluzornih vizija o nekontrolisanoj „meži svih mreža". Možda je sada preciznije govoriti o „Mreži nacionalnih i ostalih mreža u svetu" (Radojković, Stojković, Vranješ, 2015: 179). Prerane prognoze da je besmisleno govoriti o nacionalnim modelima medijskih sistema, ili nacionalnim modelima upravljanja internetom, u vremenu koje dolazi, a koje će, pod uticajem globalizacije biti uniformo, sada gube na argumentaciji. Internet, čini se, umesto da sruši fizičke granice i uskrati državi deo suvereniteta, poslednjih godina čini upravo suprotno. Države, pa i one demokratske, sve više iskazuju tendenciju da ovladaju internet prostorom i stave mu nacionalne uzde. Trenutni period u upravljanju internet prostorom može se okarakterisati rečenicom: *Država uzvraća udarac*.

Ukoliko je odabrani kriterijum za analizu upravo ***uloga države***, analizirani sistemi mogu biti klasifikovani u odnosu na to kolika je i kakva uloga države u upravljanju internetom. U tom slučaju u Americi bi bila prepoznata *slaba uloga države*, u Nemačkoj i Francuskoj *izražena uloga države*, kojoj se ne podređuju ljudska prava, a u Rusija *dominatna uloga države*, kojoj su podređena ljudska prava. Međutim, iako dovoljno otvorena da obuhvati većinu država, ovakva klasifikacija, bazirana na ulozi države, ne govori dovoljno o specifičnostima pojedinačnih država.

Ukoliko najpre posmatramo samo tri zemlje razvijene demokratije, obuhvaćene ovom analizom, SAD, Nemačku i Francusku, primetićemo da one imaju mnoštvo zajedničkih karakteristika, kada je o odnosu prema internet slobodama reč, ali i brojne specifikume. Ono što je zajedničko za sve njih jeste permanetno traganje za uspostavljanjem ravnoteže između nekada suprotstavljenih principa, „kao što je osiguravanje bezbednosti i javne sigurnosti bez ograničavanja drugih demokratskih principa kao što su sloboda izražavanja i privatnost" (Wright & Breindl, 2013: 2). U analiziranim zemljama ova prava različito se vrednuju. Dok je u Americi sloboda izražavanja neprikosnovena, u Nemačkoj je to dostojanstvo u komunikaciji, odnosno sloboda izražavanja proteže se sve dokle ne vređa dostojanstvo drugog. U Americi se, s druge strane, dostojanstvo legitimno žrtvuje zarad slobode izražavanja, dok sve tri zemlje žrtvuju privatnost zarad bezbednosti, odnosno nadzora kao legitimnog sredstva u borbi protiv, pre svega, teorizma. Bez namere da se vrednosno poredi da li je pravo na dostojanstvo u komunikaciji Nemačke ili gotovo bezuslovno pravo slobode izražavanja Amerike vrednije zaštite, može se zaključiti da su zaštite ovih prava uslovljene tradicionalnim odnosom prema njima, ali i aktuelnim izazovima koje donosi komunikacija na internetu.

Naime, SAD ostaje verni predstavnik liberalnog modela i kada je o internetu reč. Sloboda izražavanja je, za razliku od Francuske i Nemačke, gotovo neprikosnoveno pravo i u virtuelnom prostoru – da je sloboda onlajn-izražavanja pod zaštitom Prvog amandmana potvrđeno je još 1997. godine (*Reno vs American Liberty Civic Union*). Jedan od najsvežijih primera pomoću koga se ilustruje koliko je slobodno izražavanje značajno u Americi jeste i presuda saveznog sudije da je Trampovo blokiranje korisnika Tvitera, koji su ga kritikovali, zapravo kršenje Prvog amandmana. Dakle, politika upravljanja internetom u Americi slobodu izražavanja postavlja kao tradicionalno najznačajniju, često je suprotstavljajući nekim drugim pravima. Pravo na privatnost u Americi nije na istom nivou značaja kao sloboda izražavanja. Pravo na privatnost često je podređeno pitanjima bezbednosti, kao što smo imali prilike da vidimo kroz brojne primere i zakone. Odnosno, pravo na privatnost je sekundarno onda kada je bezbednost građana u pitanju, te je tada je nadzor opravdan – legitiman i legalan.

U Nemačkoj je, sa druge strane, pitanje dostojanstva u komunikaciji pitanje od neprikosnovenog značaja. Nemačka će rizikovati da ugrozi slobodu izražavanja, ako je cena očuvanje dostojanstva u komunikaciji, odnosno sprečavanje govora mržnje. Demokratsko-korporativna priroda nemačkog medijskog sistema ima uticaj i na odnos prema internet komunikaciji. Primetna je jaka uloga države u upravljanju onlajn-prostorom, kao i težnja ka jačoj regulaciji internet sadržaja. Međutim, uprkos jakoj ulozi države i rigoroznim zakonima, Nemačka ostaje slobodna po pitanju internet sloboda.

Francuska, sa druge strane, najveću pažnju posvećuje bezbednosti, odnosno sprečavanju terorističkog organizovanja i širenja terorističke propagande onlajn, makar to ugrozilo oba: i slobodu izražavanja i privatnost. U mediteranskom duhu, predsednik Makron ne skriva namere da će država u budućnosti imati jaču ulogu i otvoreno poziva na jaču regulaciju internet prostora. Moglo bi se zaključiti da pitanja bezbednosti imaju dominantu poziciju pri izgradnji odnosa prema internet upravljanju u Francuskoj.

Rusija, drugačija od svih ostalih analiziranih zemalja, svoj odnos prema internet pravima pokazuje nedvosmisleno, kroz regulatorni mehanizam. Etatistička priroda vidljiva u svakom zakonu i navedenom primeru oslikava njen odnos prema internet komunikaciji. Dva posmatrana prava, sloboda izražavanja i privatnost, ostaju nisko na lestvici prioriteta, ukoliko se proceni da ugrožavaju pitanja od „nacionalnog značaja".

Primetno je da svaka od država predstavljenih u radu, svoj odnos prema internetu gradi u odnosu na jednu od kategorija: sloboda, dostojanstvo, bezbednost/nadzor i država. U skladu sa tim, a na osnovu pregleda literature i analize organizacije Fridom haus, identifikovane su ***četiri intervenišuće varijable***:

- ***sloboda u internet komunikaciji***
- ***dostojanstvo u komunikaciji na internetu,***
- ***bezbednost internet korisnika kroz nadzor*** **i**
- ***etatizam***.

Navedene varijable pokazale su nedvosmisleni uticaj na to *kakav će stav zauzeti država prema upravljanju svojim internet prostorom*, i uže, gde će se na lestvici prioriteta naći dva analizirana prava – sloboda izražavanja i pravo na privatnost.

Sve navedene varijable posledica su jednog od dva momenta, ili predstavljaju njihovu sinergiju: *istorijskog* i *aktuelnog*. Naime, etatizam u Rusiji, dostojanstvo u komunikaciji u Nemačkoj i sloboda komunikacije u Americi nedvosmisleno su se iz tradicionalnih sistema prelile i u onlajn, dok je bezbednost u internet komunikaciji kroz nadzor pre instant reakcija na aktuelne događaje negoli istorijski uslovljena, kao što smo videli na primeru Francuske. Međutim, svaka od varijabli odražava se na onlajn-komunikaciju u sadašnjosti, te je delimično uvek uslovljena aktuelnim izazovima u internet prostoru.

Većina definisanih varijabli može se prepoznati u politikama upravljanja internetom u svim analiziranim zemljama. Sloboda u komunikaciji, odnosno sloboda izražavanja svakako je ustavom zagarantovana u svim demokratskim zemljama, ali je razlika u tome da li ovo pravo neprikosnoveno ili se ipak ugrožava ukoliko mu se suprotstavi pravo koje je prioritetnije. Takođe, bezbednost u

komunikaciji deo je svih analiziranih politika interneta, ali se može tumačiti dvojako u zavisnosti od toga kojim se mehanizmima ostvaruje: da li je nadzor legalan i opravdan ili pak zloupotrebljen.

Dostojanstvo u komunikaciji istorijski je povezano sa Nemačkom, ali je isto tako visoko prioritetno i u francuskom modelu upravljanja internetom. Kada je reč o etatizmu, može mu se pristupiti na više načina, ali u ovoj analizi određen je kao povinovanje svih društvenih odnosa, između ostalih i komunikacije, državi. Tako posmatrana ova varijabla gotovo je isključivo prepoznata u Rusiji, premda se u nekim primerima može videti i u demokratskim zemljama koje regulatornim mehanizmima štite „pitanja od nacionalnog značaja", a koja su ponekad nejasno definsana i sklona zloupotrebi.

Na osnovu svega navedenog, modeli državnog upravljanja internetom mogu se definisati u odnosnu na kriterijum – *dominantne intervenišuće varijable* u određenoj zemlji. Već je istaknuto da su sve varijable u većoj ili manjoj meri prepoznate u svim zemljama, ali isto tako se u svakoj od zemalja jedna intervenišuća varijabla iskristalisala kao dominantna. Pretpostavlja se da će dominatna varijabla imati veliki uticaj na sveukupnu izgradnju nacionalne politike internet upravljanja u određenoj zemlji.

U SAD dominatna intervenišuća varijabla jeste *sloboda u internet komunikaciji*, i, iako je bezbednost/nadzor takođe visoko kotirana, etatizam je tradicionalno hijerarhijski najmanje značajan (Grafikon 12).

Grafikon 12 Intervenišuće varijable u internet upravljanju – SAD

S obzirom na hijerahijski prikaz intervenišućih varijabli, moglo bi da se zaključi da je sloboda izražavanja, kao jedno od analiziranih prava, ostala najznačajnije pravo i u onlajn-komunikaciji. O ovome svedoči i zaštita onlajn-izražavanja Prvim amandmanom, ali i presude kojima je pravo na slobodno izražavanje na internetu bilo odbranjeno čak i kada je tužena strana bio predsednik Amerike. Na ovakav odnos prema slobodi izražavanja uticaj pre svega ima tradicionalni odnos SAD prema ovom pravu.

Ipak, visoko na hijerarhijskoj lestvici pozicioniran je nadzor internet komunikacije od strane države, koji je, između ostalog, posledica antiterorističke strategije. S obzirom na široku primenu različitih mehanizama za praćenje internet komunikacije korisnika, kao i na česte kritike upućene na račun legitimnosti i zakonitosti ovih mehanizama, nadzor je isto tako mogao biti pozicioniran kao dominantna varijabla. Međutim, prednost je u ovom slučaju data slobodi u komunikaciji, jer je u poređenju sa drugim analiziranim zemljama ova varijabla bila najizraženija u Americi. Varijable kao

što su dostojanstvo u komunikaciji i etatizam zanemarljive su na primeru Amerike, posebno ukoliko uporedimo njihov značaj u drugim analiziranim zemljama.

Dakle, sloboda izražavanja ostaje prioritetno pravo u onlajn-komunikaciji u Americi, dok na pravo na privatnost utiče visoko pozicionirana varijabla nadzora/bezbednosti. Drugim rečima, ukoliko je, prema bezbednosnim procenama, nadzor neophodan mehanizam za praćenje, na primer, potencijalnih terorističkih akcija, pravo na privatnost postaje ništavno. O tome svedoče i ranije navedeni primeri povrede ovog prava, čak i onda kada je primena takvog mehanizma bila zloupotrebljena, iako pravdana argumentom bezbednosti.

Ovaj model državnog upravljanja internetom nazvan je ***liberalni model upravljanja internetom.*** Naziv je usaglašen sa nazivom tradicionalnog medijskog sistema SAD, koji su ponudili Halin i Manćini. Argument za takav odabir, odnosno usaglašavanje naziva, nalazi se u činjenici da se komunikaciona politika dominatna u SAD iz tradicionalnog sistema prelila i u onlajn-sferu, pa su sloboda izražavanja i dominacija privatnih aktera, uz ograničenu ulogu države, ostali stožer u izgradnji politike upravljanja internetom.

Za razliku od Amerike, u Nemačkoj je dominatna intervenišuća varijabla *dostojanstvo u komunikaciji*, koja je direktno uticala i na usvajanje kontroverznog Zakona o Fejsbuku. Ova varijabla deluje gotovo istovremeno sa drugopozicioniranom varijablom bezbednosti/nadzora, jer je preduslov obezbeđivanja dostojanstvene komunikacije, odnosno brobe protiv govora mržnje, praćenje internet komunikacije (Grafikon 13).

Grafikon 13 Intervenišuće varijable u internet upravljanju – Nemačka

Sloboda u komunikaciji na internetu, kao trećepozicionirana, ne sugeriše da je internet prostor u Nemačkoj zatvoren ili autoritarno uređen, već oslikava odnos između intervenišuće varijable – dostojanstva u komunikaciji, i ostalih varijabli. U slučaju Nemačke, u borbi protiv govora mržnje i u težnji za dostojanstvenom komunikacijom na internetu, sloboda u komunikaciji gubi na prioritetu. Dakle, intervenišuća varijabla utiče direktno na pozicioniranje prava na slobodno izražavanje, uslovljavajući ga komunikacijom koja je dostojanstvena.

S obzirom na to da je nadzor takođe visokopozicioniran, dovodi se u pitanje i poštovanje prava na privatnost na mreži. Međutim, tradicionalno je pravo na privatnost u evropskim zemljama, pa i u Nemačkoj, pravo od značaja. Za razliku od, na primer, SAD, u Nemačkoj je pravo na privatnost

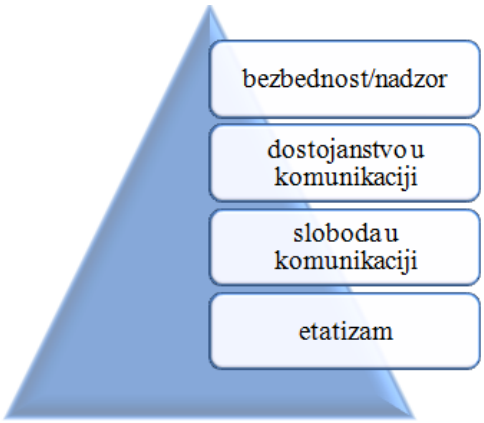
zaštićeno strožom regulacijom, na nivou EU, ali i nacionalnim zakonodavstvom. Međutim, brojni su primeri, o kojima je bilo reči, kojima je i Nemačka pokazala težnju za neosnovanim nadzorom nad onlajn podacima-korisnika i komunikacijom na internetu.

Ipak, ukoliko se vodimo utvrđenom hijerahijom varijabli, sloboda izražavanja niža je na listi prioriteta od prava na privatnost jer je dostojanstvo u komunikaciji, koje ugrožava slobodu izražavanja, intervenišuća varijabla i ima snažniji uticaj od varijable bezbednosti/nadzora, koja potencijalno ugrožava pravo na privatnost.

Etatizam je marginalna varijabla ukoliko joj, kako smo to već predočili, pristupimo kao negativnoj praksi podređivanja svih društvenih odnosa državi. Međutim, iako poslednja u hijerarhiji, ona ima daleko veći uticaj u Nemačkoj nego što je to bio slučaj sa Amerikom. Kada ovu varijablu sagledamo šire, u kontekstu uloge države u upravljanju internet prostorom, Nemačka poslednjih godina pokazuje sve izraženiju tendenciju da državu pozicionira kao cetralnog aktera u upravljanju internet prostorom, što se ogleda i kroz brojne primere novousvojenih zakona kojima se reguliše internet komunikacija.

Francuska je slična Nemačkoj u pogledu odnosa prema internet upravljanju. U obe zemlje jača težnja za većom regulacijom, iako je u oba slučaja etatizam poslednji u hijerarhiji varijabli zbog već obrazloženih argumenata.

Sa druge strane, za razliku od Nemačke, u Francuskoj je *bezbednost/nadzor* dominantna intervenišuća varijabla pri upravljanju internet prostorom, dok je dostojanstvo u komunikaciji, odnosno sprečavanje govora mržnje, takođe tradicionalno značajna varijabla (Grafikon 14).



Grafikon 14 Intervenišuće varijable u internet upravljanju - Francuska

Na osnovu analize internet upravljanja u Francuskoj, nadzor nad internet komunikacijom sa ciljem sprečavanja terorističkog organizovanja iskristalisao se kao dominantan. Međutim, osim ove varijable, koja je određena kao dominantna, dostojanstvo u komunikaciji takođe je značajna varijabla. Potonja varijabla, ovde shvaćena u širem kontekstu, značajna je jer se odnosi i na filtriranje sadržaja koje slavi terorizam, podstiče na terorizam ili na bilo koji drugi način promoviše terorizam, a ne samo na sprečavanje govora mržnje u užem smislu, kako je to slučaj sa Nemačkom.

U odnosu na to koja je dominatna intervenišuća varijabla može se zaključiti da su sloboda izražavanja i pravo na privatnost podređene bezbednosti – odnosno da ih ugrožava nadzor nad internet komunikacijama. Ovome dodatno doprinosi i odbrana dostojanstvene komunikacije kojom se filtrira neželjen sadržaj koji na bilo koji način promoviše nacističku ideologiju ili terorističke akcije, kao što je to bio slučaj sa aktivistkinjom i političarem, osuđenim na uslovnu, odnosno zatvorsku kaznu, zbog komentara na društvenim mrežama.

Francuska kao demokratska zemlja, sa mediteranskim korenima, iskazuje pretenzije ka jačoj regulaciji internet prostora, odnosno ka aktivnijem učešću države u upravljanju komunikacijom na internetu. Istorijski uticaj ogleda se u borbi za dostojanstvenu komunikaciju i u sprečavanju govora mržnje regulatornim mehanizmima, dok se vođena aktuelnim impulsima antiterorističke strategije, fokusira na regulaciju korisničkog sadržaja kojim se terorizam podstiče i slavi. Kontroverzne odluke u ovoj oblasti, ilustrovane ranijim primerima, ukazuju da su sloboda izražavanja i pravo na privatnost podređene bezbednosnim pitanjima i sprečavanju govora mržnje.

Model državnog upravljanja internetom prepoznat u Nemačkoj i Francuskoj u ovom radu nazvan je ***balansirani model državnog upravljanja internetom.*** Slične po intenzitetu učešća države, ove dve zemlje iskazuju konstantnu težnju za uspostavljanjem balansa između poštovanja osnovnih prava internet korisnika, sa jedne strane, i pooštravanja regulalatornih mehanizama, sa druge, kojima se često zarad zaštite jednog ugrožava neko drugo pravo internet korisnika. Iako je u obema prepoznat balansirani model, Francuska i Nemačka razlikuju se u odnosu na to koje kategorije favorizuju pri izgradnji politike upravljanja internetom. Pri pokušaju uspostavljanja balansa među kategorijama koje su u ovom radu definisane kao intervenišuće varijable, u različitim sistemima prepoznaju se različiti načini pregovaranja, a ponekad i prevladavanja jedne nauštrb neke druge/ili drugih kategorija. U Francuskoj su, na primer, bezbednost kroz nadzor, kao dominatna varijabla, i poštovanje privatnosti internet korisnika u konstantnom odnosu prevladavanja, sa ciljem uspostavljanja balansa između ovih dveju kategorija. U Nemačkoj su, pak, dostojanstvo u komunikaciji, prepoznato kao intervenišuća varijabla, i pravo na slobodno izražavanje u stalnom odnosu pregovaranja i prevladavanja.

Za razliku od svih ostalih zemalja, koje su bile predmet analize, u Rusiji je dominantna intervenišuća varijabla *etatizam*. Odnosno, analizirana dva prava, sloboda izražavanja i pravo na privatnost, podređena su, pre svega, proceni da li je delovanje korisnika na internetu u skladu sa interesima države (Grafikon 15).

Grafikon 15 Intervenišuće varijable u internet upravljanju – Rusija

Bezbednost, tačnije nadzor, kojim bi se, kako se to u regulativnim aktima najčešće navodi, očuvala bezbednost u komunikaciji, sledeća je varijabla po značaju. Naime, praćenje internet komunikacije i sankcionisanje korisnika najčešće su u Rusiji u odnosu na ostale analizirane zemlje.

Težnja ka stvaranju zatvorenog internet prostora, ili onog što Krenikov i Kravčenko (Khrennikov&Kravchenko, 2019)[311] nazivaju „Putinovim internetom" po ugledu na Kinu, vidljiva je u svakom segmentu analize. Od regulatornih mehanizama, kojima se ozakonjuju različite vrste cenzure, filtriranja, blokiranja i nadzora, do čak nelegalnih praksi kojima se korsnicima interneta u Rusiji uskraćuje pravo na slobodno izražavanje ili narušava pravo na privatnost.

S obzirom na to da se državnim interesima podređuju svi ostali interesi, uključujući i interese internet korisnika kao građana Rusije, jasno je da su dva analizirana prava, sloboda izražavanja i pravo na privatnost, nisko na lestvici prioriteta. Premda su predočeni i primeri nadzora i narušavanja ovih prava korisnika i u demokratskim zemljama, ovde se pravi razlika između narušavanja prava kao konstante – stalnih praksi, koje su često i legalizovane, kakav je slučaj u Rusiji, i sporadičnih slučajava zloupotrebe regulatornih mehanizama – kakav je slučaj sa demokratskim zemljama.

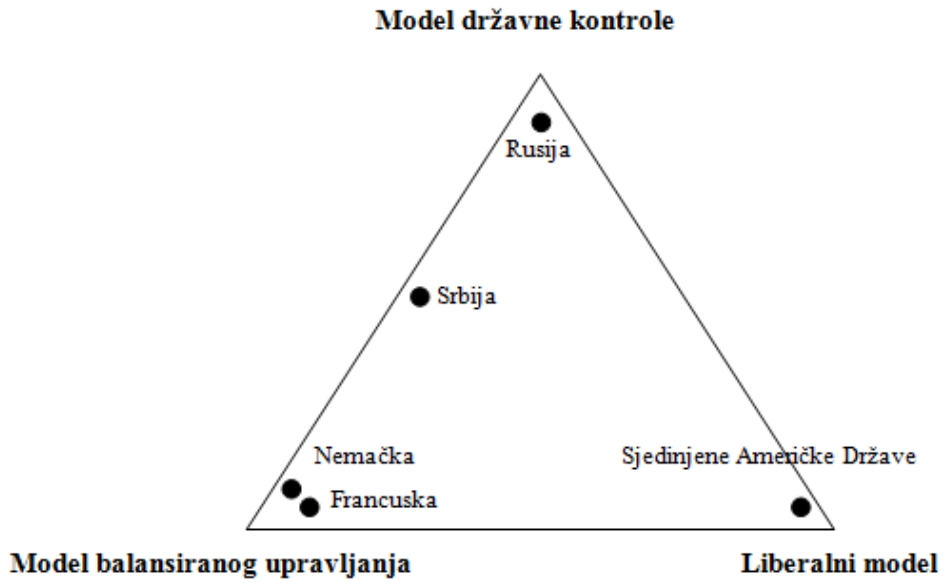
Zbg svega navedenog, model državnog upravljanja internetom u Rusiji u ovom radu nazvan je **model državne kontrole**.

***

Tri modela državnog upravljanja internetom – *model državne kontrole*, *model balansiranog upravljanja internetom* i *liberalni model*, definisana u ovom radu, samo u teorijskom smislu mogu biti isključivi. Međutim, u praksi se države češće služe kombinacijom navedenih modela, koji se mogu pozicionirati kao bliži nekom od modela ili između dva modela, s tim što mogu biti bliži ili dalji od drugih modela upravljanja. Za grafički prikaz takvih odnosa država prema ponuđenim modelima u ovom radu preuzet je model prikaza koji su koristili Halin i Manćini pri pozicioniranju različitih zemalja u odnosu na modele medijskih sistema koje su definisali (Grafikon 16)[312].

[311] Khrennikov&Kravchenko (5 May 2019). Putin Wants What China's Xi Already Has: His Own Internet. The Moscow Times: https://www.themoscowtimes.com/2019/03/05/putin-wants-what-chinas-xi-already-has-his-own-internet-a64707 (pristupljeno: 08. 05. 2019).

[312] Pozicionirane su samo one države koje su bile predmet analize u ovom radu. Kao što je već navedeno, Rusija je najbliža modelu državne kontrole, SAD liberalnom modelu, dok su Nemačka i Francuska najbliže modelu balansiranog upravljanja internetom.



Grafikon 16 Odnos pojedinačnih slučajeva prema trima modelima državnog upravljanja internetom (prikaz inspirisan prikazom Halina i Mańcinija, 2004: 70).

U ovom delu uvedena je i Srbija, jer je njen odnos prema internetu detaljno analiziran u trećem poglavlju disertacije. Na osnovu analize predstavljene u tom delu rada, može se zaključiti da je ona pozicionirana između balansiranog modela upravljanja internetom i modela državne kontrole. Naime, Srbija tradicionalno nije bliska liberalnim modelima, što je analiza sprovedena u disertaciji i potvrdila. Kao zemlja kandidat za članstvo u EU, Srbija pokazuje sličnost sa balansiranim modelima. Pri upravljanju svojim internet prostorom, Srbija, sa jedne strane, teži da uspostavi ravnotežu između poštovanja prava internet korisnika i ispuni EU standarde, dok, sa druge strane, Srbija iskazuje težnju da očuva mehanizame kontrole nad internet prostorom. Međutim, kao što su rezultati analize regulatornog okvira Srbije u oblasti upravljanja internetom pokazali, iako usvaja zakone po preporuci EU, Srbija često koristi mehanizme kontrole, i to kroz nadzor i krivično gonjenje svojih građana, čime im ugrožava i privatnost i slobodu izražavanja. Ovakvi postupci čine je bliskom modelu državne kontrole upravljanja internetom.

S obzirom na to da pokazuje karakteristike oba modela, i balansiranog upravljanja i državne kontrole, Srbija je pozicionirana između ova dva modela državnog upravljanja internetom, kao što je prikazano u Grafikonu 16.

6.6. Ka novom modelu upravljanja internetom

Mit o internetu bez granica je razbijen. Sama činjenica da države imaju tehničke mogućnosti da upravljaju internet prostorom već dovoljno govori u prilog prethodno navedenoj tezi. Kako navode Radojković, Stojković i Vranješ: „Internet može takođe biti kontrolisan kako od strane autoritarnih vlada tako i od nekih koje sebe nazivaju demokratskim" (Radojković, Stojković, Vranješ, 2015: 166). Ono o čemu možemo polemisati jeste u kojoj meri, na koje načine i sa kakvim motivima države koriste takve mehanizme kontrole.

Jasno je da će demokratske i autoritarne vlade imati drugačiji pristup internet upravljanju. Dok kod autoritarnih vlada možemo da vidimo primere korišćenja ogoljene cenzure i blokiranja pristupa, demokratske države koriste sofisticiranije metode u kontrolisanju protoka informacija na internetu. Kako Rajt i Brajndl (Wright & Breindl) navode: „Filtriranje je novi politički alat liberalnih demokratija, i sve više postaje globalna norma za isticanje državnog suvereniteta onlajn" (2013: 2).

Međutim, ne može se ni privatnim kompanijama oduzeti značaj jer one su te koje tvore internet prostor. Iako gotovo svi primeri navedeni u radu oslikavaju odnos koji bi mogao biti opisan kao borba za dominantni položaj na mreži između država i privatnih kompanija, ovaj rad zagovara stanovište po kojem je kooperacija u upravljanju internetom ključ stvaranja funkcionalnog sajber prostora.

Uzimajući u obzir najznačajnije aktere i njihove uloge u sjaber prostoru, zadatak ovog poglavlja jeste da ponudi model koji bi predstavljao jednu vrstu ideal-tipskog modela upravljanja internetom.

Modeli su značajna alatka u teorijskom promatranju – „Model pokazuje funkcionisanje sistema na nivou njegovih teorijskih postavki, znači, nezavisno od konkretnih okolnosti koje mogu u bilo kojoj meri da ih dovedu u pitanje" (Radojković, Stojković, 2004: 29). Pored ovoga, kako Radojković i Stojković navode (2004), modeli nam pomažu da ukažemo na zajedničke karakteristike sistema, da na hipotetičkom nivou istražujemo kako on funkcioniše, te da prikažemo rezultate do kojih smo došli na jednostavan način.

Klasifikacije modela, međutim, mogu često navesti na pogrešan smer. Mnogobrojni su pokušaji klasifikovanja medijskih sistema kojima su zamerani normativni karakter, izostanak empirije, te hladnoratovska dihotomija (Kleinsteuber & Thomass, 2010). Komparativni pristup, kakav je i Halinov i Manćinijev, pak, zahteva empiriju, rad na terenu, iscrpna istraživanja i materijal. Zbog toga, ponuđeni model upravljanja internetom dat u ovome radu ne pretenduje da bude primenljiv na sve okolnosti, u svakom trenutku, već da prikaže najznačajnije aktere i njihove međusobne odnose u različitim okolnostima.

Model upravljanja internetom, koji će biti predstavljen u nastavku, uključuje primere dobre prakse, dok teži da negativne prakse svede na minimum. Iako ideal-tipski modeli nikada ne mogu u potpunosti da ostvare svoju praktičnu primenu, postojanje ovakvih modela, makar i samo u teorijskom smislu, značajno je iz najmanje dva razloga. Prvo, jer imaju ulogu uzora na koji se mogu ugledati modeli u nastajanju. Drugo, jer mogu biti jedna vrsta korektora postojećim sistemima.

Pri konstituisanju modela uzeta je u obzir uloga tri aktera, odnosno zainteresovanih strana, koji su centralna tema ove disertacije: *država*, *privatni akteri* i *korisnici*, te kategorija koja se u sva tri slučaja nametnula kao nezaobilazna – *odgovornost*.

Naime, kada je u trećem poglavlju razmatrana ulogu države u upravljanju internetom i zaštiti prava korisnika, zaključak je, ukratko, bio sledeći: *regulacija je moguća, nije nužno negativna, ali mora biti odgovorna*. Odgovornost države odnosi se na odgovornost prema, pre svega, internet korisnicima, njenim građanima, i tada se ogleda u zaštiti prava korisnika kroz regulatorne mehanizme; ali i na odgovornost prema privatnim akterima, i tada se odgovornost ogleda u delu kada ih država aktivno uključuje u izgradnju komunikacione politike, uzimajući u obzir i tržišna pravila.

Zagovornici odgovornosti privatnih aktera, internet intermedijatora, sve su glasniji poslednjih godina. U četvrtom poglavlju, pri analizi njihove uloge u internet upravljanju, izveden je sledeći zaključak: *privatni akteri, pored države, imaju dominatnu poziciju u internet prostoru, njihova komercijalna priroda ne može biti zanemarena, ali ih to ne oslobađa od odgovornosti, koja se najjasnije uočava u njihovim samoregulatornim politikama*. I njihova odgovornost je dvojaka. Sa jedne strane, ona podrazumeva odgovornost prema krajnjim korisnicima njihovih usluga, dok se, sa druge strane, naročito poslednjih godina, uočava trend sve izraženije odgovornosti privatnih aktera u odnosu prema državama na čijim teritorijama pružaju svoje usluge, odnosno odgovorno poslovanje kroz poštovanje nacionalnih zakona.

Istraživanje o internet korisnicima, predstavljeno u petom poglavlju, pokazalo je sledeće: *internet korisnici su svesni potencijalnih opasnosti na internetu, ali ne čine dovoljno da se zaštite u sajber prostoru, pokazujući tako nizak stepen individualne odgovornosti*. Odgovornost korisnika možda je i najkompleksnija jer se može tumačiti iz više uglova. Pod individualnom odgovornošću podrazumeva se, pre svega: 1) odgovornost prema sebi, odnosno preduzimanje svih dostupnih mera da se zaštite prilikom korišćenja usluga privatnih kompanija, 2) odgovornost prema drugim korisnicima, odnosno poštovanje prava drugih internet korisnika, 3) odgovornost prema privatnim kompanijama, kroz poštovanje „pravila ponašanja" na koje su pristali prihvatanjem uslova korišćenja, i 4) odgovornost prema državi, odnosno poštovanje zakonskih odredbi koje se odnose na internet komunikaciju.

Odgovornost je dakle centralni koncept ponuđenog ideal-tipskog modela. Odabiru ovog koncepta može se zameriti njegova fluidnost i nemogućnost jednoznačnog određenja, ali to isto može da se tumači i kao njegova prednost. Naime, koncept odgovornosti dovoljno je fleksibilan i višeznačan, i kao takav primenljiv na različite aspekte u internet komunikaciji i na sve aktere koji u tom procesu učestvuju.

Model predložen u ovoj disertaciji nazvan je ***model cirkularne odgovornosti upravljanja internetom*** (Grafikon 17)

Grafikon 17 Model cirkularne odgovornosti upravljanja internetom

Prikazani model podrazumeva cirkularnu odgovornost, odnosno – svi akteri u ovom procesu upućeni su jedni na druge, dok je centralni koncept odgovornosti ono što osigurava uspešnu interakciju između njih. Ukoliko samo jedna karika popusti, dolazi do disbalansa. Ukoliko bi država, na primer, otkazala odgovornost u odnosu prema korisnicima, koristila bi svoje mehanizme da im naruši prava na internetu, umesto da ih pospešuje i štiti. Ukoliko država nema odgovoran odnos prema privatnim akterima, postoji potencijalna opasnost od narušavanja koncepta kooperacije i učešća privatnih aktera u odgovornom upravljanju internetom.

Ukoliko pak privatni akteri ne postupaju sa dužnom odgovornošću prema krajnjim korisnicima, ugrožavaju njihova prava i urušavaju sam koncept cirukalrne odgovornosti. Privatni akteri mogu iskazati neodgovornost i prema državi na čijoj teritoriji pružaju svoje usluge, tako što ne bi poštovali „nacionalna pravila ponašanja" koja su deo njene regulative.

Korisnici, takođe, mogu ispoljiti neodgovornost na više načina: tako što neće biti odgovorni prema sebi, odnosno neće preduzeti mere zaštite onlajn; ili neće biti odgovorni u odnosu prema državi, odnosno neće poštovati njenu regulativu u ovoj oblasti, a mogu i da krše pravila ponašanja na koje su pristali prihvatanjem uslova korišćenja privatnih kompanija, narušavajući validnost tzv. elektronskog ugovora.

Jasno je da se u praksi često dešava narušavanje koncepta cirkularne odgovornosti. To je bilo obrazloženo i u svim prethodnim poglavljima, u kojima je odgovornost ova tri aktera detaljno analizirana. Cirkularni model, da bi nesmetano funkcionisao, podrazumeva istovremeno prisustvo odgovornosti sva tri aktera. Ukoliko jedna karika otkaže odgovornost, krug se prekida i dolazi do disbalansa.

Ovaj funkcionalistički model, dakle, nedvosmisleno teži održavanju ravnoteže. Međutim, on nije statičan, kao ni okruženje koje opisuje. Dinamika je sastavni deo njegovog funkcionisanja. Korisnici, država i privatni akteri međusobno se kontrolišu, opominju jedni druge ukoliko nečija odgovornost zakaže, a zatim se sistem regeneriše, i uspostavlja na novom nivou. Kritikovan manjak odgovornosti privatnih aktera kada je reč o zaštiti ličnih podataka korisnika, na primer, doveo je do usvajanja različitih vrsta regulatornih mehanizama kojima se podaci korisnika štite, što je uslovilo privatne aktere da u skladu sa novonastalom situacijom menjaju svoje samoregulatorne politike.

Odgovornost je i pri ovoj promeni imala centralnu ulogu, uslovljavajući model da se izgradi na složenijom nivou, koji je sada uključio dodatne regulatorne i samoregulatorne mehanizme.

Trebalo bi istaći, takođe, da nemaju svi akteri isti položaj u različitim sistemima. Korisnicima je u predloženom modelu dodeljen povlašćeni položaj u odnosu na ostale aktere, jer bi se stepen uspešnosti modela mogao meriti, pre svega, odgovornim odnosom države i privatnih aktera prema korisnicima. Kada je o dva preostala aktera reč, njihov uticaj razlikuje se u različitim sistemima. Tako su, na primer, u Americi privatni akteri dominatniji, a uloga države slabija, dok u ostalim zemljama država ima izraženiji uticaj – naročito u Rusiji, gde je položaj države dominatan.

Model cirkularne odgovornosti može da trpi dominaciju države ili privatnih aktera u meri u kojoj se ona ne odražava negativno na korisnike. Model ostaje funkcionalan u sistemima gde je izražena uloga države imala za cilj da regulacijom pospeši prava korisnika, kao što je to slučaj sa Nemačkom i Francuskom. Ovaj model cirkularne odgovornosti sa izraženom ulogom države nazvan je – ***tip A*** (Grafikon 18). Sa druge strane, izraženiji uticaj privatnih aktera, koji većinski ne narušava prava korisnika, prepoznat u Americi, nazvan je ***model cirkularne odgovornosti – tip B*** (Grafikon 19).

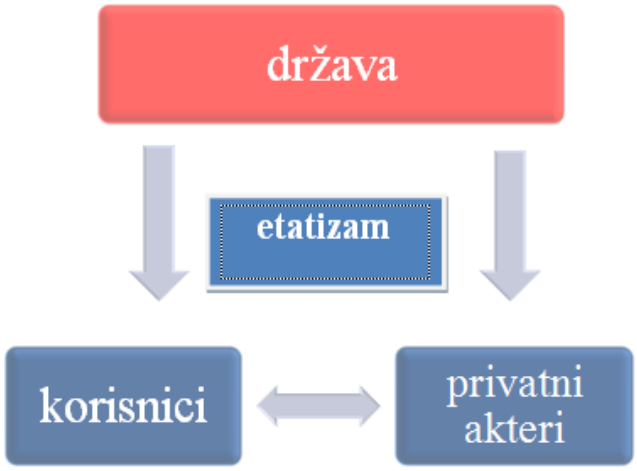
Grafikon 18 Model cirkularne odgovornosti - tip A

Grafikon 19 Model cirkularne odgovornosti - tip B

Dakle, model može ostati nenarušen, ukoliko je odgovornost zadržana kao centralni koncept. U prvom slučaju, tipom A ovog modela opisuju se odnosi u sistemima u kojima je vidljiv uticaj regulacije interneta – država ima značajnu ulogu, ali internet prostor ostaje slobodan, a korisnici i odgovornost prema njima, u najvećem broju slučajeva, zadržavaju svoju značajnu poziciju (Nemačka i Francuska).

Takođe, tip B ovog modela pokazuje izraženu ulogu jednog od aktera, u ovom slučaju privatnih kompanija, ali je, kao i kod tipa A, odgovornost centralna, a korisnici i njihova prava, u najvećem broju slučajeva, ne gube na značaju. Cirkularni model, dakle, još uvek ima svoju primenu i uspeva da funkcioniše, balansirajući nešto drugačije odnose u poređenju sa ideal-tipskim modelom (Sjedinjene Američke Države).

Ukoliko je, međutim, uloga jednog od ova dva aktera prenaglašena do mere koja podrazumeva dominantni položaj, potiskujući korisnike sa povlašćene pozicije, dok kategoriju odgovornosti menja interesnim konceptima, model se urušava. Za ilustraciju ovog modela može se upotrebiti primer Rusije. U tom slučaju država bi bila centralni akter, a etatizam ključni koncept (Grafikon 20). Ovo je primer narušavanja balansa ideal-tipskog modela cirkularne odgovornosti upravljanja internetom koji je nazvan ***etatistički model upravljanja internetom***.



Grafikon 20 Etatistički model upravljanja internetom

Narušavanja ravnoteže podrazumevala bi pozicioniranje privatnih aktera kao centralnih, dok bi ključni koncept odgovornosti bio smenjen konceptom komercijalne isplativosti (Grafikon 21). Ovaj model nazvan je ***komercijalnim modelom upravljanja internetom***.

Grafikon 21 Komercijalni model upravljanja internetom

Primeri komercijalnog modela, kao disbalansa ideal-tipskog modela, mogu se često videti u pojedinačnim situacijama u svim liberalnim zemljama. U Americi, na primer, kao predstavniku liberalnih sistema, čija se politika upravljanja internetom bazira većinski na samoregulaciji, česti su primeri dominacije privatnih kompanija u internet upravljanju. Najsvežiji primer jeste afera Kembridž analitika, koja je reaktivirala pitanja odgovornosti privatnih kompanija. Borba Amerike da uspostavi

balans i vrati sistem u ravnotežu ogledala se u saslušanju čelnika privatne kompanije pred Kongresom. Dakle, disbalans u upravljanju inicirao je aktivnije učešće države koja se poslužila ključnim konceptom, konceptom odgovornosti prema korisnicima.

Oba tipa disbalansa modela cirkularne odgovornosti, etatistički model i komercijalni model, mogu biti privremeni ili se mogu ustaliti kao trajni modeli upravljanja internetom. Njihove karakteristike mogu se gotovo svakodnevno uočavati u različitim sistemima. Prema kriterijumu vremena potrebnog da se disbalans ukloni, odnosno da se sistem vrati u stanje koje smo definisali kroz idela-tipski model cirkularne odgovornosti, disbalansi mogu biti:

(a) ***kratkotrajni sa kratkim efektom*** – sistem se vraća u ravnotežu gotovo neprimetno. Primeri ovakvog tipa disbalansa često nisu javno vidljivi, jer njihov značaj ne zavređuje medijsko pokrivanje. Možemo ih prepoznati kroz, na primer, prakse međusobnog prijavljivanja korisnika, koje su posledica objavljivanja nepoželjnog sadržaja. Efekat je najčešće usko usmeren, ka jednom korisniku ili manjoj grupi korisnika, rešava se u predviđenom roku i ne ostavlja javno vidljive i dugotrajne efekte.

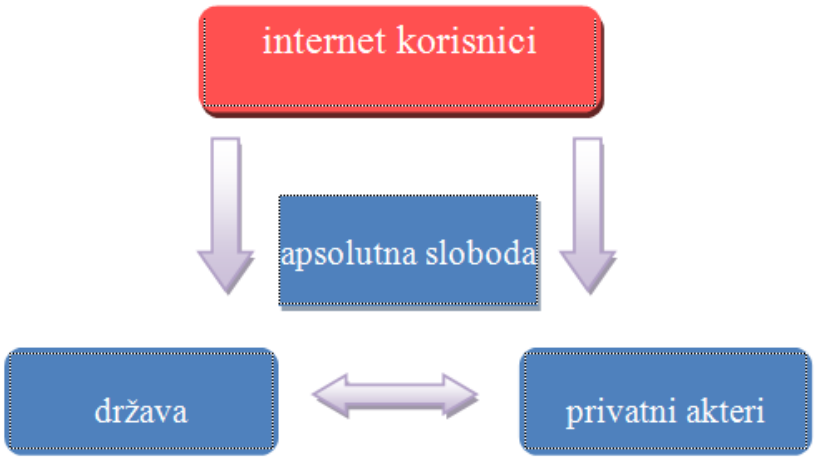
(b) ***kratkotrajni sa dugim efektom*** – posledice disbalansa vidljive su i nakon brzog vraćanja u ravnotežu. Kao primer ovakvog disbalansa možemo navesti aferu Kembridž analitika. Naime, disbalans koji je uslovilo neovlašćeno korišćenje ličnih podataka korisnika Fejsbuka izazvao je trenutnu reakciju, ali su posledice bile dugotrajne i ogledale su se u sudskim procesima, menjanju politike Fejsbuka, dok je efekat vidljiv i danas, kroz smanjeno poverenje korisnika u kompaniju Fejsbuk.

(c) ***dugotrajni sa potencijalom vraćanja u ravnotežu*** – disbalans dugo traje, ali se prepoznaje težnja za približivanjem modelu cirkularne odgovornosti. Primer ovog tipa disbalansa prepoznajemo kod država koje su u nedavnoj istoriji promenile svoje uređenje, te je izgradnja novog modela upravljanja komunikacionim sistemom složena i polarizovana između težnje za hvatanjem koraka sa zemljama razvijene demokratije i primene autoritarnih praksi. Takav slučaj može se prepoznati u Srbiji koja kao kandidat za članstvo u EU regulativu usklađuje sa evropskim standardom, ali istovremeno primenjuje i tradicionalne metode upravljanja komunikacionim procesima oflajn i onlajn.

(d) ***dugotrajni bez izgleda povratka u ravnotežu*** – disbalans traje toliko dugo da se prepoznaje kao permanetno stanje. Za islustraciju ovog tipa disbalansa možemo uzeti modele koji su još u svom začetku izgrađeni kao etatistički modeli – oni u kojima je država dominatni akter, a etatizam centralni koncept. Države u kojima prepoznajemo ovaj tip disbalnsa ne pokazuju težnju za uspostavljanjem ravnoteže između glavnih aktera u upravljanju internetom na način na koji smo je mi definisali. Mogu čak i da pokazuju težnju za što izraženijim disbalansom, jer je ono što mi prepoznajemo kao disbalans u takvim sistemima zapravo stanje ravnoteže, odnosno model upravljanja internetom trajno je etatistički.

Treći tip disbalansa ideal-tipskog modela cirkularne odgovornosti vidljiv je u pokušaju korisnika da ostvare najveću moguću slobodu pri korišćenju internet usluga, oslobađajući se od

regulatornih stega. Takav model je u radu nazvan ***model apsolutne slobode***, odnosno ***anarhični model*** (Grafikon 22).



Grafikon 22 Model apsolutne slobode/anarhični model

Ovaj model karakteriše se težnjom korisnika da stvore internet prostor koji će biti oslobođen od svake vrste autoriteta i vlasti i najčešće je prepoznat kao *deep web* ili *dark web*. *Deep web* je termin koji se koristi za: „označavanje sadržaja na internetu koji, iz različitih tehničkih razloga, ne indeksiraju pretraživači"; sa druge strane, *dark web* je: „deo *deep web*-a koji je namerno skriven i nedostupan putem standardnih veb pretraživača" (Chertoff & Simon, 2015: 1). Prema pojedinim podacima *deep web* je 500 puta veći od vidljivog veba (Baker & Baker, 2013, prema Chertoff & Simon, 2015).

Najpoznatiji pretraživač u okviru *deep web*-a jeste Tor (engl. *Tor*), koji svojim korisnicima nudi mogućnost anonimnog korišćenja internet usluga bez identifikovanja njihove lokacije. Ovakav način korišćenja interneta ima obe strane, i dobru i lošu. Naročito značajan za komunikaciju u autoritarnim režimima, *deep web* omogućava korisnicima da razmenjuju informacije bez mogućnosti ulaska u trag njihovim lokacijama i identitetu. U tom smislu ovakav vid komunikacije može da zaštiti novinare, zviždače, uzbinjavače i druge aktiviste u autoritarnim režimima. Sa druge strane, *deep web* je pogodan virtuelni prostor za različite kriminalne aktivnosti kao što su prodaja oružja i narkotika, širenje (dečje) pornografije, terorističko organizovanje i slično (Chertoff & Simon, 2015; Ghappour, 2017).

S obzirom na mogućnosti njegove primene, od izvorne ideje apsolutne slobode, odnosno prostora koji se samoreguliše, *deep web* se danas sve češće dovodi u vezu sa zloupotrebom slobode koja vodi anarhiji. Ovaj model je zbog toga i imenovan dvojako, kao model apsolutne slobode, odnosno anarhični model, u zavisnosti od toga u koje svrhe korisnici koriste slobodu.

Poslednji disbalans koji konstruiše treći model upravljanja internetom – anarhični, u ovom radu posmatra se kao poseban, odvojen od prva dva modela, jer se odnosi na potpuno drugi virtuelni prostor, izdvojen od vidljivog veba, a o kojem je kroz čitavu disertaciju bilo reči. Ipak, naveden je kao jedan od potencijalnih modela upravljanja internetom jer se nije mogla zanemariti činjenica da kao takav postoji i ima široke implikacije na internet komunikaciju u celini.

***

Predloženi ideal-tipski model cirkularne odgovornosti jeste dinamični model koji u osnovi teži da održi ravnotežu. Ravnoteža se održava samo kada je odgovornost centralni koncept. Dinamika predloženog modela ogleda se u mogućnosti stalne promene dominatnog aktera, čime se ne narušava ravnotežu dokle god te promene ne ugrožavaju prava korisnika. Ukoliko država ili privatni akteri postanu dominatni na način koji podređuje korisnike i koncept odgovornosti menja interesnim konceptima, dolazi do disbalansa predloženog modela. Disbalansi mogu biti privremeni ili trajni. Ukoliko su trajni, konstruišu nove modele: *etatistički, komercijalni* i *anarhični model upravljanja internetom*.

Kratkotrajni disbalansi, i sa kratkim i sa dugim efektom, česti su, a neki od njih su gotovo svakodnevni – oni mogu biti i korisni jer vode uspostavljanju nove ravnoteže, na višem nivou. Disbalansi mogu biti pak i dugotrajni, pa i permanentni, kada je teško govoriti o disbalansu, jer je u takvim sistemima takvo stanje zapravo stanje ravnoteže.

Ideal-tipski model cirkularne odgovornosti ne može biti u potpunosti ostvaren, ali je potreban jer pruža dobru polaznu osnovu za poređenje sa postojećim sistemima. Upravo zbog toga je njegov prikaz pojednostavljen, a broj aktera sveden na najznačajnije. Predloženi model mogao je da uključi i nadnacionalne institucije, kao i odnos između samih internet korisnika, ali je zaključeno da bi simplifikovan prikaz vodio većoj primenljivosti i razumevanju.

Nadnacionalne institucije jesu značajni akteri u upravljanju internetom, ali je na primeru analiziranih zemalja pokazano da čak i zemlje koje su deo međunarodnih zajednica, kakva je EU, svoj odnos prema internetu grade prevashodno kroz nacionalnu regulaciju. Takođe, odnos između korisnika interneta jeste značajna komponenta individualne odgovornosti, ali je njihov odnos unapred regulisan, odnosno samoregulisan, te nije bilo neophodno isticati posebno i time usložnjavati model.

Koncept odgovornosti, kao centralni koncept u predloženom modelu, može biti osporen sa aspekta njegove višeznačnosti. Međutim, model upravljanja internetom, koji je i sam višeznačan i konstantno promenljiv, nemoguće je graditi oko koncepta koji nije dovoljno otvoren da se istovremeno odnosi i na državu i na privatne aktere i na korisnike. Šta se podrazumeva pod odgovornošću u odnosu na sve pomenute aktere, detaljno je obrazloženo i u svim prethodnim poglavljima.

7. Zaključak

U ovom radu analizirane su uloge tri ključna aktera kada je reč o upravljanju internetom – ***države***, ***internet intermedijatora*** i ***internet korisnika***, sa aspekta poštovanja prava internet korisnika, posebno prava na slobodno izražavanje i prava na privatnost, odnosno zaštitu ličnih podataka. Svodeći predmet na dva pomenuta prava, cilj je, u užem smislu, bio da se utvrdi na koji način se navedeni akteri odnose prema navedenim pravima „na mreži", a u širem, da se sprovede detaljna analiza uloga navedenih aktera pri upravljanju internetom.

Da bi se došlo do željenih odgovora, analiza je sprovedena tako da se svakom od istaknutih aktera pristupi pojedinačno, odnosno da se najpre utvrdi kakva je uloga države u zaštiti prava internet korisnika, zatim kakva je uloga internet intermedijatora, i na kraju, kakva je uloga internet korisnika. Struktura disertacije pratila je postavljene ciljeve, te je analiza svakog od tri aktera predstavljena kroz po jedno poglavlje, dok je poslednje poglavlje imalo za cilj da uporedi različite politike upravljanja internetom i na kraju ponudi ideal-tipski model koji obuhvata sva tri analizirana aktera. Najznačajniji nalazi po poglavljima biće predstavljeni u nastavku.

1) Jurisdikcija država u doba interneta često je osporavana, ponekad u meri koja državi negira bilo kakvu moć. Iako nadnacionalna tela imaju značajno mesto u izgradnji politika u ovoj oblasti i upravljanju internetom, uloga države nije ništavna, čak bi se, na osnovu primera navedenih u trećem poglvlju, moglo zaključiti da je sve intenzivnija.

U ovom radu ***uloga države*** u zaštiti prava internet korisnika analizirana je na primeru Srbije. Cilj je bio da se testira postavljena hipoteza: *(H1): Regulatorni okvir Srbije, u delu koji se tiče slobode izražavanja i prava na privatnost na internetu, nije u potpunosti posvećen zaštiti građana/korisnika, već jednim delom ide u prilog intermedijatora i same države, narušavajući prava korisnika.*

Testiranje ove hipoteze podrazumevalo je analizu regulatornog okvira Srbije u delu kojim se reguliše internet komunikacija, odnosno kojim se reguliše poštovanje navedena dva prava, pregled sekundarne istraživačke građe i literature, posebno istraživanja koja su sprovele organizacije nevladinog sektora, kao i izveštaja Poverenika za zaštitu informacija od javnog značaja i zaštitu ličnih podataka. Takođe, predočeni su i primeri kršenja ovih prava koji su bili medijski pokriveni. Rezultati analize pokazali su da država često isključuje civilni sektor iz rasprava prilikom donošenja novih zakona u ovoj oblasti, smernice nevladinog sektora se ignorišu, dok se internet korisnici suočavaju sa prijavama, pa i privođenjem zbog komentara na društvenim mrežama i portalima. Takođe, serije hakerskih napada na onlajn-medije neposredno nakon objavljivanja tekstova kojima se kritikuje vladajuća stranka išle su u korist prvoj hipotezi.

Analiza regulatornog okvira Srbije kada je reč o poštovanju privatnosti internet korisnika, odnosno njihovih ličnih podataka, obuhvatila je dva zakona o zaštiti podataka o ličnosti. Naime, prilikom prve analize na snazi je bio stari zakon o zaštiti podataka o ličnosti, dok je u novembru 2018. godine usvojen novi zakon. Odlučeno je da obe analize budu deo istraživanja, odnosno da se naknadno doda i analiza novog zakona. Analiza starog zakona bila je značajna jer su u vreme dok je taj zakon bio na snazi zabeležena mnogobrojna kršenja zakonskih odredbi. Masovno curenje ličnih podataka građana Srbije na internetu, u pojedinim slučajevima i politički motivisano, dokazano praćenje internet aktivnosti građana, te presretanje njihove komunikacije bez legalnog razloga, nereagovanje tužilaštva na brojne prijave Poverenika i/ili odugovlačenje sudskih sporova do zastarenja slučajeva, samo su neki

od primera koji su, takođe, govorili u prilog postavljenoj hipotezi, ali i u prilog neslaganju regulative i prakse.

Usvajanje novog zakona učinilo se kao pozitivan iskorak, jer je novi Zakon o zaštiti podataka o ličnosti usklađen sa evropskom regulativom (GDPR). Međutim, ponovno isključivanje civilnog sektora iz javne rasprave i ignorisanje predloženih amandmana, kao i ignorisanje preporuka i komentara Evropske komisije na nacrt novog zakona, bili su presudni za potvrđivanje prve hipoteze.

2) Drugi značajan akter – ***internet intermedijatori***, bio je predmet analize u četvrtom poglavlju. Analiza je svedena na dva internet intermedijatora: pretraživač Gugl i društvenu mrežu Fejsbuk jer su to intermedijatori koji su u najneposrednijoj vezi sa internet korisnicima. Njihova uloga u kreiranju internet pejzaža i upravljanju onlajn-iskustvom internet korisnika potvrđena je, dok je njihova odgovornost, kao aktera koji imaju funkcije nalik-medijskim, detaljno analizirana. Zaključeno je da ovi privatni akteri nisu samo puki prenosioci sadržaja, već da umnogome utiču na oblikovanje informacijskog iskustva korisnika, te da u tom smislu imaju i odgovornost koja prevazilazi odgovornost tehno-kompanije, kako se često samopercipiraju. Cilj nije bio da se internet intermedijatori izjednače sa medijima u tradicionalnom smislu, već da se ukaže na njihovu značajnu ulogu koja ne mora nužno značiti identifikaciju sa medijskim kompanijama. Međutim, njihova odgovornost prema korisnicima trealo bi da bude proporcionalna njihovoj ulozi u globalizovanom informaciono-komunikacionom sistemu.

U ovom poglavlju disertacije analizirane su samoregulatorne politike kompanija Gugl i Fejsbuk, naročito u delu koji se tiče poštovanja prava na slobodno izražavanje i prava na privatnost internet korisnika. Samoregulatorna politika Gugla istovetna je u svim zemljama, dok je samoregulatorna politika Fejsbuka senzitivnija na nacionalnu regulativu, te se u različitim zemljama razlikuje.

Predmet analize bili su uslovi korišćenja, kao vid samoregulacije, kojima se regulišu odnosi između kompanija (Fejsbuka i Gugla) i korisnika. Uslovi korišćenja upoređeni su sa propisima EU. Uslovi korišćenja Gugla preuzeti su u Srbiji, jer su njegovi uslovi svuda isti, dok su uslovi korišćenja Fejsbuka preuzeti u Austriji, kao zemlji članici EU, da bi poređenje sa propisima EU bilo smisleno. Cilj ovog poglavlja bio je da se odgovori na postavljeno istraživačko pitanje: ***Da li je samoregulatorna politika internet intermedijatora u delu koji se tiče poštovanja prava na privatnost i slobodu izražavanja u skladu sa interesima korisnika?*** Odnosno, da se testira postavljena hipoteza: *H2: Samoregulatorna politika internet intermedijatora ne garantuje apsolutnu zaštitu prava na privatnost i slobodno izražavanje korisnicima.* Na osnovu sprovedene analize zaključeno je da samoregulatorne politike obe kompanije nisu u potpunosti usklađene sa regulativom EU, te da ne garantuju apsolutnu zaštitu navedena dva prava internet korisnicima. Naime, kao najznačajniji nalazi istaknuti su:

- *izostanak afirmativnog pristanka na uslove korišćenja,*
- *netransparentnost u pogledu deljenja podataka korisnika sa trećim licima i*
- *netransparentnost u pogledu zadržavanja i brisanja podataka korisnika.*

Sve navedeno eksplicitno je propisano EU regulativom. Međutim, kompanije Gugl i Fejsbuk svojim korisnicima ne nude fer izbor pri sklapanju tzv. elektronskog ugovora (uslova korišćenja). Isključivim zahtevima, koji se mogu sumirati rečenicom – *Pristani ili odustani*, ove kompanije uslovljavaju svoje korisnike da prihvate njihov način poslovanja i ophođenja. Takođe, korisnicima se ne daje jasan uvid u to koja treća lica imaju pristup njihovim podacima, kao ni na koji način i u koje svrhe Fejsbuk i Gugl dele podatke korisnika sa drugim kompanijama sa kojima sarađuju.

Još jedan značajan nalaz odnosi se na upotrebu kompleksnog, prevashodno tehničkog jezika, kojim se kompanije služe pri formulisanju svojih politika. Ovakav jezik težak je za razumevanje prosečnim korisnicima, što takođe dovodi u pitanje njihov afirmativni pristanak. Pored ovoga, opširnost u predstavljanju uslova korišćenja još jedna je prepreka za afirmativni pristanak. Već je bilo reči o tome da je za detaljno iščitavanje svih segmenata uslova potrebno nekoliko sati, a ukoliko korisnik želi da isprati svaki link kojim se povezuju delovi samoregulativne politike, može se govoriti i o danima provedenim u iščitavanju uslova korišćenja. Može se pretpostaviti da korisnici pristaju na uslove, koje nisu razumeli, ili ih nisu ni pročitali.

Iako je EU regulativom (GDPR) jasno navedeno da je vreme zadržavanja podataka potrebno svesti na minimum, te da je neopravdano zadržavanje ličnih podataka neprihvatljivo, obe kompanije nemaju jasan propis o ovom pitanju, već dvosmisleno i nejasno definišu rokove zadržavanja ličnih podataka. Pored svega navedenog, obe kompanije prikupljaju prekomernu količinu ličnih podataka, što je dokazano analizom njihovih uslova korišćenja, iako je EU propisima jasno navedeno da se lični podaci prikupljaju u meri koja opravdava svrhu prikupljanja, odnosno samo ukoliko su neophodni za pružanje konkretne usluge.

Kada je reč o slobodi izražavanja, pod kojom se podrazumeva pravo na širenje i dobijanje informacija iz različitih izvora, dokazano je upravljanje informacijama koje se korisnicima sugerišu kao najznačajnije za njih, na Fejsbukovom *News Feed*, odnosno u rezultatima pretrage Gugla, što jasno ukazuje na to da obe kompanije mogu algoritamski da upravljaju informacijskim iskustvom na internetu. Odnosno, mogu sugerisati određene teme kao značajne, dok druge mogu da potisnu do mere koja podrazumeva njihovo nepojavljivanje u pretragama. Navedeno ukazuje da su obe kompanije mnogo više od samo tehničkih posrednika ili tehno-giganata, te da one preuzimaju uloge vratara na internetu.

Pored analize, pregled sličnih istraživanja i primeri mnogobrojnih afera kojima je ilustrovano na koji način mogu biti zloupotrebljeni podaci korisnika potvrdili su postavljenu hipotezu, odnosno dokazali da samoregulatorne politike kompanija Fejsbuk i Gugl ne garantuju apsolutnu zaštitu prava na privatnost i slobodno izražavanje korisnika. U takvom okruženju, korisnicima ne preostaje ništa drugo nego da veruju da kompanije neće zloupotrebiti njihove podatke, te da neće manipulisati njhihovim informacijskim iskustvom.

3) Peto poglavlje imalo je za cilj da utvrdi koliko je ***internet korisnicima*** u Srbiji stalo do poštovanja njihovih prava, te koliko je njihovo poverenje u državu i privatne kompanije, i na kraju, koliki je stepen njihove individualne odgovornosti pri korišćenju internet usluga. Kako bi se testirale postavljene hipoteze, sprovedena je veb-anketa koju je u periodu od mesec dana popunilo 783 ispitanika. Upitnik je sadržao četiri integralna dela. Prvim delom ispitivan je generalni odnos internet korisnika prema zaštiti njihovih prava na internetu – prava na privatnost i slobodno izražavanje; drugi set pitanja imao je za cilj da ispita koliko je poverenje internet korisnika u državu kada je reč o zaštiti njihovih prava; treći set pitanja testirao je poverenje u privatne aktere – Gugl i Fejsbuk; dok se četvrtim setom utvrđivala individualna odgovornost korisnika pri korišćenju usluga navedenih kompanija.

Prva hipoteza u ovom poglavlju, odnosno treća u disertaciji glasi: *H3: Internet korisnici u Srbiji osećaju se nesigurno prilikom deljenja ličnih podataka na internetu*, dok se pomoćnim hipotezama pretpostavilo da internet korisnici u Srbiji smatraju da njihovu privatnost ugrožavaju i država i privatni akteri (Gugl i Fejsbuk). Rezultati ankete potvrdili su navedenu hipotezu. Naime, više od polovine ispitanika smatra da podaci koje dele na internetu nisu zaštićeni, dok samo šestina smatra da Vlada Srbije ne ugrožava njihovu privatnost na internetu, a 5% ispitanika veruje da Vlada Srbije ne prati

njihove aktivnosti na internetu. Kada je reč o poverenju u privatne kompanije, samo 11,8% ispitanika zadovoljno je zaštitom podataka na Fejsbuku, dok je za Gugl taj procenat neznatno veći – 13%.

Četvrtom hipotezom testirano je poverenje internet korisnika u državu i privatne kompanije kada je reč o slobodnom izražavanju na internetu: *H4: Internet korisnici u Srbiji ne veruju u odgovornost internet intermedijatora i pravne mogućnosti države, kada je reč o zaštiti njihovog prava na slobodno izražavanje u onlajn prostoru.* I ova hipoteza je nedvosmisleno potvrđena. Naime, gotovo polovina ispitanika potvrdila je da se oseća nesigurno i zabrinuto prilikom iznošenja stavova onlajn kojima kritikuje rad Vlade Srbije, i u tom kontekstu nešto više od polovine smatra da Vlada Srbije ugrožava slobodu izražavanja internet korisnicima. Kada je reč o privatnim kompanijama, nešto manje od polovine ispitanika smatra da Fejsbuk može da im ugrozi slobodu izražavanja, dok je za Gugl taj broj manji – trećina ispitanika. Rezultati su pokazali da korisnici iskazuju nepoverenje u odnosu na oba aktera, međutim, taj procenat je veći kada je reč o državi.

Nakon dokazanog nepoverenja u državu i privatne aktere, kada je reč o zaštiti njihovih prava onlajn, kroz naredni set pitanja testirana je individualna odgovornost korisnika, odnosno da li korisnici koriste sve dostupne mehanizme da zaštite svoja prava na internetu. U skladu sa tim, postavljena hipoteza glasi: *H5: Internet korisnici u Srbiji ne iskazuju visok stepen individualne odgovornosti kada je o zaštiti njihovih prava na internetu reč***.** Pretpostavljeno je da korisnici neće iskazati visok stepen odgovornosti, odnosno da nisu upoznati sa najznačajnijim segmentima uslova korišćenja kompanija čiji su korisnici, ali i da ne koriste u dovoljnoj meri individualna podešavanja koja kompanije nude korisnicima. Kako bi se testirala ova hipoteza, upitnikom su bila predviđena kontrolna pitanja, odnosno tvrdnje koje su preuzete iz uslova korišćenja kompanija, a o kojima su ispitanici iskazivali stepen saglasnosti (*Da, Nisam siguran, Ne*). Rezultati su pokazali da četvrtina ispitanika nije promenila individualna podešavanja privatnosti. Kada je reč o uslovima korišćenja, ukršteni su odgovori na pitanje *Da li ste pročitali uslove korišćenja?,* na koje je trećina ispitanika odgovorila potvrdno, sa odgovorima na kontrolna pitanja. Rezultati su pokazali da polovina ispitanika koja je potvrdno odgovorila na pitanje nije dala tačne odgovore na kontrolna pitanja, što sugeriše da su ispitanici ili dali poželjan odgovor ili su smatrali da su dovoljno upoznati sa uslovima na osnovu letimičnog čitanja ili nisu razumeli pročitano zbog složenosti jezika i tehničkih termina.

Na osnovu svih navedenih rezultata i potvrđenih hipoteza, zaključeno je da internet korisnici u Srbiji nemaju poverenje u državu ni u privatne aktere da će im zaštiti prava pri korišćenju usluga. Takođe, iako potvrđuju visok stepen nepoverenja u pogledu zaštite njihovih prava na internetu, korisnici iskazuju nizak stepen individualne odgovornosti.

4) Nakon sveobuhvatne analize uloga tri ključna aktera – države, privatnih kompanija i internet korisnika, šesto poglavlje imalo je dva cilja:

a) da se poređenjem različitih načina upravljanja internetom u oblasti, pre svega, poštovanja prava korisnika, ukaže na različite pristupe i ponudi ***klasifikacija modela državnog upravljanja internetom*** i

b) da se ***ponudi ideal-tipski model upravljanja internetom***, koji bi uključio sva tri aktera, a bazirao bi se na konceptu odgovornosti koji u širem kontekstu podrazumeva zaštitu prava korisnika.

a) Odabir zemalja, koje su bile predmet analize u ovom poglavlju, pratio je ponuđene modele medijskih sistema Halina i Manćinija, jer je pretpostavljeno da će odnos prema informaciono-komunikacionom sistemu u tradicionalnom smislu imati uticaj i na odnos prema komunikaciji na

internetu. U skladu sa njihovom klasifikacijom, odabrane zemlje bile su: SAD – predstavnik liberalnog model, Nemačka – predstavnik demokratsko-korporativnog modela i Francuska – predstavnik mediteranskog modela. Pored toga, analizi je dodata i Rusija, kao predstavnik postsocijalističkih zemalja, a sa ciljem utvrđivanja razlika između načina na koji se razvijene demokratske zemlje i postsocijalističke zemlje odnose prema internetu.

Za analizu odabranih zemalja korišćena je sekundarna istraživačka građa, pre svega, izveštaji organizacije Fridom haus za 2018. godine, ali i pregled literature i istraživanja koja su za predmet analize imala odabrane zemlje. Nakon detaljne analize, definisane su četiri intervenišuće varijable koje su se iskristalisale kao najdominantnije kada je reč o odnosu određene države prema internet komunikaciji:

- ***sloboda u internet komunikaciji***
- ***dostojanstvo u komunikaciji na internetu,***
- ***bezbednost internet korisnika kroz nadzor*** i
- ***etatizam***.

U odnosu na to koja je od navedenih varijabli bila dominantna pri izgradnji regulatornog okvira i uopšteno upravljanja internetom u analiziranim zemljama, definisana su tri modela državnog upravljanja internetom:

- ***Liberalni model,***
- ***Model državne kontrole*** i
- ***Balansirani model upravljanja internetom.***

U ***liberalnom modelu*** intervenišuća varijabla je sloboda u internet komunikaciji, i ovoj varijabli su podređene sve ostale varijable. Nadzor internet komunikacije može biti visoko kotiran, ali je u odnosu na ostale modele podređen slobodi u komunikaciji. Dostojanstvo u komunikaciji i etatizam su gotovo zanemarljive. Ovakav model prepoznat je u upravlju internetom u SAD.

Model državne kontrole podrazumeva etatizam kao najdominantniju varijablu. Njoj su podređene sve ostale varijable. Da bi se državna kontrola sprovodila nesmetano, nadzor nad internet komunikacijom takođe je visokokotirana varijabla, dok su u skladu sa tim dostojanstvo u komunikaciji i sloboda izražavanja najmanje značajne. Ovaj model državnog upravljanja internetom prepoznat je u Rusiji.

Balansirani model upravljanja internetom predstavlja konstantnu težnju države da balansira između nekada sukobljenih prava u onlajn-prostoru kako bi zaštitila vrednost koja joj je prioritetna. Na to koja će varijabla biti prioritetna može uticati istorijski kontekst, aktuelni izazovi, ili kombinacija oba nabedena momenta. Ovaj model prepoznat je u Francuskoj i Nemačkoj. Razlika između ovih zemalja, odnosno između njhovog upravljanja internetom, jeste u tome što je u Nemačkoj tradicionalno značajno dostojanstvo u komunikaciji prioritetno, te se ovoj varijabli podređuju ostale, s tim što se uočava konstanta težnja za održanjem balansa između dostojanstva u komunikaciji, sa jedne, i slobode izražavanja, sa druge strane. U Francuskoj su aktuelni izazovi, učestali teroristički napadi u poslednjih pet godina, varijablu bezbednosti kroz nadozor pozicionirali kao intervenišuću, te se njoj podređuju

ostale varijable. Balans je vidljiv u konstantnom prevladavanju između osiguravanja bezbednog internet prostora i neopravdanog nadzora internet korisnika.

S obzirom na to da se u većini država pri upravljanju internetom može uočiti smena definisanih varijabli, odnosno promena pozicije, pri čemu jedna intervenišuća nije u svakom trenutku i u svim okolnostima dominatna, većina država se može pozicionirati kao bliža nekom od ponuđenih modela upravljanja, a može se pozicionirati i između dva modela, ukoliko iskazuje kombinaciju njihovih karakteristika.

Zbog toga što ***Srbija***, prema analizi sprovedenoj u trećem poglavlju, iskazuje karakteristike dva navedena modela – balansiranog modela upravljanja internetom i modela državne kontrole – pozicionirana je između dva navedena modela. Sa jedne strane, Srbija teži da uspostavi balans u poštovanju prava internet korisnika, sledeći preporuke EU, kao kandidat za članstvo, dok sa druge strane, koristi različite mehanizme kontrole i nadzora, koji su često politički motivisani.

b) ***Definisanje ideal-tipskog modela*** izdvojeno je kao poseban i poslednji nalaz u disertaciji, jer sumira sve prethodne rezultate i uključuje sve analizirane aktere. Predložen model, izgrađen oko koncepta *odgovornosti*, nazvan je ***model cirkularne odgovornosti upravljanja internetom***. Odgovornost je cirkularna jer podrazumeva međusobnu odgovornost svih uključenih strana – države, privatnih aktera i internet korisnika.

Ovaj funkcionalistički model upravljanja internetom je u apsolutnoj ravnoteži samo onda kada je država odgovorna prema korisnicima i privatnim kompanijama – privatne kompanije joj uzvraćaju odgovornost i ujedno su odgovorne prema svojim korisnicima dok korisnici uzvraćaju odgovornost i jednim i drugim, ali iskazuju i individualnu odgovornost, odnosno odgovorno koriste internet usluge.

Apsolutna ravnoteža moguća je samo u teorijskom smislu. U praksi je izglednije da će neki od aktera koji su u poziciji moći – država ili privatni akteri, zauzeti dominantniju poziciju u odnosu na druge aktere. S tim u vezi, definisana su dva tipa modela cirkularne odgovornosti: ***tip A*** – u kojem je država dominatan akter, ali ne narušava prava drugih aktera, bar ne u meri koja može da poremeti ravnotežu. Takav model možemo da prepoznamo u već analiziranim zemljama, ***Nemačkoj i Francuskoj***, gde je uloga države izražena, ali je sistem i dalje u ravnoteži, odnosno odgovornost je i dalje centralni koncept. ***Tip B modela cirkularne odgovornosti*** podrazumeva da su privatni akteri dominantniji u odnosu na ostale, ali takođe u meri koja u najvećem broju slučajeva ne narušava ravnotežu sistema, odnosno odgovornost prema preostala dva aktera je očuvana kao centralni koncept. Takvom modelu najbliži je analizirani primer SAD.

Međutim, kada dođe do izraženog disbalansa, odnosno kada jedan od aktera dominatan u meri koja narušava ravnotežu, a koncept odgovornosti menja konceptima komercijalne isplativosti, etatizma ili apsolutne slobode/anarhije, ideal-tipski model cirkularne odgovornosti se urušava. Disbalansi mogu biti kratkotrajni ili dugotrajni, kada se mogu odrediti kao zasebni modeli.

Ukoliko je država dominatan akter, a etatizam koncept oko kojeg se model izgrađuje i kojem se sve ostale vrednosti podređuju, reč je o ***etatističkom modelu upravljanja internetom***.

Ukoliko je komercijalna isplativost centralni koncept, a privatni akteri dominantni u meri koja narušava ravnotežu, reč je o ***komercijalnom modelu upravljanja internetom***.

Narušavanje ravnoteže, odnosno disbalansi, mogu biti različiti u odnosu na intenzitet i trajanje:

- ***kratkotrajni sa kratkim efektom,***
- ***kratkotrajni sa dugim efektom,***
- ***dugotrajni sa potencijalom vraćanja u ravnotežu*** i
- ***dugotrajni bez izgleda povratka u ravnotežu***.

Prva tri mogu biti definisana kao prolazno stanje disbalnsa jer je povratak u ravnotežu moguć, ponekad i vrlo izvesan. Međutim, kada je reč o poslednjem disbalansu, gde ne postoji mogućnost i/ili težnja ka vraćanju u ravnotežu, reč je o modelu koji se ne može odrediti kao disbalans već kao zasebni model upravljanja internetom. U takvim sistemima, ono što je u ovom radu opisano kao disbalans ideal-tipskog modela, zapravo je stanje ravnoteže.

Posebno je predstavljen i treći tip disbalnsa koji može biti percipiran kao samostalni model – reč je o ***modelu apsolutne slobode/anarhičnom modelu upravljanja internetom***. Ovaj model se prepoznaje onda kada su korisnici ti koji su dominantni akteri, zaobilazeći nametnute autoritete i regulativu. Najčešće se ogleda u *deep web*-u. Model je izgrađen oko koncepta apsolutne slobode koja može biti percipirana pozitivno – onda kada se koristi u dobre svrhe (novinari, uzbunjivači, zviždači, aktivisti), ali i izuzetno negativno – onda kada se zloupotrebljava za sprovođenje kriminalnih aktivnosti. U drugom slučaju je bliža anarhiji, mada se time ne sugeriše da je *deep web* prostor koji je apsolutno izuzet od bilo kakve regulative i sankcija već se nazivom naglašavaju pretenzije korisnika koje su anarhične.

Poslednji model je izdvojen u odnosu na prva dva jer je u disertaciji sve vreme bio analiziran vidljiv veb i svi akteri bili su posmatrani u tom kontekstu. *Deep web* nije bio predmet analize, ali je značajno ukazati i na postojanje jednog takvog modela koji može biti predmet nekih budućih analiza u kontekstu ponuđenih modela.

Ideal-tipski model upravljanja internetom, predstavljen u ovoj disertaciji, može se osloniti na teorijsko promišljanje Entoni Gidensa (Anthony Giddens, 1998) o *poverenju u apstraktne sisteme*. U knjizi *Posledice modernosti*, Gidens je, ukazujući na razliku između premodernih i modernih društava, koncept poverenja predstavio kao jedan od ključnih koncepata. Kako autor smatra, u premodernom društvu poverenje je uspostavljano „u društvenim vezama oblikovanim u okolnostima zajedničkog prisustva“ (Gidens, 1998: 84); dok poverenje koje karakteriše moderna društva, predstavlja verovanje u „simboličke znake ili ekspertske sisteme“, što Gidens naziva *apstraktnim sistemima* (1998: 84).

Poverenje u apstraktne sisteme, odnosno u eksperte, podrazumeva da pojedinac u modernom društvu ne mora, i ne može, da gradi poverenje na osnovu ličnog poznanstva i bliskosti, već to čini u odnosu prema pojedincima koje nikada nije upoznao, ali ih smatra ekspertima u datoj oblasti, pa njihovu ekspertizu ne dovodi u pitanje, čak ni ne razmišlja o njoj. Da bi ilustrovao ovaj princip, Gidens navodi primer putovanja avionom: „putnik može da se ukrca u avion u Londonu i stigne za desetak sati u Los Anđeles, i pri tom može biti dosta sigurna ne samo u to da će putovanje biti bezbedno nego i da će stići u vreme vrlo približno predviđenom“ (Gidens, 1998: 111).

Koncept odgovornosti, ponuđen kao centralni u ideal-tipskom modelu upravljanja internetom, u širem smislu se može dovesti u vezu sa Gidensovim konceptom poverenja. Naime, internet korisnici

prilikom korišćenja internet usluga moraju imati minimum poverenja da će ostali akteri – država i internet intermedijatori, biti odgovorni u pogledu postupanja sa, na primer, njihovim ličnim podacima, koje im ostavljaju na raspolaganje, ili da će biti odgovorni u smislu ograničenog korišćenja mehanizama kojima im mogu uskratiti slobodu izražavanja.

Za internet korisnike su pojedinci, ili grupa pojedinaca, koji odlučuju o izgradnji politika u oblasti upravljanja internetom, bili oni deo njihovih vlada ili uposlenici privatnih aktera, depersonalizovani. Korisnici o njima mogu da razmišljaju kroz kategoriju apstraktnih sistema, i bliže ekspertskih sistema, ali ih ne poznaju, niti ih prepoznaju kao pojedince. Prilikom korišćenja internet usluga, korisnik može da veruje da je regulatorni mehanizam, koji će ga zaštiti od zloupotreba, predložen i usvojen od strane tima eksperata, te da je kod koji pokreće internet usluge i proizvode programiran od strane stručnjaka, bez namere da korisnike zloupotrebe.

Svakako da korisnici, iako laici, mogu imati informacije i saznanja na osnovu kojih grade odnos poverenja ili nepoverenja u sisteme i eksperte. Takva saznanja ili iskustva dostupna su im, pre svega, kako Gidens smatra, „putem komunikacijskih medija i drugih izvora“ (1998: 93). Na primer, medijska pokrivenost afere Fesjbuk u vezi sa Kembridž analitikom, dovela je do slabljenja poverenja korisnika u ovu društvenu mrežu. Takođe, možemo da pretpostavimo da je medijsko izveštavanje o curenju ličnih podataka miliona građana Srbije uticalo na korisnike koji su bili ispitanici u ovom radu da iskažu nizak stepen poverenja u državu, kada je reč zaštita njihovih prava na internetu.

Da bi ilustrovao ljude koji žive u vremenu modernosti, Gidens koristi sliku *zmajevih kočija*[313]:

> „Jureću mašinu ogromne snage kojom možemo da upravljamo do određene mere, kolektivno, kao ljudska bića, ali koja takođe preti da se otrgne od naše kontrole i raspadne se na komadiće. Zmajeva kočija mrvi one koji joj se opiru, i ako postoje periodi kada izgleda kao da se kreće ravno, postoje periodi kada greškom krivuda i skreće u nepredvidivom smeru. Vožnja nipošto nije sasvim neprijatna ili bez zadovoljstava, ona često može da ushićuje i da nudi anticipacije pune nade. Ali, sve dok institucije modernosti budu postojale, mi nikada nećemo moći da u potpunosti kontrolišemo ni smer ni brzinu kretanja. Uz to, mi nikada nećemo moći da se osećamo potpuno sigurnim, jer je teren kojim se krećemo ispunjen rizicima koji mogu imati teške posledice. Osećanje ontološke sigurnosti i egzistencijalne anksioznosti postojaće zajedno, u ambivalentnom odnosu“ (1998: 134).

Slika zmajevih kočija može se primeniti i kao ilustracija života ljudi u doba interneta. Svakom onlajn-iskustvu prete mnogobrojni rizici, dok se istovremeno svojom brzinom, dostupnošću, riznicom informacija i interakcijom, korisnicima nudi ushićenje i osećaj povremene kontrole i moći. Neograničeno novo, koje se svakodnevno, gotovo iz minuta u minut, nudi, budi kod korisnika istovremeno osećaj radoznalosti i anksioznosti. Neučestvovanje stvara osećaj otuđenosti i isključenosti, a učestvovanje konstantnu neizvesnost. U takvim okolnostima internet korisnicima ne preostaje ništa drugo nego da veruju u ekspertizu i odgovornost onih koji upravljaju internetom, ali i da budu svesni svoje odgovornosti.

[313] juggernaut – „Termin potiče od Hindu reči Jagannath, „gospodar sveta“, i predstavlja jednu od titula Krišne. Jedan idol ovog božanstva svake godine je vožen po ulicama u ogromnim kolima, pod koja su se, kažu, bacali njegovi sledbenici, da bi ih smrvili njihovi točkovi“ (Gidens, 1998: 134).

Literatura

1. Acquisti, A., & Gross, R. (2006). „Imagined communities: Awareness, information sharing, and privacy on the Facebook“. In *International workshop on privacy enhancing technologies.* Springer, Berlin, Heidelberg, pp. 36–58.

2. Ahlert, C., Marsden, C., & Yung, C. (2004). *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation* [URL]: http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf

3. Allcott, H., & Gentzkow, M. (2017). "Social media and fake news in the 2016 election". *Journal of Economic Perspectives*, *31*(2), pp. 211–36.

4. Andrew, C. (2007). *Human Rights – A Very Short Introduction*. Oxford University Press.

5. Andrews, D., Nonnecke, B., & Preece, J. (2003). „Electronic survey methodology: A case study in reaching hard-to-involve Internet users“. *International journal of human-computer interaction*, 16(2), pp. 185–210.

6. Ang, P. H. (2001). „The Role of Self-regulation of Privacy and the Internet“. *Journal of Interactive advertising*, *1*(2), pp. 1-9.

7. Bal, F. (1997). *Moć medija*. Clio: Beograd.

8. Barvajz, P., Gordno, D. (2005). „Ekonomija: Ekonomija i mediji“. U: *Uvod u studije medija*. Ur. Brigs i Kobli. Beograd: Klio. str. 302–335.

9. Barzilai-Nahon, K. (2008). "Toward a theory of network gatekeeping: A framework for exploring information control". *Journal of the Association for Information Science and Technology*, *59*(9), pp. 1493–1512.

10. Beitz, C. R. (2011). *The idea of human rights*. Oxford University Press.

11. Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press

12. Beresforda, A. R., Küblerb, D., & Preibuscha, S. (2012). "Unwillingness to pay for privacy: A field experiment". *Economics Letters*, *117*, pp. 25–27.

13. Black, J. (2001). „Decentring Regulation: Understanding the role of regulation and self-regulation in a'post-regulatory'world“. *Current legal problems*, *54*(1), pp. 103–146.

14. Börzel, T. A., & Risse, T. (2005). „Public-private partnerships: Effective and legitimate tools of international governance“. *Complex sovereignty: Reconstructing political authority in the twenty first century*, pp. 195–216.

15. Brady, A. M. (2006). "Guiding hand: The role of the CCP Central Propaganda Department in the current era". *Westminster Papers in Communication and Culture*, *3*(1). pp. 58–77.

16. Brigs, A., Kobli, P. (2005). *Uvod u studije medija*. Beograd: Clio.

17. Bruns, A., Highfield, T., & Burgess, J. (2013). "The Arab Spring and social media audiences: English and Arabic Twitter users and their networks". *American Behavioral Scientist*, *57*(7), pp. 871–898.

18. Cannataci, J. A., & Bonnici, J. P. M. (2003). „Can self-regulation satisfy the transnational requisite of successful Internet regulation?“. *International Review of Law, Computers & Technology*, *17*(1), pp. 51–61.

19. Carlson, M. (2007). "Order versus access: News search engines and the challenge to traditional journalistic roles". *Media, Culture & Society*, *29*(6), pp. 1014–1030.

20. Castells, M. (2013). *Communication power*. OUP Oxford.

21. Chertoff, M., & Simon, T. (2015). *The impact of the dark web on internet governance and cyber security. Centre for International Governance Innovation and the Royal Institute for International Affairs*. pp. 1–8. [Available online]: https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security

22. Clapham, A. (2007). *Human rights: a very short introduction*. Oxford University Press.

23. Cotter, T. (2005). "Some Observations on the Law and Economics of Intermediaries". *Michigan State Law Review*, Vol. 1, pp. 67–85.

24. Couper, M. P., & Miller, P. V. (2008). "Web survey methods: Introduction". *Public Opinion Quarterly*, *72*(5), pp. 831–835.

25. De Filippi, P. (2014). „Big data, big responsibilities“. *Internet Policy Review*, *3*(1).

26. de Vey Mestdagh, C. N. J., & Rijgersberg, R. W. (2010). „Internet governance and global self regulation: theoretical and empirical building blocks for a general theory of self regulation“. *Legisprudence*, *4*(3), pp. 385–404.

27. Deibert, R., & Rohozinski, R. (2010). „Control and subversion in Russian cyberspace“. In: *Access controlled: The shaping of power, rights, and rule in cyberspace*, pp. 15–34.

28. Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: security, identity, and resistance in Asian cyberspace*. MIT Press.

29. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Haraszti, M. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Mit Press.

30. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. (2008). *Access denied: The practice and policy of global internet filtering*. Mit Press.

31. DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Mit Press.

32. DeNardis, L. (2010). "The privatization of Internet governance". *Yale Information Society Project Working Paper Draft*. Paper presented at Fifth Annual GigaNet Symposium, Vilnius, Lithuania.

33. DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

34. DeNardis, L., & Hackl, A. M. (2015). "Internet governance by social media platforms". *Telecommunications Policy, 39*(9), pp. 761–770.

35. Dimitrijević, V., Paunović, M., Đerić, V. (1997). *Ljudska prava: udžbenik*. Beograd: Beogradski centar za ljudska prava.

36. Drezner, D. W. (2004). "The global governance of the Internet: bringing the state back in". *Political Science Quarterly, 119*(3), pp. 477–498.

37. Dutton, W. (2018). "Networked publics: multi-disciplinary perspectives on big policy issues". *Internet Policy Review*. 7(2). pp. 1–15.

38. Esteve, A. (2017). „The business of personal data: Google, Facebook, and privacy issues in the EU and the USA“. *International Data Privacy Law*, *7*(1), pp. 36–47.

39. Faris, R., Villeneuve, N. (2008). "Measuring Global Internet Filtering". In: *Access denied: The practice and policy of global internet filtering.* Eds. 25. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. pp. 5–29.

40. Fazlioglu, M. (2013). „Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet“. *International Data Privacy Law*, *3*(3), pp. 149–157.

41. Feintuck, M., Varney, M. (2006). *Media regulation, public interest and the law*. Edinburgh University Press.

42. Flew, T., & Waisbord, S. (2015). The ongoing significance of national media systems in the context of media globalization. *Media, Culture & Society*, *37*(4), 620-636.

43. Ganley, P., & Allgrove, B. (2006). „Net neutrality: A user's guide". *Computer law & security report*, *22*, pp. 454–463.

44. Ghappour, A. (2017). "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web". *Stan. L. Rev.*, *69*, pp. 1075–1136.

45. Gidens, E. (1998). *Posledice modernosti*. Beograd: Filip Višnjić.

46. Goggin, G., Vromen, A., Weatherall, K., Martin, F., Webb, A., Sunman, L., & Bailo, F. (2017). "Digital Rights in Australia". *Sydney Law School Research Paper No. 18/23.* Available at SSRN*:* *https://ssrn.com/abstract=3090774*.

47. Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford University Press.

48. Govani, T., & Pashley, H. (2005). "Student awareness of the privacy implications when using Facebook". *Unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science*, *9*, pp. 1–17.

49. Gregg, B. (2012). „Politics Disembodied and Deterritorialized:The Internet as Human Rights Resource". *Theorizing Modern Society as a Dynamic Process*. pp. 209–233.

50. Grimmelmann, J. (2007). "The structure of search engine law". *Iowa L. Rev.*, *93*, 1. pp. 1–63.

51. Gross, R., & Acquisti, A. (2005). "Information revelation and privacy in online social networks". In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80.

52. Groves, R. M., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2004). *Survey Methodology*. John Wiley & Sons, Inc: New Jersey.

53. Hadži-Vidanovic V., Milanović M. (2006). *Ne smetajte, uživam u svojim pravima i slobodama*. Beograd: Beogradski centar za ljudska prava.

54. Hallin, D. C., & Mancini, P. (2004). *Comparing media systems: Three models of media and politics*. Cambridge university press.

55. Hallin, D. C., & Mancini, P. (Eds.). (2012). *Comparing media systems beyond the Western world*. Cambridge University Press.

56. Harvi, S. (2005). "Politika: Kreiranje politike medija". U: *Uvod u studije medija*, Ur. Brigs i Kobli. Beograd: Klio. str. 335–355.

57. Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment.

58. Helberger, N. (2014). *Convergence, Information intermediaries and media pluralism, mapping the legal, social and economic issues at hand: a quick scan*. URL: https://www.ivir.nl/publicaties/download/Information_intermediaries_and_media_pluralism.pdf

59. Herman, E. S., Mekčesni, R. V. (2004). *Globalni mediji*. Clio, Beograd.

60. Hick, S., Halpin, E., & Hoskins, E. (Eds.). (2016). *Human rights and the Internet*. Springer.

61. Huseinspahić, E. (2009). „Pravni značaj francuske Deklaracije o pravima čoveka i građanina iz 1789. godine". *Naučni skup sa međunarodnim učešćem Sinergija*. str. 240–243.

62. Introna, L. D., & Nissenbaum, H. (2000). "Shaping the Web: Why the politics of search engines matters". *The information society*, *16*(3), pp. 169–185.

63. Jackson, B. F. (2014). "Censorship and Freedom of Expression in the Age of Facebook". *NML Rev.*, *44*, pp. 121–167.

64. Jakubowicz, K. (2009). "A new notion of media?". In *1st Council of Europe Conference of Ministers Responsible for Media and New Communication Services, Council of Europe, Strasbourg Cedex: Council of Europe*.

65. Jakubowicz, K., & Sükösd, M. (Eds.). (2008). *Finding the right place on the map: Central and Eastern European media change in a global perspective*. Intellect Books.

66. Johnson, D. R., & Post, D. (1996). „Law and borders: The rise of law in cyberspace". *Stanford Law Review*, pp. 1367–1402.

67. Jurišić, K. (1999). „Globalizacija i ljudska prava". *Politička misao: časopis za politologiju*, *36*(1), str. 70–82.

68. Kaplan, A. M., & Haenlein, M. (2010). "Users of the world, unite! The challenges and opportunities of Social Media". *Business horizons*, *53*(1), pp. 59–68.

69. Khor, L. (2011). „Human Rights and Network Power". *Human Rights Quarterly*, Vol. 33, No. 1, pp. 105–127.

70. Kirkpatrick, D. (2011). *The Facebook effect: The inside story of the company that is connecting the world*. Simon and Schuster.

71. Kleinsteuber, H. J., & Thomass, B. (2010). "Comparing media systems: the European dimension". *CM-časopis za upravljanje komuniciranjem*, *5*(16), pp. 5–20.

72. Klimkiewicz, B. (2009). "Is the clash of rationalities leading nowhere? Media pluralism in European regulatory policies". *Press freedom and pluralism in Europe: Concepts and conditions*, pp. 62–64.

73. Kohl, U. (2012). "The rise and rise of online intermediaries in the governance of the Internet and beyond–connectivity intermediaries". *International Review of Law, Computers & Technology*, *26*(2-3), pp. 185–210.

74. Kohl, U. (2013). "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)". *International Journal of Law and Information Technology*, *21*(2), pp. 187–234.

75. Laidlaw, E. B. (2008). „Private power, public interest: An examination of search engine accountability". *International Journal of Law and Information Technology*, *17*(1), pp. 113–145.

76. Laidlaw, E. B. (2010) "A framework for identifying Internet information gatekeepers". *International Review of Law, Computers & Technology*. 24: 3, pp. 263–276.

77. Lessing, L. (2006). *Code: Version 2.0*. New York: Basic Books

78. Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). "Analyzing Facebook privacy settings: user expectations vs. reality". In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. pp. 61–70.

79. Lorimer, R. (1998). *Masovne komunikacije*. Clio: Beograd.

80. Maletić, V., Dakić, J. (2012). "Internet, socijalne mreže i ljudska prava". *Zbornik radova INFOTEH Jahorina*, *11*, pp. 771–776.

81. Mansell, R. (2015). „The public's interest in intermediaries". *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, 17(6), pp. 8–18.

82. Marsden, C. T. (Ed.). (2000). *Regulating the global information society* (Vol. 2). Psychology Press.

83. Mayntz, R. (2002). „Common goods and governance". *Common goods: Reinventing European and international governance*, pp. 15–27.

84. McCombs, M. E., & Shaw, D. L. (1972). "The agenda-setting function of mass media". *Public opinion quarterly*, *36*(2), pp. 176–187.

85. McDonald, A. M., & Cranor, L. F. (2008). „The cost of reading privacy policies“. *ISJLP, 4*, pp. 543–565.

86. McQuail, D. (1995). *Media performance: Mass communication and the public interest*. Sage.

87. McQuail, D. (2008). “Journalism as a public occupation: alternative images”. *Democracy, journalism and technology: new developments in an enlarged Europe: the Intellectual work of ECREA's*. pp. 47–59.

88. Mek Kvejl, D. (1994). Stari kontinent–novi mediji. *Nova, Beograd*.

89. Metzl, J. F. (1996). „Information technology and human rights“. *Human Rights Quarterly*, *18*(4), pp. 705–746.

90. Milivojević, S. (2017). “Šta je novo u novim medijima”. *Reč – Časopis za književnost i kulturu i društvena pitanja*. br. 87/33, Fabrika knjiga. str. 159–172. URL: http://www.fabrikaknjiga.co.rs/wp-content/uploads/2017/12/REC-87-33-str.159.pdf

91. Milojević, A. Radojković, M. (2016). “Revizija teorije o čuvarima kapija: oživljavanje modela u informacionom društvu”. U: Pralica, Dejan (ur.), Šinković, Norbert (ur.). *Digitalne medijske tehnologije i društveno-obrazovne promene. 5*, (Medijska istraživanja, Zbornik 5). Novi Sad: Filozofski fakultet, Odsek za medijske studije, str. 185–194.

92. Moore, M. (2016). “Tech giants and civic power”. *Centre for the Study of Media, Communication and Power*. King's College London.

93. Morando, F., Iemma, R., & Raiteri, E. (2014). “Privacy evaluation: what empirical research on users' valuation of personal data tells us”. *Internet Policy Review*, *3*(2).

94. Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. MIT press.

95. Mueller, M. L. (2015). “Hyper-transparency and social control: Social media as magnets for regulation”. *Telecomm. Policy*, *39*(9). pp. 804–810.

96. Musiani, F. (2013). “Dangerous Liaisons? Governments, companies and Internet governance”. *Internet Policy Review*, 2(1). URL: https://policyreview.info/articles/analysis/dangerous-liaisons-governments-companies-and-internet-governance

97. Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance*. Springer.

98. Napoli, P. M. (2015). "Social media and the public interest: Governance of news platforms in the realm of individual and algorithmic gatekeepers". *Telecommunications Policy*, *39*(9), pp. 751–760.

99. Negrin, R. (2005). "Modeli medijskih institucija: Medijske institucije u Evropi". U: Uvod u studije medija. Ur. Brigs i Kobli. Beograd: Klio. str. 355–374.

100. Negroponte, N. (1996). *Being digital*. Vintage.

101. Nielsen, R. K. (2013). "The Uneven Digital Revolution". In Newman, Nic & Levy, David A. L. (Eds.) Reuters Institute Digital News Report 2013. *Tracking the Future of News*, pp. 85–88.

102. Ninković-Slavnić, D. N. (2016). *Publika digitalnih medija: informisanje na internetu* (Doktorska disertacija, Univerzitet u Beogradu, Fakultet političkih nauka).

103. Nocetti, J. (2015). "Contest and conquest: Russia and global internet governance". *International Affairs*, *91*(1), pp. 111–130.

104. Obar, J. A., & Wildman, S. S. (2015). "Social media definition and the governance challenge: An introduction to the special issue". *Telecommunications Policy* 39. pp. 745–750.

105. Olmstead, K., & Smith, A. (2017a). What the Public Knows About Cybersecurity. *PewResearchCenter*, *March*, *22*.

106. Olmstead, K., & Smith, A. (2017b). *Americans and cybersecurity*. Washington, DC: Pew Research Center.

107. Palfrey, J. (2010). „Four phases of internet regulation". *Social Research*, pp. 981–996.

108. Papacharissi, Z. (2009). „The virtual sphere 2.0: The Internet, the public sphere, and beyond". *Routledge handbook of Internet politics*, pp. 230–245.

109. Parmelee, J. H., & Bichard, S. L. (2011). *Politics and the Twitter revolution: How tweets influence the relationship between political leaders and the public*. Lexington Books.

110. Pasquale, F. (2010). „Beyond innovation and competition: The need for qualified transparency in internet intermediaries". *Nw. UL Rev.*, *104*, pp. 105–173.

111. Perecman, E., & Curran, S. R. (2006). *A handbook for social science field research: essays & bibliographic sources on research design and methods*. Sage Publications.

112. Perritt, H. H. (1998). "The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance". *Indiana Journal of Global Legal Studies*, pp. 423–442.

113. Pitkänen, O., & Tuunainen, V. K. (2012). "Disclosing Personal Data Socially—An Empirical Study on Facebook Users' Privacy Awareness". *Journal of Information Privacy and Security*, *8*(1), pp. 3–29.

114. Post, D. G. (1998). "The Unsettled Paradox: The Internet, the State, and the Consent of the Governed". *Indiana Journal of Global Legal Studies*, pp. 521–543.

115. Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power*. MIT press.

116. Price, M. E., & Verhulst, S. (2000). „The concept of self-regulation and the internet". In J. Waltermann & M. Machill (Eds.), *Protecting our children on the internet: Towards a new culture of responsibility*, pp. 133–198. Bertelsmann Foundation Publishers. Retrieved from http://repository.upenn.edu/asc_papers/142

117. Radojković, M. (1987). *Međunarodno komuniciranje*. Beograd: Zavod za udžbenike i nastavna sredstva.

118. Radojković, M. (2016). "Mediji i javni interes: ogled na primeru Srbije". *Mediji i javni interes*, str. 7–19.

119. Radojković, M. (2017). „Digital media in Serbia: Uses and risks". *Politeia*, *7*(13), pp. 15–27.

120. Radojković, M., Stojković, B. (2004). *Informaciono komunikacioni sistemi*. Beograd: Clio.

121. Radojković, M., Stojković, B., & Vranješ, A. (2015). Međunarodno komuniciranje u informacionom društvu. *Clio*, *Beograd*.

122. Rainie, H., Anderson, J. Q., & Albright, J. (2017). *The future of free speech, trolls, anonymity and fake news online*. Washington, DC: Pew Research Center.

123. Robertson, D. (2004). *A dictionary of human rights*. Routledge.

124. Roig, N. A. (2010). "Regulation of pluralism in France. Context, analysis and interpretation". *Revista Latina de Comunicación Social*. pp. 472–487.

125. Rosen, J., (2011). "Free Speech, Privacy, and the Web that Never Forgets". *J. on Telecomm. and High Tech. L.* 9: 345.

126. Rubinstein, I. S., & Good, N. (2013). "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents". *Berkeley Tech. LJ*, *28*, pp. 1333–1414.

127. Samuelson, P. (2000). „Five challenges for regulating the Global Information Society". In: *Regulating the global information society*. Ed. Marsden, C. T. pp. 317–333.

128. Savelyev, A. (2016). "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?". *Computer Law & Security Review*, *32*(1), pp. 128–145.

129. Schwartz, P. M. (1999). „Internet privacy and the state". *Conn. L. Rev.*, *32*, pp. 815–859.

130. Siebert, F. S., Peterson, T., Schramm, W. (1956). *Four theories of the press: The authoritarian, libertarian, social responsibility, and Soviet communist concepts of what the press should be and do*. University of Illinois Press.

131. Simmons, B. A. (2009). *Mobilizing for human rights: international law in domestic politics*. Cambridge University Press.

132. Sinclair, D. (1997). „Self-regulation versus command and control? Beyond false dichotomies". *Law & Policy*, *19*(4), pp. 529–559.

133. Singleton, S. (2015). „Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD". *Ga. J. Int'l & Comp. L.*, *44*, pp. 165–193.

134. Slaughter, A. M. (1994). "Liberal international relations theory and international economic law". *Am. UJ Int'l L. & Pol'y*, *10*, pp. 717–743.

135. Smith, R. K. (2014). *Textbook on international human rights*. Oxford University Press.

136. Stein, L. & Sinha, N. (2002). "New Global Media and the Role of the State". In L. Lievrouw & S. Livingstone (Eds.), *Handbook of New Media*. California: Sage Publications, pp. 410–31. Updated student edition released 2006, Sage Publications.

137. Surčulija Milojević, J. (2010). "Regulatorni izazovi slobode izražavanja na Internetu". U: *Sloboda izražavanja na Internetu*. Ur: J. Surčulija. str. 17–25. Centar za razvoj Interneta: Beograd

138. Surčulija Milojević, J. (2016). *Dozvoljenost ograničenja slobode izražavanja u skladu sa evropskim instrumentima i medijskim zakonodavstvom Republike Srbije* (Doktorska disertacija, Univerzitet u Beogradu-Pravni fakultet).

139. Thomson, M. (2015). "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries". *Vand. J. Ent. & Tech. L*,Vol. 18:4, pp. 783–848.

140. Tomić, B., (2016). "Model i praksa medijskih udruženja Srbije". *Kultura polisa*, god. XIII, br. 31, str. 535–546.

141. Tow, W. N. F. H., Dell, P., & Venable, J. (2010). "Understanding information disclosure behaviour in Australian Facebook users". *Journal of Information Technology*, *25*(2), pp. 126–136.

142. Van Cuilenburg, J., & McQuail, D. (2003). "Media policy paradigm shifts: Towards a new communications policy paradigm". *European journal of communication*, *18*(2), pp. 181–207.

143. Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

144. Van Dijck, J. (2014). "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology". *Surveillance & Society*, *12*(2), pp. 197–208.

145. Van Eijk, N. (2006). "Search engines: seek and ye shall find? The position of search engines in law". *IRIS plus*, *2*. URL: https://pdfs.semanticscholar.org/a2b7/063a341fb55c4732255753958c071b1c3006.pdf

146. van Kokswijk, J. (2010). „Social Control in Online Society--Advantages of Self-Regulation on the Internet". In *Cyberworlds (CW), 2010 International Conference,* pp. 239–246.

147. Vanderstoep, S.,W., Johnston, D. (2009). *RESEARCH METHODS FOR EVERYDAY LIFE: Blending Qualitative and Quantitative Approaches*. San Francisco: A Wiley Imprint.

148. Vartanova, E. (2012). "The Russian media model in the context of post-Soviet dynamics". Eds. Hallin & Mancini. In: *Comparing media systems beyond the Western world*. pp. 119–142.

149. Veljanovski, R. (2009). "Medijska koncentracija, javnost vlasništva i pokušaj regulacije u Srbiji". *CM*. broj 13, godina IV, str. 57–79.

150. Veljanovski, R. (2017). „Ljudska prava i odgovornost novinara". *Mediji, novinarstvo i ljudska prava*, str. 7–18.

151. Villeneuve, N., (2010). "Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online". In: *Access controlled: The shaping of power, rights, and rule in cyberspace.* Eds. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Haraszti, M. pp. 55–71.

152. Vobič, I., & Milojević, A. (2012). „Societal roles of online journalists in Slovenia and Serbia: Self-perceptions in relation to the audience and print journalists". *Participations. Journal of Audience and Reception Studies*, *9*(2), pp. 469–491.

153. Wagner, B. (2014). „The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective". *Politics*. Vol. 34(1), pp. 58–71.

154. Wagner, B. (2016). *Global Free Expression-Governing the Boundaries of Internet Content*. Cham, Switzerland: Springer International Publishing.

155. Wagner, M. S. (2013). „Google glass: A preemptive look at privacy concerns“. *J. on Telecomm. & High Tech. L.*, *11*, 477.

156. Ward, D. (2005). "Media concentration and pluralism: regulation, realities and the council of Europe's Standards in the television sector. Report: The role of media freedom and pluralism in strengthening democracy". In *European Commission for Democracy Through Law (Venice Commission), Unidem, Campus Trieste Seminar*.

157. Watney, M. (2007). "State surveillance of the internet: human rights infringement or e-security mechanism?". *Int. J. of Electronic Security and Digital Forensics*, Vol. 1, No. 1, pp.42–54.

158. Weiser, P. J. (2001). „Internet Governance, Standard Setting, and Self-Regulation“. *N. Ky. L. Rev.*, *28*, pp. 822–846.

159. Wolfgang, B., & Minna, N. (2005). *Razumevanje ljudskih prava: priručnik o obrazovanju za ljudska prava*. Beograd: Beogradski centar za ljudska prava.

160. Wright, J. & Breindl, Y. (2013). "Internet filtering trends in liberal democracies: French and German regulatory debates". *Internet Policy Review*, 2(2). pp. 1–9.

161. Wu, T. S. (1996). "Cyberspace Sovereignty – The Internet and the International System". *Harv. JL & Tech.*, *10*, 647.

Internet izvori

1. *About Google News*, videti putem linka: https://www.google.com/intl/en_us/about_google_news.html (poesećeno: 10. 03. 2018. godine).

2. Akcioni plan za Poglavlje 23. Dostupno na: https://www.mpravde.gov.rs/files/Akcioni%20plan%20PG%2023%20Treci%20nacrt-%20Konacna%20verzija1.pdf (pristupljeno: 11. 01. 2019. godine).

3. Alexa https://www.alexa.com/topsites (pristupljeno: 20. 05. 2018. godine).

4. *Alexa. Top sites in Russia*. Dostupno na: https://www.alexa.com/topsites/countries/RU (pristupljeno 02. 03. 2019. godine).

5. Alexey Sidorenko (26 March 2010). „Russia: Website Closed By Police Order“. *Global Voices Advocacy*. Dostupno na: https://advox.globalvoices.org/2010/03/26/russia-website-closed-by-police-order (pristupljeno 06. 12. 2017.godine).

6. Alistair Chalrton (May 09 2018). *Artificial intelligence has become the backbone of everything Google does*. Gear Brain. https://www.gearbrain.com/google-uses-artificial-intelligence-everywhere-2567302875.html (pristupljeno 05. 01. 2019. godine).

7. Alphabet company: https://abc.xyz/ (pristupljeno 26. 06. 2018. godine).

8. Amandman civilnog sektora na član 40. Zakona o zaštiti podataka o ličnosti. Dostupno na: https://www.sharefoundation.info/wp-content/uploads/Predlog-amandmana-na-ZZPL-Partneri-Srbija-i-Share-fondacija.pdf (pristupljeno: 11. 01. 2019. godine).

9. Anđela Milivojević, Milica Stojanović. (28. jun 2017. godine). “Privatnost građana godinama na izvolite”. *CINS*. Dostupno na: https://www.cins.rs/news/srpski/article/privatnost-gradjana-godinama-na-izvolite (02. 02. 2018. godine).

10. Andrew, M. (2014). “Digital distributors cannot escape their editorial responsibilities”. *Media Policy Blog*. http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/digital-distributors-cannot-escape-their-editorial-responsibilities/ (pristupljeno 06. 03. 2018. godine).

11. ANEM: Zakon o javnom informisanju 1988. http://anem.org.rs/sr/medijskaScena/uFokusu/story/7452/Zakon+o+javnom+informisanju.html (pristupljeno 11.11.2017. godine).

12. Article 5 Federal Trade Commission Act*:* https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf (pristupljeno 02. 03. 2019. godine).

13. BBC News. (04. August 2012). Q&A: News of the World phone-hacking scandal: http://www.bbc.com/news/uk-11195407 (pristupljeno 12. 11. 2017. godine).

14. BBC. (Nov 17 2016). LinkedIn blocked by Russian authorities. Dostupno na: https://www.bbc.com/news/technology-38014501 (pristupljeno 02. 03. 2019. godine).

15. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Dostupno na: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules (pristupljeno 10. 12. 2017. godine).

16. Beta. (18. jun 2015. godine). „Sajt Peščanika pod žestokim hakerskim napadima”. *N1*. Dostupno na: http://rs.n1info.com/a70020/Vesti/Hakerski-napad-na-sajt-Pescanika.html (pristupljeno 02. 02. 2018. godine).

17. Bloomberg. (10 Apr. 2018). „Facebook Cambridge Analytica Scandal: 10 Questions Answered". *Fortune*. Dostupno na: http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/ (pristupljeno 05. 05 .2018. godine).

18. Brendan I. Koerner. (June 2002). „From Russia with Lopht". *Legal Affairs*. Dostupno na: http://www.legalaffairs.org/issues/May-June-2002/feature_koerner_mayjun2002.msp (pristupljeno 13. 12. 2017. godine).

19. Cambridge Analytica: https://cambridgeanalytica.org/ (pristupljeno 07. 05. 2018. godine).

20. Carole Cadwalladr, Emma Graham-Harrison. (17 Mar. 2018). „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *The Guardian*. Dostupno na: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (pristupljeno 04. 05. 2018. godine).

21. Cecilia Kang. (December 14, 2017). „F.C.C. Repeals Net Neutrality Rules". *The New York Times.* Dostupno na: https://www.nytimes.com/2017/12/14/technology/net-neutrality-repeal-vote.htm l (pristupljeno 15. 12. 2017. godine).

22. Château de Bossey. (2005). *Report of the Working Group on Internet Governance*. Dostupno na: https://www.wgig.org/docs/WGIGREPORT.pdf (pristupljeno 14. 12. 2017. godine).

23. Chibber, K. (December 1, 2014). „American cultural imperialism has a new name: GAFA", *Quartz*: http://qz.com/303947/us-cultural-imperialism-has-a-new-name-gafa/ (pristupljeno 22. 02. 2018).

24. Chris Chambers (1 Jul 2014). „Facebook fiasco: was Cornell's study of 'emotional contagion' an ethics breach?". *The Guardian*. https://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach (pristupljeno 05. 04. 2018. godine).

25. Christian Howard. (07 May 2018). „Introducing Google AI". *Google AI Blog*. https://ai.googleblog.com/2018/05/introducing-google-ai.html (pristupljeno 05. 01. 2019. godine).

26. CINS/Share fondacija. (20. novembar 2017. godine). „Neobaveštena ministarka: Da li je gotov nacrt zakona o zaštiti podataka o ličnosti?", *CINS*. Dostupno na: https://www.cins.rs/news/srpski/article/neobavestena-ministarka-da-li-je-gotov-nacrt-zakona-o-zastiti-podataka-o-licnosti (pristupljeno 03. 02. 2018. godine).

27. CM/Rec(2007)16. Preporuka dostupna na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d4a39 (pristupljeno: 03. 05. 2018. godine).

28. CNIL. (Sep 21 2015). *Right to delisting: Google informal appeal rejected.* https://www.cnil.fr/fr/node/15814 (pristupljeno: 22. 04. 2019. godine).

29. Cody Kapocsi. (September 14 2018). „What is the USA FREEDOM Act? What's So Free About It?". *Cloudwards.* Dostupno na: https://www.cloudwards.net/freedom-act/ (pristupljeno 03. 03. 2019. godine).

30. Committee to Protect Journalists. (October 13, 2016). *CPJ chairman says Trump is threat to press freedom*. Dostupno na: https://cpj.org/2016/10/cpj-chairman-says-trump-is-threat-to-press-freedom.php (pristupljeno: 02. 03. 2019. godine).

31. *Communication Act of 1934*. Dostupno na: https://transition.fcc.gov/Reports/1934new.pdf (pristupljeno 10. 12. 2017. godine).

32. *Communications Act 2003*. Dostupan na: http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf (pristupljeno 12. 11. 2017. godine).

33. *Conseil supérieur de l'audiovisue.* Dostupno na: http://www.csa.fr/en/The-CSA/An-Independent-Authority-to-Protect-Audiovisual-Communication-Freedom (pristupljeno, 12. 11. 2017. godine).

34. *Convencion on Cybercrime*. Council of Europe. Dostupno na: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (pristupljeno 14. 12. 2017. godine).

35. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Dostupno na: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (pristupljeno 03. 02. 2017. godine).

36. Danilo Redžepović (april 2015. godine). „Kako je hakovan Teleprompter". *Peščanik*. Dostupno na: http://pescanik.net/kako-je-hakovan-teleprompter/ (pristupljeno 01. 02. 2018. godine).

37. Dave Gershgorn & Mike Murphy (October 12, 2017). „Facebook is hiring more people to moderate content than Twitter has at its entire company". *QUARTZ*. https://qz.com/1101455/facebook-fb-is-hiring-more-people-to-moderate-content-than-twitter-twtr-has-at-its-entire-company/ (pristupljeno 04. 04. 2018. godine).

38. Dave Smith. (12 Aug. 2014). „The 11 Most Important Google Acquisitions Ever“. *Business Insider*. http://www.businessinsider.com/important-google-acquisitions-2014-8 (pristupljeno 23. 06. 2018. godine).

39. David Kaye (18 Dec. 2017). „How Europe's New Internet Laws Threaten Freedom of Expression“. *Foreign Affairs*. https://www.foreignaffairs.com/articles/europe/2017-12-18/how-europes-new-internet-laws-threaten-freedom-expression (pristupljeno: 04. 05. 2018. godine).

40. David Meyer. (January 21, 2019). „Russia: We're suing Facebook, Twitter for snubbing law on storing users' data locally“. *ZDNet*. Dostupno na: https://www.zdnet.com/article/russia-were-suing-facebook-twitter-for-snubbing-law-on-storing-users-data-locally/ (pristupljeno 03. 03. 2019. godine).

41. *Declaration on freedom of communication on the Internet*. Dostupno na: http://www.osce.org/fom/31507?download=true (pristupljeno 28. 01. 2018. godine).

42. *Deklaracija o pravima čoveka i građanina*. Dostupno na: https://www.slideshare.net/GordanaComic/francuska-deklaracija-o-pravima-oveka-i-gradjanina-iz-1789 (pristupljeno 10. 01.2018. godine).

43. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Dostupno na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046 (pristupljeno 23. 06. 2018. godine).

44. *Direktiva (EU) 2016/680 evropskog parlamenta i veća od 27. aprila 2016. o zaštiti pojedinaca u vezi sa obradom ličnih podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili progona krivičnih dela ili izvršavanja krivičnih sankcija i o slobodnom kretanju takvih podataka o stavljanju izvan snage Okvirne odluke Veća 2008/977/PUP*. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L0680&from=EN (pristupljeno: 11. 01. 2019. godine).

45. *Direktiva 95/46/EZ Evropskog parlamenta i Veća (1995) o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom protoku takvih podataka*. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A31995L0046 (pristupljeno 20. 06. 2018. godine).

46. *Direktiva o privatnosti i elektronskim komunikacijama*. Dostupno na: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32002L0058 (pristupljeno 03.02.2018. godine).

47. Dodt, S., Larson, J. & Angwin, J. (Oct. 18, 2017). „Facebook Allowed Questionable Ads in German Election Despite Warnings“. *ProPublica*. Dostupno na: https://www.propublica.org/article/facebook-allowed-questionable-ads-in-german-election-

despite-warnings?utm_source=pardot&utm_medium=email&utm_campaign=dailynewsletter (pristupljeno 02. 02. 2019. godine).

48. Dutton, H. W., Dopatka, A., Hills, M., Law, G., Nash, V. (2011). „Freedom of Connection Freedom of Expression". *UNESCO*. Dostupno na: https://unesdoc.unesco.org/ark:/48223/pf0000191594 (pristupljeno 03. 02. 2017. godine).

49. Electronic Frointer Fondation. *Computer Fraud And Abuse Act Reform*. Dostupno na: https://www.eff.org/issues/cfaa (pristupljeno: 03. 03. 2019. godine).

50. Electronic Frontier Foundation. CDA 230. *The Most Important Law Protecting Internet Speech*, dostupno na: https://www.eff.org/issues/cda230 (pristupljeno: 02. 03. 2019. godine).

51. Elliot Harmon (March 21, 2018). „How Congress Censored the Internet". *Electronic Frontier Foundation*. Dostupno na: https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet (pristupljeno: 02. 03. 2019. godine).

52. *EU Human Rights Guidelines on Freedom of Expression Online and Offline*. Dostupno na: https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf (pristupljeno 29. 01. 2018. godine).

53. Evropska komisija. *Nova era zaštite podataka u EU: Šta se menja nakon maja 2018.* Dostupno na: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf (pristupljeno 20. 06. 2018. godine).

54. *Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda*. Dostupno na: http://www.sostelefon.org.rs/zakoni/14.%20Evropska%20konvencija%20za%20zastitu%20ljudskih%20prava%20i%20osnovnih.pdf (pristupljeno 02. 02. 2017. godine).

55. Evropski Parlament, 2012. *Rezolucija o zaštiti dece u digitalnom svetu*. Dostupno na: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012IP0428&from=EN (pristupljeno 14. 12. 2017. godine).

56. *Exclusive interview with Facebook's Sheryl Sandberg*. Dostupno na: https://www.axios.com/exclusive-interview-with-facebooks-sheryl-sandberg-1513306121-64e900b7-55da-4087-afee-92713cbbfa81.html (pristupljeno: 04. 03. 2018. godine).

57. *Facebook Business* alatke. Dostupno na: https://www.facebook.com/help/331509497253087 (pristupljeno 07. 02. 2019. godine).

58. Fejsbuk, *Istraživanja*. Dostupno na: https://research.fb.com/ (pristupljeno 08. 02. 2019. godine).

59. Fejsbuk, Centar za pomoć. Dostupno na: https://www.facebook.com/help/207216349317757?helpref=related (pristupljeno 07. 02. 2019. godine).

60. Fejsbuk, *News room*, Company Info: https://newsroom.fb.com/company-info/ (pristupljeno 29. 04. 2018. godine).

61. Fejsbuk, *Politika o podacima*. Dostupno na: https://www.facebook.com/about/privacy/update/printable (pristupljeno 07. 02. 2019. godine).

62. Fejsbuk, *Standardi zajednice na Fejsbuku*. Dostupno na: https://www.facebook.com/communitystandards/ (pristupljeno 07. 02. 2019. godine).

63. Fejsbuk, *Trending Review Guidelines.* Dostupno na: https://fbnewsroomus.files.wordpress.com/2016/05/full-trending-review-guidelines.pdf (pristupljeno 04. 03. 2018. godine).

64. Fejsbuk, *Uslovi korišćenja u Austriji.* Dostupno na: https://www.facebook.com/legal/terms/plain_text_terms (pristupljeno 07. 02. 2019. godine).

65. Fondacija *Share*. (15. novembar 2018. godine). „Usvojen Zakon o zaštiti podataka o ličnosti". Dostupno na: https://www.sharefoundation.info/sr/usvojen-zakon-o-zastiti-podataka-o-licnosti/ (pristupljeno: 11. 01. 2019. godine).

66. Fondacija *Share*. (maj 2017. godine). „Strategija informacione bezbednosti usvojena bez javne rasprave". Dostupno na: *http://www.shareconference.net/sh/vesti/strategija-informacione-bezbednosti-usvojena-bez-javne-rasprave* (pristupljeno 04. 02. 2018. godine).

67. Fondacija *Share*. Dostupno na: http://www.shareconference.net/sh (pristupljeno 31. 01. 2018. godine).

68. Fondacija *Share*. *Monitoring digitalnih prava i sloboda u Srbiji*, 2016. godina. Dostupno na: https://labs.rs/Documents/Monitoring_digitalnih_prava_i_sloboda_izvestajza_2016_srb.pdf (pristupljeno 28. 01. 2018. godine).

69. Freedom House. (2017). *Freedom of the Press 2017 – China*. Dostupno na: https://freedomhouse.org/report/freedom-press/2017/china (pristupljeno 12. 11. 2017. godine).

70. Freedom House. (2017). *Freedom of the Press 2017 - United Kingdom*. Dostupno na: https://freedomhouse.org/report/freedom-press/2017/united-kingdom (pristupljeno 12. 11. 2017. godine).

71. *General Data Protection Regulation*. Dostupno na: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 (pristupljeno 02. 02. 2018. godine).

72. Glenn Greenwald. (Jun 6 2013). „NSA collecting phone records of millions of Verizon customers daily“. *The Guardian*. Dostupno na: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (pristupljeno 03. 03. 2019. godine).

73. Goodman, E. P., & Powles, J. (September 28th 2016). „Facebook and Google: Most powerful and secretive empires we've ever known”. *The Guardian*, https://www.theguardian.com/technology/2016/sep/28/google-facebook-powerful-secretive-empire-transparency (pristupljeno 05. 03. 2018. godine).

74. Gottfried, J., & Shearer, E. (2016). *News Use Across Social Medial Platforms 2016*. Pew Research Center. Dostupno na: https://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/ (pristupljeno 05. 03. 2018. godine).

75. Gouvernement.fr. *Reinforcing internal security and the fight against terrorism*. https://www.gouvernement.fr/en/reinforcing-internal-security-and-the-fight-against-terrorism (pristupljeno 23. 04. 2019. godine).

76. *Government online censorship in Serbia worrying trend*, says OSCE media freedom representative, Stockhlom, May 2014. Dostupno na: http://www.osce.org/fom/119173 (pristupljeno 01. 02. 2018. godine).

77. Griffith, E. (10 December 2017). „Memo to Facebook: How to Tell if You’re a Media Company“. *Wired*. https://www.wired.com/story/memo-to-facebook-how-to-tell-if-youre-a-media-company/ (pristupljeno 12. 02. 2018. godine).

78. Gugl, *Borba protiv nepoželjnog sadržaja*. Dostupno na: https://www.google.com/intl/sr/insidesearch/howsearchworks/fighting-spam.html (pristupljeno 23. 06. 2018. godine).

79. Gugl, *Politika privatnosti*. Dostupno na: https://policies.google.com/privacy (pristupljeno 23. 06. 2018. godine).

80. Gugl, *Pravni okvir za prenos podataka*. Dostupno na: https://policies.google.com/privacy/frameworks?hl=sr (pristupljeno 21. 10. 2018. godine).

81. Gugl, *Uslovi korišćenja usluga*. Dostupno na: https://policies.google.com/terms (pristupljeno 23. 06. 2018. godine).

82. Gugl. *Gugl nalog: Pomoć, Upravljajte lokacijom*. Dostupno na: https://support.google.com/accounts/answer/3467281?p=privpol_location&visit_id=1-636658807163676682-840908512&rd=1 (pristupljeno 23. 06. 2018. godine).

83. Gugl. *Guglovi izveštaji o transparentnosti*. Dostupno na: https://transparencyreport.google.com/user-data/overview (pristupljeno 26. 06. 2018. godine).

84. Gugl. *Guglovi izveštaji o transparentnosti. Izveštaj o Srbiji*. Dostupno na: https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:RS;time:&lu=user_requests_report_period (pristupljeno 23. 06. 2018. godine).

85. Gugl. *Infografika, Kako pretraživanje funkcioniše*. Dostupno na: https://static.googleusercontent.com/media/www.google.com/en//intl/sr/insidesearch/howsearchworks/assets/searchInfographic.pdf (pristupljeno 23. 06. 2018. godine).

86. Gugl. *Istorijat Gugla*. Dostupno na: https://www.google.com/about/our-story/ (pristupljeno 23. 06. 2018. godine).

87. Gugl. *Kako Gugl koristi kolačiće*. Dostupno na: https://policies.google.com/technologies/cookies (pristupljeno 23. 06. 2018. godine).

88. Gugl. *Kako Gugl zadržava podatke koje prikupljamo.* Dostupno na: https://policies.google.com/technologies/retention (pristupljeno 23. 06. 2018. godine).

89. Gugl. *Our latest quality improvements for Search*. Dostupno na: https://blog.google/products/search/our-latest-quality-improvements-search/ (pristupljeno 23. 06. 2018. godine).

90. Gugl. *Popisivanje i indeksiranje*. Dostupno na: https://static.googleusercontent.com/media/www.google.com/en//intl/sr/insidesearch/howsearchworks/assets/searchInfographic.pdf (pristupljeno 23. 06. 2018. godine).

91. Gugl. *Spisak svih afilijacija Gugla u EU dostupan na*. Dostupno na: https://privacy.google.com/businesses/affiliates/ (pristupljeno 23. 06. 2018. godine).

92. Gugl. *Vodič za privatnost za Gugl proizvode*. Dostupno na: https://policies.google.com/technologies/product-privacy (pristupljeno 23. 06. 2018. godine).

93. Gugl. *Vrste kolačića koje koristi Gugl*. Dostupno na: https://policies.google.com/technologies/types (pristupljeno 27. 06. 2018. godine).

94. Gugl. *Ključni termini.* Dostupno na: https://policies.google.com/privacy/key-terms#toc-terms-personal-info (pristupljeno 23. 06. 2018. godine).

95. *Guiding Principles on Business and Human Rights* (2011). Dostupno na: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (pristupljeno 23. 06. 2018. godine).

96. Heidi Towerk (May 16, 2017). „How Germany Is Tackling Hate Speech". *Foreign Affairs*. Dostupno na: https://www.foreignaffairs.com/articles/germany/2017-05-16/how-germany-tackling-hate-speech (pristupljeno 03. 02. 2019. godine).

97. Helberger, N., & Trilling, D. (2016). „Facebook is a news editor: the real issues to be concerned about". *LSE blog*. Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2016/05/26/facebook-is-a-news-editor-the-real-issues-to-be-concerned-about/ (pristupljeno: 25. 03. 2018. godine).

98. Herb Weisbaum. (Apr.18. 2018). „Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal". *NBCNews*. Dostupno na: https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011 (pristupljeno 04. 05. 2018. godine).

99. Herrman J. and Savage C. (May 23, 2018). „Trump's Blocking of Twitter Users Is Unconstitutional, Judge Says". *The New York Times*. Dostupno na: https://www.nytimes.com/2018/05/23/business/media/trump-twitter-block.html (pristupljeno 02. 03. 2019. godine).

100. *Independent Press Standards Organisation - the independent regulator of most of the UK's newspapers and magazines.* Dostupno na: https://www.ipso.co.uk (pristupljeno 12. 11. 2017. godine)

101. Inhoffen, L. (April, 2017). „Mehrheit der Deutschen findet Gesetzentwurf gegen Hasskommentare sinnvoll". *YouGov*. Dostupno na: https://yougov.de/news/2017/04/15/mehrheit-der-deutschen-findet-gesetzentwurf-gegen-/ (pristupljeno 01. 02. 2019. godine).

102. Insajder. (09. novembar, 2018. godine). "Zakon o zaštiti podataka o ličnosti usvojen bez predloženih korekcija". Dostupno na: https://insajder.net/sr/sajt/vazno/12512/ (pristupljeno: 11. 01. 2019. godine).

103. *International Covenant on Civil and Political Rights, General comment No. 34*. Dostupno na: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (pristupljeno 28. 01. 2018. godine).

104. *International Covenant on Civil and Political Rights.* Dostupno na: http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf (pristupljeno 28. 01. 2018. godine).

105. Internet Governance Forum 2018; *Speech by French President Emmanuel Macron*. Dostupno na: https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron (pristupljeno 11. 03. 2019. godine).

106. Internet World Stats. Dostupno na: http://www.internetworldstats.com/stats9.htm (pristupljeno 03.02.2018. godine).

107. Izveštaj organizacije Fridom haus „Internet sloboda 2018" za Francusku. Dostupno na: https://freedomhouse.org/report/freedom-net/2018/france (pristupljeno 20. 03. 2019. godine).

108. Izveštaj organizacije Fridom haus „Internet sloboda 2018“ za Nemačku. Dostupno na: https://freedomhouse.org/report/freedom-net/2018/germany (pristupljeno 01. 02. 2019. godine).

109. Izveštaj organizacije Fridom haus „Internet sloboda 2018“ za Rusiju. Dostupno na: https://freedomhouse.org/report/freedom-net/2018/russia. (pristupljeno 02. 03. 2019. godine).

110. Izveštaj organizacije Fridom haus „Internet sloboda 2018“ za SAD. Dostupno na: https://freedomhouse.org/report/freedom-net/2018/united-states (pristupljeno 02. 03. 2019. godine).

111. Izveštaj Poverenika za pristup informacijama od javnog značaja za 2016. godinu. Dostupno na: https://www.poverenik.rs/sr-yu/izvetaji-poverenika.html (pristupljeno 02. 02. 2018. godine).

112. Jason Abbruzzese. (April 10, 2018). „We run ads“. *NBC News*. Dostupno na: https://www.nbcnews.com/card/we-run-ads-n864606 (pristupljeno 04. 05. 2018. godine).

113. Jason Abbruzzese. (Jul 14, 2014). **„**Seeing More Politics in Your News Feed? Facebook Boosts Partisan Sites“. *Mashable*. https://mashable.com/2014/07/13/facebook-politics-partisan-newsfeed/#b9NVIoG3maql (pristupljeno 05. 04. 2018. godine).

114. Jenny Gesley (July 11, 2017). „Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under 'Facebook Act'“. *The Law Library of Congress*. Dostupno na: http://www.loc.gov/law/foreign-news/article/germany-social-media-platforms-to-be-held-accountable-for-hosted-content-under-facebook-act/ (pristupljeno 03. 02. 2019. godine).

115. John Perry Barlow. (February 8, 1996). *A Declaration of the Independence of Cyberspace.* Davos, Switzerland. Dostupno na: https://www.eff.org/cyberspace-independence (pristupljeno, 05. 12. 2017. godine).

116. Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. Case C‑131/12. Dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 (pristupljeno 24. 06. 2018. godine).

117. Jutjub. Promo klipovi politike privatnosti Gugla. Dostupno na: https://www.youtube.com/watch?time_continue=57&v=YlmVKT3Zvhw (pristupljeno 23. 06. 2018. godine).

118. Kar-Gupta & Rosemain. (May 16 2017). „Facebook fined 150,000 euros by French data watchdog“. *Reuters*. https://uk.reuters.com/article/us-facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUKKCN18C10C (pristupljeno 23. 04. 2019. godine).

119. Khrennikov&Kravchenko (5 May 2019). „Putin Wants What China’s Xi Already Has: His Own Internet“. *The Moscow Times*. Dostupno na:

https://www.themoscowtimes.com/2019/03/05/putin-wants-what-chinas-xi-already-has-his-own-internet-a64707 (pristupljeno: 08. 05. 2019).

120. Kinstler, L. (Nov 2, 2017). „Can Germany Fix Facebook?“ *The Atlantic*. Dostupno na: https://www.theatlantic.com/international/archive/2017/11/germany-facebook/543258/ (pristupljeno: 02. 02. 2019. godine).

121. Kollewe, J. (2 May 2017). „Google and Facebook bring in one-fifth of global ad revenue”. *The Guardian*. Dostupno na: https://www.theguardian.com/media/2017/may/02/google-and-facebook-bring-in-one-fifth-of-global-ad-revenue (pristupljeno 17. 02. 2018. godine).

122. Komentar Evropske komisije na Nacrt Zakona o zaštiti podataka o ličnosti. Dostupno na: http://www.partners-serbia.org/komentari-evropske-komisije-o-nacrtu-zakona-o-zastiti-podataka-o-licnosti-konacno-dostupni-javnosti/ (pristupljeno: 11. 01. 2019. godine).

123. Komunikacija Komisije Evropskom parlamentu i Veću: Veća zaštita i nove prilike – Komisija daje smernice za direktnu primenu Opšte uredbe o zaštiti podataka od 25. maja 2018. godine. Dostupno na: https://ec.europa.eu/transparency/regdoc/rep/1/2018/HR/COM-2018-43-F1-HR-MAIN-PART-1.PDF (pristupljeno 20. 06. 2018. godine).

124. Kovach., S. (October 12, 2017). „Facebook and the rest of Big Tech are now Big Media, and it's time we start treating them that way”. *Business Insider*. Dostupno na: http://www.businessinsider.com/facebook-and-google-are-now-media-companies-2017-10 (pristupljeno 20. 03. 2018. godine).

125. Krivični zakonik Republike Srbije. Dostupan na: http://www.paragraf.rs/propisi/krivicni_zakonik.html (pristupljeno 31. 01. 2018. godine).

126. Krivokapić, D., Petrovski, A. (2018). *Vodič kroz GDPR i zaštitu podataka o ličnosti: MOJI PODACI, MOJA PRAVA*. Share Fondacija, NS Press DOO Novi Sad. Dostupno na: https://resursi.sharefoundation.info/wp-content/uploads/2018/07/Podaci-u-doba-interneta-Final.pdf (pristupljeno 03. 09. 2018. godine).

127. Lance Ulanoff. (January 30, 2014). „Facebook Paper Is Content — But Don’t Call Facebook a Media Company“. *Mashable*. Dostupno na: https://mashable.com/2014/01/30/facebook-paper-app-analysis/#QAVeHyWSpqqq (pristupljeno 03. 02. 2017. godine).

128. Leighton Andrews. (December 13, 2016). „We need European regulation of Facebook and Google“. *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/12/13/we-need-european-regulation-of-facebook-and-google/ (pristupljeno 03. 02. 2017. godine).

129. Liam Tung. (September 11, 2015). „Apple reportedly takes up Moscow datacentre to comply with Russia's personal data law“. *ZDNet*. Dostupno na: https://www.zdnet.com/article/apple-reportedly-takes-up-moscow-datacentre-to-comply-with-russias-personal-data-law/ . (pristupljeno 03. 03. 2019. godine).

130. Maja Nikolić (05. jun 2017. godine). “Kad policija ‘hapsi’ tviter, imejl i mobilni telefon”. *N1*. Dostupno na: http://rs.n1info.com/a273957/Vesti/Vesti/Kad-policija-hapsi-tviter-imejl-i-mobilni-telefon.html (pristupljeno 31. 01. 2018. godine).

131. Mansell, R. (27 November 2014). „Governing the gatekeepers: is formal regulation needed?“. *Media Policy Blog*. Dostupno na: http://eprints.lse.ac.uk/80359/ (pristupljeno 23.02.2018. godine).

132. Marcelo Thompson. (August 1, 2016). Responsible Communication by Internet Intermediaries. *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/08/01/responsible-communication-by-internet-intermediaries/ (pristupljeno 05. 02. 2017. godine).

133. Maria Kiselyova & Jack Stubbs. (April 16, 2018). „Russia starts blocking Telegram messenger“. *Reuters*. Dostupno na: https://www.reuters.com/article/us-russia-telegram-blocking/russia-starts-blocking-telegram-messenger-idUSKBN1HN13J (pristupljeno 04. 03. 2019. godine).

134. Mario Pejović (31. mart, 2018). “Društvene mreže – najbolji špijuni”. *Al Jezeera Balkans*. Dostupno na: http://balkans.aljazeera.net/vijesti/drustvene-mreze-najbolji-spijuni (pristupljeno 03. 04. 2018. godine).

135. Martin de Bourmont. (January 30, 2018). „Is a Court Case in Texas the First Prosecution of a ‘Black Identity Extremist’?“. *Foreign Policy*. Dostupno na: https://foreignpolicy.com/2018/01/30/is-a-court-case-in-texas-the-first-prosecution-of-a-black-identity-extremist/ (pristupljeno 03. 03. 2019. godine).

136. Matthew Sheffield (18 Oct. 2017). „Fake news or free speech: Is Google cracking down on left media?“. *Salon*. Dostupno na: https://www.salon.com/2017/10/18/fake-news-or-free-speech-is-google-cracking-down-on-left-media/ (pristupljeno 24.06.2018. godine).

137. Mendel, T., Andrew, P., Ben, W., Dixie, H., Natalia, T. (2012). „Global Survey on Internet privacy and Freedom of Expression“. *UNESCO*. Dostupno na: https://unesdoc.unesco.org/ark:/48223/pf0000218273 (pristupljeno 03. 02. 2017. godine).

138. Michael Birnbaum. (July 31, 2014). „Russian blogger law puts new restrictions on Internet freedoms“. *The Washington Post*. Dostupno na: https://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-

freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html?utm_term=.e6f6cd636416 (pristupljeno 02. 03. 2019. godine).

139. Miller, A. (2014). „Digital distributors cannot escape their editorial responsibilities". *LSE blog*. Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/digital-distributors-cannot-escape-their-editorial-responsibilities/ (pristupljeno 13. 03. 2018. godine).

140. Miodrag Sovilj. (25. mart 2017. godine). "Šabić o iscurelim podacima: Ogroman broj krivičnih dela". *N1*. Dostupno na: http://rs.n1info.com/a237666/Vesti/Vesti/Sabic-o-iscurelim-podacima-Ogroman-broj-krivicnih-dela.html (pristupljeno 02. 02. 2018. godine).

141. Miodrag Sovilj. (mart 2017. godine). "Šta stranke znaju o vama?. *N1*. Dostupno na: http://rs.n1info.com/a237644/Vesti/Vesti/Sta-stranke-znaju-o-vama-Procurili-podaci-400.000-gradjana.html (pristupljeno 03. 02. 2018. godine).

142. Mitchell, A., Gottfried,J.,& Matsa K., E. (2015). „Facebook Top Source for Political News Among Millennials". *Pew Research Centre*. Dostupno na: https://www.journalism.org/2015/06/01/facebook-top-source-for-political-news-among-millennials/ (pristupljeno 05. 02. 2017. godine).

143. Mitchell, A., Simmons, K., Matsa, K. E., & Silver, L. (2018). „Publics globally want unbiased news coverage, but are divided on whether their news media deliver". *Pew Research Center's Global Attitudes Project*. Dostupno na: http://www.pewglobal.org/2018/01/11/detailed-tables-global-media-habits/ (pristupljeno 20. 10. 2018. godine).

144. Moore, M. (2 April 2017). „Society will be defined by how we deal with tech giants", *Guardian*. Dostupno na: https://www.theguardian.com/commentisfree/2017/apr/01/brexit-britain-respond-tech-giants-civic-role-googleapple-facebook-amazon-eu (pristupljeno, 14. 02. 2018. godine).

145. *N1*. (21.10.2018. godine). "Iz novog zakona obrisana reč zakon, svi građani u opasnosti". Dostupno na: http://rs.n1info.com/Vesti/a429536/Sabic-i-Krivokapic-o-Predlogu-zakona-o-zastiti-podataka.html (pristupljeno 11. 01. 2019. godine).

146. Napoli, P. (2014). „Digital intermediaries and the public interest standard in algorithm governance". *LSE Media Policy Project Blog*. Dostupno na: http://blogs.lse.ac.uk/mediapolicyproject/2014/11/07/digital-intermediaries-and-the-public-interest-standard-in-algorithm-governance/ (pristupljeno 04. 05. 2018. godine).

147. Natali Helberger. (September 15, 2016). „Facebook is a new breed of editor: a social editor". *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/09/15/facebook-is-a-new-breed-of-editor-a-social-editor/ (pristupljeno 03. 02. 2017. godine).

148. Naughton, J. (2016). „Digital Dominance: forget the 'digital' bit". *LSE blog*. Dostupno na: https://blogs.lse.ac.uk/mediapolicyproject/2016/07/12/digital-dominance-forget-the-digital-bit/ (pristupljeno 04. 02. 2017. godine).

149. NetzDG. Dostupno na: https://germanlawarchive.iuscomp.org/?p=1245 (pristupljeno 02. 02. 2019. godine).

150. Nikolaj Nielsen. (10 Oct. 2014). „Freedom of expression complicates EU law on 'right to be forgotten'". *Euobserver*. Dostupno na: https://euobserver.com/justice/126011 (pristupljeno 23. 05. 2018. godine).

151. *Office of Communications.* Dostupno na: https://www.ofcom.org.uk/ (pristupljeno 12. 11. 2017. godine).

152. Olga Razumovskaya. *(*April 10 2015). „Google Moves Some Servers to Russian Data Centers". *The Wall Street Journal*. Dostupno na: https://www.wsj.com/articles/google-moves-some-servers-to-russian-data-centers-1428680491 (pristupljeno 03. 03. 2019. godine).

153. *OpenNet Initiative*. Dostupno na: https://opennet.net/about-filtering (pristupljeno: 09. 12. 2017. godine).

154. *Oxford dictionary*. Dostupno na: https://en.oxforddictionaries.com/definition/troll (pristupljeno 23. 08. 2018. godine).

155. Perset, K. (2010). "The Economic and Social Role of Internet Intermediaries". OECD *Digital Economy Papers*, No. 171, OECD Publishing. URL: http://dx.doi.org/10.1787/5kmh79zzs8vb-en (pristupljeno 23. 08. 2018. godine).

156. Pew Research Centre. (September 21, 2016). „The state of privacy in post-Snowden America". *Fact Tank*. Dostupno na: https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (pristupljeno 04. 02. 2017. godine).

157. Pismo Povrenika Šabića Narodnoj skupštini Republike Srbije povodom člana 40 Zakona o zaštiti podataka o ličnosti. Dostupno na: https://www.poverenik.rs/images/stories/dokumentacija-nova/pismaorganima/pismoposlanicimaZZPLCL40.pdf (pristupljeno 11. 01. 2019. godine).

158. Politička deklaracija: *Sloboda izražavanja i demokratija u digitalnoj eri: Mogućnosti, prava, odgovornosti.* Dostupno na: http://www.kultura.gov.rs/cyr/aktuelnosti/politicka-deklaracija---sloboda-izrazavanja-i-demokratija-u-digitalnoj-eri (pristupljeno 29. 01. 2018. godine).

159. Politička deklaracija*: Sloboda izražavanja i demokratija u digitalnoj eri: Mogućnosti, prava, odgovornosti Rezolucija broj 1: Sloboda interneta.* Dostupno na:

http://www.kultura.gov.rs/cyr/aktuelnosti/politicka-deklaracija---sloboda-izrazavanja-i-demokratija-u-digitalnoj-eri (pristupljeno 29. 01. 2018. godine).

160. *Povelja Evropske unije o ljudskim pravima.* Dostupno na: http://ravnopravnost.gov.rs/wp-content/uploads/2012/11/images_files_Povelja%20Evropske%20unije%20o%20osnovnim%20pravima.pdf (pristupljeno 20. 06. 2018. godine).

161. *Pregovaračka poglavlja 23 i 24 – O čemu pregovaramo?.* Dostupno na: https://www.mpravde.gov.rs/tekst/7029/vodic-za-novinare-poglavlja-23-i-24-o-cemu-pregovaramo.php (pristupljeno 03. 02. 2018. godine).

162. Preporuka CM/Rec(2014)6 komiteta ministara državama članicama o vodiču o ljudskim pravima za korisnike interneta. Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f4d (pristupljeno 20. 06. 2018. godine).

163. Press Complaints Commission. Dostupno na: http://www.pcc.org.uk (pristupljeno 12. 11. 2017. godine).

164. *Privacy Shield*. Dostupno na: https://www.privacyshield.gov/welcome (pristupljeno 21. 10. 2018. godine).

165. Projekat „Slobodno izražavanje i zaštita privatnosti na internetu u Srbiji“, *Yucom*. Dostupno na: http://www.yucom.org.rs/sloboda-izrazavanja-i-zastita-privatnosti-na-internetu-u-srbiji/ (pristupljeno 02. 02. 2018. godine).

166. Radmilo Marković (27. oktobar 2016. godine). “Javi Đuri da blokira Fejsbuk”. *Vreme*. Dostupno na: https://www.vreme.com/cms/view.php?id=1438089&print=yes (pristupljeno 05. 05. 2017. godine).

167. Rainie, L. (2016). „The state of privacy in post-Snowden America“. *Pew Research Centre*. Dostupno na: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (pristupljeno 05. 05. 2017. godine).

168. RATEL, Tehnički uslovi. Dostupno na: http://www.ratel.rs/editor_files/File/dozvole/uputstva/Tehnicki_uslovi-internet.pdf (pristupljeno 07. 02. 2017. godine).

169. Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns. Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4a3d (pristupljeno 25. 03. 2018. godine).

170. Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies). Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0 (pristupljeno 03. 03. 2018. godine).

171. *Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines*. Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87 (pristupljeno 24. 06. 2018. godine).

172. *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member State on the protection of human rights with regard to social networking services.* Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b (pristupljeno 25. 06. 2018. godine).

173. *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries*, dostupna na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14 (pristupljeno 23. 06. 2018. godine).

174. *Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business.* Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1ad4 (pristupljeno 27. 06. 2018. godine).

175. *Remarks Of FCC Chairman Ajit Pai at the Newseum*. Washington DC, April 26, 2017. Dostupno na: https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0426/DOC-344590A1.pdf (pristupljeno 15. 12. 2017. godine).

176. *Reolution 68/167: The right to privacy in the digital age.* Dostupno na: https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf (pristupljeno 28. 01. 2018. godine).

177. Report of the Tunis phase of the World Summit on the Information Society. (16–18 November 2005). Tunis, Kram Palexpo. Dostupno na: http://www.itu.int/net/wsis/docs2/tunis/off/9rev1.pdf (pristupljeno 17. 12. 2017. godine).

178. Reporters Without Boders. (July 19, 2017). *Russian bill is copy-and-paste of Germany's hate speech law*. Dostupno na: https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law (pristupljeno 04. 03. 2019. godine).

179. Republički zavod za statistiku (2018). *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2018. Domaćinstva/pojedinci, preduzeća*. Beograd. Dostupno na: http://publikacije.stat.gov.rs/G2018/Pdf/G201816013.pdf (pristupljeno 03. 02. 2018. godine).

180. Republički zavod za statistiku. *Upotreba interneta*. Dostupno na: http://www.stat.gov.rs/WebSite/repository/documents/00/02/64/26/17-Informacione_tehnologije.pdf (pristupljeno 03. 02. 2018. godine).

181. *Review of BBC Internal Governance*. Dostupno na: http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/about/how_we_govern/governance_review_2013.pdf (pristupljeno 12. 11. 2017. godine).

182. *Rezolucija 56/83.* UN. Dostupno na: http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf (pristupljeno 14. 12. 2017. godine).

183. *Royal Charter, BBC*. Dostupno na: http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/about/how_we_govern/2016/charter.pdf (pristupljeno 12. 11. 2017. godine).

184. RTV Kruševac (09. septembar, 2017. godine). "Privedene dve žene zbog pretnji Vučiću i Gašiću na Fejsbuku". *N1*. Dostupno na: http://rs.n1info.com/a316666/Vesti/Vesti/Privedene-dve-zenske-osobe-zbog-pretnji-Vucicu-i-Gasicu.html (pristupljeno 31. 01. 2018. godine).

185. Ruddick, G. (16 November 2017). "Katharine Viner: in turbulent times, we need good journalism more than ever". *The Guardian*. Dostupno na: https://www.theguardian.com/media/2017/nov/16/katharine-viner-we-need-public-interest-journalism-in-turbulent-digital-age (pristupljeno 16. 02. 2018. godine).

186. Ruddick, G. (27 November 2017)." Society faces 'tsunami of harms' from lack of online regulation". *The Guardian*. Dostupno na: https://www.theguardian.com/media/2017/nov/27/society-faces-tsunami-of-harms-from-lack-of-online-regulation (pristupljeno 22. 02. 2018. godine).

187. Sami Ben Gharbia, (18 September 2007). "Russian LiveJournal blogger could face three-year sentence". *Global Voices Advocacy*. Dostupno na: https://advox.globalvoices.org/2007/09/18/russian-livejournal-blogger-could-face-three-year-sentence (pristupljeno 06. 12. 2017.godine).

188. Samuel Gibbs. (16 Feb 2018). "Facebook ordered to stop collecting user data by Belgian court". *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court (pristupljeno 06. 05. 2018. godine).

189. *Saopštenje Centra za istraživačko novinarstvo Srbije*, decembar 2013. godine. Dostupno na: http://www.nuns.rs/info/statements/20821/saopstenje-centra-za-istrazivacko-novinarstvo-srbije.html (pristupljeno 02. 01. 2018. godine).

190. Savet Evrope, 2012. Konvencija o zaštiti dece od seksualne eksploaticije i seksualnog zlostavljanja. Dostupno na: https://rm.coe.int/168046e1e1 (pristupljeno 14. 12. 2017. godine).

191. Scott, M. (March 24 2016). „Google Fined by French Privacy Regulator". *The New York Times*. Dostupno na: https://www.nytimes.com/2016/03/25/technology/google-fined-by-french-privacy-regulator.html?_r=0 (pristupljeno 22. 04. 2019. godine).

192. Section 222 Telecommunications Act. Dostupno na: https://www.law.cornell.edu/uscode/text/47/222 (pristupljeno 02. 03. 2019. godine).

193. Sergey Brin, Lawrence Page. *The Anatomy of a Large-Scale Hypertextual Web Search Engine*. Dostupno na: http://infolab.stanford.edu/~backrub/google.html (pristupljeno 23. 06. 2018. godine).

194. Shalal, A., Auchard, E., (Sep. 22, 2017). „German election campaign largely unaffected by fake news or bots". *Reuters*. Dostupno na: https://www.reuters.com/article/us-germany-election-fake/german-election-campaign-largely-unaffected-by-fake-news-or-bots-idUSKCN1BX258 (pristupljeno 04. 02. 2019. godine).

195. Shashi Jayakumar. (March 13, 2018). „Germany's NetzDG: Template for Dealing with Fake News?". *RSIS Commentary. No. 41*. Dostupno na: https://www.rsis.edu.sg/wp-content/uploads/2018/03/CO18041.pdf (pristupljeno: 02. 02. 2019. godine).

196. Shead, S. (May 30, 2017). Facebook said Germany's plan to tackle fake news would make social media companies delete legal content. *Business Insider*. Dostupno na: https://www.businessinsider.com/facebook-says-germany-fake-news-plans-comply-with-eu-law-2017-5?r=UK&IR=T (pristupljeno: 02. 02. 2019. godine).

197. Slučaj *Reno vs American Liberty Civic Union.* Dostupno na: https://supreme.justia.com/cases/federal/us/521/844/ (pristupljeno 02. 03. 2019. godine).

198. *Stash Invest.* Dostupno na: https://learn.stashinvest.com/companies-brands-owned-google (pristupljeno 23. 06. 2018. godine).

199. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine. Dostupno na: http://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html (pristupljeno 03. 02. 2018. godine).

200. Strategija Saveta Evrope za upravljanje internetom 2016-2019. Dostupno na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60 (pristupljeno 17. 12. 2017. godine).

201. Strategije razvoja informacione bezbednosti za period od 2017. do 2020. godine. Dostupno na: http://www.srbija.gov.rs/vesti/dokumenti_sekcija.php?id=45678 (pristupljeno 04. 02. 2018. godine).

202. *Terms of Services. Didn't read*. Dostupno na: https://tosdr.org/ (pristupljeno 20.08.2018. godine).

203. The Moscow Times. (July 1, 2018). „Russia's 'Big Brother' Law Enters Into Force". Dostupno na: https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066 (pristupljeno 03. 03. 2019. godine).

204. The USA PATRIOT Act. Dostupno na: https://www.justice.gov/archive/ll/highlights.htm (pristupljeno 03. 03. 2019. godine).

205. Thielman., S. (12 May 2017). „Facebook news selection is in hands of editors not algorithms, documents show". *The Guardian*. Dostupno na: https://www.theguardian.com/technology/2016/may/12/facebook-trending-news-leaked-documents-editor-guidelines (pristupljeno 24. 02. 2018. godine).

206. *TrustArc*. Dostupno na: https://feedback-form.truste.com/watchdog/request (pristupljeno 07. 02. 2019. godine).

207. UNESCO. (2009). *Series of Internet Freedom*. Dostupno na: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publications-by-series/unesco-series-on-internet-freedom/ (pristupljeno 03. 02. 2017. godine).

208. Uredba (EU) 2016/679 Evropskog parlamenta i Veća (2016) o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka. Dostupno na: http://esigurnost.org/wp-content/uploads/2018/01/GDPR-Uredba-2016.679.pdf (pristupljeno 20. 06. 2018. godine).

209. US Press Freedom Tracker. (April 5, 2018). „Journalist Manuel Duran, arrested while covering immigration protest, could be deported by ICE". Dostupno na: https://pressfreedomtracker.us/all-incidents/journalist-manuel-duran-arrested-while-covering-immigration-protest-could-be-deported-ice/ (pristupljeno 03. 03. 2019. godine).

210. Ustav Republike Nemačke. Dostupno na: https://www.btg-bestellservice.de/pdf/80201000.pdf (pristupljeno: 01. 02. 2019. godine).

211. Ustav Republike Srbije. Dostupno na: http://www.paragraf.rs/propisi/ustav_republike_srbije.html (pristupljeno 30. 01. 2018. godine).

212. Ustav SAD na srpskom jeziku. Dostupno na: http://www.prafak.ni.ac.rs/files/nast_mat/Ustav_SAD_sprski.pdf (pristupljeno 02. 03. 2019. godine).

213. Veronica Khokhlova, (15 July 2008). „Russia: One Year in Prison for Blog Comment. *Global Voices Advocacy*. Dostupno na: https://advox.globalvoices.org/2008/07/15/russia-one-year-in-prison-for-blog-comment (pristupljeno 06. 12. 2017. godine).

214. World Summit on the Information Society. (Geneva 2003). *Plan of Action*. Dostupno na: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf (pristupljeno 14. 12. 2017. godine).

215. Yucom. (decembar 2017. godine). „Sudska praksa o internetu u Srbiji suprotna Evropskom sudu". Dostupno na: http://www.yucom.org.rs/sudska-praksa-o-internetu-u-srbiji-suprotna-evropskom-sudu/ (pristupljeno 02. 02. 2018. godine).

216. Zakon o elektronskim komunikacijama. Dostupno na: http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html (pristupljeno 01. 02. 2018. godine).

217. Zakon o javnom informisanju i medijima. Dostupno na: http://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html (pristupljeno 30. 01. 2018. godine).

218. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Dostupno na: http://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html (pristupljeno 02. 02. 2018. godine).

219. Zakon o zaštiti podataka o ličnosti iz 2018. godine. Dostupan je na sajtu Poverenika: https://www.poverenik.rs/sr-yu/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B84.html (pristupljeno 11. 01. 2019. godine).

220. Zakon o zaštiti podataka o ličnosti. Dostupno na: http://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html (pristupljeno 02. 02. 2018. godine).

Lista grafikona u radu

Lista tabela u radu

Lista slika u radu

Biografija

Marta Mitrović je rođena 19. novembra 1989. godine u Leskovcu. Diplomirala je na Filozofskom fakultetu, Univerziteta u Nišu, na smeru za novinarstvo sa prosečnom ocenom 9,35. Master studije novinarstva je, takođe, završila na Filozofskom fakuletu u Nišu, sa prosečnom ocenom 10. Master rad na temu „Marginalizacija beletrističkih žanrova u srpskoj dnevnoj štampi“, pod mentorstvom prof. dr Tatjane Vulić, odbranila je najvišom ocenom. Univerzitet je 2013. godine izabrao za najboljeg master studenta Univerziteta u Nišu.

Od 2013. godine zaposlena je na Filozofskom fakultetu u Nišu, na smeru za komunikologiju i novinarstvo, najpre kao saradnik u nastavi, a potom u zvanju asistenta u užoj naučnoj oblasti Komunikologija, jezik i studije medija. Sekretar je časopisa *Media Studies and Applied Ethics*. Učestvovala je na dva domaća naučnoistraživačka projekta.

Objavila je više radova u domaćim i inostranim časopisima, među kojima su: Vulić Tatjana, Mitrović Marta, (2015), „Smart Phone Apss as a Source of Information for students“, *Rethinking education by leveraging the eLearning pillar of the Digital Agenda for Europe*, Vol. 1: pp. 320-326; Vujović Marija, Mitrović Marta, Obradović Neven. ‚(2018)., "Women and Olympic Games: Media Coverage", Teme, No. 4: pp. 1113-1137; Vulić Tatjana, Mitrović Marta, (2016), „Virtuelne zajednice: označavanje značenja u onlajn prostoru“, Kultura polisa, godina XIII, broj 31: str. 559-573. Kultura – Polis; Mitrović Marta, Obradović Neven. (2014), „(Mis)use of anonymous sources in the tabloids in Serbia: Comparative analysis of content of serbian tabloids Blic and Kurir“. Facta universitatis – Series Philosophy, Sociology, Psychology and History. Vol. 13, No 3: pp. 147 – 158. University of Niš, Niš. Predstavljala je svoje radove na naučnim skupovima u zemlji i inostranstvu.

Prilozi

Prilog 1 - Upitnik

Demografski podaci

Pol:	M		Ž	
Godine starosti:	18-38	39-59	60+	
Mesto stanovanja:	urbana sredina		ruralna sredina	
Obrazovanje:	osnovnoškolsko	srednjoškolsko	visokoškolsko	postdiplomsko
Profesionalno usmerenje:	društveno-humanistička oblast	tehničko-tehnološka oblast	oblast prirodnih nauka	pravno-ekonomska oblast

Odnos prema slobodi izražavanja i privatnosti na internetu

Smatram da su moji podaci koje delim na internetu zaštićeni.	Ne	Nisam siguran	Da
Smatram da mi je sloboda izražavanja na internetu zagarantovana.	Ne	Nisam siguran	Da
Smatram da je moguće zaštiti privatnost na internetu.	Ne	Nisam siguran	Da
Osećam se slobodno da objavljujem svoje stavove onlajn.	Ne	Nisam siguran	Da
Čitam Uslove korišćenja (Fejsbuka, Gugla), pre nego što ih prihvatim.	Ne	Nisam siguran	Da

Odnos prema kompaniji Fejsbuk kada je reč o slobodi izražavanja i privatnosti

Upoznat/a sam sa politikom privatnosti Fejsbuka.	Ne	Nisam siguran	Da
Smatram da bi svako trebalo da vodi računa o svojoj privatnosti na Fejsbuku.	Ne	Nisam siguran	Da
Promenio/la sam podrazumevana podešavanja na Fejsbuku, koja se odnose na privatnost, i na taj način dodatno zaštitio/la svoju privatnost.	Ne	Nisam siguran	Da
Većinu mojih objava na Fejsbuku mogu da vide i oni koji mi nisu prijatelji.	Ne	Nisam siguran	Da
Fejsbuk ima moju dozvolu da koristi podatke sa mog uređaja, računara ili mobilnog telefona.	Ne	Nisam siguran	Da
Fejsbuk ima moju dozvolu da pristupi zvučniku i kameri na mom uređaju, računaru ili mobilnom telefonu.	Ne	Nisam siguran	Da
Fejsbuk ima moju dozvolu da pristupi mojim mejl i telefonskim kontaktima.	Ne	Nisam siguran	Da

Fejsbuk ima moju dozvolu da pristupi mojoj galeriji, slikama sačuvanim na memoriji uređaja.	Ne	Nisam siguran	Da
Fejsbuk ima moju dozvolu da moje podatke ustupa trećim licima, kompanijama sa kojima sarađuje.	Ne	Nisam siguran	Da
Zadovoljan sam načinom na koji Fesbuk štiti moju privatnost.	Ne	Nisam siguran	Da
Smatram da bi Fejsbuk trebalo da bude transparentniji u pogledu deljenja podataka svojih korisnika sa trećim licima, drugim kompanijama.	Ne	Nisam siguran	Da
Smatram da imam pravo da znam kojim licima i kojim povodom je Fejsbuk prosledio moje podatke.	Ne	Nisam siguran	Da
Smatram da kompanija Fejsbuk može da mi uskrati slobodu izražavanja.	Ne	Nisam siguran	Da
Smatram da Fejsbuk manipulše objavama koje se pojavljuju na mom News Feed-u.	Ne	Nisam siguran	Da

	aktuelnosti			*hronologiji*			*interesovanji ma korisnika*			*sponzorstvima*		
Smatram da se objave na News Feed-u pojavljuju po:	Ne	Nisam siguan	Da	Ne	Nisamsiguran	Da	Ne	Nisam siguran	Da	Ne	Nisam siguran	Da

Prava internet korisnika na Fejsbuku najviše su ugrožena od:	drugih Fejsbuk korisnika	kompanije Fejsbuk	trećih lica, kao što su reklamne agencije, agencije za statistiku i slično	države

Odnos prema kompaniji Gugl kada je reč o privatnosti i slobodi izražavanja

Smatram da Gugl i aplikacije povezane sa njim, štite moju privatnost i lične podatke.	Ne	Nisam siguran	Da
Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe podacima sa mog uređaja: mobilnog telefona, tableta, računara i slično.	Ne	Nisam siguran	Da
Gugl i aplikacije povezane sa njim imaju moju dozvolu da prate moje aktivnosti na internetu.	Ne	Nisam siguran	Da
Gugl i aplikacije povezane sa njim imaju moju dozvolu pristupe mojim kontaktima na mejlu.	Ne	Nisam siguran	Da
Gugl i aplikacije povezane sa njim imaju moju dozvolu da pristupe sadržaju mojih mejlova.	Ne	Nisam siguran	Da
Smatram da Gugl ne može imati uticaj na moju slobodu izražavanja.	Ne	Nisam siguran	Da
Smatram da pretraživač Gugl manipuliše rezultatima pretrage.	Ne	Nisam siguran	Da
Prilikom pretrage putem Gugla informacije koje dobijem kao rezulatat pretrage rangiraju se prema:			

značaju			*aktuelnosti*			*hronologiji*			*interesovanjima korisnika*			*sponzorstvima*		
Ne	Nisam siguran	Da	Ne	Nisam siguran	Da	Ne	Nisam siguran	Da	Ne	Nisam siguran	Da	Ne	Nisam siguran	Da

Šta je prema vašem mišljenju to što bi kompanije, poput Gugla i Fejsbuka, trebalo da urade da bi se osećali sigurnije kada koristite njihove usluge:			
a). da budu transparentiji u pogledu deljenja mojih podataka	Ne	Nisam siguran	Da
b). da poboljšaju politiku privatnosti,	Ne	Nisam siguran	Da
c). da odlučnije preuzmu odgovornost za svoje poslovanje,	Ne	Nisam siguran	Da
d). da na jednostavniji način upoznaju korisnike sa načinom poslovanja	Ne	Nisam siguran	Da

Odnos prema Republici Srbiji kada je reč o slobodi izražavanja i privatnosti na internetu

Smatram da Vlada RS narušava privatnost internet korisnika.	Ne	Nisam siguran	Da
Smatram da Vlada i Vladine agencije RS prate aktivnosti internet korisnika u Srbiji.	Ne	Nisam siguran	Da
Osećam se nesigurno ili zabrinuto pri onlajn deljenju stavova koji kritikuju Vladu Srbije.	Ne	Nisam siguran	Da
Smatram da Vlada i Vladine agencije RS ugrožavaju slobodu izražavanja internet korisnicima u Srbiji.	Ne	Nisam siguran	Da

Kada bih znao da Vlada RS može da pristupi sadržajima koje delim na internetu, bez sudskog naloga, čak i kada su te objave privatne, putem mejla ili direktnih poruka na društvenim mrežama, osećao/osećala bih da Vlada:

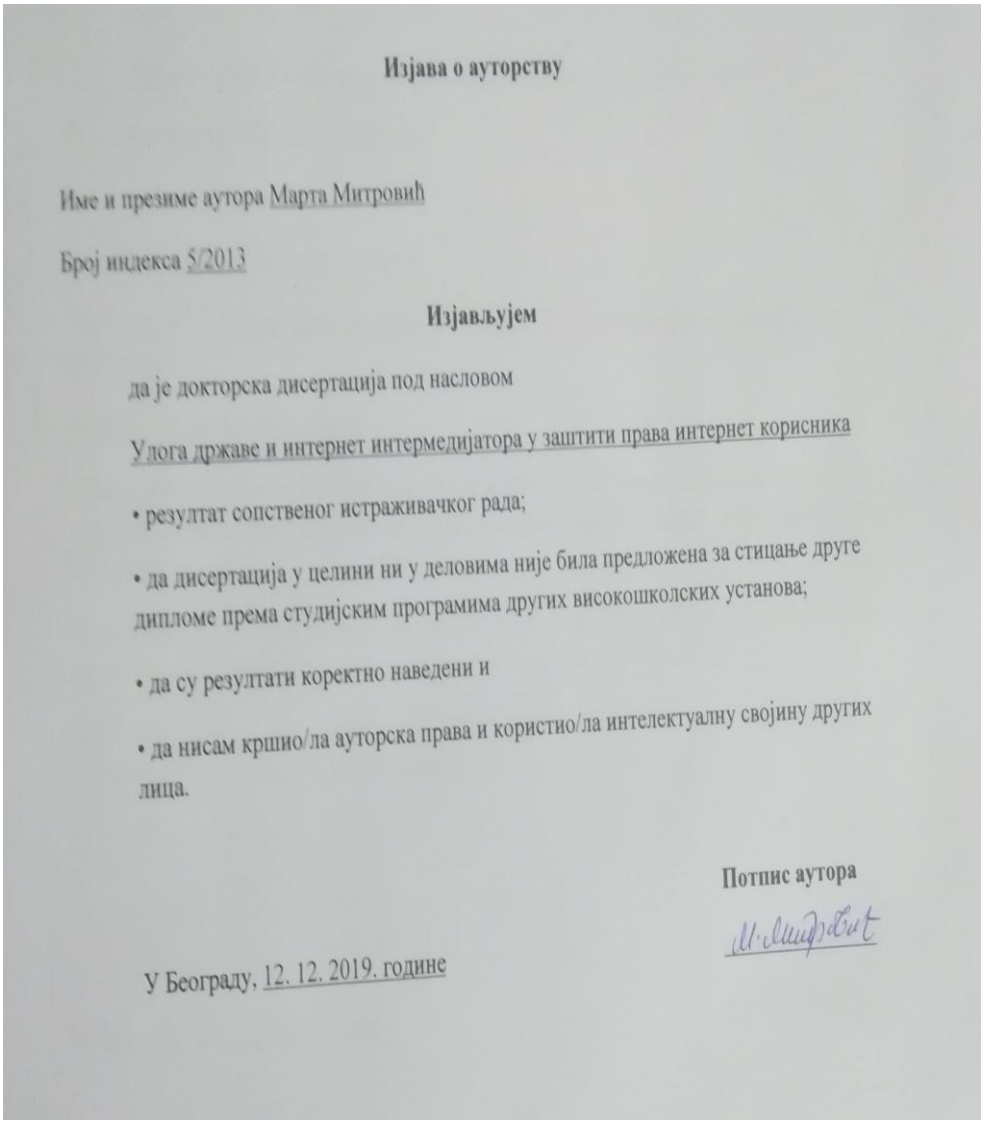
a). ugrožava moju privatnost.			b). ugrožava moju slobodu izražavanja.			c). štiti bezbednost svih građana		
Ne	Nisam siguran	Da	Ne	Nisam siguran	Da	Ne	Nisam siguran	Da

Smatram da bi Vlada RS mogla da me zaštiti ukoliko bi neka privatna kompanija zloupotrebila moje podatke deljene onlajn kroz:

a). jasno zakonodavstvo	Ne	Nisam siguran	Da
b). nacionalna tela oformljena specijalno u svrhu monitoringa rada privatnih kompanija na internetu	Ne	Nisam siguran	Da
c). zakonom predviđeno sankcionisanje privatnih internet kompanija	Ne	Nisam siguran	Da

d). veću saradnju sa privatnim kompanijama na internetu	Ne	Nisam siguran	Da
e). veće učešće u regulisanju internet prostora	Ne	Nisam siguran	Da
Smatram da bi država trebalo da uzme veće učešće u regulaciji internet prostora.	Ne	Nisam siguran	Da
Smatram da bi internet kompanije trebalo da u saradnji sa državama osiguraju internet prostor.	Ne	Nisam siguran	Da
Smatram da je najbolji način uređivanja internet prostora prepuštanje privatnim kompanijama da same kreiraju politike i upravljaju podacima, bez učešća država.	Ne	Nisam siguran	Da
Ukoliko bih morao/morala da biram, moje podatke koje delim onlajn bih prepustio/la na čuvanje:	privatnim kompanijama (Fejsbuku, Guglu)		državi

Prilog 2 – Izjava o autorstvu



Изјава о ауторству

Име и презиме аутора Марта Митровић

Број индекса 5/2013

Изјављујем

да је докторска дисертација под насловом

Улога државе и интернет интермедијатора у заштити права интернет корисника

• резултат сопственог истраживачког рада;

• да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;

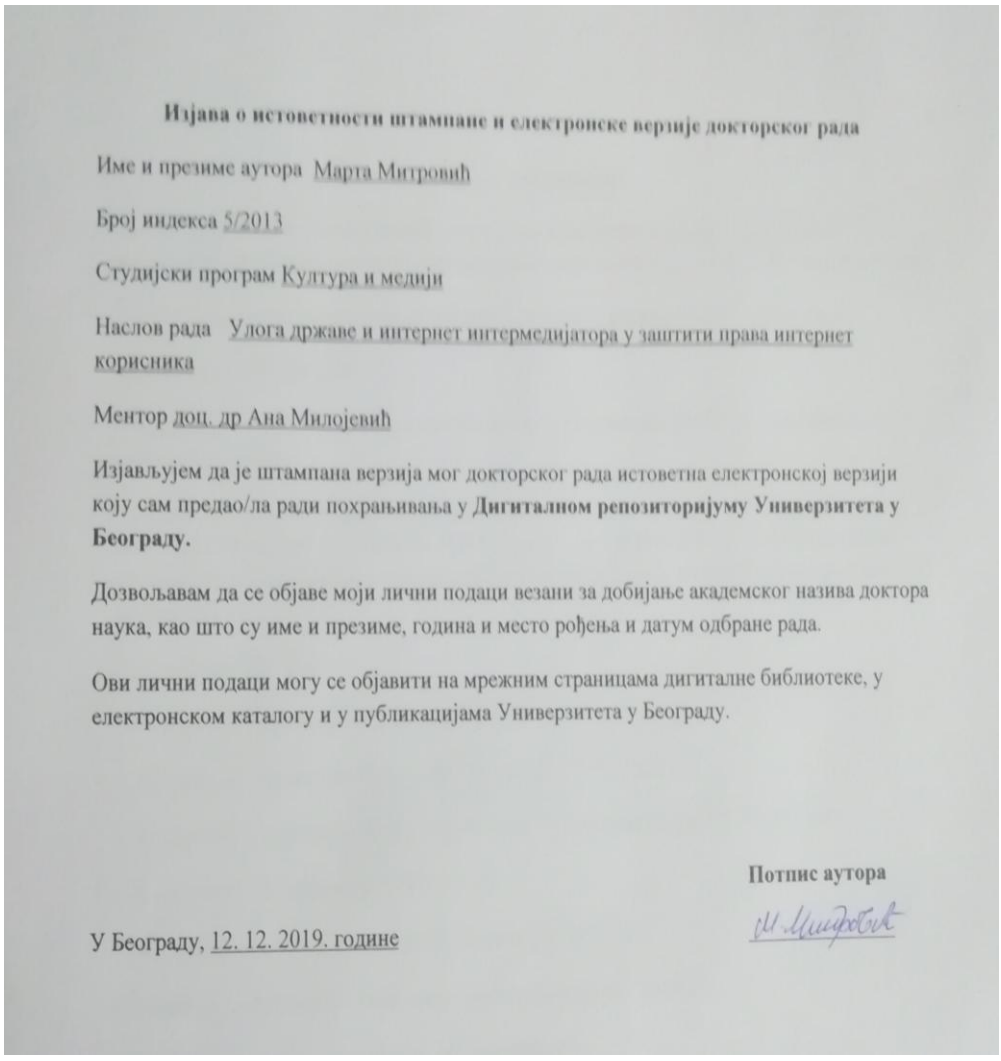
• да су резултати коректно наведени и

• да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 12. 12. 2019. године

Prilog 3 – Prilog o istovetnosti štampane i elektronske verzije doktorskog rada



Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Марта Митровић

Број индекса 5/2013

Студијски програм Култура и медији

Наслов рада Улога државе и интернет интермедијатора у заштити права интернет корисника

Ментор доц. др Ана Милојевић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањивања у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 12. 12. 2019. године

Prilog 4 – Izjava o korišćenju

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Улога државе и интернет интермедијатора у заштити права интернет корисника

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.

Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, 12. 12. 2019. године

1. **Ауторство**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. **Ауторство – некомерцијално**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. **Ауторство – некомерцијално – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. **Ауторство – некомерцијално – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. **Ауторство – без прерада**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. **Ауторство – делити под истим условима**. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.