DEMO-KRACIJA I *BIG TECH*

REGULACIJA ZA SUŽIVOT

GONG

IMPRESSUM

Autor:
Tin Puljić

Grafička obrada:
Sven Sorić

ISBN 978-953-7960-26-1

Zagreb, prosinac 2021.

NAKLADNIK: GONG

Izvršna direktorica
Oriana Ivković Novokmet

Ulica Valentina Vodnika 4
10 000 Zagreb

e-mail: gong@gong.hr
web: www.gong.hr

Gong je Centar znanja u području građanskog aktivizma i izgradnje demokratskih institucija društva u okviru Razvojne suradnje s Nacionalnom zakladom za razvoj civilnoga društva.

DEMOKRACIJA I *BIG TECH* —REGULACIJA ZA SUŽIVOT

DEMOKRACIJA I *BIG TECH* —REGULACIJA ZA SUŽIVOT

Uspon društvenih mreža stubokom je promijenio svakodnevni život ljudi diljem svijeta. Postojanje komunikacijskih platformi koje omogućavaju neprestanu i laku povezanost nije samo stvorilo novu dimenziju društvenoga života, već je otključalo i širok spektar organizacijskih i poslovnih mogućnosti. Društvene mreže samo su dio općeg fenomena digitalizacije društva i ekonomije — živimo u eri digitalnih usluga, u dobu kada se kupoprodajne aktivnosti, pristup osobnim dokumentima, obrazovni programi i aktivnosti, kultura te zabava i razbibriga u sve većoj mjeri sele *online*, u elektronske oblike i podatkovni promet, te se globalno tržište roba i usluga u skladu s time transformira i prilagođava.

Potencijali društvenih mreža i velikih tehnoloških kompanija ne postoje odvojeno od sfere politike. Štoviše, komunikacijska i podatkovna moć društvenih mreža i njihovih kreatora duboko je isprepletena s područjem političkoga, mijenjajući ga i oblikujući. Društvene mreže promijenile su načine i navike informiranja građana, izazvavši medijski *mainstream* na nezapamćene načine, te zamutile granice između informacije i dezinformacije te istine i laži — i to do te mjere da je 2016. godine Oxford Dictionaries za riječ godine proglasio *post-truth*[1], koncept koji objašnjava specifičnu atmosferu anksioznosti i nesigurnosti stvorenu kao posljedica manjka jasnih putokaza za razlikovanje istine od neistine u javnoj sferi. Golema količina podataka koja se skuplja o korisnicima društvenih mreža te interneta općenito otvara i opasne mogućnosti malverzacija i manipulacije u političkoj sferi i sferi javnoga diskursa, a profit koji tim putem stvaraju velike tehnološke kompanije stvara poticaj za nastavak takvih modela poslovanja. Cilj je ovoga članka propitati vezu društvenih mreža, korporativne tehnološke elite i politike; odnosno konkretnije njihov utjecaj i suživot s demokracijom, te analizirati mogućnosti regulacije i zauzdavanja njihova potencijala za negativne učinke po demokratsko društvo kroz izlaganje i opis trenutnih metoda te potencijalnih budućih rješenja.

DRUŠTVENE MREŽE I DEMOKRATSKA JAVNA SFERA

Društvene mreže na djelovanje građana u demokratskom društvu utječu kroz dva vida djelovanja — kao komunikacijske platforme te kao platforme za prikupljanje podataka.

1 BBC — https://bbc.in/3npnhgT

Po pitanju aspekta komunikacije, društvene mreže opasnima čini upravo ona karakteristika koju bismo mogli nazvati i najdemokratičnijom — govoriti može svatko. Dok je za plasiranje informacije u javnu sferu putem *mainstream* medija nužan dug proces obrade (analiza i obrada podataka, provjera činjenica, odobrenje uredništva medijske kuće itd.), komunikacija na društvenim medijima više nalikuje struji svijesti. Ne postoji barijera između misli i njihova komuniciranja stotinama, tisućama ili stotinama tisuća ljudi; komunikacija je udaljena tek jedan klik. Komunikacija se odvija potpuno slobodno, ali i nezamislivo brzo. Broj ljudi koji stupi u interakciju s određenom objavom ili člankom na društvenim mrežama eksponencijalno se povećava sa svakim daljnjim dijeljenjem; odnosno, svaki sljedeći korisnik dijeljenjem određenoga sadržaja taj sadržaj čini dostupnim i vidljivim svim ljudima s kojima je povezan na nekoj društvenoj mreži, te se tako stvara nepregledan lanac širenja sadržaja.

Mogućnost slobodne i brze komunikacije isprva se čini kao demokratski raj, deliberativna demokracija temeljena na etici diskursa kakvom ju je zamislio Jürgen Habermas, u kojoj opće društvo građana poput senzora reagira na podražaje u političkoj sferi te komunicirajući svoje reakcije i preferencije utječe na politički sustav. Komunikacija sa širokim brojem ljudi bez cenzure i kontrole, a time i sa značajno smanjenom mogućnošću supresije od strane vladajućih, čini se kao idealan način da se ozbilji komunikacijska moć građanstva te svakome udijeli privilegija da govori i da se izrazi, te time sudjeluje u političkoj sferi i u usmjeravanju djelovanja političkih institucija.

Problem s ovakvim pogledom jest što je isuviše naivan, odnosno što pretpostavlja da će se komunikacija odvijati u dobroj vjeri. Ako uzmemo da će svi akteri djelovati u pravcu onoga što bismo rousseauovski mogli nazvati općom voljom, stavljajući osobne interese sa strane kako bi se uobličio društveni interes na osnovu kojega će se krojiti pravac djelovanja države, tada su društvene mreže zaista pomak prema idealu demokracije. Ipak, u analizi njihova utjecaja na demokraciju valja uzeti u obzir realnu sliku. U jednakoj mjeri u kojoj društvene mreže mogu imati pozitivan učinak, mogu imati i negativan te poguban.

Eklatantan primjer negativnoga učinka društvenih mreža kao komunikacijske platforme pruža nam pandemija bolesti COVID-19. Društvene su mreže, poglavito Facebook (uključujući platforme Instagram

i WhatsApp koje se nalaze pod vlasništvom Facebooka) i Twitter, služile kao rasadnik dezinformacija o bolesti, cjepivima i njihovoj učinkovitosti, te javnozdravstvenim mjerama poput nošenja maski. Na pojedinačnim profilima i grupama mogle su se naći tvrdnje kako je cijepljenje tek paravan za globalni plan čipiranja stanovništva iza kojega stoji Bill Gates, kako cjepiva čine ljudska tijela ranjivima na navodno pogubno djelovanje 5G tehnologije, te kako je cijela pandemija zapravo „plandemija" orkestrirana kako bi poslužila navodnim malicioznim planovima bogatih elita. Istraživanje provedeno od strane regionalne *fact-checking* mreže SEE Check[2] u kojemu se analiziraju dezinformacije o pandemiji koje su članice mreže raskrinkavale u periodu od početka pandemije do kraja listopada 2020. godine pokazalo je da je glavni izvor dezinformacija na području zemalja bivše Jugoslavije (osim Slovenije, koja nije obuhvaćena istraživanjem) bio upravo Facebook. Na području Hrvatske, čak 45.84% svih dezinformativnih objava raskrinkanih od strane portala Faktograf[3] poteklo je s Facebooka, daleko više nego s bilo kojeg drugog izvora. Sličan obrazac vidljiv je i van regije. Na uzorku od 225 dezinformativne objave na engleskom jeziku, studija instituta Reuters baziranog na oxfordskom sveučilištu utvrdila je da je 69% analiziranih dezinformacija poteklo s društvenih mreža[4]. Stvarni opseg dezinformacija koje kolaju društvenim mrežama zasigurno je mnogo veći no što statistika može obuhvatiti — slijedom brzine komunikacije na društvenim mrežama, najčešće je nemoguće utvrditi originalni izvor određene dezinformacije, niti mapirati njen puni doseg. Primjeri eksponencijalnog širenja dezinformativnih objava mogu se uočiti u čitavoj regiji. Jedan takav primjer jest viralan video pseudoznanstvenice Erne Selimović, objavljen na njenome Facebook profilu[5], u kojemu Selimović optužuje nacionalne vlade za „zaprašivanje nanopartikulama teških metala" koje potom navodno reagiraju sa 5G zračenjem i stvaraju bolest kod ljudi. Za simptome koronavirusa prema Selimović nije kriv virus, već „oksidativni stres" i stanje straha. Potom Selimović svoju pseudoznanstvenu priču povezuje sa Billom Gatesom i njegovom navodnom

2 Disinformation during COVID-19 pandemic (Friedrich Naumann Foundation For Freedom) — https://bit.ly/3owX0fQ

3 Gong je do studenog 2021. bio nakladnik Faktografa

4 Reuters Institute — https://bit.ly/304NeWp

5 Erna Selimović (Facebook profil) — https://bit.ly/3HvqfZi

kontrolom nad Svjetskom zdravstvenom organizacijom te planom da se kroz „ID2020 projekt“ ljudima nametne cjepivo koje će „nas lišiti naše slobodne volje i svega onoga ljudskog u nama“ ugrađujući čip u ljudsko tijelo. Prema podacima portala Raskrinkavanje.ba, video je unutar prvih 24 sata od objave podijeljen preko 23000 puta te je već dan nakon objave pregledan preko 502000 puta[6].

Potencijal društvenih mreža za širenje dezinformacija nije bitan samo u smislu izravnog utjecaja na ljudsko ponašanje, već i u smislu ugrožavanja osnova demokratskoga sustava. Temeljna premisa demokracije jest mogućnost građanina da donese informiranu odluku, a pretpostavka za tu premisu je dostupnost provjerenih i točnih informacija na temelju kojih građanin procjenjuje svoje interese i preferencije te politički djeluje. U trenutku kada se granica između istine i neistine zamućuje, a javna sfera postaje sve zagađenija dezinformacijama, sama pretpostavka demokracije dovedena je u pitanje.

Dezinformativni potencijal društvenih mreža postaje još opasniji u sprezi s populizmom. Populističko uokviravanje sfere političkoga svodi se na podjelu političkog polja, kako navodi nizozemski politolog Cas Mudde, „na dvije antagonističke skupine — običan narod i korumpiranu elitu“ (Mudde, 2004: 543, cit. prema Šalaj, 2012: 57)[7]. Unutar te dihotomije populist je onaj koji odabire biti zastupnik naroda, te je time drugačiji — nije dio establišmenta, već je iskren i dobronamjeran. Koncept društvenih mreža kao polja slobodne i necenzurirane komunikacije izvrsno se uklapa u populistički *framework* — s jedne strane stoje *mainstream* mediji, sluge i plaćenici svirepe te okrutne elite; a s druge obični građani i njihovi iskreni zastupnici, istinoljupci koji na društvenim mrežama šire ono za što vlast navodno ne želi da se čuje. Najznačajniji primjer takvoga djelovanja nalazimo u bivšega američkog predsjednika Donalda Trumpa, koji je u svojim javnim istupima popularizirao termin *fake news*, tvrdeći da protiv njega postoji medijska zavjera kojoj je cilj potkopati njegovu vlast i Ameriku samu. Trumpov omiljeni način komunikacije bio je upravo putem društvenih mreža, ponajviše putem Twittera, a te je kanale koristio ne samo tijekom svojega mandata već i u pokušaju aktivne sabotaže demokratskog procesa, potičući (direktno i indirektno) nasilne prosvjede i

6 Raskrinkavanje.ba — https://bit.ly/3nN8Znm

7 Šalaj, Berto (2012) Što je populizam? *Političke analize* 3(11): 55-61.

napad na zgradu Kongresa tijekom prebrojavanja elektorskih glasova poslije predsjedničkih izbora. Prema Facebookovim podacima, na dan je spomenutih prosvjeda za širenje dezinformacija najčešće prijavljivan profil na platformi Instagram bio upravo Trumpov — @realdonaldtrump[8]. Na puno manjoj razini, ali na sličan način djelovali su određeni akteri u Hrvatskoj. Bivši saborski zastupnik Ivan Pernar, primjerice, koristio je svoj Facebook profil za aktivno širenje dezinformacija o novom koronavirusu te o cijepljenju, kako za COVID-19 tako i za ostale bolesti. Recentniji je primjer pak molekularni biolog i donedavni član Znanstvenog savjeta Vlade RH Gordan Lauc, koji je koristio svoju platformu i pristup javnoj sferi za širenje dezinformacija vezanih uz pandemiju — više je puta prognozirao kraj ili slom pandemije (među ostalim i ovoga ljeta[9] kada je ustvrdio da je najgori dio pandemije prošao; po trenutnoj epidemiološkoj situaciji vidi se da to nije slučaj) tvrdeći da je upozoravanje na opasnost od virusa tek „pandemijski marketing", pozivao je građane na prosvjedovanje protiv COVID potvrda[10] direktno podrivajući napore u sprječavanju virusa te kampanji cijepljenja, te je više puta iznosio činjenično netočne i obmanjujuće tvrdnje[11].

9

Na spomenutim primjerima razvidno je da dezinformativni potencijal društvenih mreža nije ograničen samo na opće građanstvo, već da ga vrlo često ciljano i s namjerom koriste akteri službene politike, podrivajući demokratski sustav iznutra te izravno utječući na političko ponašanje, političko nasilje te ishode političkih procesa poput parlamentarnih ili predsjedničkih izbora. Slijedom toga, regulacija društvenih mreža neophodna je kako bi se zauzdali njihovi negativni utjecaji.

Utjecaj društvenih mreža na demokraciju valja promotriti i kroz njihovu ulogu kao platforme za prikupljanje podataka o korisnicima. Algoritmi na društvenim mrežama određuju koja će se vrsta sadržaja, te koliko često, prikazivati korisnicima ovisno o procjeni vjerojatnosti da korisnik želi vidjeti takav sadržaj. To čine prikupljajući podatke o količini vremena koju korisnici provode u interakciji s određenim tipom sadr-

8 The Washington Post — https://wapo.st/3wUeWVB

9 Novi List — https://bit.ly/3HMFJrI

10 Tportal — https://bit.ly/3nM9UHQ

11 Faktograf — https://bit.ly/3FGl2Mu

žaja, o vrsti sadržaja koji korisnici najčešće pregledavaju te o obrascima njihova ponašanja na društvenim mrežama. Ovisno o tome, *feed* koji svaki pojedini korisnik vidi biva prilagođenim i personaliziranim. Ponovno, isprva se ovo doima kao isključivo pozitivan element društvenih mreža — sloboda personaliziranja iskustva na društvenim mrežama čini se kao način da korisnici iz njih poluče maksimalnu učinkovitost i užitak. U kontekstu političke sfere, ipak, ovdje leži i opasnost. Algoritmi na društvenim mrežama stvaraju tzv. komore odjeka (*echo chambers*) — prikazujući korisnicima samo one vrste sadržaja s kojima su do tada ostvarili interakciju, zatvaraju ih u vlastita stajališta te izoliraju od potencijalnih kontraargumenata njihovim uvjerenjima. Ovo je pogotovo važno kod političkog sadržaja — ukoliko pojedinac koji se nalazi na određenom dijelu ideološkog spektra na društvenim medijima vidi samo sadržaje s tog dijela spektra, stvara se dojam da su njegova uvjerenja poduprta pregrštom dokaza, dok su dokazi za bilo kakvo suprotno stajalište tek sporadični, te ih se kao takve može ignorirati. Na ovaj se način potpiruje potvrdna pristranost (*confirmation bias*), odnosno tendencija da se prihvaća samo one dokaze i podatke koji podupiru vlastito stajalište, time izbjegavajući duboko neugodan osjećaj kognitivne disonance. Uzevši da je pretpostavka zdrave demokracije da postoji dostupnost i zastupljenost informacija i stajališta sa svih dijelova ideološkog spektra, te da kroz njihovo sučeljavanje u javnoj sferi građani izgrađuju svoja osobna koherentna uvjerenja (stoga, primjerice, uoči izbora postoje predizborne kampanje, predstavljanja programa, debate, i slično), ovaj je fenomen izrazito opasan za demokratsko društvo. Ne samo da građane odvaja od deliberacije u javnoj sferi, već to često čini bez njihove svijesti a samim time i bez informiranoga pristanka — još jedne osobine slobodnoga građanina.

Druga opasna dimenzija prikupljanja podataka jest njihova aktivna zloupotreba. Najpoznatiji je takav primjer skandal vezan uz konzultantsku tvrtku Cambridge Analytica. Spomenuta je firma naručila izradu aplikacije *This is Your Digital Life*, čija je uloga trebala biti da ispitanici, uz informirani pristanak, odgovaraju na niz istraživačkih pitanja. Facebook je aplikaciji dopustio da prikuplja podatke ne samo od ispitanika, već i od korisnika koje su ispitanici imali na listi prijatelja na Facebooku, čime je Cambridge Analytica prikupila podatke o više desetaka milijuna korisnika bez njihova znanja i pristanka, a te je podatke kasnije ustupljivala za potrebe predsjedničke kampanje

Donalda Trumpa uoči američkih predsjedničkih izbora 2016. godine[12]. Kako navodi Julie Carrie Wong, novinarka britanskog lista The Guardian, ono zastrašujuće u aferi Cambridge Analytica jest upravo to da se nije radilo o sigurnosnom propustu ili kakvom hakerskom napadu, već o tome da je Facebookov sustav radio upravo onako kako je i zamišljeno — prikupljajući podatke i ustupajući ih trećoj strani[13]. Afera Cambridge Analytica nije prvi takav primjer — istraga New York Timesa iz 2018. godine otkrila je kako je Facebook podatke o svojim korisnicima ustupao drugim velikim kompanijama poput Yahooa, Microsofta i Amazona[14], a kroz svoj sustav omogućavanja reklamnog prostora raznim akterima (koji mogu biti tržišni akteri poput kompanija, ali i politički akteri) putem kojega je moguće stvarati targetirane reklame prilagođene osobina određene skupine potencijalnih kupaca robe i usluga praktički izravno omogućava spomenutim akterima pristup osobnim podacima korisnika. Razlog zašto je Cambridge Analytica skandal posebno problematičan jest to što je izravno utjecao na ishode političkih procesa, narušivši jednakost unutar izbornog procesa time što je određenim kandidatima omogućen pristup resursima koje drugi nisu posjedovali, te (mnogo važnije) prekršivši osnovno ljudsko pravo na privatnost. U ovome slučaju povreda prava na privatnost nije bila ograničena samo na izravnu povredu, već je narušila mogućnost oštećenih građana da slobodno i pod svojim uvjetima sudjeluju u demokratskom procesu. Jedan od temelja demokratskoga sustava jest mogućnost da se u političku sferu slobodno stupa te slobodno od nje izlazi; odnosno, sloboda političkog djelovanja mora podrazumijevati i emancipaciju od obveze takvoga djelovanja. U ovom su slučaju građani u obliku metapodataka van svoje volje uključeni u politički proces, te su ti metapodaci potom iskorišteni za manipulaciju procesom.

Ne mogu se poreći pozitivni učinci društvenih mreža — osiguravanjem pristupačne i jednostavne komunikacije pospješuju javni diskurs, omogućavaju platformu za organizaciju doprinoseći slobodi udruživanja, te su u nizu primjera igrale važnu ulogu u promicanju i izgradnji demokracije (primjerice tijekom Arapskog proljeća, kada su se skupine aktivista organizirale putem društvenih mreža, napose u Egiptu, te koristile

12 New York Times — https://nyti.ms/3oCDZZr

13 The Guardian — https://bit.ly/3kKEobh

14 New York Times — https://nyti.ms/3Fmme7u

društvene mreže kako bi globalno komunicirale o događanjima na terenu[15]). Ipak, jednako tako mora se uzeti u obzir i njihov negativni potencijal, te valja razmotriti rješenja za njegovo zauzdavanje.

KAKO REGULIRATI NEGATIVNE UČINKE?

Prva je mogućnost prepustiti stvar nevidljivoj ruci tržišta — pretpostavka teoretičara tržišne ekonomije nalagala bi da budući da velike tehnološke kompanije kao i svi drugi tržišni akteri ovise o zadržavanju povjerenja korisnika, one također imaju poticaj na samoregulaciju te da će nakon skandala poput spomenute afere Cambridge Analytica promijeniti svoje djelovanje. Na prvi pogled činilo bi se da je uistinu tako. Nakon Cambridge Analytica skandala, Facebook je suspendirao na desetke tisuća problematičnih aplikacija izrađenih od strane oko 400 *developera* od kojih neki nisu surađivali u Facebookovoj internoj istrazi[16], te uveo opciju „*clear history*"[17] putem koje korisnici mogu izbrisati podatke koje Facebook o njima skuplja dok koriste opcije pretraživanja. Tijekom američkih predsjedničkih izbora 2020. godine uveden je niz mjera za suzbijanje dezinformacija[18], uključujući označavanje objava ovisno o tome dolaze li iz provjerenih izvora, smanjivanje dosega problematičnih objava, smanjivanje broja ljudi koje administratori mogu pozivati u Facebook grupe u cilju suzbijanja skupina kao što je QAnon te osnivanje tzv. *Civic Integrity* skupine čiji je zadatak bio borba protiv dezinformacija. Nakon nasilnih prosvjeda na Kapitolu, Facebook je uklonio profil Donalda Trumpa do daljnjega.

Iako su svi ovi primjeri pohvalni, samoregulacija nije ni približno idealno rješenje. Zviždačica i bivša članica Facebookove *Civic Integrity* skupine Frances Haugen nedavno je američkom Kongresu i nizu medijskih kuća ustupila niz Facebookovih internih dokumenata koji otkrivaju čitav pregršt problema u djelovanju ove društvene mreže. Kao prvo, otkriveno je da je velika količina javnih izjava predsjednika Facebooka Marka Zuckerberga naprosto netočna — primjerice, Zuckerberg je na saslušanju pred Kongresom tvrdio da Facebook uklanja 94% objava koje sadrže govor mržnje na platformi prije nego što ga

15 Pew Research Center — https://pewrsr.ch/3Ft0C9I

16 CNBC — https://cnb.cx/3CsJP13

17 The Verge — https://bit.ly/3r1i69d

18 The Washington Post — https://wapo.st/3wUeWVB

ijedan korisnik uopće prijavi, dok interne studije procjenjuju da se radi tek o 5% svih takvih objava[19]. Nadalje, Facebook ulaže tek mizernu količinu sredstava u suzbijanje dezinformacija i govora mržnje van SAD-a te u svijetu u razvoju. Prema podacima iz 2020., čak 84% sredstava usmjerenih u tu svrhu namijenjeno je za teritorij SAD-a, a ostalih 16% otpada na „ostatak svijeta", što uključuje zemlje sve od Francuske i Italije pa do Indije (gdje je manjak regulacije govora mržnje izravno dovodio do etnički motiviranog nasilja, primarno prema muslimanima iz regije Kašmir)[20]. Naposljetku, otkriveno je i da je Facebook bio u posjedu podataka o tome na koji način, kojom brzinom i od strane kojeg broja ljudi se dezinformacije o pandemiji bolesti COVID-19 šire na njegovim platformama, no odbijao ih je ustupiti političkim institucijama koje su ih tražile[21], time izravno ugrožavajući borbu protiv dezinformacija. Razlog tome nalazi se u profitnom motivu svih tržišnih aktera — što je veća količina korisnika društvenih mreža (pa makar oni širili dezinformacije), te što je veća količina podataka kojom one raspolažu, to im je ujedno i veći potencijal za ostvarenje financijske dobiti.

S obzirom na rečeno, prepustiti pitanje regulacije velikih kompanija i njihovih društvenih mreža njima samima nije dostatno rješenje.

Jedno od rješenja koje se nameće u borbi protiv dezinformacija jest *fact-checking*, odnosno provjera istinitosti podataka sadržanih u objavama na društvenim mrežama. Udruženje *International Fact Checking Network* (IFCN) okuplja preko stotinu *fact-checking* organizacija uključujući i hrvatski Faktograf.hr, te se članice udruženja kao neovisna i nepolitička tijela bave raskrinkavanjem dezinformacija kroz izravne odgovore na određene objave te kroz analize i studije, označavanjem dezinformativnih objava na društvenim mrežama kao što su Facebook i Twitter (što im je omogućeno kroz dogovore i partnerstvo sa spomenutim platformama — i Facebook i Twitter imaju sklopljene dogovore s članicama IFCN-a), upozoravanjem djelitelja dezinformativnih sadržaja te smanjenjem dosega takvih objava. Uloga je *fact-checkinga* upozoriti korisnike društvenih mreža da sadržaj koji konzumiraju potencijalno dolazi iz neprovjerenih izvora te smanjiti utjecaj dezinformacija u javnoj sferi.

19 The Washington Post — https://wapo.st/30AhkEV

20 The Washington Post — https://wapo.st/30BpqgE

21 The Washington Post — https://wapo.st/3wXg6zB

Ipak, *fact-checking* ima svoja ograničenja. Kao prvo, ispravljanje netočnih podataka i prezentiranje točnih ne mora rezultirati u promjeni uvjerenja i ponašanja kod konzumenata sadržaja. Tim znanstvenika s pariških sveučilišta Sciences Po i Ecole d'économie de Paris proveo je istraživanje[22] u kojemu su skupini od 2480 francuskih glasača prezentirali činjenično netočne izjave o izbjegličkoj krizi radikalno desne kandidatkinje Marine Le Pen, a nekima od njih potom i točne podatke o istim pitanjima, te je utvrđeno da izlaganje činjenicama ne utječe u relevantnoj mjeri na politička uvjerenja ili podršku određenome kandidatu (Barrera i sur., 2020). Ispravljanje netočnih podataka ne znači ujedno i uspješnu promjenu kompletnoga sustava uvjerenja, što znači da politički akteri koji šire dezinformacija često ne gube podršku čak i u momentu kada ih se aktivno prozove i ispravi. Nadalje, ljudi su snažno averzivni prema onome što dovodi u pitanje njihov identitet i njegove temelje. Budući da su ideološka identifikacija te identifikacija s političkim strankama snažni elementi identiteta, suočavanje s dokazima o njihovoj problematičnosti (u ovom slučaju, o sudjelovanju u širenju dezinformacija) stvara osjećaj kognitivne disonance te izaziva prirodnu reakciju odbacivanja takvih podataka te čak povećanja podrške spomenutim akterima (Pereira i Van Bavel, 2018)[23]. Konačno, receptivnost prema *fact-checkingu* ovisi o apriornim percepcijama koje pojedinci imaju prema organizacijama koje provode *fact-checking*. Ako je osoba uvjerena da je trenutna pandemija zapravo globalna zavjera, ili da postoji urota *mainstream* medija protiv njoj omiljena političkoga kandidata, tada će se djelovanje *fact-checking* organizacija shvaćati kao nastavak navodne zavjere ili urote i pokušaj da se zataška istina (dovoljno je promotriti komentare na Facebook stranici portala Faktograf.hr kako bi se uvjerilo u istinitost ove tvrdnje).

Čak i pod pretpostavkom da navedeni problemi ne postoje te da je *fact-checking* nedvosmisleno efikasan, upitno je do koje je mjere moguće računati na tehnološke kompanije da same dosljedno i detaljno provode činjenične provjere te označavaju i/ili uklanjaju

22 Barrera, Oscar; Guriev, Sergei; Henry, Emeric; Zhuravskaya, Ekaterina (2020) Facts, alternative facts, and fact checking in times of post-truth politics. *Journal of Public Economics* 182: 104-123.

23 Pereira, Andrea i Van Bavel, Jay J. (2018) The Partisan Brain: An Identity-Based Model of Political Belief. *Trends in cognitive sciences* 22(3): 213-224.

dezinformativni sadržaj. Studija provedena od strane neprofitne organizacije Avaaz[24], primjerice, ukazuje na to kako Facebook ne čini ni približno dovoljno kako bi ograničio širenje dezinformacija na svojoj platformi. Studija je pokazala kako su napori Facebooka na ovoj fronti u 2021. godini čak i oslabili za 1% u odnosu na prethodnu godinu, te da je stanje pogotovo loše po pitanju sadržaja koji nije na engleskome jeziku — 56% takvoga sadržaja ne dočeka nikakvu reakciju od strane Facebooka. Također, prosječno vrijeme između objave određenog dezinformativnog sadržaja i njegove oznake kao takvoga tijekom 2021. godine bilo je 28 dana — drugim riječima, čak i onaj sadržaj koji na koncu bude označen kao dezinformativan ima na raspolaganju bogatu zalihu vremena tijekom kojega se nemilice dijeli kako na Facebooku, tako i na drugim društvenim mrežama te interakcijama licem u lice. Nadalje, sam je Facebookov algoritam za identifikaciju dezinformacija manjkav. Istražujući 119 Facebook stranica koje su širile dezinformativne sadržaje, Avaazova studija[25] utvrdila je kako postoje vrlo jednostavni načini za zaobilazak Facebookova algoritma. Iako je algoritam u teoriji načinjen s ciljem da po identifikaciji određene dezinformativne objave označi i sve alternativne verzije te objave, širitelji dezinformacija uspijevali su izbjeći označavanje banalnim koracima kao što je promjena fonta, promjena pozadinske boje vizualnog sadržaja ili pak *cropping* slika u objavi. Unutar uzorka od 738 objava koje je Facebookov algoritam trebao prepoznati i označiti, tek 4%[26] dobilo je oznaku. Spomenute su objave kumulativno pogledane preko 140 milijuna puta. Ukratko, ne samo da *fact-checking* ima strukturalne manjkavosti, već postoji i konzistentan manjak voljnog momenta velikih tehnoloških kompanija kao što je Facebook da ga dosljedno implementiraju.

Kako bi se pokušalo obuhvatnije riješiti problem, sljedeći je korak zakonska regulacija. Ovdje će fokus biti na dvama zakonskim prijedlozima Europske komisije — Zakonu o digitalnim uslugama (*Digital Services Act* — DSA) i Zakonu o digitalnim tržištima (*Digital Markets Act* — DMA) — kao primjerima takva zakonskoga djelovanja. Nacrt DSA[27] predviđa niz mjera koje bi svakako predstavljale regulativni

24 Avaaz — https://bit.ly/30YGpJy

25 CNN — https://cnn.it/3r5mnZ2

26 Mashable — https://bit.ly/3DKZGNg

27 EUR-Lex — https://bit.ly/3qIq4Ut

napredak. Člankom 14 predviđa se implementacija lako dostupnih mehanizama prijave neprimjerenog ili protuzakonitog sadržaja, dok članak 19 tome pridodaje obvezu da se prijave podnesene od strane „označivača od povjerenja" (*trusted flaggers*) kao što su to ranije spomenute *fact-checking* organizacije promptno procesuiraju, čime bi se osiguralo efikasan nadzor nad neželjenim sadržajem. U svrhu osiguranja transparentnosti, članci 17 i 18 predviđaju postojanje internog mehanizma rješavanja prigovora putem kojega bi oštećene strane, odnosno one strane čiji je sadržaj uklonjen, mogle podnijeti žalbu; te previđaju i mogućnost vansudskog rješavanja spora putem arbitraže ako žalba ne bude riješena interno. Članci 26-32 dodatno podebljavaju obveze vrlo velikih *online* platformi (*very large online platforms*) — spomenute su platforme u sklopu pružanja usluga na teritoriju EU obvezne minimalno jednom godišnje provoditi procjene sistemskog rizika od pojave negativnog sadržaja, ugroza po pravo na privatnost, informiranje i slobodno istraživanje te manipulacije uslugama platforme koje mogu ugroziti javno zdravlje, javni diskurs te druga relevantna područja ljudskog života. Platforme su dužne implementirati mjere za suzbijanje utvrđenog sistemskog rizika, a mjere mogu uključivati promjene u algoritmima, smanjenje dosega određenog sadržaja te pojačavanje nadzora sadržaja. Kako bi se osiguralo poštivanje ovih odredbi, platforme su se dužne bar jedanput godišnje podvrgnuti vanjskoj reviziji od strane nezavisnog ovlaštenog tijela, te imenovati povjerenika za usklađenost poslovanja s provizijama DSA. U svrhu poboljšanja transparentnosti, člankom 29 uvodi se obveza objavljivanja parametara koje algoritmi platforme (tzv. sustavi preporuka; *recommender systems*) koriste za prikazivanje sadržaja korisnicima, te jasnog predočavanja svih opcija koje korisnici imaju da modificiraju intenzitet tih parametara., od kojih bar jedna mora biti nevezana s profiliranjem korisnika. Većina ovdje spomenutih odredbi ide ruku pod ruku s člankom 13, koji predviđa (minimalno) godišnju objavu izvještaja o svim koracima moderiranja sadržaja koje su platforme poduzele. Neke od ostalih odredbi uključuju javnu objavu broja zaposlenih u sferi moderacije sadržaja te jezika koje spomenuti zaposlenici govore, snažnije obveze prijavljivanja nezakonitog djelovanja te provjere korisnika koji koriste *online* platforme za prodaju dobara i usluga, te obvezu obavještavanja korisnika u slučaju da vidljivost njihova sadržaja ograničena ili zarada od objavljivanja sadržaja zamrznuta. Za provedbu odredbi akta ovlaštena bi bila Europska komisija.

Iako je DSA ekstenzivan zakonski akt, te predstavlja snažan korak prema daljnjoj uspješnoj regulaciji, nije bez svojih nedostataka. Kako bi se spriječila zlouporaba osobnih podataka protivno volje korisnicima, kritičari trenutnog nacrta DSA kao što je mreža European Digital Rights, čiji je i Gong pridruženi član, predlažu[28] da se kao obvezna osnovna postavka na *online* platformama uvede nekorištenje bilo kakvih podataka koje korisnici nisu sami svojevoljno ustupili, uključujući i tzv. pretpostavljene podatke (*inferred data*) odnosno algoritmičke zaključke o profilu korisnika ovisno o količini interakcije s određenim tipovima sadržaja. Iz EDRi-ja upozoravaju kako regulacija mora adresirati manipulativni poslovni model big techa i razumjeti ekonomske interese koje platforme poput Facebooka imaju u poticanju štetnog ponašanja. Govor mržnje, dezinformacije i druge vrste problematičnog sadržaja postaju viralne i dolaze na vrh preporučenog sadržaja kao rezultat sadašnjeg poslovnog modela koji traži "pažnju". Veća pažnja znači veću prikovanost za oglase. Zato nije dobro poticati platforme da usvajaju mehanizme uklanjanja ili označavanja spornog sadržaja, ukoliko taj manipulativni temeljni poslovni model[29] ostaje isti.

17 Nadalje, traži se i aktivna rasprava o alternativnim sustavima preporuka[30], odnosno o mogućnosti da treće strane (bilo kompanija ili neprofitna organizacija) razviju zasebne algoritme za preporučivanje sadržaja te da potom korisnicima bude omogućeno svjesno odabrati preferirani sustav preporuka. Ovakav bi sistem osigurao veću kontrolu korisnicima nad osobnim podacima, ali i otvorio prostor natjecanju manjih tehnoloških kompanija odnosno *start-upova* u kreaciji spomenutih algoritama. Mnogi su članovi civilnoga društva zabrinuti i oko prijedloga Odbora za pravna pitanja Europskog parlamenta prema kojemu bi se iz regulacije predviđene u DSA isključile medijske publikacije, čime bi bilo onemogućeno da se umanji doseg, ukloni ili označi bilo koji sadržaj objavljen od strane medijskih organizacija. Kako se upozorava u otvorenom pismu[31] na stranicama organizacije EU Disinfo Lab, praktički je nemoguće povući jasnu liniju između onoga što jest medijska publikacija i onoga što to nije, te je mnogim

28 EDRI — https://bit.ly/3CLlneN

29 EDRI https://bit.ly/30q7dCR

30 Article19 — https://bit.ly/32ltuSM

31 EU Disinfo Lab — https://bit.ly/30QjH73

širiteljima dezinformacija element strategije upravo to što se teže predstaviti kao kredibilni medijski izvori. Uvođenje ovakve klauzule omogućilo bi stvaranje pravne sive zone unutar propozicija DSA, ali i proširilo prostor velikim tehnološkim kompanijama da arbitrarno odlučuju o tome koji će sadržaj nadgledati, a koji neće. Jedan od ključnih zahtjeva mreže EDRi je i interoperabilnost, odnosno mogućnost da korisnici komuniciraju preko granice platformi sa svojim prijateljima i pratiteljima[32].

Razvidno je kako je iz izvora eksternih političkim tijelima EU moguće izvući konstruktivne preporuke za daljnje korake, te je ovakav aktivni nadzor civilnog društva i nezavisnih organizacija nad kreacijom europske legislative nužan preduvjet za uspostavu kvalitetnih regulativnih okvira stoga što omogućava izražavanje volje europskih građana, ali i stoga što predstavlja svojevrstan *checks & balances* mehanizam u vidu vanjskoga nadgledanja, te je prema tome nužno aktivno uključiti spomenute aktere u proces izgradnje pravnog okvira.

Zakon o digitalnim tržištima[33] također se kreće u smjeru ograničavanja moći društvenih mreža, odnosno tehnoloških divova općenito, polazeći od pretpostavke da dosadašnje politike tržišnog natjecanja to nisu učinile u dovoljnoj mjeri. Središnji članci ovoga prijedloga jesu članci 5 i 6. Odredbe članka 5, među ostalim, sprječavaju kompanije označene kao *gatekeepers* (izrazito tržišno moćne kompanije)[34] u sjedinjavanju podataka skupljenih na različitim platformama (primjerice, Facebook ne može koristiti podatke prikupljene na Instagramu kako bi targetirao reklamni sadržaj korisnicima Facebooka). Nadalje, sprječava se ponuda istih usluga po različitim cijenama i pod različitim uvjetima, ograničava se moć kompanija da spriječe mogućnost tržišnih aktera koji djeluju na njihovim platformama da podnose pritužbe nadležnim tijelima, te se zahtijeva transparentnost

32 EDRi https://bit.ly/3DW7I54

33 EUR-Lex – https://bit.ly/3qGW3V0

34 Prema definiciji Europske komisije, *gatekeeperi* su one kompanije koje su tijekom protekle tri godine ostvarile promet od minimalno 6.5 milijardi eura na tlu Europe te čija tržišna kapitalizacija iznosi minimalno 65 milijardi eura u protekloj financijskoj godini. Nadalje, za definiciju *gatekeepera* kompanija mora imati više od 45 milijuna mjesečnih korisnika te više od deset tisuća godišnjih aktivnih poslovnih korisnika u EU.

u postavljanju cijena za reklamni prostor. Članak 6 DMA primarno onemogućava kompanije da favoriziraju sebe u ponudi usluga. Primjerice, ako je korisnik u potrazi za digitalnim pomoćnikom, Amazonu bi bilo zabranjeno Alexi dodijeliti drugačiji tretman prilikom ponude usluga negoli ijednom drugom konkurentskom proizvodu kao što su Siri ili Cortana. Nadalje, položaj korisnika osnažuje se ograničavanjem mogućnosti kompanija da koriste nejavne podatke, među kojima su i podaci generirani od strane korisnika. Nadalje, zahtijeva se mogućnost korisnika da uklone unaprijed instalirane aplikacije sa svojih uređaja — primjerice, korisnici Androida mogli bi ukloniti Google Play Store, a korisnici iPhonea Apple App Store. Ovim pomacima u pravima korisnika nastavlja se pozitivni trend ojačavanja pravnog položaja korisnika društvenih mreža i digitalnih usluga započet usvajanjem Opće uredbe o zaštiti podataka (GDPR), koja je uvelike pridonijela vraćanju nadzora nad podacima u ruke korisnika. Naravno, motivacija za donošenje DMA nije isključivo altruizam, već se uvelike tiče i želje EU da omogući europskim tehnološkim firmama bolje natjecateljsko okruženje, no to ne umanjuje vrijednost ovoga akta.

Iako su spomenuti prijedlozi obećavajući, ključno je pitanje implementacije. S obzirom na golem kapital kojega posjeduju velike tehnološke firme, upitno je hoće li novčane kazne i slični penali imati ikakav relevantan utjecaj na njihovo djelovanje. Sličan obrazac uočavamo i kod drugih bogatih korporativnih aktera — naftne kompanije, primjerice, već desetljećima plaćaju odštete za zagađenje okoliša koje su prouzročile, no to nije uvelike promijenilo njihovo djelovanje. Spomenute kompanije imaju dovoljne novčane rezerve da mogu naprosto računati na određenu količinu plaćenih kazni i stvoriti pričuvne fondove za takve prilike, te nastaviti svoje djelovanje. Ako ne bude omogućeno da se provedbom akata poput DMA i DSA značajno ograniči poslovanje kompanije koje krše njihove odredbe, malo je vjerojatno da će oni polučiti velik uspjeh. Budući da je Europskoj Uniji u interesu da velike tehnološke kompanije nastave pružati svoje usluge njenim građanima, također je upitno hoće li strogih kazni biti (trenutno se predviđa da bi kompanije mogle plaćati kazne u iznosu do 10% njihova godišnjega prihoda[35], što se čini relativno malenim iznosom s obzirom na kapital koji su akumulirale kroz godine te nastavljaju akumulirati). S obzirom na rečeno, iako je regulacija idejno dobro rješenje,

35 Politico — https://politi.co/3FUVifg

te trenutno postoje kvalitetni prijedlozi pravnih okvira, regulacija je uvijek ograničena učinkovitom implementacijom na koju se ne može sa sigurnošću računati. Bez ograničenja poslovanja, ili novčanih kazni toliko velikih da ugrožavaju dugoročne planove kompanija, strah da regulacija neće biti dovoljno snažan alat ostaje opravdanim.

RJEŠENJA ZA BUDUĆNOST — *BREAK UP BIG TECH*, ILI PAK NEŠTO DRUGO?

Oštra mjera o kojoj se u svjetlu skandala koji okružuju velike tehnološke kompanije opetovano razgovara jest *breaking up*, odnosno „kidanje" kompanija na manje nezavisne dijelove — pod tim bi rješenjem, primjerice, WhatsApp i Instagram postali zasebne kompanije neovisne o Facebooku. Glavna bi korist ovakvoga poteza bilo razbijanje monopola na podatke koje posjeduju ove kompanije — ne samo da podaci ne bi više bili u potpunosti centralizirani i time ranjiviji na probijanja sigurnosnog sustava, nego bi smanjenjem količine podataka kojima barataju pojedinačne kompanije pala i njihova moć da utječu kako na privatnost korisnika, tako i na političke ishode. Uz spomenuto rezoniranje postoje i tržišni argumenti. Onemogućavanjem monopola ili oligopola te stvaranjem većeg broja tržišnih aktera potaklo bi se natjecanje u pružanju usluga, koje bi vodilo inovacijama i jeftinijim uslugama jer bi se veći broj kompanija natjecao za jedne te iste korisnike; a među spomenutim inovacijama vjerojatno bi se našli i mehanizmi očuvanja privatnosti jer bi svaki ponuđač usluga korisnicima u teoriji želio omogućiti sigurniji pristup uslugama. Kidanjem kompanija tako bi se doskočilo ranije spomenutom problemu u regulaciji — činjenici da su trenutno premoćne i prebogate da bi ih se kažnjavanjem ugrozilo (*too big to fail*).

Trenutni događaji oko Facebooka potakli su američku Federalnu trgovinsku komisiju na tužbu[36] protiv Facebooka (pri čemu u tome nije usamljena — tužbe podnose i privatne kompanije, napose one koje su Facebookovim djelovanjem izbačene s tržišta[37]) na osnovu kršenja antitrustovskih zakona koja je u lipnju inicijalno odbačena pa kasnije nadopunjena analizama o udjelu tržišta kojega kontrolira

36 New York Times — https://nyti.ms/3cN8R3Q

37 New York Times — https://nyti.ms/315uRvB

Facebook te o njegovu pripajanju WhatsAppa i Instagrama u svrhu eliminacije konkurencije. Ključan dio tužbe jest zahtjev za kidanjem Facebooka kao rješenjem problema njegove monopolističke pozicije. Ipak, usvajanje tužbe ne znači automatski i prihvaćanje zahtjeva za kidanjem kompanije, a kako prisilno komadanje „prirodno" nastalih tržišnih aktera sa sobom nosi stigmu državne intervencije u slobodno tržište i onemogućavanja slobodnog, meritokratskog poslovanja, od čega političke elite (pogotovo u centripetalnim zapadnim političkim sustavima gdje su najjače stranke one lijevoga i desnoga centra) u principu uvelike zaziru, upitno je koliko će dugo perzistirati politička volja za predlaganjem ovakvih rješenja u momentu kada se prašina podignuta trenutnim skandalom donekle slegne. Čak i kada spomenuta inicijalna barijera dugotrajne političke volje ne bi bila prisutna, postoji niz daljnjih problema s ovakvim rješenjem. Ranije spomenuta zviždačica Haugen drži da bi kidanje velikih tehnoloških kompanija bilo kontraproduktivno[38]. Haugen smatra da su Facebookova ulaganja u sigurnost informacija te mjere protiv špijunaže i terorizma ionako premalene, te da bi smanjenje njegova kapitala dovelo do daljnjih rezova u navedenim sektorima čime bi se stvorio strukturalan sigurnosni rizik. Također, s obzirom na golem broj korisnika platformi poput Facebooka i Instagrama, broj ljudi izložen rizicima boravka na društvenim mrežama također bi ostao isti. Neovisno o argumentima koje nudi Haugen, valja spomenuti i tržišni protuargument. Izrazito velike količine kapitala koje su ove kompanije akumulirale omogućava im da dio svojih usluga nude besplatno (primjer su Googleovi servisi poput Google Mapsa ili Gmaila) bez rizika po financijsku sigurnost. Manje kompanije imale bi manju sposobnost nastaviti pružati usluge na taj način, te manje kapaciteta za ulaganje u istraživanja i razvoj (*research & development*). Ukratko, iako kidanje kompanija rješava dio ranije navedenih problema, vjerojatno bi stvorilo istu takvu količinu novih.

Drugih rješenja u aktualnim raspravama nema mnogo. Izvještaj u autorstvu organizacija European Digital Rights, Access Now i Civil Liberties Union for Europe[39] dotakao se određenih alternativnih rješenja. Spominje se korištenje umjetne inteligencije, odnosno softvera za prepoznavanje i uklanjanje dezinformacija i govora mržnje, no ističe se i kako je problem dezinformacija izrazito nijansiran te

38 Business Insider – https://bit.ly/3HyZN0D

39 EDRI.org – https://bit.ly/3CnbvHX

kako trenutni kapaciteti umjetne inteligencije za strojno učenje nisu dostatni za rješenje ovoga pitanja. lako je moguće zamisliti da će spomenuti kapaciteti u budućnosti porasti, trenutno se ne radi o vijabilnom rješenju. Izvještaj spominje i ograničavanje anonimnosti aktera na internetu — anonimnost stvara i osjećaj nedodirljivosti; odnosno, ukoliko je identitet pojedinca nepoznat, on se osjeća sigurnim prilikom komunikacije, a time i zaštićenim prilikom širenja dezinformacija. Ipak, pravo na privatnost jedno je od temeljnih ljudskih prava te osnovnih vrijednosti koje svojom pravnom stečevinom EU pokušava sačuvati, te bi takvi koraci stvorili opasan presedan. Spomenuti se izvještaj na kraju okreće rješenjima koja su spomenuta i u ovom članku — uz promicanje medijske pismenosti, zazivaju se snažnije te konkretnije regulative (poput ranije spomenutih alternativnih sustava preporuka) kojima bi se ograničili negativni potencijali društvenih mreža i tehnoloških kompanija općenito.

Iz svega navedenoga u tekstu razvidno je da ne postoji rješenje koje bi bilo *deus ex machina* te trzajem čarobnoga štapića razriješilo sve probleme vezane uz društvene mreže. Najbolji smjer djelovanja vjerojatno je eklektična kombinacija sviju navedenih rješenja, ovisno o vremenu i mjestu. Lako je moguće da će, kako tehnologija bude napredovala, budućnost ponuditi nove solucije — a vjerojatno i nove probleme. Preostaje jedino sa problemima ići ukorak.