NOVI OBLICI MANIPULIRANJA U DIGITALIZIRANOM PROSTORU JAVNOG ZNANJA I POTREBA ZA USPOSTAVOM DIGITALNOG I PODATKOVNOG SUVERENITETA

Nikola Mlinac*, Gordan Akrap,
Jadranka Lasić-Lazić**

---

* Nikola Mlinac (Split, 1977.) magistar je pomorskog i općeg prometnog prava. Student je na zadnjoj godini poslijediplomskog doktorskog studija na Odsjeku za informacijske znanosti i komunikologiju Filozofskog fakulteta Sveučilišta u Zagrebu. Stavovi izraženi u ovom članku osobni su stavovi autora i ni pod kojim se uvjetima ne mogu smatrati službenim stavovima institucije u kojoj je autor članka zaposlen.

** prof.dr.sc.Jadranka Lasić Lazić (Požega, 1949.) pohađala je i završila gimnaziju u Požegi. Na Filozofskome fakultetu Sveučilišta u Zagrebu diplomirala je filozofiju i jugoslavenske jezike i književnosti 1975. godine. Magisterij znanosti stječe nakon završenog Poslijediplomskog studija informacijskih znanosti Sveučilišta u Zagrebu magistriravši na temi „Pedagoško-animatorski rad s djecom u dječjim odjelima narodnih knjižnica“. Doktorat znanosti stječe iz područja informacijskih znanosti 1991. godine na Sveučilištu u Sarajevu obranom doktorske disertacije „Razvoj bibliotečno informacijskih sustava“. Redoviti je profesor u trajnome zvanju. U Zavodu za informacijske znanosti od 2000. obnaša dužnost urednice uredivši tri zbornika i dvije knjige. Autorica je ili koautorica četiriju knjiga, te preko osamdeset znanstvenih i stručnih članaka u domaćim i stranim časopisima.

DOI: https://doi.org/10.37458/nstf.21.3.1

Sažetak

Društvene mreže, nove informacijsko-komunikacijske tehnologije i sustavi za brzo i globalno komuniciranje te razmjenu brojnih informacijskih sadržaja, doveli su do radikalnih promjena u odnosu na procese prikupljanja, obrade, pretvorbe, pohrane i tumačenja obavijesti i na njima utemeljenih odluka i djelovanja. Obavijesti u cyber prostoru te javno znanje koje u njemu nastaje i koje se distribuira korištenjem tehnoloških sredstava, podložno je novim mogućnostima manipuliranja s realnošću. Društvo znanja i sustavna digitalizacija znanja, koja se temelje na točnim i provjerenim informacijama, postala su podložna financijskim interesima privatnih tehnoloških korporacija koje vlastite poslovne modele globalnog komuniciranja stavljaju ispred pouzdane i sigurne razmjene točnih i istinitih znanja. Javljaju se tako novi oblici manipuliranja u digitalnom prostoru, koji iskorištavaju platforme za ostvarivanje vlastitih političkih i drugih srodnih interesa u širem kontekstu unutarnjih, lokalnih, nacionalnih, regi-

Dr. Jadranka Lasić Lazić dobitnica je (2008.) godišnje nagrade Filozofskog fakulteta za rezultate postignute u teorijskom i praktičnom radu u razvoju i afirmaciji informacijskih znanosti i za izniman doprinos u promicanju e-učenja i načina usvajanja znanja i vještina koje nudi informacijska znanost.

onalnih i međunarodnih sukoba. Jedan od mogućih odgovora na zlouporabu tog prostora je u mehanizmima stvaranja, oblikovanja te očuvanja podatkovnog i digitalnog suvereniteta država (i međudržavnih integracijskih zajednica) koji treba biti stvoren na temeljnim društvenim i demokratskim načelima slobode izražavanja, odgovornosti i transparentnosti.

Ključne riječi: digitalizirani prostor javnog znanja, društvene mreže, algoritmi, umjetna inteligencija, (dez)informacije, cyber prostor, digitalni i podatkovni suverenitet.

Abstract

The social media, new information and communications technologies, and systems for fast global communication and exchange of various information content, have led to radical changes regarding the information gathering, processing, conversion, storage, and interpretation processes as well as the decisions and actions based on them. Information and public knowledge originating in cyberspace, being distributed through technology, is susceptible to new ways of reality manipulation. The society of knowledge and systemic digitalization of knowledge have become subject to financial interest of privately-owned tech corporations which put their own business models of global communication before a reliable and safe exchange of

accurate and true knowledge. Due to the design of default algorithm settings and artificial intelligence used for making profit, privately-owned tech corporations avoid responsibility for negative consequences and misuse of their platforms. Meanwhile, they have become important social, political, and economic factors. They exercise a strong influence over various policies. Various actors, including states, terrorist, radical, and extremist organizations, use the platforms for achieving their own political and other interest in a wide context of internal, local, national, regional, and international conflicts.

The idea behind cyberspace is one with the aim of fast, reliable and safe exchange of accurate and true knowledge. One of possible responses to the misuse of that space lies within the mechanisms of creation, formation, and preservation of states' data and digital sovereignty (and that of supranational integrations), which should be based on fundamental democratic principles of the freedom of expression, responsibility, and transparency.

Keywords: digitalized public knowledge space, social media, algorithms, artificial intelligence, (mis)information, cyberspace, digital and data sovereignty.

Uvod

Razvoj informacijsko – komunikacijskih tehnologija i sustava promijenio je društveni i politički svijet. Razlog drastičnih promjena nalazi se u isprepletenosti informacijsko-komunikacijskih tehnologija i sustava, interneta i računalnih mreža zbog kojih je društvo umreženije nego ikad prije. Pojava društvenih mreža kao sredstava koji omogućavaju brzo globalno komuniciranje te razmjenu brojnih informacijskih sadržaja, koje razvijaju i kojima upravljaju velike privatne korporacije s globalnim dosegom, doveli su do radikalnih promjena kako društvo komunicira te kako doživljava i tumači procese, događaje i pojave oko sebe. Ova globalna komunikacijska mreža nadmoćna je u odnosu na lokalne mreže ali i nacionalne informacijske infrastrukture. Posljedice su nove digitalne zajednice korisnika, novi komunikacijski obrasci interaktivne višesmjerne razmjene podataka i informacija, nove konfiguracije znanja, novi tipovi pismenosti, i novi sustavi (utemeljeni na novim potrebama) edukacije.

Pretpostavka lokalne i nacionalne participacije u globalnom informacijskom prostoru planska je i sustavna digitalizacija znanja. Što znači da je javno znanje koje se stvara i postoji u cyber prostoru podložno i oblikovanju i upravljanju u većoj mjeri nego što je javno znanje u konvencionalnoj formi i na konvencionalnim medijima.[1] Proces stvaranja znanja trebao bi biti neprekinuti niz događanja, interakcije simbola iz svijeta koji nas o-

[1] Miroslav Tuđman, Projekt: Oblikovanje i upravljanje javnim znanjem u informacijskom prostoru 2007.-2016., Filozofski fakultet, Zagreb, dostupno na: http://zprojekti.mzos.hr/public/c-prikaz_det.asp?psid=0&ID=2394

kružuje sa svijetom obavijesti, te našim unutarnjim mogućnostima vrednovanja i prosuđivanja zahvaćene stvarnosti. Očito postojanje različitih domena u odnosu na procese prikupljanja, obrade, pretvorbe, pohrane i tumačenja obavijesti te odluka i na njima utemeljenih djelovanja, navodi na potrebu podjele svijeta koji nas okružuje, i u kojem djelujemo, na tri različite domene: domenu fizičkog svijeta, informacijsku domenu i kognitivnu domenu[2].

Interakcija, odnosno sinergijsko djelovanje procesa koji se odvijaju u ovim domenama i kroz njih, omogućava stvaranje novih i primjenjivih znanja te donošenje korisnih odluka.[3] Međutim, za brojne sigurnosne izazove koji proizlaze iz digitalnog prostora, ne vrijede pravila koja vrijede u domeni fizičke stvarnosti. Razlog tome su nove informacijsko – komunikacijske tehnologije i sustavi komuniciranja koji se razvijaju na platformama društvenih mreža. Nove tehnologije algoritama i umjetne inteligencije svojom tehnološkom sposobnošću i svojom moći mijenjaju percepciju o realnom svijetu, stvarnosti, činjenicama koje nas okružuju čime negativno utječu na pouzdanu i sigurnu razmjenu točnih i istinitih znanja.

Društvene mreže i javno (umreženo) znanje

Kategorizacija, kvantifikacija i agregiranje podataka, stavova, mišljenja i emocija u baze podataka i njihova daljnja algoritamska obrada na

[2] Gordan, Akrap: Informacijske strategije i operacije u oblikovanju javnog znanja, doktorska disertacija, Sveučilište u Zagrebu, Filozofski fakultet, Zagreb, 2011.

[3] Ibid.

društvenim mrežama, otvorili su nove mogućnosti u razumijevanju i vrednovanju složenih društvenih pojava. Istovremeno su otvorile i nove mogućnosti manipuliranja s realnošću i sustavnom digitalizacijom znanja koje se temelji na točnim i provjerenim informacijama. Aktivnosti na društvenim mrežama postale su novi oblik neposredne interakcije između pojedinaca, organizacija i društva te raznih politika.

U tako konfiguriranoj virtualnoj stvarnosti, istinita, pouzdana i vjerodostojna realnost nije više ta s pomoću koje se kontrolira i verificira točnost prikaza. Zato su moguće različite manipulacije: moguće je manipulirati s realnošću s pomoću (dez)informacija, ali isto tako moguće je s pomoću informacija raditi preinake i mijenjati realnost.[4]

U takvom digitaliziranom okruženju privatne tehnološke korporacije koje upravljaju društvenim mrežama, svoje poslovne modele te njihov dizajn kojim spajaju pojedince, organizacije i društvo i preko kojih se kreiraju politike, temelje na algoritamskoj obradi podataka i informacija koje njihovi korisnici pohranjuju na njihovim društvenim mrežama. Istovremeno te, ogromne količine osobnih i poslovnih podataka i informacija, prodaju s ciljem stjecanja znatnog ekonomskog profita. U ovakvom novom okruženju informacije se povezuju, odnosno umrežuju i integriraju, provjeravaju i dopunjavaju s ostalim dostupnim podacima i informacijama.

[4] Tuđman, Miroslav, Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb, (2008).

Poanta je u tome da sama realnost, odnosno svijet u kojem danas živimo, nije više kriterij nadzora i provjere točnosti i pouzdanosti obavijesti koje „prikazuju“ tu realnost. Drugim riječima, spoznaja je izgubila primat nad komunikacijom (Ibid). Važnu, ako ne i presudnu ulogu u ovakvom okruženju u kojem sve više dominiraju informacijski sadržaji s društvenih mreža zauzimaju razni algoritmi[5] čija se učinkovitost nadopunjuje i poboljšava umjetnom inteligencijom[6]. Algoritmi

[5] Algoritmi su ključan čimbenik funkcioniranja digitalnih tehnologija i društvenih mreža. Oni predstavljaju skup pravila koja precizno definiraju redoslijed nekih operacija koje računalo slijedi kako bi riješilo neki problem. U tehničkom smislu, računala algoritme obično koriste kako bi obavljala svoje funkcije ili kako bi obrađivali podatke mnogo većom brzinom i s boljom preciznošću nego što to zahtijeva ručno izvršavanje nekog zadatka. Algoritmi predstavljaju zajedničku poveznicu svim aplikacijama i svim društvenim mrežama koji iz ogromnog skupa prikupljenih podataka i informacija odabiru one podatke i informacije koje će prikazati njihovim korisnicima. Drugim riječima, algoritam na temelju određenog skupa pravila isporučuje prilagođene (personalizirane) vijesti, odlučuje koji će podatak biti najrelevantniji i koja će informacija biti adekvatna za pojedinu kategoriju publika. Ne brinući o njihovoj točnosti, istinitosti, potpunosti i pouzdanosti.

[6] Umjetna inteligencija podrazumijeva korištenje računalnih sistema za simuliranje inteligentnih odgovora unošenjem i obradom informacija. Umjetna inteligencija je u stanju prepoznavati uzorke, govor i vizualne percepcije. U najširem definicijskom kontekstu, umjetna inteligencija ima za cilj da strojevi postanu inteligentni, i odnosno, da na temelju prikupljenih podataka donose smislene i održive odluke. Umjetna inteligencija je u stanju odrediti najbolji način djelovanja kako bi se ostva-

održavaju osnovne funkcije društvenih mreža dok aktivnosti i emocionalne podražaje svojih publika pretvaraju u digitalni oblik. Privatne korporacije koje upravljaju društvenim mrežama i koje razvijaju ove algoritme, kao što su Google i Facebook sebe ne smatraju kreatorima nego tek posrednicima u distribuciji informacijskih sadržaja koje nastaju i koji se dijele preko njihovih platformi. Za posredovanje podataka i informacija između njihovih stvaratelja i različitih, manje ili više ciljanih publika, ove korporacije koriste razne algoritme koje neki informacijski sadržaj čine više vidljivim od drugih. Međutim, iako te informacije stvaraju i dijele s drugim korisnicima i uslugama, korisnici društvenih mreža na ovaj proces ne mogu utjecati, ne mogu njime upravljati niti ga mogu kontrolirati.[7] Zbog toga su se u svom nastajanju ove korporacije opisivale nadzornim tvrtkama. Ubrzo su svoj naziv promijenile u društveno prihvatljiviji naziv: društvene mreže.[8]

rio široki i raznoliki raspon ciljeva političke, gospodarske, sigurnosne ili strateške prirode. U sljedećih 10 do 15 godina ona će biti glavni pokretač inovacija u svakoj industrijskoj grani čime će utjecati i na prirodu svakodnevnih aktivnosti ljudi u fizičkom i informacijskom okruženju.

[7] Bergh Arild, Social network centric warfare – understanding influence operations in social media, Norwegian Defence Research Establishment (2019), dostupno na: https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media

[8] Boldyreva, Elena, Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. 91-102. (2018), 10.15405/epsbs.2018.12.02.10,dostupno na: https://www.re-

U ovom kaotičnom prostoru koji je preplavljen velikim brojem osobnih i poslovnih podataka i informacija, u prvom planu nije toliko sama informacija. Fokus algoritama je na privlačenju pažnje na ciljane informacije i informacijske sadržaje. Primarni kriterij vrednovanja informacija nije istinitost već „smislenost“, tj. relevantnost informacije. Preciznosti radi, treba priznati da u informacijskoj znanosti i informacijskoj djelatnosti istina nikada nije bila kriterij za vrednovanje informacija, informacijskih procesa i sustava. [9]

Društvene mreže zbog algoritamskih sposobnosti koje održavaju njihovu osnovnu funkciju, postale su prvorazredan usmjerivač pažnje i filter ogromnog broja informacija. U procesu segmentiranja svojih korisnika, filtriranja ogromnog broja podataka i isporučivanja informacija i usluga na personalizirani način, ključnu ulogu imaju upravo algoritmi.

Oni pospješuju selektiranje informacija te prema unaprijed određenim (programiranim) kriterijima odlučuju koje su informacije po njihovoj procjeni relevantne, a koje nisu. Skidanjem takozvanih besplatnih aplikacija, društvene mreže informacije publikama nude u obliku proizvoda. Njihovi korisnici u pravom smislu postaju potrošači pažnje koja u svijetu digitalnog marketinga ima svoju tržišnu vrijednost i koja se na takvom tržištu prodaje kao roba.

searchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process

[9] Tuđman, 2008.

Algoritmi društvenih mreža u funkciji (dez)informiranja

Suštinska funkcija društvenih mreža nije u pukom širenju informacija. One teže da njihovu glavnu funkciju u stvaranju financijskog profita određuju algoritmi koji prema raznim kriterijima rangiraju sadržaje i određuju uvjete prema kojima će se sadržaji širiti, dijeliti i objavljivati.[10] Algoritmi na suptilan način oblikuju načine kako promišljamo i gledamo na stvari. Oni prate što korisnici društvenih mreža gledaju i koji im sadržaji privlače najveću pažnju. Svojim izborom na temelju uočenih postavki publikama prilagođavaju informacije i nude povratne informacije na sličan sadržaj ili temu. Ovakvo filtriranje informacija ima i negativnu konotaciju. Njihovim filtriranjem, slijedom algoritamskih odabira, nastaje takozvani *učinak jeke* kojim se ciljanim publikama unutar neke virtualne grupe, ograničava brža pristupačnost izvorima alternativnih informacija.

Na ovaj način prikazuju se samo one informacije koje su u skladu s od strane algoritma predviđenom preferencijom korisnika društvene mreže, čime se osnažuju postojeće kognitivne pristranosti publika, jača se njihova homogenizacija i one tako lakše prihvaćaju grupne stavove. Filtriranjem informacija algoritmi od svih informacija na

[10] Vilmer J.-B. Jeangène, Escorcia A., Guillaume M., Herrera J., Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, Paris (2018), dostupno na: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

internetu, pažnju publika sužavaju odnosno izlažu ih samo jednom skupu informacija, nekim sadržajima povećavaju vidljivost, a neke čine nevidljivim iako postoje na mreži. U informacijskom prostoru, što su ga oblikovali internet i nove informacijske tehnologije, daje se naslutiti da oni ne oblikuju korpus objektivnog i istinitog znanja; postojeće komunikacijske mreže nemaju zadaću organizirati i prenijeti istinite informacije, nego je njihova zadaća osigurati u javnosti dominaciju određenih informacija; odnosno u informacijskom prostoru ne postoje mehanizmi kontrole javnog znanja prema kriteriju istine i objektivnosti.[11]

Ovdje je važno naglasiti da algoritmi prepoznaju emotivne izričaje koje publike stvaraju i dijele putem društvenih mreža i da ih algoritmi rangiraju prema učincima ostvarene pažnje publike koja se mjeri brojem ostvarenih oznaka sviđanja, ne sviđanja, prosljeđivanja ili komentara. Privlačenje pažnje je važno za ono što se naziva *uokvirivanje priča*[12] što je jako bitno za oblikovanje percepcije o nekom stanju, osobi ili događaju. Stvaranjem i prenošenjem prikaza emocija bijesa, straha ili ponosa u širu društvenu raspravu bilo putem oglasa koji se plaćaju Facebooku ili putem video uradaka i fotografija na You tubu ili Twitteru u realnom vremenu, dodatno se potiče angažman onih koji ih pregledavaju.

Kada algoritmi prepoznaju da ekstremni sadržaji s nabijenim emocijama privlače najviše pažnje, oni takve ili slične nove sadržaje dodatno usmjeravaju prema tim publikama. To je način kako se

[11] Tuđman, 2008.

[12] Singer W.P. i Brooking T. Emerson, LikeWar: The Weaponization of Social Media, (2018).

isticanjem negativnih emocionalnih stanja publike na društvenim mrežama može potaknuti na demonstracije ili ulične proteste.[13] Dodatna negativna konotacija algoritama i društvenih mreža je i u tome da se na ovaj način na društvenim mrežama automatizacijom usklađuju i pojačavaju radikalni, nasilni i ekstremni stavovi[14] da se javnost dodatno polarizira te da dezinformacije dobivaju veću vjerodostojnost.[15]

[13] Nye Joseph, Protecting Democracy in an Era of Cyber Information War, Belfer Center for Science and International Affairs, Harvard Kennedy School, SAD (2019), dostupno na:https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war

[14] Van Alstyne Marshall, Brynjolfsson Erik, Global Village or Cyberbalkans: Modeling and Measuring the Integration of Electronic Communities, (2005), dostupno na: https://www.researchgate.net/publication/220535041_Global_Village_or_Cyber-Balkans_Modeling_and_Measuring_the_Integration_of_Electronic_Communities

[15] Flore Massimo, Balahur Alexandra, Podavini Aldo, Verile Marco, Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda, Publications Office of the European Union, Luxembourg, (2019), dostupno na: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC116009/understanding_citizens_vulnerabilities_to_disinformation.pdf Autori ovo svoje zapažanje temelje na zaključcima istraživanja *Algorithms and Intrusions: Emergent Stakeholder Discourses on the Co-option of Audiences' Creativity and Data (*Vesnić-Alujević, Stehling M., Jorge A., Marôpo L., Springer International Publishing (2018); *Strategic Opportunities (and Challenges)of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification* (Newell S., Marabelli M., Journal of Strategic Information Systems (2015) i

Odgovornost za informacijsko ponašanje i posljedice tog ponašanja na društvenim mrežama

Tumačenja privatnih korporacija koje upravljaju društvenim mrežama da su posrednici, a ne stvaratelji informacija, vrlo je bitna radi utvrđivanja tko će biti odgovoran za širenje dezinformacija i sadržaja kojim se u društvu potiče ili propagira terorizam, radikalizacija i ekstremizam.[16] Smatrajući sebe samo posrednicima, ove korporacije izbjegavaju odgovornost za postavljene sadržaje. No brojni primjeri društvenih pojava diljem svijeta ukazuju da se ove korporacije suočavaju sa sigurnosnim, društvenim i političkim posljedicama i tumačenjima zlouporabe njihovih platformi od strane raznih državnih i nedržavnih aktera. Države diljem svijeta postupno su osvijestile činjenicu da ove korporacije, zbog svog dizajna i algoritamskih „tvorničkih" postavki, ostvaruju snažan utjecaj nad njihovim domaćim politikama te u međunarodnim sukobima. Društvene mreže postale su toliko moćne da se mogu uspoređivati s vladama.[17]

Njihovi proizvodi i usluge dovele su do neželjenih društvenih podjela. Između 2012. i 2017. oko 50 država koje su strahovale od terorizma, ekstremizma ili naprosto od stvaranja i distribucije lažnih vijesti, odnosno dezinformacija, donijele su zakone kojima se ograničava sloboda govora njihovih građana na mreži. Čak i u SAD-u, gdje se

The Ethics of Algorithms: Mapping the Debate, Big Data & Society (Mittelstadt B., Allo P., Taddeo M, Vol. 3(2) (2017).

[16] Vilmer, Escorcia, Guillaume, Herrera, 2018.

[17] Singer i Brooking, 2018.

nalazi sjedište ovih ogromnih privatnih korporacija, nova generacija političara koja razumije modernu tehnologiju razmatrala je donošenje novih vladinih regulacija ukoliko ove korporacije same ne pooštre pravila ponašanja na svojim platformama.[18]

Vlasnici Facebooka, Twittera i sličnih tvrtki, u osnovi ne žele veću kontrolu nad svojim platformama jer je središnji element njihovog poslovnog modela argument da su oni tek posrednici, a ne pružatelji informacija. Glavni argument im daje članak 230. američkog Zakona o pristojnoj komunikaciji (engl. U.S. Communication Decency Act) koji kaže da se „niti jedan pružatelj ili korisnik interaktivne računalne usluge neće tretirati kao izdavač ili govornik bilo koje informacije koju je omogućio drugi davatelj informacijskog sadržaja".[19] Drugim riječima ovo znači da krivnju snosi izvor bilo kakvog problematičnog sadržaja, a ne platforma koja pruža uslugu prenošenja takvog sadržaja. Ista autorica tumači da je spomenuti članak 230 vrlo liberalna interpretacija slobode govora koju ovaj članak štiti do te mjere da dopušta čak i govor mržnje. To je stvorilo određena trvenja koja nisu svojstvena samo u SAD-u jer se zbog globalnog dosega u bezgraničnom prostoru interneta s radikalizacijom i ekstremizmom u društvu i uplitanjem vanjskih aktera u unutarnje političke procese preko društvenih mreža, danas susreću brojne države.

[18] Ibid.

[19] Oates Sarah. The easy weaponization of social media: why profit has trumped security for U.S. companies, Digi War (2020). https://doi.org/10.1057/s42984-020-00012-z

S obzirom da Facebook trenutno predstavlja najpopularniju društvenu mrežu po svojoj rasprostranjenosti i po broju aktivnih korisnika te da svoj, skoro se usudimo reći digitalni monopol širi i na mobilne aplikacije za masovnu komunikaciju kao što su WhatsApp i Instagram, vlade i društva diljem svijeta se nalaze u istoj dilemi. Spomenuti članak zapravo je otvorio vrata globalnom digitalnom sukobljavanju jer su nepostojeće "digitalne granice" otvorile put brojnim dezinformacijama, bez obzira na njihove stvaratelje.[20]

Drugim riječima u društvo je uveden novi komunikacijski sustav koji u sebi nosi moćan virus dezinformacija u kojem je Facebook, kao nositelj ovog problema, prema tom tumačenju ekskulpiran od odgovornosti. Autorica tumači da je američki model slobode govora kroz spomenuti članak uspostavio sustav koji omogućava da se u državama širom svijeta dezinformacijama mogu vrlo lako podrivati demokracije. Argumente vidi u tome da se ne radi o tome da ove korporacije toga nisu svjesne ili da su čak naivne u pogledu načina na koje razni akteri njihove platforme koriste za širenje dezinformacija, nego problem vidi u njihovom snažnom ekonomskom motivu da zadrže trenutni model laissez-faire[21]. Ističe tri ključna segmenta njihovog poslovnog modela. To

[20] Ibid.

[21] Hrvatska enciklopedija navodi da ovaj pojam u francuskom jeziku u prijevodu znači *pustiti da se radi,* kojim se izražava liberalni zahtjev da se iz gospodarskog života ukloni svako miješanje države i da se samostalnim ekonomskim subjektima prepusti nesmetano poslovanje prema vlastitim željama i interesima, koje svoje odnose uređuju ugovorima u skladu s autonomnom logikom ekonomskog ži-

su: potrebe oglašivača koje su im važnije od potreba korisnika; gotovo nema provjere identiteta onoga tko postavlja sadržaj; da se štetan sadržaj praktički ne moderira, a ukoliko se i moderira u pravilu se obavlja automatizirano što se do sada, kako opisuje autorica, pokazalo prilično neučinkovitim.

SAD-e u kojima je sjedište ovih tvrtki, ali i druge države, postale su svjesne opasnosti i negativnih društvenih posljedica koje su proizašle iz zlouporabe njihovog dizajna i algoritamskih „tvorničkih" postavki. Pogotovo nakon što su razni akteri, od država do terorističkih, radikalnih i ekstremističkih organizacija, platforme društvenih mreža počeli iskorištavati za ostvarivanje vlastitih širih političkih i drugih srodnih interesa i ciljeva. Međutim, u izgradnji djelotvornog odgovora protiv zlonamjernog korištenja platformi društvenih mreža ubrzo se pojavio problem te se ispostavilo da to nije nimalo lak i jednostavan zadatak, dokle god ove tehnološke korporacije ustrajavaju na vlastitom poslovnom modelu i dizajnu društvenih mreža. Borba protiv dezinformacija i drugih štetnih društvenih pojava koje proizlaze iz zlouporabe društvenih mreža, vrlo je zahtjevna dok god postoje okolnosti u kojima moćne privatne korporacije predstavljaju ključne čvorove za distribuciju sadržaja bez preuzimanja odgovornosti.[22] Veliki broj dokazanih primjera o ulozi društvenih mreža u negativnim društvenim konotacijama više nije moguće ignorirati.

vota u uvjetima neograničene slobode proizvođača i potrošača, slobodne poduzetničke inicijative i zaštite privatnoga vlasništva.

[22] Oates, 2020.

Međutim, ove korporacije u svojoj obrani i dalje ističu dva ključna argumenta. To su sloboda govora i sloboda prenošenja ideja. Pri tom odgovornost za negativne posljedice po društvo ograničavaju isključivo na zlouporabu njihovih platformi od strane drugih. Osnovna točka koju ističu pristaše ovakvog stava je da su društvene mreže sredstvo za postizanje pozitivnih društvenih promjena, no ipak ako je tomu tako ove tvrtke pokazuju vrlo malo sposobnosti ili želje da svoje poslovne modele prilagode nacionalnim zakonima ili normama.[23]

U međuvremenu, dok ove korporacije privatnog kapitala odbijaju prihvaćanje odgovornosti pojedine države i organizacije, razvili su sposobnosti da njihove platforme koriste dizajn i algoritme kao taktičke alate utjecaja za ostvarivanje širih ciljeva. Njihov dizajn, brzina u prenošenju informacija, anonimnost i neposrednost u komunikaciji dovelo je do novih oblika organiziranja uličnih prosvjeda, društvenih nemira, političkih i društvenih prevrata. Terorističkim organizacijama poslužile su za mobilizaciju, regrutaciju i širenje ekstremističke i radikalne propagande, političkim strankama za politički marketing. Državama su olakšale uplitanja u unutarnje političke i društvene procese u drugim državama.

Proizvode i usluge privatnih korporacija, koje se temelje na tehnologijama digitalnog marketinga, državni i nedržavni akteri koriste za efikasnije širenje dezinformacija i izgradnju strateških narativa kojima nastoje postići vlastite vanjsko političke interese. Drugim riječima, algoritme koje su velike privatne korporacije razvile radi vlastitog profita drugi akteri su pretvorili u taktičke alate u informacijskom ratu u kojem im društvene mreže

[23] Ibid.

služe za upravljanje novom kategorijom djelovanja: (cyber) operacijama utjecaja.

U kontekstu informacijskog ratovanja bitno je pojasniti da algoritmi imaju ulogu donositelja odluka o rasponu publika koje će se ciljati (dez)informacijama kroz forme plaćenih oglasa tvrtkama koje upravljaju društvenim mrežama.[24] U toj borbi algoritmi imaju ulogu oružja koje ima jednaku učinkovitost kao i psihološko vojno djelovanje.[25] Ovdje je također bitno istaknuti da se (dez)informacijama u informacijskom ratu publike nastoje dodatno polarizirati i da ih se nastoji (de)mobilizirati na neku željenu akciju ili reakciju. Algoritmi pri tome omogućavaju anonimnost djelovanja, smanjuju mogućnost naknadnog propitivanja dezinformacija pogotovo kad se plasiraju preko lažnih identiteta.[26] Istraživanja ukazuju da algoritamske postavke i dizajn društvenih mreža pogoduje širenju dezinformacija i izazivanju brzih i emotivno nabijenih odgovora.[27] Algoritmi su digitalni strojevi utjecaja i najzaslužniji su da su društvene

[24] Neudert Lisa Maria i Marchal Nahema, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, Brussels (2019), dostupno na: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf

[25] Flore, Balahur, Podavini i Verile, 2019.

[26] Jamieson Hall Kathleen, Messages, Micro-Targeting, and New Media Technologies, The Forum 11 (2013), dostupno na: https://doi.org/10.1515/for-2013-0052

[27] Jones Kerry, Libert Kelsey, i Tynski Kristin, The Emotional Combinations That Make Stories Go Viral, Harvard Business Review, 2016, dostupno na: https://hbr.org/2016/05/research-the-link-between-feeling-in-control-and-viral-content

mreže postale taktički alati izvan konteksta digitalnog marketinga.[28]

Algoritmi i dezinformiranje

Ovaj cjelokupni proces automatizacije naziva se Facebookova tehnologija prilagodljivog uvjeravanja. Temelji se na prikupljenim psihografskim i demografskim podacima publika.[29] U procesu prilagodljivog uvjeravanja, algoritmi dezinformacije prilagođavaju publikama na način da s najboljim učinkom iskoriste njihove ranjivosti ovisno o željenom cilju. Facebookova tehnologija prilagodljivog uvjeravanja služi za učinkovitije uvjeravanje, utjecanje na daljnja ponašanja, izazivanje određenog osjećaja, budućih odluka i aktivnosti, ponašanja i stavova publika.[30] Ovdje je važno

[28] Nadler Anthony, Crain Matthew, Donovan Joan, Weaponizing The Digital Influence Machine, The Political Perils of Online Ad Tech (2018), dostupno na: https://datasociety.net/library/weaponizing-the-digital-influence-machine/

[29] U kategoriju psihografskih podataka ulaze aktivnosti, interesi i mišljenja, a u kategoriju demografskih podataka su identifikacijski podaci ime, prezime, godište, spol, rasna, vjerska pripadnost, zanimanje, interesi, hobiji i dr. Prikupljanjem, obradom i analizom ovih podataka algoritamskim postavkama na društvenim mrežama nastaju profili korisnika koje tvrtke poput Facebooka prodaju kao jedan od svojih proizvoda na tržištu digitalnog marketinga tvrtkama koje se bave oglašavanjem, političkim digitalnim marketingom ili bilo kome drugome.

[30] Berkovsky Shlomo, Kaptein Maurits, Zancanaro Massimo, Adaptivity and Personalization in Persuasive Technologies (2016), dostupno na: https://researchers.mq.edu.au/en/publications/adaptivity-and-personalization-in-persuasive-technologies i Markopoulos, P., Kaptein, M. C.,

napomenuti da algoritamski upravljana tehnologija prilagodljivog uvjeravanja olakšava pokretanje i vođenje cyber operacija utjecaja i informacijskog rata.

Facebookovi algoritmi u informacijskom ratu pokretaču cyber operacija utjecaja olakšavaju da na jednostavniji način isprovocira određene osjećaje kod ciljanih publika kao što su strah, nelagoda, sumnja i nepovjerenje u institucije vlasti, u rezultate izbora ili političke kampanje, da produbi društvena neslaganja i da pojača percepciju o radikalnim i ekstremnim pojavnostima u društvu ili da ih banalizira. Facebookova tehnologija prilagodljivog uvjeravanja ujedno omogućava lakšu, bržu i jednostavniju mobilizaciju publika ovisno o svrsi i kontekstu cyber operacija utjecaja. Može se raditi o (de)mobilizaciji publika za razne svrhe od izlaska ili neizlaska na izbore, na prosvjede, izazivanja sukoba i uličnih nereda do terorističkih napada ili poticanja na odlazak u rat.

Konkretno, kroz načine kako su ove velike privatne korporacije svoje korisnike klasificirali prema zajedničkim afinitetima i sklonostima, primjerice kroz prijateljstva na Facebooku ili putem hashtagova na Twitteru, informacijskim agresorima je vrlo jednostavno i lako pronaći načine i prostor za manipuliranje stavovima svojih publika. Kad se tome pridoda prodaja osobnih podatka, da algoritmi identificiraju slabosti korisnika, da mogu

Ruyter, de, B. E. R., & Aarts, E. H. L. Personalizing persuasive technologies : explicit and implicit personalization using persuasion profiles. International Journal of Human Computer Studies, 77, 38-51. https://doi.org/10.1016/j.ijhcs.2015.01.004, (2015), dostupno na: https://pure.tue.nl/ws/files/3994499/888440058546432.pdf

predviđati njihova buduća ponašanja kroz njihove objave, ostvarene klikove sviđanja ili nesviđanja te dijeljenja, mogućnost manipuliranja osjećajima, mišljenima i odlukama ciljanih publika danas su veće nego ikad prije. Iako je svjetska javnost 2018. osudila primjer Cambridge Analitike[31], bitne elemente koji omogućava manipuliranje sadržajima na Facebooku i Twitteru ove korporacije još uvijek nisu otklonile. U središtu poslovnog modela i dalje su zadržale mogućnost da se njihovim uslugama koriste lažni identiteti, da se lažnim identitetima može upravljati automatski i da se sadržaji, pa bilo oni i lažni mogu širiti automatizmom.

Osnovni problem je da su ove korporacije sa svoje strane primarno motivirane profitom, da su zbog toga smanjili prepreke ulasku u korištenju svojih usluga, a da se države i društvo u cjelini suočavaju sa štetnim posljedicama. Dodatni problem predstavlja činjenica da za nalaženje odgovora za rješavanje političkih i društvenih problema koji proizlaze iz njihovog dizajna i poslovnog modela, ove korporacije izgrađuju sisteme i iste alate koji su doveli do problema.[32] To su algoritmi čije učinke dodatno poboljšavaju umjetnom inteligencijom.

[31] Skandal Facebook – Cambridge Analytica iz 2016. izbio je zbog optužbi da je Cambridge Analytica zlouporabila podatke s Facebooka na način da ih je bez znanja njezinih korisnika iskoristila za razvijanje vlastitog modela psiho grafije temeljem kojeg su se oglasi mogli prilagođavati na manipulativne načine kako bi se, primjerice pojedine grupe glasača odvratilo od glasanja za Republikansku stranku ili kako bi ih se odvratilo od izlaska na izbore.

[32] Singer i Brooking, 2018.

Ti programi nisu lojalni niti jednoj organizaciji nego samo svojim stvarateljima koji su ih napisali i koji ih mogu prilagođavati shodno stvarateljevim potrebama i ciljevima, ali koji u mrežnoj komunikaciji sve više i ubrzanije zamjenjuju ljude. Promjena sustava u kojem bi umjetna inteligencija otkrivala lažne identitete i druge negativne konotacije skupa je i glomazna, no ipak je moguća.[33] Međutim, dublji problem je u tome da Facebooku i Twitteru ova mogućnost regulacije ne odgovara jer oni svoju poslovnu dobit, u velikoj mjeri, temelje na ogromnom broju korisnika tako da im nije u interesu da korisnike obeshrabre da za aktivnosti na njihovim platformama legaliziraju stvarnim osobnim podacima.[34] Iako ove korporacije javno osuđuju te povremeno uklanjaju lažne račune, one u stvarnosti podupiru poslovni model koji se temelji na iskorištavanju emocionalno nabijenih sadržaja jer im ovakvi sadržaji pokreću angažman korisnika i privlače njihovu pažnju publika isključivo iz komercijalnih razloga.

Ovakve tehnologije i algoritmi na kojima korporacije grade dizajn i funkcionalnost svojih platformi za umrežavanje doveli su do glavnog paradoksa društvenih mreža. One su trebale bolje povezivati ljudske zajednice. Međutim, one su stvorile virtualni prostor znanja sa sve većim brojem digitalno podijeljenih grupa koje su zasićene ogromnom količinom (dez)informacija. Paradoks je da su otvorili nove mogućnosti vrlo jednostavnog stvaranja i brze distribucije dezinformacija

[33] Oates, 2020.

[34] Ibid.

kojima se može napadati čitav (kao i pojedinačni) „informacijski sustav“ nekog društva odnosno njegovo opće, javno znanje.[35]

Ovakva algoritmizacija podataka može dovesti do upravljanog građanstva i do fragmentiranosti sfere javnog znanja. Međutim znanstveni dokazi tome još uvijek nisu dovoljno istraženi[36] pa će ovom fenomenu biti potrebno posvetiti dodatna istraživanja.

Algoritmi društvenih mreža i sigurnosni društveni paradoks

Paradoks je u tome da su algoritmi doveli do toga da se kroz javne rasprave naglašavaju postojeće društvene slabosti i pojavnosti kao što su polarizacija, ekstremizam i radikalne krajnosti u shvaćanjima i tumačenjima različitih društvenih pojava. Paradoks je što algoritmi bez obzira na istinitost sadržaja, popularnost nekih sadržaja koji u sebi mogu imati dezinformacije ili teorije urote, mjeri i rangira prema ostvarenim učincima pažnje, a ne prema kriteriju objektivne istine. Time izravno potkopavaju osjećaje ciljanih publika o tome što je istina a što je laž. Paradoks je i u tome da se osobni podaci korisnika društvenih mreža koriste protiv njih samih kako bi korporacije od prodaje njihovih podataka i od ogla-

[35] Henriksen Ellen Emilie, Big data, microtargeting, and governmentality in cybertimes, The case of the Facebook-Cambridge Analytica data scandal, Master thesis in political science, Department of Political Science University of Oslo, (2019), dostupno na: https://www.duo.uio.no/handle/10852/69743

[36] Neudert i Marchal, 2019.

šavanja ostvarile veći profit. Radi se o algoritamskom razvrstavanju informacija što je među prvima usavršio Facebook predstavljajući javnosti ove proizvode željom i interesom da poboljša živote svojim korisnicima.[37] Međutim iz brojnih primjera vidljivo je da su se društvene mreže pretvorile u alate za isticanje, između ostalog, i najgorih ljudskih tendencija te da ih razni akteri iskorištavaju i zloupotrebljavaju. Ove nove informacijsko-komunikacijske tehnologije i sustavi najprije su se počeli iskorištavati za marketinške i financijske svrhe. Potom, od 2000-tih pogotovo u SAD-u počele su se koristiti za politički marketing tako da je bilo samo pitanje vremena kada će se iskoristiti i u strategijama informacijskog ratovanja.

Nedostatna regulacija aktivnosti na društvenim mrežama i nedovoljno reguliran cyber prostor dovela je do zlonamjernog iskorištavanja društvenih mreža. To je razlog zbog kojeg se njihovoj zloupotrebi ne mogu pripisati atributi izravne agresije te se shodno tome ne mogu primijeniti pravila koja vrijede za oružane sukobe. Raznim akterima se pogoduje da tehnologije i tehnike digitalnog marketinga, dizajn društvenih mreža i algoritamske „tvorničke“ postavke privatnih korporacija koriste za vođenje informacijskog sukoba/rata kroz nove oblike sukobljavanja u cyber/kiber prostoru. Dva su bitna razloga tome.

[37] Bakshy, Eytan et al. Exposure to ideologically diverse news and opinion on Facebook. Science 348, str. 1130 - 1132 (2015), dostupno na: https://www.semanticscholar.org/paper/Exposure-to-ideologically-diverse-news-and-opinion-Bakshy-Messing/c8665198592b52ba122e5cf84032a9bc1c61eade

Prvi je da su same društvene mreže svojim dizajnom otvorile mogućnosti zlouporabe, a drugi je sam cyber prostor jer on još uvijek nije dovoljno regulirano okruženje.

Korpus javnog znanja i društvene mreže

Korpus javnog znanja jasno je definiran. Korpus javnog znanja dio je korpusa otvorenog znanja.[38] On je određen sadržajem koji postoji u javnom informacijskom prostoru, koji u njemu ima dominantan položaj i status. Ovaj korpus se, uglavnom, oblikuje pod utjecajem različitih javnih medija. U različitim društvima i zajednicama, korpusi javnog znanja mogu biti bitno različitog sadržaja.[39]

Dok je vrijednost i kvaliteta sadržaja bila odlučujuća hoće li se neki rad tiskati i distribuirati, u prostoru javnog znanja postojala je znatno manja količina dezinformacija. Jednostavno, dezinformacije se nije moglo toliko brzo i široko distribuirati toliko koliko se to može danas uporabom društvenih mreža i aplikacija za mobilno komuniciranje. Tehnologije i tehnike dezinformiranja su iste. Ali je sredstvo znatno jednostavnije što dovodi do bržeg i intenzivnijeg širenja, a time i utjecaja dezinformacija. Novost je u mogućnostima zlonamjernog iskorištavanja društvenih mreža i algoritamskih rješenja koji održavaju njihove osnovne funkcije i poslovni model.

Nastojanja država da utječu na politička i društvena stanja, mišljenja i ponašanja širokim spektrom publika u drugim državama nisu novost niti

[38] Tuđman, 2008.

[39] Ibid.

je novost u manipuliraju informacijama u političke ili diplomatske svrhe. Novost je u brzinama i mogućnostima manipuliranja informacijskim sadržajima pomoću digitalnih tehnika kojima se takvi sadržaji obrađuju. U novim formama informacijskog rata poslovni model ovih korporacija razni akteri koriste za manipuliranje prostorom javnog znanja te ih koriste kao vektore napada. Zbog svega navedenog prostor javnog znanja postao je dostupniji i podložniji vanjskim utjecajima.

Drugim riječima prostor javnog znanja postao je lakša meta. Fokus je na manipuliranju vjerovanjima, stavovima, shvaćanjima, činjenicama i ponašanjima na jedan vrlo agresivan način i s namjerom da se protivničkom društvu ubacivanjem straha, tjeskobe, neizvjesnosti i sumnje naruše procesi odlučivanja. Ovi ciljevi postižu se, između ostalog, i algoritamskim ubrzavanjem i širenjem uznemirujućih i manipulativnih informacijskih sadržaja i dezinformacija, ne po kriteriju istinitosti i točnosti nego prema kriteriju ostvarene pažnje. Sve ove zlonamjerne aktivnosti omogućavaju društvene mreže zbog neadekvatne regulacije, njihovih postavki i dizajna koji omogućavaju njihovu zlouporabu.

Segmentiranje publika u virtualnom prostoru dovelo je do dodatne polarizacije, radikalizacije i ektremizacije društvenih pojava u stvarnom svijetu. Lažni identiteti, automatizirano upravljanje i automatizirano stvaranje i anonimno diseminiranje (dez)informacija velikom brzinom i velikog dometa bez posrednika razni akteri iskorištavaju kao standard u novim oblicima informacijskog rata. Ove negativne promjene i trendovi negativno utječu na sposobnost opažanja kako se procjenjuju stvari, ideje, problemi, događaji i kako se

procjenjuju drugi i njihovo ponašanje što posljedično utječe i na donošenje odluka i što u konačnici utječe i na razine percepcije i razumijevanje vrste znanja koje nas okružuju.

Razni akteri ove negativnosti koriste za stvaranje utjecaja na konkurentni ili protivnički prostor javnog znanja. Pomoću opisanih algoritamskih rješenja i informacijsko-komunikacijskih alata i tehnika danas se pomoću društvenih mreža nastoje razbiti konkurentski društveni i politički konstrukti.

Društvene mreže i algoritmi pokrenuli su proces stvaranja novih formi organiziranja društva i prostora javnog znanja. Ako se ovaj proces koji zbog novih tehnologija nezaustavljivo napreduje, ne bude pravno regulirao budućnost društva i prostor javnog znanja mogli bi biti suočeni s dodatnim formama segregacije kojima će upravljati algoritmi i umjetna inteligencija. A oni će biti u funkciji ostvarivanja ciljeva svojih stvaratelja.

Tehnologije same po sebi nisu loše, one su sveopća konstanta društvenog napretka, one se ne mogu izbjeći no društvo se zajedno s tehnologijom mora transformirati kako nebi postalo taoc vlastitog tehnološkog razvoja kojeg sve više diktiraju algoritmi, umjetna inteligencija i baze velikih podataka. Zato razvoj i iskorištavanje algoritamskog upravljanja ljudskim ponašanjima ne smije ostati neregulirano. Društvo mora biti spremno odgovoriti na izazove koje ovakva tehnološka revolucija nosi sa sobom.

U SAD-u se trenutno vodi snažna marketinška i politička borba u kojoj s jedne strane stoje političke elite koje su odgovorne za sigurnost, stabilnost i pozitivnu i odgovornu budućnost vlastitog društva i učinkovitost državnih institucija, dok s

druge strane stoje navedene velike tehnološke korporacije koje zbog negativnih posljedica i odbijanja reguliranja vlastitog poslovnog modela ugrožavaju i produbljuju postojeće probleme (društvene, gospodarske, političke, sigurnosne, financijske i dr.) američkog društva. Kao što je navedeno zbog nepostojanja digitalnih granica s ovim problemima se suočavaju sve države i sva društva svijeta.

Nove informacijske tehnologije zloupotrebljavaju cyber informacijski prostor u pravcu koji je potpuno drugačiji u odnosu na razloge zbog kojih je zamišljen i stvoren. Cyber prostor je stvoren radi brze, pouzdane i sigurne razmjene točnih i istinitih podataka, informacija i znanja, radi njihovog očuvanja, pohrane i naknadnog sigurnog i pouzdanog korištenja. Dosadašnje iskustvo uči nas da stvaranje ovog potpuno novog informacijskog prostora „globalnog javnog znanja" ima za posljedicu i novu preraspodjelu moći u tom globalnom prostoru: na mjesto nacionalnih, regionalnih ili lokalnih moćnika nastupa globalna moć. U tom prostoru djeluju globalni igrači, s globalnim vrijednostima (tehnologije, informacije, tržište, slobodan protok ljudi, dobara, financija, „nova" ljudska prava itd.) koje su počele potiskivati univerzalne vrijednosti (osobnu i nacionalnu slobodu, demokraciju, kulturu, temeljna ljudska prava itd.). Ove globalne promjene u prostoru javnog znanja imaju za posljedicu i promjenu konfiguracije ukupnog društvenog znanja, koje će se reorganizirati koristeći istu infrastrukturu.[40]

[40] Ibid.

Podatkovni i digitalni suverenitet

Jedan od mogućih odgovora je u mehanizmima stvaranja, oblikovanja te očuvanja podatkovnog i digitalnog suvereniteta država (i međudržavnih intergacijskih zajednica) na temelju kojeg bi, kao što utvrđuju suverenitet unutar vlastitih fizičkih granica, izgradili suverenitet i u vlastitom digitalnom prostoru unutar kojeg bi se uspostavila bolja pravila ponašanja. Jedan od pozitivnih pomaka u tom smjeru predstavlja Berlinska deklaracija koju su države članice EU-a usvojile u prosincu 2020. Digitalna transformacija podrazumijeva sudjelovanje čitavog društva u digitalnom prostoru, poštivanje temeljnih prava i demokratskih vrijednosti, jačanje međusobnog povjerenja, podizanje razine digitalne pismenosti i stvaranje sustava umjetne inteligencije koji će poticati otpornost i održivost na temeljnim vrijednostima i interesima ljudi i javnog sektora.[41] Izgradnja ovakvih mehanizama ima za cilj jačati politike digitalnog suvereniteta kojim će države jačati vlastite sposobnosti u digitalnom prostoru za pružanje, primanje i razmjenu usluga radi učinkovitog međusobnog djelovanja.

Suverenitet država su temeljne vrijednosti i temeljni okviri po kojima se organiziraju poruke u mainstream medijima. Sa stajališta organizacije znanja možemo reći da je suverenitet jedan od generičkih koncepata u novoj mapi javnog znanja. Generički pojmovi funkcioniraju kao predodžbene sheme za organizaciju poruka, motivaciju publike i prepoznavanje aktera u javnoj

[41] Europska komisija, EU Member States sign the Berlin Declaration on Digital Society, dostupno na https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_en

komunikaciji. One su žarišne točke sustava poruka i tvore čvorne točke mape znanja jedne zajednice koja dijeli iste vrijednosti, ima zajedničke interese te stvara i rabi ista znanja u ostvarivanju svojih ciljeva.[42] Odgovornost informacijske znanosti za javno znanje u informacijskom prostoru može biti prvenstveno u izradi standarda i alata za oblikovanje i upravljanje javnim znanjem kako bi se osigurao čisti informacijski prostor, dostupnost objektivnim informacijama, i ravnopravnost u razmjeni znanja.[43]

Temeljna načela na kojima se treba graditi nacionalni i međudržavni podatkovni i digitalni suverenitet počivaju na promoviranju, očuvanju i razvijanju načela demokracije i slobode govora; na razvijanju transparentnosti i zaštiti ljudskih prava; sprječavanju monopola, cenzure i širenja dezinformacija; te na uspostavljanju mehanizama odgovornosti za nešto što je napisano, objavljeno i podijeljeno pri čemu bi javni interes trebao biti ispred privatnih i korporativnih interesa.

U tom cilju zadaća nacionalnih vlada i multinacionalnih organizacija treba biti uspostava sigurnih i pouzdanih mehanizama kojima bi se definirala pravila ponašanja i kojima bi se uspostavili zakoni koji bi vrijedili za ponašanje u cyber svijetu. Ovi mehanizmi bi trebali pridonijeti izgradnji učinkovite, sigurne, pouzdane, obnovljive i otporne kritične informacijsko-komunikacijske infrastrukture; daljnjem istraživanju, razvoju i provedbi temeljnih načela te razvijanju sposobnosti reagiranja na različite prijetnje. Temeljna načela nacionalnog i međudržavnog podatkovnog i digitalnog

[42] Tuđman, 2008.

[43] Tuđman, 2007.-2016.

suvereniteta trebaju počivati i na sustavima umjetne inteligencije ali ne na način da su algoritmi i umjetna inteligencija donositelji odluka nego da se njihove prednosti i kvalitete iskorištavaju kao preporuke o kojima će konačne odluke donositi društvo.

Jedno od temeljnih načela koji bi trebali osigurati provedbu podatkovnog i digitalnog suvereniteta počiva na transparentnoj interakciji, koordinaciji i zajedničkom radu državnih i međunarodnih institucija s privatnim, javnim, akademskim sektorom.[44] Takvim se pristupom mogu, te trebaju, spriječiti sve one aktivnosti velikih tehnoloških kompanija koje teže preuzimanju dijelova suvereniteta koje imaju države i međudržavne organizacije. Države i međudržavne organizacije moraju biti ti čimbenici koji će određivati „pravila ponašanja i djelovanja", a ne da tehnološke tvrtke same sebi definiraju pravila te same prate, nadziru i kontroliraju tu primjenu. Takvo ponašanje velikih tehnoloških tvrtki koje teže ka preuzimanju dijela suvereniteta se može tumačiti kao moderni tehnološki neo-imperijalizam.

Zaključak:

Drastične promjene u stvaranju, raspodjeli i manipuliranju javnog znanja do kojih su dovele privatne globalno rasprostranjene tehnološke korporacije, traže nove odgovore s ciljem stvaranja mehanizama odgovornosti za nešto što je napisano, objavljeno i podijeljeno u cyber prostoru.

[44] Gordan, Akrap; Slavko, Vidović; Hrvoje, Sagrak: Digitalni suverenitet: što, zašto, kako, predavanje na petom Zagreb Security Forum 2020.

Ovim mehanizmima definirala bi se pravila ponašanja i uspostavili bi se novi zakonodavni okviri koji bi vrijedili za ponašanje u cyber svijetu.

Tehnologije i algoritmi na kojima privatne tehnološke korporacije grade dizajn i funkcionalnost svojih platformi za umrežavanje doveli su do glavnog paradoksa društvenih mreža: umjesto boljeg povezivanja ljudskih zajednica stvorile su virtualni prostor znanja sa sve većim brojem digitalno podijeljenih grupa koje su zasićene ogromnom količinom (dez)informacija; otvorile su nove mogućnosti vrlo jednostavnog stvaranja i brze distribucije dezinformacija kojima se može napadati čitav (kao i pojedinačni) „informacijski sustav“ nekog društva odnosno njegovo opće, javno znanje; one kroz javne rasprave naglašavaju postojeće društvene slabosti i pojavnosti kao što su polarizacija, ekstremizam i radikalne krajnosti u shvaćanjima i tumačenjima različitih društvenih pojava; algoritmi bez obzira na istinitost sadržaja, popularnost nekih sadržaja koji u sebi mogu imati dezinformacije ili teorije urote, mjeri i rangira prema ostvarenim učincima pažnje, a ne prema kriteriju objektivne istine, a osobne podatke korisnika društvenih mreža koriste protiv njih samih kako bi korporacije od prodaje njihovih podataka i od oglašavanja ostvarile veći profit.

Nedostatna regulacija ovakvih aktivnosti na društvenim mrežama i nedovoljno reguliran cyber prostor dovela je do njihove zloupotrebe za vođenje informacijskog sukoba/rata kroz nove oblike sukobljavanja u cyber/kiber prostoru. Jedan od odgovora informacijske znanosti za javno znanje bila bi uspostava mehanizama nacionalnog i međudržavnog podatkovnog i digitalnog suvereniteta. Utemeljeni na osnovnim društvenim i demokratskim načelima podatkovni i digitalni suverenitet predstavljao bi novi standardni

obrazac kojima bi se oblikovalo i upravljalo javnim znanjem na objektivnim informacijama i transparentnoj i ravnopravnoj razmjeni točnih i provjerenih informacija.

Bibliografija:

1. Akrap, Gordan, Informacijske strategije i operacije u oblikovanju javnog znanja, doktorska disertacija, Sveučilište u Zagrebu, Filozofski fakultet, Zagreb, 2011.
2. Akrap, Gordan; Slavko, Vidović; Hrvoje, Sagrak: Digitalni suverenitet: što, zašto, kako, predavanje na petom Zagreb Security Forum 2020.
3. Bakshy, Eytan et al. Exposure to ideologically diverse news and opinion on Facebook. Science 348, str. 1130 - 1132 (2015), dostupno na: https://www.semanticscholar.org/paper/Exposure-to-ideologically-diverse-news-and-opinion-Bakshy-Messing/c8665198592b52ba122e5cf84032a9bc1c61eade
4. Bergh Arild, Social network centric warfare – understanding influence operations in social media, Norwegian Defence Research Establishment (2019), dostupno na: https://www.ffi.no/en/publications-archive/social-network-centric-warfare-understanding-influence-operations-in-social-media
5. Berkovsky Shlomo, Kaptein Maurits, Zancanaro Massimo, Adaptivity and Personalization in Persuasive Technologies (2016), dostupno na:

https://researchers.mq.edu.au/en/publications/adaptivity-and-personalization-in-persuasive-technologies
6. Boldyreva, Elena, Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. 91-102. (2018), 10.15405/epsbs.2018.12.02.10, dostupno na: https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process
7. Europska komisija, EU Member States sign the Berlin Declaration on Digital Society, dostupno na https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_en
8. Flore Massimo, Balahur Alexandra, Podavini Aldo, Verile Marco, Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda, Publications Office of the European Union, Luxembourg, (2019), dostupno na: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC116009/understanding_citizens_vulnerabilities_to_disinformation.pdf
9. Jamieson Hall Kathleen, Messages, Micro-Targeting, and New Media Technologies, The Forum 11 (2013), dostupno na: https://doi.org/10.1515/for-2013-0052
10. Markopoulos, P., Kaptein, M. C., Ruyter, de, B. E. R., & Aarts, E. H. L. Personalizing persuasive technologies : explicit and implicit personalization using persuasion profiles. International Journal of Human Computer Studies, 77, 38-51. https://doi.org/10.1016/j.ijhcs.2015.01.004, (2015), dostupno na: https://pure.tue.nl/ws/files/3994499/888440058546432.pdf
11. Kerry Jones, Kelsey Libert, i Kristin Tynski, The Emotional Combinations That Make Stories Go Viral, Harvard Business Review,

2016, dostupno na: https://hbr.org/2016/05/research-the-link-between-feeling-in-control-and-viral-content
12. Henriksen Ellen Emilie, Big data, microtargeting, and governmentality in cybertimes, The case of the Facebook-Cambridge Analytica data scandal, Master thesis in political science, Department of Political Science University of Oslo, (2019), dostupno na: https://www.duo.uio.no/handle/10852/69743
13. Nadler Anthony, Crain Matthew, Donovan Joan, Weaponizing The Digital Influence Machine, The Political Perils of Online Ad Tech (2018), dostupno na: https://datasociety.net/library/weaponizing-the-digital-influence-machine/
14. Neudert Lisa Maria i Marchal Nahema, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, Brussels (2019), dostupno na: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf
15. Nye Joseph, Protecting Democracy in an Era of Cyber Information War, Belfer Center for Science and International Affairs, Harvard Kennedy School, SAD (2019). dostupno na:https://www.belfercenter.org/publication/protecting-democracy-era-cyber-information-war
16. Oates Sarah. The easy weaponization of social media: why profit has trumped security for U.S. companies, Digi War (2020). https://doi.org/10.1057/s42984-020-00012-z
17. Singer W.P. i Brooking T. Emerson, LikeWar: The Weaponization of Social Media, (2018).
18. Tuđman, Miroslav, Projekt: Oblikovanje i upravljanje javnim znanjem u informacijskom prostoru 2007.-2016., Filozofski fakultet,

Zagreb, dostupno na: http://zprojekti.mzos.hr/public/c-prikaz_det.asp?psid=0&ID=2394
19. Tuđman, Miroslav, Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb, (2008).
20. Van Alstyne Marshall, Brynjolfsson Erik, Global Village or Cyberbalkans: Modeling and Measuring the Integration of Electronic Communities, (2005), dostupno na: https://www.researchgate.net/publication/220535041_Global_Village_or_Cyber-Balkans_Modeling_and_Measuring_the_Integration_of_Electronic_Communities
21. Vilmer J.-B. Jeangène, Escorcia A., Guillaume M., Herrera J., Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, Paris (2018), dostupno na: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf