FBIM Transactions
DOI 10.12709/fbim.07.07.01.18

IZAZOV ZLOUPOTREBE INFORMACIONIH TEHNOLOGIJA ZA JAVNO INFORMISANJE

CHALLENGE OF THE ABUSE OF INFORMATION TECHNOLOGIES FOR PUBLIC INFORMATION

Miroslav D. Stevanović
Akademija za nacionalnu bezbednost

Dragan Ž. Đurđević
Akademija za nacionalnu bezbednost

JEL Kategorija rada: **H19**, **H52**, **Y80**,

Apstrakt

U ovom članku posmatramo informisanje kao proces činjenja javno dostupnim podataka i informacija, njihovom distribucijom u kiber prostoru. S obzirom da je informisanje osnovno pravo svake individue i obaveza javnih vlasti, pojava fenomena nazvanog „lažne vesti" implicira da javne vlasti ne uspevaju, u savremenim uslovima, da obezbede pravo na objektivno i tačno informisanje. Problem koji fokusiramo je u kom obimu informacione tehnologije mogu biti instrumentalizovane za relativizovanje funkcije javnog informisanja. U navedenom kontekstu, cilj rada je da se izoluju mehanizmi zloupotrebe, kako bi ih bilo moguća blagovremeno prepoznati i suprotstaviti se štetnim posledicama u realnom prostoru. Metodološki, rad se zasniva na fenomenološkoj distinkciji značaja utiska naspram na faktičkog stanja, kako bi se došlo do realne vrednosne dimenzije informisanja. Pokazatelji dobijeni na taj način podvrgnuti su analizi sa aspekta potencijalnog strukturalnog i funkcionalnog uticaja sistematske instrumentalizacije informacionih tehnologija za nametanje mnjenja umesto informisanja. Rezultati analize ukazuju da postoji niz rizika koji proističu iz neuređene i nekontrolisane masovne primene informacionih tehnologija, a koji potiču iz neravnopravnog položaja učesnika u kiber prostoru. Nalazi daju osnova za zaključak da potencijalni rizici uključuju i moguće ofanzivno delovanje, te da zahtevaju uređenje preuzimanja i prenošenja informacija i podataka u nacionalnom kiber prostoru. U tom kontekstu, čini se da evaluacije informacionih tehnologija ne može biti prepuštna autarhičnim inicijativama, već da mora biti predmet sistematske ocene od strane relevantnih forenzičkih tela.

Ključne reči: *percepcija, narativ, geoprostorno prikupljanje podataka, metapodaci, prikupljanje podataka o ljudskom domenu*

Abstract

In this article, we view public information as a process of making available data and information through their distribution, primarily in cyberspace. Given that information is the fundamental right of every individual and obligation of public authority, the emergence of a phenomenon called "fake news"

Adresa autora zaduženog za korespodenciju:
Miroslav Stevanović
mstvnv297@gmail.com

implies that, in contemporary conditions, public authorities fail to secure the right to objective and accurate information. The problem we are focusing on is the extent to which information technology can be instrumentalised to relativise the public information function. In this context, the goal of the work is to isolate the abuse mechanisms, so that they can be timely identified and harmful consequences counteracted in the realm. Methodologically, the work is based on the phenomenological distinction between the importance of the impression and the factual situation in order to reach the real value dimension of information. The indicators obtained in this way are analysed from the perspective of the potential structural and functional impact of systematic instrumentalisation of information technologies to impose opinions instead of informing. The results of the analysis point to the existence of a number of risks arising from the unregulated and uncontrolled mass application of information technologies, which stem from the unequal position of the participants in the cyberspace. Findngs provide a basis for the conclusion that potential risks include possible offensive action and require the organisation of the download and transmission of information and data in the national cyberspace. In this context, it seems that information technology evaluations cannot be left to autarchical initiatives, but must be subject to a systematic assessment by relevant forensic bodies.

***Keywords**: perception, narrativa, geospatial intelligence, metadata, human domain intelligence*

1. UVOD

Informacione tehnologije, sa aspekta funkcije u informisanju, predstavljaju upotrebu računara da se arhiviraju, pronađu, prenose ili manipuliše, s jedne strane, nizom kvalitativnih i kvantitativnih promenljivih kao činjenicama koje su osnov za rezonovanje, raspravu ili kalkulaciju (podaci) i, s druge, oblicima i formama koje pružaju deo ili celovit odgovor na neke neizvesnosti, u smislu komunikacije ili dobijanja apstraktnih ili obaveštajnih saznanja (informacije). Ako se posmatra strukturalno, informacione tehnologije obuhvataju sve oblike tehnologije koje uključuju bilo kakav oblik digitalnih (elektronskih) podataka i informacija. Podaci i informacije, u kontekstu analize potencijalne zloupotrebe informacionih tehnologija u informisanju, odnosno kontekstualizovani sa aspekta učesnika u kiber informacionom prostoru, predstavljaju svaki stimulans koji za prijemnika ima neko značenje u određenom misaonom kontekstu.

U skladu sa navedenim, informacioni prostor se doktrinarno može odrediti prema različitim unutrašnjim pravilnostima. Ovaj pojam, s jedne strane, obuhvata set misaonih koncepata i uzajamnih odnosa između njih koje određeni informacioni sistem održava, u smislu kognitivnog prostora (Newby, 2001). U tom smislu, pojam informacioni prostor opisuje opseg mogućih vrednosti ili značenja koji podatak ili informacija mogu imatu u okviru datih pravila i okolnosti. S druge strane, ovaj pojam istovremeno podrzumeva i tip informacionog dizajna u kojem su prenosioci predstave o podatku/informaciji locirani u načelnom prostoru, odnosno prostoru u kojem njihova lokacija i smer imaju značenje tako da postoji mogućnost njihovog mapiranja i navigacije (MIT Artificial Intelligence Laboratory, 1998) U navedenom smislu, informatcioni prostor bi predstavljao ono što nas informativno okružuje, te bi preuzimanje fajlova, korišćenje pretraživanja i ulazak na web stranice predstavljalo kretanje kroz informacioni prostor.

Pored navedenih određenja, koji se zasnivaju na sadržini (materijalistička), informacioni prostor je moguće odrediti i idealistički. Tako se, na primer, može posmatrati kao ukupni rezultat semantičke aktivnosti čovečanstva, kao svet prihvaćenih naziva i značenja, u sprezi sa ontološkim svetom. Kako je informacioni prostor izvorni koncept nemoguće ga je definisati precizno, osim da predstavlja dijalektičku suprotnost materijalnom, fizičkom, objektivnom prostoru. Idealistički posmatrano, informacioni prostor bi predstavljao konceptualni okvir za kodifikovanje, apstrakciju i prenošenje podtaka i informacija kroz društveni sistem (Boisot,1995).

U informacionom prostoru, zloupotreba informacionih tehnologija, apstrahujući sama značenjska preferiranja budući da ona ne predstavljaju isključivo posledice takve zloupotrebe, može se odraziti kroz ograničavanje suprotnog mišljenja (regulatorno zarobljavanje), kroz skrivanje poruka (prikrivena cenzura) i kroz pojačavanje linije mišljenja. Sama zloupotreba se, suštinski, sastoji u tome da se informacione tehnologije, koje predstavljaju javni alat i sredstvo, postavljaju kao učesnici u komunikaciji,

ali bez interaktivnih odlika sa drugim učesnicima u javnom prostoru (Karatas; Zihni, 2010).

Na taj način preobražaj ka društvu znanja, kakvom se nominalno teži u informacionom dobu, praktično se podvrgava digitalnoj pristrasnosti. Problem se ispostavlja kao društveno-tehnički. Naime, kako se primećuje u teoriji, on obuhvata značaj, s jedne strane, informacionih tehnologija, odnosno transparentnost i neutralnost platformi i, s druge, administriranja i odgovornosti za informacioni prostor javnih vlasti (Reddick, 2012).

Ovaj problem je višedimenzionalan, budući da obuhvata preduzetničku, bezbednosnu i političku komponentu informacionih tehnologija u informacionom prostoru. Kako informacija ima javnu funkciju, u smislu da oblikuje mnjenje, činioci koji tome doprinose (uključujući informacione tehnologije) mora se posmatrati u kontekstu motivacije javnosti. Kako, sa aspekta korporativnih vlasnika platformi, podatak I informacija postaju roba na tržištu, empirijsko posmatranje je ograničeno na uticaje i stavove.

Informacione tehnologije ne funkcionišu u vakuumu ili izolovano od konteksta u kome se koriste te je neophodno odrediti radni pojam njihove zloupotrebe. U kontekstu ovog rada, pod zloupotrebom informacionih tehnologija podrazumeva se njihovo korišćenje (najčešće od strane korporativnih vlasnika tehnologija) radi uticaja na oblikovanje mnjenja u isključivom interesu nosilaca vlasti ili javnog sektora.

2. INFORMACIONE TEHNOLOGIJE U JAVNOM INFORMISANJU

Primeri naizgled organizovanog postavljanja poruka na mreži su široko opisani u literaturi i medijima i mnogi autori ovo smatraju kao realnost u kiber informacionom prostoru. Javni akteri, međutim, po pravilu negiraju da se pribegavaju takvoj praksi i tvrde da su isključivo posvećeni objektivnom informisanju. Informaciono doba je eksponiralo ulogu koju u distribuciji poruka, pored medija, imaju platforme koje su u vlasništvu i kojima upravljanju privatne korporacije, koje se formalno ne bave javnim informisanjem niti javnim politikama i naizgled su neutralni u procesu informisanja. Njihova uloga u informacionom prostoru proističe iz pozicije pružaoca tehnoloških usluga, posredstvom kojih imaju indirektan pristup učesnicima u na mreži i direktan pristup njihovim metapodacima (Stevanović, Đurđević, 2018).

Zbog kontrolne uloge koju imaju u tehnološkoj strukturi kiber prostora, ove korporacije su u poziciji da utiču na sve koji se informišu u kiber prostoru, a posebno na učesnike u društvenim mrežama. Njihov uticaj na korisnike može biti indirektan, kroz promociju pozitivnih ili negativnih osećanja o određenoj temi, s jedne, ikroz izazivanje podložnosti određenim emocijama kod učesnika na mreži, s druge strane,. Sledstveno, ove korporaciji su u poziciji da mogu netransparentno da utiču na vrednosne afinitete i prijemčivost informacija na društvenom, pa čak i na porodičnom i privatnom nivou (Miltiadis, Novo-Corti, 2012). U tom, kontekstu, posebno se apostrofira značajan uticaj društvenih mreža na privatnost, povezanost i prijemčivost podataka i informacija, usled čega kompanija koja upravlja mrežom može praktično uticati na sadržaj života u realnom prostoru.

S obzirom da ove kompanije nisu odgovorne za informacije, niti su legitimni politički činioci, mogućnost da oblikuju narative može generisati izazove za demokratske procese i slobode. Osim uticaja vlasnika tehnologija na širenja narativa, umesto objektivnog informisanja, ove kompanije su u poziciji da iz diskursa u kiber informacionom prostoru neposredno eliminišu ili promovišu poruke određene sadržine i učesnike koji zagovaraju takav sadržaj.

Posmatrajući plasiranje narativa u kiber prostoru, može se konstatovati da su u kratkom periodu javno eksponirani mnogi primeri koji svedoče da je uticaj privatnih tehnoloških kompanija na informacioni prostor postao stvarnost.

Tokom predsedničke kampanje u Sjedinjenim Američkim Državama 2016. godine, Facebook je jednostrano gasio veliki broj naloga korisnika koji su agitovali za opozicionog kandidata, ali i onih koji su propagirali afirmativne stavove o nekim pitanjima za koja se taj kandidat zalagao (poput o vojsci, pravu na posedovanje oružja, kontroli granica i hrišćanstvu). Pomenuta kompanija je nastavila takav trend i nedavno uvela softversku aplikaciju na društvenoj mreži kojom upravlja, u svrhu "nezavisnei provjere činjenica", navodno sa ciljem da se eliminišu postovi koji pronose "lažne vesti", što se u praksi svelo skoro isključivo na one koji promovišu konzervativne stavove.

Tokom predizborne kampanje u Francuskoj, Facebook je samoinicijativno na svojoj društvenoj mreži ugasio 30.000 računa, uz obrazloženje da se radi o „lažnim računima“, ali isključivo onih koji su podržavali konzervativnu kandidatkinju (Ali; Associated Press, 2017).

Krajem 2017. i početkom 2018. godine, Twitter je na društvenoj mreži kojom upravlja sproveo kampanju za smanjenje autoriteta zagovornika konzervativne ideološke provenijencije (uključujući libertarijanske). Ova društvena mreža je prethodno, pod izgovorom da je obavezna da obezbedi primenu sopstvenih smernica protiv nasilja i maltretiranja, jednostrano, bez javno poznatih pravila i procedure, izbrisala neke automatske naloge i korisnike zbog navodnog kršenja pravila te mreže. Jedan od izvršnih menadžera Twitter-a svedočio je pred Komitetom za obaveštajne poslove Kongresa SAD, u novembru 2017. godine, da je kompanija smanjila rejting članka objavljenog na portalu, koji se nije uklapao u dominantni narativ i uprkos tome uspeo da zaobiđe algoritam i dospe na vrh opcije trendova (i kao takav privlači korisnike).

Google je pokrenuo niz aktivnosti sa ciljem da na pretraživaču kojem upravlja direktno promeni rezultate pretrage i blokira pristup određenim sajtovima. Ova kompanija je posebno značajna za najširi krug korisnika, jer kontroliše pretraživač koji je prvi dostupan korisnicima koji traže informacije na mreži. Stoga, manipulisanje rezultatima koje korisnici smatraju objektivnim stanjem predstavlja veštačko usmeravanje korisnika i održavanje predrasuda o temi.

Sa Google-om povezana kompanija Youtube takođe je iz svoje mreže uklanjala "desničarske" kanale, bez transparentnog postupka, samo na osnovu procene anonimnih tela unutar kompanije da su na njima prekršeni kompanijski uslovi usluge. S obzirom da se radi o privatnoj kompaniji, a da uklanjanje nije vršeno na osnovu zakonske obaveze, interesantna je opservacija da su neki od uklonjenih kanala kanala imali milijardu pristupa i milione pretplatnika i bili na ovoj mreži više od jedne decenije, što implicira da odluka nije bila motivisana komercijalnom interesom. U oktobru 2017, zaposleni Youtube su priznali da je portal Infowars-a na ovoj mreži cenzurisan, u sklopu interne operacije kompanije uvedene radi uklanjanja objavljenih video zapisa koji navodno šire lažne informacije, na osnovu žalbe privatne Kablovske mreže vesti (CNN).

Arbitrarnost i moć tehnoloških monopolista na mreži, koja predstavlja javno dobro, otvara, kada se radi o mreži kao informacionom prostoru, pitanje nepristrasnog rukovanja tehnologijom, koji ne bi omogućavao prikrivenu cenzuru. Empirijski posmatrano, vlasnici informacionih tehnologija imaju mogućnost da algoritamski, netransparentno, praktično vrše "izbor" propulzivnog sadržaja na Internetu, kontrolišu ideje u kiber informativnom prostoru, kao I da masovno ciljaju sa porukama. Ako je svrha informisanja stvaranje kompetentnog mnjenja, ove mogućnosti kompanijama predstavljaju izazov kao oblik propagande i dezinformisanja.

Čini se da u kiber informacionom prostoru, kada se radi o javnom informisanju, postoji nivo simbioze između korporativnih monopolista informacionih tehnologija i korporativnih medija sa globalnim domašajem, poput CNN. Naime, sposobnost postojećih softvera da praktično kreiraju sadržaj dostigla je nivo da je otežano da se u kiber prostoru percepira razlika između informacije/podatka od poluinformacija ili dezinformacija koje se plasiraju uklanjanjem sadržaja, upućivanjem, favorizovanjem ili drugim načinima zbunjivanja korisnika. Ova simbioza se posebno ogleda u favorizovanju i uvećanom prikazivanju dometa velikih medijskih sistema, čak i kada ankete ukazuju na nizak nivo poverenja u njihovo izveštavanje. Osnovni problem može se svesti na to da se informacioni prostor koristi kao medijum za kreiranje narativa, umesto za izveštavanje, što ga pretvara u poprište borbe za kontrolu informacija.

Suočeni sa tehnološkim monopolom, potencijalni izvori drugačijih informacija primorani su da povlađuju kompanijama čije tehnološke sisteme i usluge moraju da koriste kako bi obezbedili prisustvo u informacionom prostoru. Ukoliko te kompanije ograničavaju mogućnost predstavljanja drugačijih činjenica, takvo postupanje bi predstavljao udar na informacioni prostor na mreži. Naime, prisustvo na mreži je u informacionom dobu racionalno ponašanje. U tom kontekstu, sajtovi postaju javni prostor, te uticaj na informisanje, posebno činilaca koji nemaju formalnu funkciju informisanja, ne bi smeo bitinetransparentan i bez osnova u zakonu.

Velike tehnološke kompanije imaju monopol u oblasti informacionih tehnologija i nad medijima, Kako, danas, savremeni čovek sve više vremena provodi ped ekranom ili na mrežama, preko kojih dobija neophodne podatke i informacije, informacione tehnologije imaju objektivnu ulogu u informisanju javnosti.

3. OPŠTE FUNKCIJE UZURPACIJE

Informacije i podaci su, u savremenom svetu, vitalni element koji povezuje ideje, ljude, prostor, znanje i kapital. Informacioni prostor moguće je usmeravati alatima kojima se klasifikuju pojmovi i kontroliše vokabular. Demokratske implikacije mogućnosti da individua aktivno participira u kiber prostoru ogledaju se širenju prostora za razmišljanje i učešće, u smislu da reakcije na osnovu dostupnog sadržaja tvore novi informacioni prostor, u kome se istovremeno kristališe i javno mnjenje.

Sa aspekta tehnološkog uticaja na stvaranje i oblikovanje informativnog prostora u materijalnom smislu, mogu se izvesti četiri opšte funkcije instrumentalizacije kiber prostora za uzurpaciju informacionog prostora: a) masovna tehnološka kontrola mišljenja; b) oblikovanje nerealne percepcije; c) negativne kampanje protiv ideja i individua i d) sredstvo u igri moći (Chalmers, 2003).

a) Masovna tehnološka kontrola mišljenja

Specijalizovani softveri omogućili su da se prevaziđe problem praćenja ogromne količine dostupnih podataka. Iinicijalno se radilo o praktičnim alatima za sistematsko praćenje tema, za potrebe specijalizovanih službi da pretražuju veliki broj dokumenata, grupisanjem tema. Ova tehnološka mogućnost daje kvalitativnu prednost korisnicima koji su u mogućnosti da takav softver koriste u kiber prostoru. Naime, praktični značaj ove mogućnosti za usmeravanje mnjenja i narativa može se uporediti sa zloupotrebom informacionog prostora plasiranjem podataka, informacija i narativa preko uticajnih medija, pod okriljem interesa nacionalne bezbednosti, a najočitije u situacijama sukoba. Primer simbioze obaveštajnih službi, medija i interneta u oblikovanju narativa je tokom NATO agresije na bivšu SR Jugoslaviju. Naime, CNN i Nacionalni javni radio (NPR) su priznali da su tokom vojne operacije u njima bile stacionirane jedinice za psihološke operacije američke vojske. Činjenica da su vojni propagandisti bili u redakcijama medija koji su bili u funkciji propagande podriva pretpostavku o nezavisnosti privatnih informativnih medija.

Od uviđenja ovih softvera, posmatrano u širem kontekstu, kompanije poput Google, Amazon, Facebook i Twitter su demonstrirali moć svojih platformi, da manipulisanjem sadržaja na mreži kanališu emocije i svest korisnika u realnom svetu. Posledica prepoznavanja te moći, u kontekstu dizajniranja i kontrole narativa i javnog mnjenja, je to da su aktivnosti na mreži danas dobile široku primenu u političkim kampanjama.

b) Oblikovanje nerealne percepcije

Suočavanje u informacionom prostoru postalo je sastavni deo različitih vojnih i civilnih operacija. U tom kontekstu, društvene mreže su zbog svojih odlika, dometa i uticaja, postale nezaobilazne za organizovanje, mobilisanje i širenje ideja i za dolaženje do podataka i informacija. Domet društvenih mreža, posebno sa masovnom upotrebom mobilnih telefona, omogućava više kanala za prenos poruka, što ih čini pogodnim kao organizacioni mehanizam i moćno sredstvo za mobilisanja svesti.

Društvene mreže su pogodne za širenje dezinformacija ili kampanja za podrivanje morala ili uticaja i za pokretanje reakcija ciljne grupe. Relativno novi fenomen u tom kontekstu je konkurencija uticaja na percepcije na mreži (rat narativa). Javno poznata taktika u tom kontekstu je upotreba trolova da se započne diskusija i izazovu komentari, kako bi se pokrivali afirmativni i/ili napadali negativni stavovi (Đurđević; Stevanović, 2017). U oblikovanju narativa, sve značajniju ulogu imaju entiteti koji se oslanjaju na tehnologije veštačke inteligencije, preko kojih se pronose informacije ili dezinformacije ili poluinformacije (chat robots, Chatbots). Na primer, Google-ov tip četbot tehnologije reaguje u razgovorima po algoritmima, programiranim na bazi primera iz "trening-dijaloga". Facebook takođe ulaže u razvoj četbot tehnologija koje mogu da simuliraju razgovore ljudi u komunikaciji.

Sa povećanom ulogom društvenih mreža u informacionom prostoru, učesnici na mreži sve više ne moraju da istražuju vesti, jer su izloženi informacijama i tako se obaveštavaju preko drugih individua i društvenih mreža. Na taj način

su izloženi riziku da uverenja o javnim poslovima grade na indirektnom informisanju. Naime, informacioni prostor koji nudi širok spektar izbora *eo ipso* generiše izazov za demokratske procese, jer dovodi do produbljivanja praznina u političkom znanju na osnovu preferencija sadržaja, interesa i načina korišćenja. Pojedinci koji nasumično konzumiraju vesti ne mogu postići napredak u političkom znanju i pored količine informacija budući da, kako se u primećuje u teoriji, aktivno učenje nije srazmerno dostupnom medijskom sadržaju, već pravilnom odabiru informacija.

c) Negativne kampanje

Američka obaveštajna zajednica je upozorila na rizik od spoljnog "finansiranja akademskih institucija i neprofitnih organizacija koje se bave istraživanjem i obrazovanjem kako bi se sprečila istraživanja koja su nepovoljna po finansijere, kao taktike za podsticanje povoljnih stavova i autocenzure". Ova procena je relevantna u kontekstu zloupotreba informacionih tehnologija u kiber informacionom prostoru utoliko što implicira mogućnost zloupotrebe kreiranje mnjenja za obaveštajne, *ergo* i druge informativne operacije.

Kako se samo upozorenje izvodi iz kontemplacije, bez činjeničnih nalaza, čini se da je osnovni motiv upozorenja upravo vezan sa problem dometa velikih američkih kompanija koje pružaju usluge društvenih mreža. U tom smislu ukazuje navod iz izveštaja da kineska aplikacija WeeChat ima više od milijardu korisnika, što joj omogućava da se finansira na američkom tržištu novca. Kako američka obaveštajna zajednica procenjuje da kineski pružaoci ovih usluga imaju određenu kontrolu nad sadržajem i prikupljanjem ličnih podataka, po logici stvari sledi da i je imaju i američke kompanije u tom sektoru. Imajući u vidu da velike tehnološke kompanije iz Silikonske doline imaju ugovore sa američkim saveznim agencijama, posebno sa CIA i NSA, ne može se isključiti mogućnost da američku obaveštajnu zajednicu iritira konkurencija u kiber prostoru. Rezultat ovakvih manipulacija ilustruju brojni primeri. Tako je plasiran narativ kako se Iran fokusira na špijuniranje i kiber operacije protiv SAD i njenih saveznika, iako je u kiber prostoru apsolutna dominacija američkih kopanija i službi, te je taj diskurs notorno u funkciji stvaranja negativnog raspoloženja. Isto se može konstatovati i za rezultat istraživanja sprovedenog u trenutku zategnutih odnosa sa Severnom Korejom, da 8o% Amerikanaca smatra kao kritičnu pretnju sa kojim se suočava i severnokorejske operacije u kiber prostoru.

d) Sredstvo u igri moći

Društveni mediji prenose vesti, poput radia, štampe ili TV. Sa njihovim stalnim emitovanjem u informacioni prostor kod korisnika je rastuće uverenje da se podrazumeva da su informisani, iako ne ulažu ciljane napore u tom pravcu. Kada se kod građana postigne svest da bitne vesti dolaze same, smanjuje se verovatnoća da će oni aktivno tražiti ili proveravati raspoložive informacije. Tako se informisanje svodi na uticaj simboličke komunikacije, a važnu ulogu u tome imaju utisci koji dominiraju na društvenim mrežama.

Učesnici na mreži su danas sve više orijentisani na društvene mreže, a posebno mladi. Prema statistikama za 2017. godinu, evidentirano oko 2,6 milijardi korisnika društvenih mreža širom sveta. Takav nalaz, bez obzira na tačnost statistike, uslovljava da promocija na društvenim medijima postaje obavezna taktika u komunikaciji sa javnošću. Važnu ulogu u strukturiranja odgovarajućeg pristupa imaju Facebook, sa 2.01 milijardu korisnika mesečno, od kojih 88 odsto godišta između 18 i 29 i Twitter, sa 328 miliona korisnika mesečno, od kojih je 36 odsto između 18 i 29 godina. Interakcija mladih je važna pa su razvijene posebne aplikacije za komunikaciju unutar ove populacije, poput Snapchat (dostupan samo preko mobilnih telefona), koji dnevno ima oko 166 miliona korisnika, od kojih 56% između 18 i 29 godina, ili Facebook-ov, Instagram, koji je postao popularan među mladima.

4. RIZICI VEZANI ZA NAČIN KOMUNIKACIJE

Društveni mediji, uvodeći niz opcija koje omogućavaju i pružaju, nameću promene u načinu komunikacije. Kao sredstvo komunikacije, društvene imaju, najmanje, sledeća dejstva:

- doprinose stvaranju osećaja hitnosti i potrebe da se dele poruke (uključujući o privatim životima);
- omogućavaju ličnu predstavu o udaljenim mestima i nepoznatim događajima;
- promovišu opštu priču i detalje, ali ne fokusiraju relevantne informacije;

- donose vesti u živote mlađih generacija; i
- pružaju mogućnost emitovanja uživo i imaju mobilizacijski učinak.

Međutim, kada se radi o razumevanju širokog spektra vesti o političkim i javnim pitanjima, korišćenje društvenih mreža za informisanje ne može da nadomesti potrebu za tradicionalnim izveštavanjem. Izvori informacija u kiber prostoru stvaraju linije priča kroz različite vrste objavljive ličnih mišljenja i uvida. Kako raste popularnost i prihvatanje društvenih medija raste, više korisnika istražuje diskusiju o informacijama i podacima, čak i kada se radi o kriznim situacijama. Zbog toga je stvaranje strateških narativa u centru savremenih strategija komunikacije u poslovanju, politici i vojnim operacijama. Borba narativa postala je poluga i međunarodne politike, a u tom okviru društvene mreže postaju neophodni alat za nadmetanje.

Posledica društvenih mreža je da osnažuju individuu, tako što omogućavaju da deluje u mreži na načine koji nisu vidljivi. Kao takvi su ujedno pogodni za diversifikaciju i unapređenje propagandnih i psiholoških operacija, kao metoda uticaja na javno mnjenje.

Oblikovanja narativa, osim uticaja na prilagođavanje svesti, utiče i na institucionalni aspekt sistema nacionalne bezbednosti. Naime, promena percepcije o bezbednosno indikativnoj prirodi pojave ne menja činjenice, već samo njihovo značenje (poimanje). Otuda je oslanjanje na informacione tehnologije problematično, budući da one nemaju logički kapacitet, te efikasnost iziskuje da se prethodno odrede segmenti koji istim činjenicama daju novo značenje. Kako je nacionalna bezbednost vrednosno objektivna kategorija, ona zavisi od percepcije, zbog čega se kao problem ispostavlja blagovremeno prepoznavanje izazova i razumevanje i identifikovanje pretnji i rizika, što zahteva odgovarajući kapacitet za kreativno i vrednosno razmišljanje u procesu odlučivanja (Stevanović, Đurđević, 2015).

Jednostavnost korišćenja i pristupačnosti društvenih medija, te razvoj strategija digitalne manipulacije, prisiljavaju obaveštajne službe, vojne strategе i kreatore politike da se prilagode toj stvarnosti. Javno eksponiran skandal, vezano za političku konsultantsku kompaniju Cambridge Analytica (CA), otkrio je mogućnosti zloupotrebe neovlašćenog prikupljanja podataka korisnika Facebook-a. CA je, naime, koristila nemoralne taktike kako bi se uticalo na izbore. To je, između ostalog, obuhvatalo Facebook ažuriranja, putem reklama, da bi stiglo do korisnika koji objavljuju poruke. Facebook je dopustio CA pristup podacima o svojim korisnicima i o njihovim prijateljima u toj mreži, čak i onima koji nisu instalirali aplikaciju, niti su prihvatili da dele svoje lične podatke, što je omogućilo programerima sa Univerziteta Kembridž da brzo kreiraju baze podataka i tajni uticaj na demokratske procese. Sa aspekta uticaja informacionih tehnologija na institucionalizaciju upravljanja informacijama i međuljudske odnose posebno treba imati u vidu mogućnost geoprostornog prikupljanja podataka, budući da predstavlja rizik za privatnost ličnih podataka na mreži.

Termin geoprostorni koristi se da izrazi kolektivitet podataka i prateće tehnologije sa geografskom ili lokacijskom komponentom, odnosno zapisa koji u skupu podataka sadrže lokacijske informacije vezane za njih (na primer, u obliku koordinata, adrese, grada). Geoprostorni podaci mogu poticati iz sistema u kojima se geografske informacije čuvaju i integrišu u geografske softverske programe tako da se mogu kreirati, čuvati, koristiti, analizirati i vizualizovati (mapirati). Sajtovi društvenih mreža, na primer, koriste "check-in" koji korisnicima omogućava da svoje statusne podatke označe geografski.
Za prikupljanje, manipulaciju i skladištenje geografskih podataka i informacija koriste se geoprostorne tehnologije. Radi se o opsegu alata koji omogućavaju geografsko mapiranje i analizu zemlje i ljudskih društava. Među takvima su:
- daljinska detekcija, kojom se dolazi do slike i podataka sa različitih kamera, uređaja i senzorskih platformi. Kako neki od ovih izvora pokazuju detalje od jednog metra ili manje, takve slike mogu biti zloupotrebljene za praćenje ljudskih potreba, navika i kršenje ljudskih prava.
- geografski informacioni sistem (GIS), što obuhvata skup softverskih alata za mapiranje i analizu geografski određenih podataka. GIS se može koristiti za utvrđivanje geografskih obrasca u drugim podacima, uključujući i vezano za ljudsko ponašanje i navike.
- sistem globalnog pozicioniranja (GPS) obuhvata mrežu satelita američkod Sekretarijata odbrane koja pruža precizne koordinatne lokacije civilnim i

vojnim korisnicima sa odgovarajućom opremom za prijem (sličan evropski sistem nazvan Galileo trebalo bi da postane operativan narednih godina dok ruski sistem funkcioniše, ali je ograničen).
- internet mapiranje obuhvata softverske programe (poput Google Earth) i aplikacije na mreži (poput Microsoft Virtual Earth) koje menjaju način razmišljanja i razmene geoprostornih podataka. Kretanje u korisničkom interfejsu omogućava dostupnost takvih tehnologija, zbog čega su te tehnologije podstakle mrežu nacionalnih bezbednosnih, naučnih i komercijalnih satelita. Visokokvalitetni hardver i podaci su sada široko dostupni, te je omogućeno prikupljanje niza geoprostornih podataka, bez adekvatne kontrole i regulative u pogledu korištenja podataka, što predstavlja izazov za zaštitu podataka o ličnosti.

Geoprostorno prikupljanje podataka omogućava fuziju kartografskih podataka da konvencionalnim obaveštajnim podacima državnih agencija. Ono je zasnovano na aktivnosti i, posmatrano sa aspekta manipulacija u informativnom prostoru, pogodno je za istraživanje relevantnih obrazaca, odnosno istraživanje ljudskog domena.

Kiber prostor može biti zloupotrebljen ciljano, okupirajući ga informacijama, dezinformacijama i poluinformacijama, kako bi se neurofiziološki uticalo na ponašanje. U tom kontekstu, posebno je eksponirana zloupotreba metapodataka, odnosno podataka o sadržaju najčešće korišćenih klikova na mreži, što omogućava predstavu o individui i afinitetima i, u skladu sa tim, uticaj na percepciju.

Navedeno ukazuje da ključni nosioci komunikacionih tehnologija u kiber prostoru, funkcionalno, predstavljaju činioce koji imaju uticaj na izbor, dinamiku i promociju sadržaja, s jedne, kao i činioce uticaja na oblikovanje mnjenja u određenom periodu. Ova funkcionalna odlika može se konstatovati na primerima podrivanja tradicionalnih vrednosti (poput obojenih revolucija), kada cilj nisu institucije (zbog čega su pogodni nenasilni metodi), već nametanje odgovarajućih narativa u informativnom prostoru. Na primer, aplikacija društvene mreže Telegram, pokrenuta 2013. godine, omogućava razmenu poruka u grupama do 5.000 ljudi i bezbedno šifrovane komunikacije. Vlasti nekoliko zemalja (Rusija, Jermenija) ukazivale su da je ova mreža korišćena u planiranju terorističkih napada i uličnih protesta. Takva funkcionalna uloga omogućava sistemsku instrumentalizaciju informacionih tehnologija, odnosno strukturalne pozicije vlasnika tih tehnologija u informisanju javnosti, iako njihova profesionalna aktivnost ne uključuje informisanje javnosti.

U navedenom kontekstu, informacione tehnologije mogu u informacionom prostoru biti zloupotrebljene, najopštije posmatrano, nelegitimnim korišćenjem (zloupotreba sistema) ili podrivanjem sistema (sistemska zloupotreba).

Kao zloupotreba sistema može se kvalifikovati korišćenje tehnologija na način koji obuhvata: neovlašćen pristup podacima; neovlašćeno korišćenje podataka ili informacija iz informacionih sistema; kršenje privatnosti ličnih podataka; neovlašćeno otkrivanje poverljivih ili osetljivih informacija; neovlašćeni pristup računarskim sistemim trećih strana; prenos neželjenih materijala; imitiranje drugog pojedinca preko mreže pomoću njihovog pristupa; prekomerno preuzimanje, skladištenje, datoteka ili podataka koji nisu direktno povezani sa zadatkom korisnika; Instaliranje neovlašćenog softvera, aplikacije ili dodataka, kao i preuzimanje nedozvoljenih materijala.

Kao sistemska zloupotreba mogu se smatrati operacije kojima se bilo neovlašćeno korumpira ili uništava informacioni sistem ili podaci tj. informacije, uključujući ubacivanjem računarskih virusa ili zlonamernog softvera kako bi se korumpirala računarska ili mrežna oprema, softver ili podaci, ili obezbedio neovlašćeni pristup korisničkom imenu, lozinkama ili identifikacionim detaljima.

Analizu opsega zloupotreba informacionih tehnologija u informacionom prostoru teško je posmatrati kao neutralnu pojavu. U tom smislu ukazuje primer kanadskog premijera, inače poznatog kao jednog od najzastupljenijih emitera poruka na Twitter-u i Instagram-u, koji je uprkos svojoj dominantnoj poziciji u informativnom prostoru Kanade javno zapretio direktorki Facebook-a u toj državi da će se suočiti sa „strožijom“ regulativom ukoliko ne reši objavljivanje statusa koje on smatra „lažnim“ (Boutilier, 2018). Istraživanja mogućih zloupotreba na koje ovaj primer ukazuje, do sada su obično potcenjivala nivo saradnje nacionalnih

sistema bezbednosti i tehnoloških monopolista u kreiranju javnog mnjenja. Ovakvo stajalište bi trebalo uvažavati, bez obzira na problm dokazivosti. Alford i Seker su, zahvaljujući dokumenatima dobijenim na osnovu Zakona o slobodi informisanja, uspeli da dokažu da je, na primer, američki sistem nacionalne bezbednosti, pre svih Centralna obaveštajna agencija (CIA) i generalštab (Pentagon) radio na više od osam stotina filmova holivudske produkcije i preko hiljadu televizijskih emisija (Alford; Secker, 2017). Ove snage su iz političkih razloga menjale scenarije, da se određene priče potisnu ili ubace u javni narativ. Kada pisac ili producent zatraže pristup imovini državnih agencija, moraju da podnesu scenario radi provere. Sekretarijat odbrane ima oficira za vezu za film i TV. Da bi se ostvarila saradnja, proizvođači moraju da potpišu sporazum o pomoći u produkciji, koji ih vezuje za odobrenu verziju scenarija. CIA nema formalni postupak provere scenarija, ali ima oficira za vezu za zabavu, koji je uspevao da se ubaci u rane faze pisanja nekih scenarija. Iako se, strogo posmatrano, ne radi o cenzuri, činjenica je da se koristi uticaj i netransparentan pritisak na narative i simboliku koji se emituju širom sveta (za Srbiju, ova knjiga je značajna jer ozbiljno preispituju uvrežene narative o Balkanu devedesetih). Kako se radi o državi koja otvoreno koristi svoju moć u inostranstvu, netransparentno oblikovanje popularne kulture za promovisanje načina razmišljanja trebalo bi posmatrati i sa aspekta hegemonije.

ZAKLJUČNA RAZMATRANJA

Veštačka inteligencija omogućava da stvarnost bude ono što algoritam predviđa. Stoga, monopol nad algoritmima nužno dovodi do mogućnosti nametanja odluka i, posledično, ograničava humanost. Kako je pokazano, Google, Facebook i Youtube već sad algoritamski ograničavaju dostupnu istinu, što predstavlja pravni problem, jer primenjuju subjektivne kriterijume i postupke u javnom prostoru.

Informisanje u praksi postaje zasnovano na aspektu programiranja i oblikovanja svesti umesto na činjenicama i događajima. Ako takvo informisanje postane prepušteno automatizmu i algoritmima, čitav sistem informisanja postaće u funkciji onih koji kontrolišu korporacije koje kontrolišu platforme. Opštije posmatrano, čini se da postoji potreba uspostavljanja ravnoteže između antropocentričnog i tehnokratskog.

Tehnološke kompanije, po prirodi svog proizvoda, zavise od državnih sistema. U simbiozi administracija i tehnoloških monopolista razvija se direktna poluga nad distribucijom vesti u kiber prostoru. Tehnološke kompanije, pravno-logički posmatrano, ne mogu imati takvu moć. Naime, nije moguće preneti ovlašćenja kojima bi se pravo na informisanje ograničavalo voljom privatnih kompanija, kao ni država, u toj oblasti.

Navedeni primeri, pak, pokazuju da su decenije strateških integracija dovele do vertikalne tehnološke integracije, koja okupira informacioni prostor na mreži. Ukidanjem u tom prostoru, individua je onemogućena da postoji u kiber prostoru, odnosno postaje „nelice“, a ako je to zbog stavova, onda su i stavovi objekat cenzure. Mogućnost privatne ucene u tom prostoru svodi se na reketiranje (naplata zaštite od sopstvenog maltretiranja). Prihvatanje ove prakse bi podrazumevalo da privatni proizvođači struje mogu da ne isporuče struju korisnicima čiji im se šporeti ne sviđaju, ili vlasnici zemlje preko koje protiče potok da ograde tok jer im se ne sviđa bilje koje se gaji vlasnik susednog zemljišta.

Analizirane mogućnosti zloupotrebe informacionih tehnologija u kiber informacionom prostoru ukazuju da savremeno doba nameće potrebu da svi profesionalni akteri u tom prostoru imaju niz sposobnosti u funkciji efikasnosti zaštite objektivnog informisanja javnosti. Prema tipu izazova sa kojim se suočava, ove sposobnosti se mogu podeliti u tri kategorije: profesionalne, upravljanja informacijama i društvene. Izuzev profesionalne, druga dva tipa sposobnosti obuhvataju i one koji se bave nadzorom i kontrolom sistema informisanja, koji je preduslov funkcionalne demokratije.

U uslovima višeslojnih izvora i izloženosti obilju i brzini dostupnih podataka i informacija naglašena je potreba da profesionalci u informativnom sektoru znaju kako istraživati (uključujući i nekonvencionalnim metodima), kako dolaziti do podataka i informacija i odabrati one relevantne za analizu, proveravati njihov kvalitet i koristiti odgovarajuće analitičke metode, kako bi se obezbedio uvid i predviđanje i formirali zaključci i sinteza. Sposobnost da se odgovori na ključne probleme obezbeđivanja uvida javnosti u odluke i

događaje je osnovni uslov suočavanja sa izazovima delatnosti. Ova sposobnost iziskuje niz veština, u koje spadaju kritičko, logično i analitičko razmišljanje, veština posmatranja, tačnost, svest za detalje, racionalnost i intelektualna radoznalost.

U uslovima rastućeg značaja višestrukih izvora informacija na mreži, važno je razumeti širi kontekst ključnih pitanja, imati odgovarajuće sagovornika i demonstrirati znanje. U okruženju brzine inputa informacija, delotvornost izvštavanja postaje zavisna od upravljanja izveštajima, projektima, procesima, vremenom i opterećenjem. Sposobnost upravljanja procesom prikupljanja informacija zahteva više veština: rad na strukturiran način, izbor ciljeva i racionalno angažovanje, otpornost na simboličku komunikaciju, odgovornost, praktičnost i posvećenost. Uz to je, čini se, neophodno imati razvijen vrednosni sistem i apstraktno mišljenje.

U uslovima intenzivne međupovezanosti na mreži, preduslov delotvornosti postaje i saradnja sa okruženjem. Uloga profesionalaca u informacionom prostoru postaje i da prevazilazi posledice obilja činjenica i mišljenja. Komuniciranje zahteva niz veština u odnosu sa ljudima: kako se stvaraju, održavaju i razvijaju relevantni odnosi i veze, kako se stiče poverenje drugih učesnika, uključujući korisnika (neprofesionalnih izvora), a posebno kako da se spoznaju i razumeju interesi u pozadini.

CITIRANA DELA

Alford, M.; Secker, T. (2017). National Security Cinema: The Shocking New Evidence of Government Control in Hollywood. CreateSpace Independent Publishing Platform.

Ali, S.S., Associated Press (2017). Accounts in France Ahead of Presidential Election. NBC News, April 15.2017. Preuzeto Jul 31, 2018 sa. https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766/

Boisot, M. H. (1995). Information Space: A Framework for Learning in Organizations, Institutions and Culture. Routledge, London.

Boutilier, A. (2018). Trudeau to Facebook: Fix your fake news problem or face stricter regulations. The Star, Feb. 8, 2018. Preuzeto Jul 31, 2018 sa: https://www.thestar.com/news/canada/2018/02/08/trudeau-to-facebook-fix-your-fake-news-problem-or-else.html

Chalmers, M. (2003). Informatics, Archtecture and Language. Höök, U: K., Benyon D., Munro A. J. (eds.), Social Navigation of Information Space. London: Springer Verlag, pp. 315-343.

Đurđević, D., Stevanović, M. (2017). Internet as a Method od Trolling Offensive Intelligence Operations in Cyberspace. *NBP Journal of Criminalistics and Law, 22*(2), 13-32.

Karatas, M., Zihni T. M. (2010). Sustainable Economic Development and the Influence of Information Technologies: Dynamics of Knowledge Society Transformation. IGI Global, Hershey/New York.

Miltiadis, L., Novo-Corti, I. (2012). Trends and Effects of Technology Advancement in the Knowledge Society. Information Science Reference, Hershey.

MIT Artificial Intelligence Laboratory (1998). The JAIR Information Space. Preuzeto Jul 31, 2018 sa: http://www.ai.mit.edu/projects/infoarch/jair/jair-help.html.

Newby G. (2001). Cognitive Space and Information Space. *Journal of the American Society for Information Science and Technology, 52*(12), 1026-1048.

Reddick, C. (2012). Public Administration and Information Technology". Jones & Bartlett Learning, Burlington/Ontario/London.

Stevanović, M., Đurđević, D. (2015). The Capacity of Perception: The Need for an Educational System in Support of the National Security. In: Grozdanić R., Jovančević, D. (eds.), Creative Education for Employment Growth: Proceedings Fourth International Conference „Employment, Education and Entrepreneurship“, 14-16 October 2015, Belgrade. Belgrade: Faculty of Business Economics and Entrepreneurship/ Chicago: Bar Code Graphics, 47-56.

Stevanović, M., Đurđević, D. (2018). The Challenges of Shaping Narratives in Cyberspace for National Security. Proceedings of the 10th Scientific Conference "Freedom and security in real and syber space", Belgrade, 08.06.2018.

Datum prve prijave: 15.08.2018.
Datum prijema korigovanog članka: 22.03.2019.
Datum prihvatanja članka: 27.03.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Stevanović, M. D., & Đurđević, D. Ž. (2019, 04 15). Izazov zloupotrebe informacionih tehnologija za javno informisanje. (Z. Čekerevac, Ur.) *FBIM Transactions, 7*(1), 159-169. doi:10.12709/fbim.07.07.01.18

*Style – **Chicago** Sixteenth Edition:*

Stevanović, Miroslav D, i Dragan Ž Đurđević. 2019. „Izazov zloupotrebe informacionih tehnologija za javno informisanje.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 159-169. doi:10.12709/fbim.07.07.01.18.

*Style – **GOST** Name Sort:*

Stevanović Miroslav D i Đurđević Dragan Ž Izazov zloupotrebe informacionih tehnologija za javno informisanje [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 159-169.

*Style – **Harvard** Anglia:*

Stevanović, M. D. & Đurđević, D. Ž., 2019. Izazov zloupotrebe informacionih tehnologija za javno informisanje. *FBIM Transactions,* 15 04, 7(1), pp. 159-169.

Style – **ISO 690** Numerical Reference:

Izazov zloupotrebe informacionih tehnologija za javno informisanje. **Stevanović, Miroslav D i Đurđević, Dragan Ž.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 159-169.