

*Msr Luka Petrović, asistent
Pravnog fakulteta Univerziteta u Kragujevcu
ORCID: 0000-0003-1045-9555*

*Izvorni naučni rad
UDK: 342.34:004.8*

DOI: <https://doi.org/10.46793/XXIIMajsko.167P>

DEMOKRATIJA U ALGORITMU: POLITIČKA KOMUNIKACIJA I PODACI O LIČNOSTI*

Rezime

Još od pojave prvih političkih partija sredinom XX veka, bilo je jasno da će politička konkurentnost kolektivnih subjekata zavisiti od njihove sposobnosti da identifikuju valjane kanale komunikacije za plasiranje poruka biračima. Pojava interneta, savremenih digitalnih tehnologija, društvenih mreža, ali i alata veštačke inteligencije (VI) označila je tehnološku revoluciju u domenu političke komunikacije. U tom kontekstu se opravdano postavlja i pitanje: da li su danas digitalne platforme i alati VI samo kanali komunikacije ili se politička moć neprimetno izmešta iz institucija u algoritme?

Autor u radu analizira modalitete na koje se podaci o ličnosti koriste u političkoj komunikaciji i ispituje zloupotrebe i negativne društvene pojave koje u tom procesu mogu nastati. Savremeni oblici političkog oglašavanja praćeni su hiperpersonalizacijom koja, na prvi pogled, nije sporna jer korisniku nudi sadržaj u skladu sa njegovim interesovanjima. Ipak, personalizacija političke poruke u praksi podriva njenu univerzalnost, što može dovesti u pitanje koherentnost i jedinstvo političkog programa. Koristeći prednosti digitalnih tehnologija, politički akteri tradicionalno informisanje zamenjuju mikrotargetiranjem, čime se biračko telo prestaje tretirati kao subjekat, već kao objekat eksploatacije, koji se ne informiše, već se njime manipuliše.

Glavni oslonac za uspešno mikrotargetiranje predstavljaju lični podaci koje građani, svesno ili nesvesno, ostavljaju u digitalnom prostoru. Ovi podaci omogućavaju psihografsko profilisanje i segmentaciju biračkog tela, radi njihove mobilizacije. Autor zato polazi od istraživačkog pitanja: mogu li savremene tehnologije učiniti demokratiju efikasnijom ili prete da je zarobe u algoritmu?

Ključne reči: demokratija, politički procesi, podaci o ličnosti, politička komunikacija, veštačka inteligencija.

* Rad je rezultat naučnoistraživačkog rada autora u okviru Programa istraživanja Pravnog fakulteta Univerziteta u Kragujevcu za 2026. godinu, koji se finansira iz sredstava Ministarstva nauke, tehnološkog razvoja i inovacija Republike Srbije.

1. Uvodna razmatranja

Analizirajući istoriju razvoja koncepta ljudskih prava možemo zaključiti da pomenutoj genezi teorijski korespondira ideja o tri tipa građanstva koju iznosi T. H. Maršal. Posmatrajući proces evolucije slobode i prava, Maršal zaključuje da se u tom procesu postepeno pojavljuju tri tipa građanstva, i to: civilno, političko i socijalno građanstvo.¹ Ipak, kao svedoci savremenog, ali još uvek nezaokruženog procesa tehnološkog i digitalnog razvoja, nužno je postaviti i pitanje: da li će sledeća faza u razvoju pojma građanstva iznedriti tip „digitalnog građanstva“?

Ekspanzivni razvoj i opšta prisutnost savremenih digitalnih tehnologija, alata veštačke inteligencije i pametnih uređaja, fundamentalno su redefinisali topografiju ljudskog delovanja, izmeštajući težište društvenih aktivnosti iz fizičke u digitalnu sferu. Savremeni tokovi trgovine, finansijskog poslovanja, edukacije, administracije, socijalne i političke komunikacije, danas se primarno realizuju posredstvom raznih platformi i digitalnih alata. Egzistirajući unutar svojevrsne „tehnološke mikrokapsule“, pojedinac kontinuirano generiše digitalni otisak, plaćajući svakodnevne digitalne aktivnosti podacima o ličnosti. U tom kontekstu, korišćenje društvenih platformi i digitalnih alata nema karakter besplatnosti, jer primarno sredstvo namirenja kompleksnijih interesa kreatora platformi postaju podaci o ličnosti, koji figuriraju kao vrsta nemonetarnog dobra.

Digitalni habitat pokazao se naročito podsticajnim za političke subjekte, koji svoje aktivnosti političke komunikacije sve više usmeravaju posredstvom kanala digitalne komunikacije, budući da im oni omogućavaju da personalizovane političke poruke upute samo precizno određenim kategorijama birača. Istaknuta prednost digitalnih platformi počiva na mogućnosti psihografskog profilisanja korisnika brojnih društvenih mreža, koji svojim aktivnostima u onlajn prostoru svakodnevno, direktno ili indirektno, otkrivaju podatke značajne za profilisanje, a samim tim i za personalizovanje sadržaja koji će im biti plasiran.

Zbog toga je nužno posvetiti posebnu pažnju analizi normativne uređenosti pitanja prikupljanja i obrade podataka o ličnosti, profilisanja i personalizovanog političkog oglašavanja, kao i sagledavanju uticaja ovih pojava na izborne procese i demokratiju uopšte.

2. Algoritamska demokratija ili oružje za mikrotargetiranje

Savremeni život pojedinaca u XXI veku uslovljen je dostignućima moderne tehnologije oličene u veštačkoj inteligenciji. Savremeni čovek sve više postaje zavisnik, jer ne može i ne ume da funkcioniše bez upotrebe sredstava, koja mu život naizgled čine lakšim i jednostavnijim.² Tehnološka dostignuća redefinisala su život

¹ Videti više: Komšić, J., *Teorije o političkim sistemima*, Beograd, 2000. str. 228; prema: T. H. Maršal.

² Đorđević, S., Matić, D., *Pravo u mreži veštačke inteligencije*, Kragujevac, 2025, str. 14.

savremenog čoveka do te mere da su brojne svakodnevne aktivnosti postale maltene nezamislive bez njihove upotrebe. U tzv. digitalnom okruženju, pojedinci svakodnevno kupuju i prodaju proizvode i usluge, obavljaju finansijske transakcije, informišu se, komuniciraju i vrše različite oblike društvene i profesionalne interakcije. Terminima "e-" i „online“ označava se svaka vrsta aktivnosti koja se, zahvaljujući tehnološkom napretku, može realizovati mnogo brže i efikasnije u digitalnoj formi. U tom smislu, sve su zastupljeniji pojmovi kao što su: onlajn bankarstvo, onlajn nastava, onlajn trgovina, e-uprava, e-poslovanje, pa čak i onlajn, odnosno e-glasanje.

Oblici građanske participacije prilagođeni digitalnom okruženju uticali su na ustanovljenje termina digitalna demokratija. Osnivač *E-Democracy* platforme, autor Stiven Klift, definiše digitalnu demokratiju kao upotrebu informaciono-komunikacionih tehnologija i strategija od strane demokratskih aktera društva u političkim i upravljačkim procesima u lokalnim zajednicama, zatim državi i na međunarodnoj sceni. Pod demokratskim akterima društva podrazumevaju se dakle vlade, izabrani zvaničnici, mediji, političke organizacije kao i građani (birači). Takođe, elektronska demokratija podrazumeva znatno veće i aktivnije učešće građana koje omogućavaju internet, mobilne komunikacije i druge tehnologije u današnjoj predstavničkoj demokratiji.³

Elektronska varijanta demokratije uslovlila je uspostavljanje novih kanala komunikacije između političkih subjekata i biračkog tela. Tradicionalni mediji, poput televizije, radija i štampanih novinskih publikacija, više ne predstavljaju dominantne posrednike u prenosu informacija ka građanima, već tu ulogu postepeno preuzimaju društvene mreže. Novinske članke tako zamenjuju kratke forme poput „*twitova*“, informativne emisije ustupaju prostor „podkastima“, dok televizijske reklame bivaju potisnute kratkim video sadržajima na društvenim mrežama kao što je mreža TikTok. Svesni da gube primat u medijskom prostoru, tradicionalni mediji zato pristupaju sopstvenoj digitalnoj transformaciji, te televizija, radio i štampa razvijaju svoja elektronska izdanja i prilagođavaju se zahtevima savremenog digitalnog okruženja.

Ipak, jedna suštinska razlika između tradicionalnih medija i društvenih mreža kao savremenih modela informisanja predstavlja tzv. uređivačko pitanje. Dok je sadržaj tradicionalnih medija uređivački podređen ljudskom faktoru, čime se garantuje prenos informacija na jedinstven i depersonalizovan način, kao urednik sadržaja koji će svakome biti plasiran na mrežama pojavljuje se algoritam VI. Obradujući ogromne količine podataka kao što su: interesovanja, ponašanja, lokacije i navike korisnika mreže, algoritmi zasnovani na veštačkoj inteligenciji u stanju su da personalizuju sadržaj shodno uočenim afinitetima korisnika. Dakle, društvene mreže kao što su: *Facebook*, *Instagram*, *TikTok*, *X*, *Reddit* i *YouTube*, koriste veštačku inteligenciju kao generator koji je u stanju da oblikuje sve što korisnici ovih platformi vide.

Personalizacija sadržaja sama po sebi nije sporna, budući da omogućava korisnicima da pristupaju informacijama u skladu sa sopstvenim interesovanjima i

³ Clift's, S., *Brief E-Democracy Definition*, Publicus.net: <https://www.publicus.net/articles/edemresources.html> 01.04.2024.

preferencijama. Tako će pojedinci čiji je predmet interesovanja sport prevashodno pratiti sportske sadržaje, dok će oni zainteresovani za politička pitanja biti izloženi informacijama koje se odnose na aktuelna politička zbivanja. Ipak, unutar ovog naizgled meritokratskog i efikasnog modela kriju se određeni rizici koji ne smeju ostati zanemareni. Personalizacija sadržaja može dovesti i do stvaranja informacionih mehurova (*filter bubbles*)⁴, u okviru kojih korisnici bivaju izloženi isključivo sadržajima koji potvrđuju njihova već postojeća uverenja. Na taj način se ograničava pristup različitim stanovištima i sužava prostor za valjano kritičko preispitivanje. U kontekstu političke komunikacije, navedena pojava dobija posebnu težinu, jer omogućava mikrotargetiranje biračkog tela i manipulaciju građanima u cilju usmeravanja njihovih političkih i izbornih odluka.

Ne treba gubiti iz vida ni da su kreatori i vlasnici digitalnih platformi privatne kompanije, čiji upravljački subjekti mogu imati i sopstvene političke stavove, pa se stoga moramo zapitati: šta bi se desilo kada bi kreatori društvenih mreža iste stavili u službu političke propagande određenog političkog subjekta. Ova činjenica dobija poseban značaj budući da danas društvene mreže imaju ključnu ulogu u distribuciji informacija i oblikovanju stavova javnog mnjenja. Prisetimo se, primera radi, angažmana Ilona Maska, vlasnika platforme X, koji je u javnosti često izražavao podršku određenim političkim opcijama, uključujući i kandidata Donalda Trampa, tokom predsedničke kampanje u Sjedinjenim Američkim Državama.

Uzimajući u obzir navedene okolnosti, nije teško zamisliti hipotetičku situaciju u kojoj algoritam određene društvene mreže uređuje sadržaj na način koji omogućava mikrotargetiranje korisnika sa ciljem da oblikuje njihove političke stavove. Primera radi, u državi X održavaju se parlamentarni izbori na kojima se kao favoriti izdvajaju dva politička subjekta. U uslovima izražene migrantske krize, značajan deo građana, vođen osećajem straha ili nesigurnosti, na društvenim mrežama prati, pretražuje i komentariše upravo sadržaje koji se odnose na ovu problematiku. Na osnovu ovih digitalnih tragova, algoritam vrši profilisanje korisnika kod kojih pitanje migracija izaziva snažne emocionalne reakcije, nakon čega im se namenski plasiraju sadržaji čiji je cilj da dodatno pojačaju osećaj straha i nesigurnosti. Na opisan način, korisnici se suptilno usmeravaju ka političkoj opciji koja zastupa restriktivnu, odnosno antimigracionu politiku.

Kada se u obzir uzmu i mogućnosti plasiranja neistinitog sadržaja, širenja lažnih informacija posredstvom *bot* naloga, kao i upotreba *deepfake* tehnologije, postaje jasno da društvene mreže mogu predstavljati izuzetno moćno i potencijalno opasno sredstvo političkog uticaja. U kombinaciji sa tehnikama mikrotargetiranja, ovi mehanizmi omogućavaju efikasnu manipulaciju biračkim telom, čime se može dovesti u pitanje autentičnost (sloboda) izborne volje građana, pa čak i suštinski obesmisлити demokratski proces.

⁴ Videti više: Pariser, E., *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press, 2011. https://hci.stanford.edu/courses/cs047n/readings/The_Filter_Bubble.pdf

3. Analiza slučaja zloupotrebe podataka - "Cambridge Analytica"

Slučaj "Cambridge Analytica" predstavlja jedan od najupečatljivijih primera političke zloupotrebe podataka o ličnosti korisnika društvenih mreža sproveden radi kreiranja i plasiranja ciljane političke propagande. Pojedini izvori navode da je kompanija za političko konsultovanje uspjela da prikupi podatke više od 50 miliona korisnika društvene mreže Fejsbuk, te da su svi prikupljeni podaci korišćeni kako bi se izgradio efikasan sistem koji može da profiliše glasače i usmeri im personalizovane političke poruke.⁵ Afera poprima globalni karakter dovođenjem u vezu kompanije sa kampanjama za predsedničke izbore u SAD i Bregzit 2016. godine.

Razvoj sistema analize podataka počinje 2013. godine kada Aleksandar Kogan, naučnik na Univerzitetu u Kembridžu, razvija aplikaciju pod nazivom "This Is Your Digital Life" (Ovo je vaš digitalni život). Kao finansijer razvoja aplikacije pojavljuje se firma za političko konsultovanje pod nazivom "Cambridge Analytica". Ona potom organizuje istraživanje u kojem bi nekoliko stotina hiljada korisnika Fejsbuka pristalo na anketiranje čiji bi rezultati bili korišćeni isključivo u istraživačke svrhe. Međutim, propustom Fejsbuka, aplikacija ne samo da prikuplja lične podatke od ispitanika, već i od prijatelja ispitanika na društvenoj mreži. Na ovaj način prikupljeni su podaci o 50 miliona korisnika mreže.⁶

U periodu od 2015. do 2017. godine listovi Gardijan i Obzerver objavljuju niz tekstova o zloupotrebi podataka korisnika, iznoseći sumnje da su zloupotrebljeni podaci korišćeni radi političkog uticaja na birače u kampanji povodom istupanja Velike Britanije iz članstva u Evropskoj uniji.⁷ 2018. godine, isti listovi prenose i svedočenje uzbunjivača, Kristofera Vajlija, koji iznosi dokaze o prikupljanju i zloupotrebi podataka korisnika Fejsbuka.

Kompanija Facebook Inc. ubrzo se našla pod lupom zbog zloupotrebe podataka. Usred skandala sa analitikom, izvršni direktor Mark Zakerberg 2018. se izvinio u ime Fejsbuka i potvrdio da će se kompanija posvetiti rešavanju problema u vezi sa politikom privatnosti mreže. Posebno je naglašeno da će Fejsbuk dobrovoljno implementirati Opštu uredbu o zaštiti podataka (GDPR) u svim oblastima u kojima Fejsbuk posluje.⁸ U julu 2019. godine kompanija Facebook Inc. je kažnjena od strane Federalne trgovinske komisije SAD, a nakon toga pristaje da plati i 100 miliona

⁵ The Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

⁶ Isto.

⁷ The Guardian, The great British Brexit robbery: how our democracy was hijacked: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexite-robbery-hijacked-democracy>

⁸ XDA, Amidst data scandal, Facebook will voluntarily enforce EU's new privacy rules "everywhere" vacy rules "everywhere": <https://www.xda-developers.com/facebook-voluntarily-enforce-eu-privacy-law/>

dolara kako bi se nagodili sa Komisijom za hartije od vrednosti. *Cambridge Analytica* proglasila je bankrot, ali izvršni direktor kompanije Aleksandar Niks i Aleksandar Kogan kažnjeni su od strane nadležnih tela Velike Britanije i SAD.⁹

Dva ključna sporna pitanja u vezi sa opisanom aferom odnosila su se na obim prikupljenih podataka, kao i na način njihovog daljeg korišćenja. Dok se u pogledu obima prikupljenih podataka u literaturi i javnosti mogu pronaći različiti i često kontradiktorni podaci, pitanje načina njihove upotrebe ostaje i danas predmet stručnih rasprava. Kompanija *Cambridge Analytica* i dalje se u javnosti dovodi u vezu sa izbornim kampanjama Teda Kruza i Donalda Trampa 2016. godine i sa kampanjom za izlazak Ujedinjenog Kraljevstva iz Evropske unije (*Brexit*).

List Gardijan 2018. godine dolazi u posed interne dokumentacije kompanije *Cambridge Analytica*, zasnovane na prezentaciji od oko 27 strana, a koju su izradili stručnjaci kompanije angažovani u kampanji Donalda Trampa 2016. godine. Njome se potvrđuje angažovanost kompanije tokom predsedničkih izbora u SAD-u 2016. godine i detaljno opisuje strategija političkog oglašavanja na osnovu podataka korisnika društvenih mreža.¹⁰

Prikupljeni podaci korisnika društvenih mreža korišćeni su dakle za psihografsko profilisanje i identifikaciju birača, koji su potom svrstavani u određene kategorije. U tom smislu, na osnovu digitalnih tragova koje su korisnici ostavljali prilikom korišćenja društvenih mreža, mogli su se utvrditi njihovi politički stavovi, nakon čega su birači klasifikovani kao pristalice, protivnici ili neopredeljeni birači. Usledila je primena raznih tehnika mikrotargetiranja, posredstvom kojih su neodlučnim biračima plasirani sadržaji usmereni na njihovo ohrabrivanje da podrže određenog kandidata, ali i na obeshrabrivanje da glasaju za protivkandidata. Istovremeno, pristalicama su upućivane one poruke u kojima se jedan od kandidata predstavlja u pozitivnom, često trijumfalnom kontekstu, dok su protivnicima plasirani sadržaji usmereni ka diskreditaciji protivkandidata.

Činjenica je da je tokom predsedničke kampanje, na gotovo svim društvenim mrežama, delovao ogroman broj lažnih (bot) naloga, kao i lažnih stranica koje su svakodnevno širile niz dezinformacija i lažnih vesti. Ove vesti uglavnom su bile usmerene na diskreditaciju kandidatkinje Hilari Klinton, pa je tako američka javnost imala prilike da čuje da je Klintonova umešana u pedofilsku mrežu čije je sedište u podrumu picerije u Vašingtonu (tzv. afera „*Pizzagate*“),.... kao i da je izjavila da će ukinuti Drugi amandman na Ustav SAD-a, koji obezbeđuje pravo na nošenje oružja. Sa druge strane, kandidat Republikanaca, prema tvrdnjama korisnika društvenih mreža, uživao je čak zvaničnu podršku poglavara Rimokatoličke crkve, Pape Franje.

⁹ Videti: <https://www.sec.gov/newsroom/press-releases/2019-140>

¹⁰ The Guardian, Leaked: Cambridge Analytica's blueprint for Trump victory: <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>

Sve ove vesti kasnije su se ispostavile kao lažne, ali se procenjuje da su iste imale uticaja na stavove birača tokom predsedničke kampanje.¹¹

Istrage zloupotrebe podataka vođene su u Velikoj Britaniji, SAD-u, ali i drugim državama. Izveštaj Komiteta za digitalizaciju, kulturu, medije i sport Donjeg doma Britanskog parlamenta (*Collins Report*), okarakterisaće napore brojnih jurisdikcija kao pravnu borbu da se održe fundamentalni demokratski principi.

Komitet u izveštaju zauzima stav o odgovornosti Fejsbuka koja se zasniva na nedovoljnoj proaktivnoj zaštiti podataka o ličnosti korisnika, gde posebno treba imati u vidu dozvolu aplikacijama i programerima aplikacija da prikupljaju lične podatke onih korisnika koji nisu dali svoj informisani pristanak.¹²¹³ U odgovoru britanske Vlade na Izveštaj Komiteta, Vlada je priznala potencijalnu pretnju demokratiji koju predstavljaju dezinformacije. Lični podaci i strukture onlajn oglašavanja mogu se dakle zloupotrebiti za namerno ciljanje ljudi lažnim ili obmanjujućim informacijama. Vlada se složila da je tzv. digitalno doba podstaklo promene u tehnikama vođenja kampanje i da bi veća transparentnost bila korisna, stoga se odgovornost može usmeriti i prema kompanijama u svrhu sprovođenja mera za povećanje transparentnosti političkog oglašavanja na društvenim mrežama.¹⁴

Izveštaj Komiteta za digitalizaciju, kulturu, medije i sport predstavlja afirmaciju potrebe za konstituisanje pravne odgovornosti subjekata koji upravljaju digitalnim platformama. Treba se dakle napustiti stav o društvenim mrežama kao „pasivnim prenosiocima poruka” i utvrditi njihova odgovornost za sadržaj koji distribuiraju. Uvođenjem standarda kontrole i proaktivne zaštite korisnika, zaštita podataka i kontrola manipulativnog sadržaja prestaju biti samo tehnička pitanja i postaju važni instrumenti za očuvanje prava na objektivno informisanje, integritet izbornog procesa i samog demokratskog poretka.

4. Zloupotreba podataka i odgovornost digitalnih giganata

Opšta uredba Evropske unije o zaštiti podataka o ličnosti – GDPR – doneta je 27. aprila 2016. godine, a njena primena otpočela je 25. maja 2018. godine. Iako ovaj propis ne predstavlja neposredan pravni odgovor na probleme zaštite podataka koji su

¹¹ Petrović, L., *Izborni procesi u digitalnom dobu*, Zbornik radova: Savremeno pravo u eri digitalizacije i održivog razvoja, Kragujevac 2025, str. 210.

¹² U slučaju Kembridž analitike misli se na fejsbuk prijatelje, lica koja su učestvovala u anketiranju.

¹³ UK Parliament, Digital, Culture, Media and Sport Committee, „Disinformation and ‘fake news’: Final Report“, London, 2019, pp. 17-23. dostupno na: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>, datum pristupa: 14.04.2026.

¹⁴ House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and ‘fake news’: Final Report: Government Response to the Committee’s Eighth Report of Session 2017–19*, Seventh Special Report of Session 2017–19, HC 2184, 2019, pp. 9-10. dostupno na: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcwmds/2184/2184.pdf> (pristupljeno: 14. aprila 2026).

eskalirali u okviru afere “*Cambridge Analytica scandal*”, zanimljivo je uočiti vremensku koincidenciju početka njene primene sa periodom u kome su brojne države nastojale da formulišu adekvatne normativne ali i institucionalne odgovore na izazove masovnog kršenja privatnosti i zloupotrebe ličnih podataka u digitalnom okruženju. Uredba posebno postaje značajna nakon odluke Mark Zakerberga da Fejsbuk dobrovoljno implementira (GDPR) u svim oblastima u kojima posluje.

Uredba (EU) 2016/679 zabranjuje obradu podataka o ličnosti kojom se otkrivaju rasno ili etničko poreklo, političko opredeljenje, verska ili filozofska ubeđenja ili pripadnost sindikatu, kao i obradu genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije fizičkog lica, podataka o zdravstvenom stanju ili podataka o seksualnom životu, odnosno seksualnoj orijentaciji fizičkog lica. Odstupanje od pravila dozvoljeno je u sledećim slučajevima: a) ako je lice na koje se podaci odnose dalo izričit pristanak za obradu tih podataka za jednu ili više konkretnih svrha, izuzev kada pravo Unije ili pravo države članice propisuje da lice na koje se podaci odnose ne može odstupati od zabrane; b) ako obradu u okviru svojih legitimnih aktivnosti, uz odgovarajuće garancije, vrši fondacija, udruženje ili bilo koje drugo neprofitno telo s političkim, filozofskim, verskim ili sindikalnim ciljem, i to pod uslovom da se obrada odnosi isključivo na članove tog tela ili na lica koja imaju redovne kontakte s njim u vezi s njegovom svrhom, i da se podaci o ličnosti ne otkrivaju izvan tog tela bez pristanka lica na koja se podaci odnose; v) ako se obrada odnosi na podatke o ličnosti za koje je očigledno da ih je objavilo lice na koje se podaci odnose; g) ako je obrada neophodna za potrebe značajnog javnog interesa, na osnovu prava Unije, ili prava države članice, a koje je srazmerno željenom cilju i kojim se poštuje suština prava na zaštitu podataka i obezbeđuju primerene i posebne mere za zaštitu osnovnih prava lica na koje se podaci odnose;¹⁵¹⁶

Posebna pažnja posvećena je pitanju odgovornosti rukovoca, u kom smislu se može razmatrati i odgovornost društvenih mreža kao digitalnih giganta. Uredba utvrđuje načela zaštite ličnih podataka (zakonitost, pravičnost, transparentnost, ograničenje svrhe, tačnost, kao i integritet i poverljivost), pri čemu je rukovalac odgovoran za usklađenost obrade sa navedenim načelima i dužan je da usklađenost i dokaže. Jasno je da se Uredbom uspostavlja pravilo prema kome je teret dokazivanja usklađenosti sa načelima obrade na strani rukovoca.

Članovima 25. i 35. utvrđuju se obaveze rukovalaca pri određivanju sredstava obrade, kao i tokom same obrade. Rukovalac je dužan da primenjuje odgovarajuće tehničke i organizacione mere koje su osmišljene radi delotvornog sprovođenja načela zaštite podataka o ličnosti, uključujući i načelo minimizacije podataka, te da u obradu integriše zaštitne mehanizme u cilju ispunjenja zahteva iz Uredbe (EU) 2016/679 i

¹⁵ Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka i o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka)

¹⁶ Uredba predviđa i druga odstupanja od pravila iz čl. 9. st. 1, ali su u tekstu navedena ona odstupanja koja bi mogla biti značajna sa aspekta obrade podataka u političke svrhe.

zaštite prava lica na koja se podaci odnose. Pored toga, rukovalac je obavezan da primenjuje i određene mere kojima se obezbeđuje da se, po podrazumevanim podešavanjima, obrada vrši isključivo nad onim podacima koji su neophodni za konkretnu svrhu. Ova obaveza obuhvata, kako količinu prikupljenih podataka, tako i obim njihove obrade, rok čuvanja i njihovu dostupnost, pri čemu se posebno zahteva da podaci o ličnosti ne budu automatski dostupni neograničenom broju lica bez intervencije rukovaoca.

U onim slučajevima kada je sasvim verovatno da će neka vrsta obrade, posebno primenom novih tehnologija, a uzimajući u obzir prirodu, obim, okolnosti i svrhe obrade, prouzrokovati veliki rizik za prava i slobode fizičkih lica, obaveza rukovaoca je da pre obrade izvrši procenu uticaja predviđenih postupaka obrade na zaštitu podataka o ličnosti. Obaveza procene uticaja na zaštitu podataka posebno se naglašava u slučaju obimnog sistematskog praćenja javno dostupnog prostora.¹⁷ Administrativnim kaznama koje se u određenim slučajevima odgovornosti pravnih lica mogu iznositi i do čak 4% ukupnog godišnjeg prometa u svetu za prethodnu finansijsku godinu, osigurava se da kršenje propisa nikome ne bude „isplativo”.

Pored Uredbe (EU) 2016/679 značajno je spomenuti da je Velika Britanija 2023. godine donela propis o bezbednosti na internetu (*The Online Safety Act- OSA*)¹⁸, čiji je cilj da učini internet prostor bezbednijim mestom. Predviđanjem odgovornosti tehnoloških kompanija za sadržaj koji generišu i plasiraju korisnici osigurava se bezbednost u onlajn prostoru i time sprečavaju potencijalne zloupotrebe podataka korisnika radi političke i druge propagande zasnovane na obmanjujućem sadržaju.

Na severnoameričkom tlu izdvojićemo slučaj Kalifornije. Prema dostupnim podacima, značajan deo neovlašćeno prikupljenih podataka u aferi “*Cambridge Analytica scandal*” odnosi se na korisnike sa tog područja što ukazuje da su građani ove države bili među najviše izloženim korisnicima. Kalifornija 2018. godine zato donosi propis pod nazivom: *California Consumer Privacy Act (CCPA)*.¹⁹ Takođe, ova država donela je i nekoliko propisa kojima se ograničava upotreba *deepfake* sadržaja u toku izbora. Zakonima se obavezuju velike onlajn platforme da uklone ili označe obmanjujuće i digitalno izmenjene sadržaje povezane sa izborima. Postojeći zakon, sve do 1. januara 2027, zabranjuje bilo kom licu da distribuira materijalno obmanjujući audio ili vizuelni materijal kandidata za izbornu funkciju sa namerom da se povredi ugled kandidata ili da se obmane glasač da glasa (za ili protiv) tog kandidata, u roku od 60 dana od izbora. Jedan od zakona je dobio i vrlo simboličan naziv: „*Zakon o odbrani demokratije od dubokih lažnih obmana*”.²⁰²¹

¹⁷ Isto. Videti: čl. 5, čl. 25, čl. 35, čl. 83.

¹⁸ Online Safety Act 2023, 2023 c. 50, UK Public General Acts, 26 October 2023. <https://www.legislation.gov.uk/ukpga/2023/50>

¹⁹ California Consumer Privacy Act (CCPA) <https://oag.ca.gov/privacy/ccpa>

²⁰ Petrović, L., *nav. članak*, str 213.

²¹ AB-2655 Defending Democracy from Deepfake Deception Act of 2024, https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2655

Izrazita normativna aktivnost usmerena prevashodno ka utvrđivanju obaveza i odgovornosti digitalnih giganta (društvenih mreža), ima za cilj uspostavljanje mehanizama za sprečavanje zloupotreba u vidu: protivzakonitog prikupljanja, obrade podataka, profilisanja, mikrotargetiranja i širenja dezinformacija. Kako su sada platforme u obavezi da uspostave transparentnost u pogledu političkog oglašavanja i da kontinuirano prate i kontrolišu sadržaje koje korisnici plasiraju, sprečava se u značajnoj meri širenje i dejstvo zlonamernih, nevidljivih, personalizovanih dezinformacija koje mogu suptilno uticati na izbornu volju, čime se uvažava pravo birača da formiraju mišljenje bez skrivenog „tehnološkog” uticaja. Kao dokaz odgovornijeg pristupa možemo navesti primer iz 2020. godine, kada je Tviter (H) saopštio da je uklonio 8.558 naloga iz Srbije koji su učestvovali u koordinisanom promovisanju jedne političke partije. Nalozi su prema tvrdnjama ove platforme uklonjeni jer su kršili politiku društvene mreže i podrivali javnu raspravu.

5. Zaključak

Svakodnevno funkcionisanje pojedinca, suštinski redefinisano pojavom interneta i alata veštačke inteligencije (VI), pogodovalo je nastanku nove vrste nemonetarnog dobra oličenog u ličnim podacima. U savremenom digitalnom poretku, privatnost kao temeljno ljudsko pravo prestaje da bude isključivo apstraktna vrednost i postaje konkretna „valuta” kojom građani plaćaju pristup blagodatima digitalnog habitata. Ovakva promena paradigme omogućila je velikim tehnološkim korporacijama da ostvare enorman profit, pozicionirajući se i kao dominantni posrednici informacija. Njihova medijska dominacija zasniva se na algoritmima koji korisnicima plasiraju personalizovan digitalni sadržaj, utvrđujući njihova interesovanja na osnovu prethodnih onlajn aktivnosti.

Prednosti tehnološkog doba postale su oslonac i političkih subjekata u izbornom nadmetanju. Premeštanje političke komunikacije iz tradicionalne medijske sfere u komunikacione kanale društvenih mreža omogućilo je efikasnost, ali je istovremeno pokazalo potencijal da ugrozi same temelje demokratskog procesa. Brojni primeri, poput afere *Cambridge Analytica*, nedvosmisleno pokazuju kapacitet algoritama za destruktivno delovanje od širenja dezinformacija do specifičnih tehnika psihografskog profilisanja i mikrotargetiranja. U takvom ambijentu, birač se transformiše iz aktivnog subjekta koji slobodno formira mišljenje u objekat manipulacije, čija se izborna volja pokušava usmeriti i preoblikovati uz pomoć suptilnog digitalnog pritiska.

Ključ za rešavanje ovih izazova pronalazimo u formulisanju odgovornosti tehnoloških giganta. Zanimljivo je da se primena Opšte uredbe Evropske unije o zaštiti podataka o ličnosti poklopila sa eskalacijom ovih problema, ali i da je svojom normativnom sadržinom uspeła da ponudi adekvatan odgovor. Uspostavljanjem preciznih pravila o transparentnosti, zakonitosti obrade i načelima obrade i što je najvažnije, adekvatnim sankcijama, napravljen je značajan pomak ka suzbijanju zloupotreba ličnih podataka u digitalnom okruženju.

Na kraju, treba napomenuti da tehnologija sama po sebi ne mora biti prepreka demokratiji, ali da njena neregulisana primena to svakako može biti. Demokratija i algoritam mogu biti partneri samo ukoliko pravo uspe da osigura da lični podaci građana ne budu sredstvo za njihovo obmanjivanje, već zaštićeno dobro kojim se niko neće nezakonito služiti radi ostvarivanja sopstvenih političkih interesa.

*Luka Petrović, LL.M., Assistant
Faculty of Law, University of Kragujevac*

DEMOCRACY IN THE ALGORITHM: POLITICAL COMMUNICATION AND PERSONAL DATA

Summary

Since the emergence of the first political parties in the mid-20th century, it has been clear that the political competitiveness of collective entities will depend on their ability to identify valid communication channels for placing messages to voters. The emergence of the Internet, modern digital technologies, social networks, but also artificial intelligence (AI) tools has marked a technological revolution in the domain of political communication. In this context, the question is justified: are digital platforms and AI tools today only channels of communication or is political power being imperceptibly shifted from institutions to algorithms?

In this paper, the author analyzes the modalities in which personal data is used in political communication and examines the abuses and negative social phenomena that can arise in this process. Modern forms of political advertising are accompanied by hyper-personalization, which, at first glance, is not controversial because it offers the user content in accordance with his interests. However, the personalization of political messages in practice undermines their universality, which can call into question the coherence and unity of the political program. Taking advantage of digital technologies, political actors replace traditional information with microtargeting, whereby the electorate ceases to be treated as a subject, but as an object of exploitation, which is not informed, but manipulated.

The main support for successful microtargeting is the personal data that citizens, consciously or unconsciously, leave in the digital space. This data enables psychographic profiling and segmentation of the electorate, for the purpose of their mobilization. The author therefore starts from the research question: can modern technologies make democracy more efficient or do they threaten to trap it in an algorithm?

Key words: *democracy, political processes, personal data, political communication, artificial intelligence.*

Literatura

- Dorđević, S., Matić, D., *Pravo u mreži veštačke inteligencije*, Kragujevac, 2025.
- Komšić, J., *Teorije o političkim sistemima*, Beograd, 2000.
- Marshall, T. H., *Citizenship and Social Class*, Cambridge University Press, Cambridge, 1950.
- Pariser, E., *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press, New York, 2011.
- Petrović, L., *Izborni procesi u digitalnom dobu*, Zbornik radova: Savremeno pravo u eri digitalizacije i održivog razvoja, Kragujevac, 2025.
- AB-2655 Defending Democracy from Deepfake Deception Act of 2024.
- California Consumer Privacy Act (CCPA).
- Online Safety Act 2023, 2023 c. 50, UK Public General Acts, 26 October 2023.
- Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka i o stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka).
- Clift, S., *Brief E-Democracy Definition*, Publicus.net, dostupno na: <https://www.publicus.net/articles/edemresources.html>, datum pristupa: 01.04.2024.
- UK Parliament, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report*, London, 2019, dostupno na: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/1791/1791.pdf>, datum pristupa: 14.04.2026.
- House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report: Government Response to the Committee's Eighth Report of Session 2017–19*, HC 2184, 2019, dostupno na: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/2184/2184.pdf>, datum pristupa: 14.04.2026.
- The Guardian, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, dostupno na: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- The Guardian, *The great British Brexit robbery: how our democracy was hijacked*, dostupno na: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>.
- The Guardian, *Leaked: Cambridge Analytica's blueprint for Trump victory*, dostupno na: <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analytica-blueprint-for-trump-victory>.
- U.S. Securities and Exchange Commission (SEC), dostupno na: <https://www.sec.gov/newsroom/press-releases/2019-140>.
- XDA Developers, *Facebook will voluntarily enforce EU's new privacy rules everywhere*, dostupno na: <https://www.xda-developers.com/facebook-voluntarily-enforce-eu-privacy-law/>.