DFC
DIGITALNI FORENZIČKI CENTAR

# BORBA ZA DEMOKRATIJU U ERI DIGITALNOG AUTORITARIZMA


DFC
DIGITALNI FORENZIČKI CENTAR

# Sadržaj

# POJMOVNIK

**A**

**ALGORITMI DRUŠTVENIH MREŽA** - skup računarskih pravila i procesa koji određuju koji se sadržaj prikazuje korisnicima i u kojem redosljedu, na osnovu različitih faktora kao što su ponašanje korisnika, interakcija i lične preferencije. Cilj mu je da pruži najrelevantniji i najprivlačniji sadržaj svakom korisniku, potičući interakciju i vrijeme provedeno na platformi.

**B**

**BOT MREŽE** – uvezana mreža automatizovanih, polu-automatizovanih ili manualno kontrolisanih naloga, koja kroz vremensku i sadržajnu koordinaciju širi određene informacije, narative, dezinformacije i propagandu.

**G**

**GLOBALNO SELO** – termin koji opisuje fenomen sve veće povezanosti čitavog svijeta usljed širenja i napredovanja tehnologije. Termin je, 1962. godine, skovao kanadski teoretičar medija Maršal Makluan.

**D**

**DEZINFORMACIJE** - namjerno i sračunato plasiranje kombinacije istinitog i lažnog sadržaja, s ciljem uticanja na javno mnjenje.

**DIGITALNI AUTORITARIZAM** - upotreba digitalnih informacionih tehnologija radi nadzora, represije i manipulacije domaćeg i stranog stanovništva.

**DIPFEJK (DEEPFAKE)** – tehnologija koja koristi vještačku inteligenciju za stvaranje hiperrealističnih lažnih video, foto i audio materijala. Često se koristi za zamjenu lica jedne osobe sa licem druge osobe, stvarajući uvjerljive lažne scene.

**DOKSING (DOXXING)** - postupak prikupljanja nečijih ličnih podataka i informacija, kao i njihovo javno objavljivanje na internetu bez dozvole, čime se žrtva izlaže neprijatnostima, rizicima, pa i mogućim opasnim situacijama.

**E**

**EHO KOMORA (ECHO CHAMBER)** - okruženje u kojem učesnici susrijeću informacije koje pojačavaju ili potvrđuju njihova prethodna uvjerenja kroz komunikaciju i ponavljanje unutar zatvorenog sistema, izolovanog od osporavanja i suprotnog mišljenja.

**I**

**INFORMACIONE OPERACIJE UTICAJA (IOU)** – namjerno i organizovano nastojanje manipulacije ili uticaja na javno mnjenje, percepcije, vjerovanja ili ponašanja publike. Uključuje strateško i plansko korišćenje različitih komunikacijskih kanala kako bi se oblikovali narativi, širile dezinformacije, podrivali demokratski procesi unutar i van zemlje, promovisali određeni politički, ekonomski i ideološki interesi, odnosno agende i degradirao integritet informacionog prostora.

**K**

**KOODRINISANO NEAUTENTIČNO PONAŠANJE** – aktivnosti i kampanje koje uključuju grupe, naloge i stranice koje koordinisano nastoje da zavaraju ljude o tome ko su i šta rade, oslanjajući se na lažne naloge. Termin koji je Fejsbuk skovao za opisivanje upotrebe više naloga, koji zajedno rade na prikazivanju lažne slike o sebi, vještačkom povećanju popularnosti sadržaja ili se bave ponašanjem koje vodi ka drugim prekršajima standarda zajednice.

**KORISNI IDIOT** - u političkom žargonu se odnosi na osobu koja podržava neku ideju ili širi propagandu, a da toga možda uopšte nije svjesna.

**L**

**LAŽNE VIJESTI** - originalni članak/medijski izvještaj koji sadrži potpuno netačne informacije i sadržaje koji nijesu zasnovani na činjenicama.

**M**

**MIKROCILJANJE (MICROTARGETING)** - oblik onlajn ciljanog oglašavanja koji analizira lične podatke kako bi identifikovao interese specifične publike ili pojedinaca i uticao na njihove akcije. Mikrociljanje se može koristiti da bi se ponudila personalizovana poruka pojedincu ili publici koristeći onlajn servis poput društvenih mreža.

**N**

**NADZORNI KAPITALIZAM** - označava široko prikupljanje i komercijalizaciju ličnih podataka od strane korporacija. Ova pojava se razlikuje od državnog nadzora, iako se mogu međusobno pojačavati. Kompanije ostvaruju profit prikupljajući i analizirajući podatke o potrošačima. Ovi podaci se potom koriste za stvaranje personalizovanih oglasa ili se prodaju drugim kompanijama za istu svrhu. Ovaj ekonomski model je najčešće povezan sa tehnološkim kompanija-

ma, poput Gugla i Fesjbuka. Pitanje nadzornog kapitalizma izazvalo je zabrinutost u vezi sa privatnošću i moći uticaja koju ove kompanije imaju na ponašanje pojedinaca i društva u cjelini.

**NARATIV** – objektiv kroz koji ljudi percipiraju sebe i okruženje, povezujući lično iskustvo sa shvatanjem kako svijet funkcioniše. Što je narativ snažniji to je vjerovatnije da će se zadržati i da će biti zapamćen. Moć narativa zavisi od nekoliko faktora: dosljednost (način na koji se neki događaj logički veže za drugi), jednostavnost (da može odmah da se shvati i proširi), odjek i prilagođavanje.

**S**

**SKLONOST POTVRDI (CONFIRMATION BIAS)** – sklonost ka traženju, interpretiranju, favorizuju i prizivanju informacija koje potvrđuju nečija uvjerenja ili hipoteze. Ljudi iskazuju ovu sklonost kada prikupljaju ili prikazuju informacije na selektivan način odnosno kada ih interpretiraju na neobjektivan način. Učinak je jači kod pitanja koja izazivaju emocije, te kod duboko usađenih vjerovanja.

**T**

**TROLOVI** - u kontekstu društvenih mreža, odnosi se na pojedince ili naloge koji namjerno izazivaju neslogu, kontroverze ili negativne reakcije postavljanjem zapaljivog, polarizujućeg ili provokativnog sadržaja.

**TROL FARMA** - entitet koji sprovodi aktivnosti informacione operacije uticaja na internetu. Aktivnosti su često sakrivene pod neupadljivim imenom, npr. agencija za odnose sa javnošću, centar za internet istraživanja, itd. Operacije trol fabrika obično su usredsrijeđene na političku ili ekonomsku sferu. Cilj operacija može biti, na primjer, napad na političke protivnike, podržavanje određenog kandidata ili opcije ili neka druga povezana aktivnost. Trol fabrike postižu svoje ciljeve koristeći, između ostalog, lažne vijesti i govor mržnje.

*Globalna sloboda se suočava sa strašnom prijetnjom. Širom svijeta, neprijatelji liberalne demokratije – oblika samouprave u kojem se priznaju ljudska prava i svaki pojedinac ima pravo na jednak tretman pred zakonom – ubrzavaju svoje napade.*

***Fridom haus izvještaj 2022***

# 1. Uvod

Institucionalizovana logika liberalne demokratije, prema kojoj demokratske vlade i zvaničnici stavljaju interese birača na prvo mjesto, već duže je pod udarom autoritarizma. To podrazumijeva centralizovanu vlast koja, pod plaštom demokratije, podstiče oštre podjele bazirane na religiji ili moralu, geografiji ili rasi, odnosno etničkoj pripadnosti. Insistiranje na različitostima opravdava autoritarizam centralizovane vlasti, uz podrazumijevajuću premisu da politička elita najbolje zna kako da narod i državu zaštiti od svih prijetećih opasnosti.

Pojava društvenih mreža početkom XXI vijeka označila je preokret na globalnom planu u načinu komunikacije, razmjene informacija i političke mobilizacije. Međutim, iako ove platforme imaju potencijal da podrže demokratske procese, one takođe pružaju autoritarnim režimima nove mogućnosti za kontrolu, manipulaciju i represiju. Kao takva, zloupotreba društvenih mreža od strane autoritarnih režima postaje akutni problem za demokratije širom svijeta.

Sa usponom digitalne tehnologije, mnogi su, poučeni iskustvom Arapskog proljeća, vjerovali da bi internet i društvene mreže mogli da budu snaga demokratizacije, koja bi relativizovala moć autoritarnih režima. U zemljama sa ograničenim slobodama medija i izražavanja, društvene mreže su služile kao izvor vijesti i informacija, nudeći alternativu državnim medijima i narativima kontrolisanim od države.

Međutim, uprkos pozitivnoj ulozi koju je tehnologija igrala u jačanju građanskog društva i demokratskih vrijednosti, početna premisa pokazala se ipak utopijskom. Isti alati koji omogućavaju ljudima da komuniciraju, organizuju se i pružaju otpor, te šire informacije o manipulacijama njihovim pravima, danas zloupotrebljavaju vlade koje su u sukobu sa demokratskim vrijednostima i idealima.

Projekcija strateških ciljeva autoritarnih režima korišćenjem društvenih mreža postala je sve učestalija pojava koja uključuje kontrolu informacija, cenzuru, dezinformacije, propagandu i praćenje građana, kao i mobilizaciju pristalica, agitovanje ideologije i uspostavljanje kontrolnih mehanizama.

Taktike uključuju plasiranje dezinformacija kako unutar, tako i van geografskih granica zemlje, nadzor nad građanima, uznemiravanje neistomišljenika

na internetu i manipulaciju javnim mnjenjem. Pomenute aktivnosti imaju duboke implikacije ne samo na individualna prava građana unutar tih režima, već i na integritet demokratskih procesa i institucija na globalnom nivou.

Algoritmima koji regulišu sadržaj na mrežama se može manipulisati kako bi bili potisnuti ili promovisani određeni stavovi, informacije, odnosno, dezinformacije. Javna dostupnost uvjerljivih dipfejk (deepfake) sadržaja i drugih oblika onlajn manipulacija baziranih na vještačkoj inteligenciji dodatno komplikuju ambijent.

Razumijevanje zloupotrebe društvenih mreža od autoritarnih režima je ključno za zaštitu demokratskog integriteta u digitalnoj eri, kada svijet postaje globalno selo, a nivo internet sloboda je u padu. Istovremeno, dvije trećine internet korisnika na svjetskom nivou živi u zemljama gdje vlasti kažnjavaju građane zbog ispoljavanja ličnih stavova u onlajn prostoru. Takođe, određene vlade su radi lakše kontrole i nadzora započele izgradnju sopstvenih digitalnih prostora, u kojima dominiraju državni narativi, dok se nezavisni mediji i kritičari marginalizuju.[1] Stoga, građani, mediji i donosioci odluka moraju biti spremni i sposobni da anticipiraju, prepoznaju, ublaže i suprotstave se pojavama koje nameće digitalni autoritarizam. Pritom je neophodno u tom procesu osigurati da društvene mreže služe kao alat za demokratsko osnaživanje, a ne kao oružje za autoritarnu kontrolu, represiju, manipulaciju i nadzor.

Ova studija ima za cilj da ukaže na fenomen digitalnog autoritarizma i zloupotrebe društvenih mreža od autoritarnih režima i predstavi taktike koje koriste i načine na koje utiču na demokratske procese i institucije. Jednako važan cilj je i da se osvijetle različiti aspekti te osjetljive teme. To će doprinijeti razvoju svijesti, ali i kreiranju strategija i politika koje mogu zaštititi demokratske i liberalne vrijednosti kojima, barem deklaratvno, teži i crnogorsko društvo.

## 1.1. Razumijevanje suštine autoritarnih režima

Autoritarni režimi su politički sistemi u kojima je moć centralizovana i održava se političkom represijom, opsežnom cenzurom i ograničenim političkim pluralizmom. U takvom sistemu, nosioci vlasti imaju snažnu, a ponekad i apsolutnu moć, često bez saglasnosti građana i sa malo brige za javno mnjenje ili individualne slobode. Tu vrstu režima karakteriše da jedan vođa ili mala grupa čelnika posjeduju nesrazmjernu političku moć koja je direktno nadređena sistemu vladanja. Tako se stvara privid funkcionisanja institucija, dok se suštinski uspostavlja piramida moći koju sačinjavaju lojalisti sa jasnim zadatkom očuvanja autoritarnog poretka, odnosno vlasti. Fingiranje demokratije ključ je opstanka takvog režima. Na pojmovnoj ravni, institucije u autoritarnim režimima imaju dvojaku ulogu – zaštitu aktuelnog društvenog poretka i stvaranje privida da su one nezavisne.

U autoritarnom režimu, građanske slobode su često ograničene, a osnovna ljudska prava se konstantno krše. Vlast održava moć koristeći se propagandom, masovnim nadzorom, cenzurom i suzbijanjem političke opozicije. Ograničena sloboda izražavanja, suzbijanje i progoni disidenata, te ograničene medijske slobode karakteristike su tih društava. Izbori, ako se i održavaju,

najčešće nijesu slobodni i fer, uz sveprisutne manipulacije, kako bi se osigurala kontinuirana dominacija vladajuće grupe.

Rusija je primjer takvih mehanizama gdje se kontrolom sistema obrazovanja, odnosno, revizijom istorije i istorijskih činjenica (kako bi aktuelna politika pronašla utemeljenje za svoje postupke u istoriji i istorijskim događajima) gradi uporište za trenutne i buduće unutrašnje planove i projekcije. U prilog pomenutoj tezi se može posmatrati Putinov odnos prema Staljinu, koji svjesno relativizuje jedan vremenski period, dominantno obilježen zločinima, logorima i revanšizmom.[2]

Ekonomske elite najčešće predstavljaju glavnu sponu između autoritarnih režima i modela za učvršćivanje moći, što se takođe vidi na primjeru Rusije, gdje su oligarsi poslije raspada Sovjetskog Saveza dobili ključne prirodne resurse, a zauzvrat su instrumentalizovali ekonomsku moć za izgradnju infrastukture regionalnih lojalista.

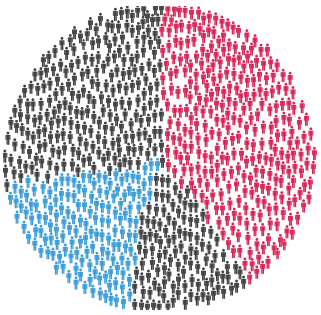
***Autoritarni režimi se formiraju iz različitih razloga i u različitim okolnostima, poput ekonomske nestabilnosti, socijalnih nemira, ili percepcije potrebe za brzom modernizacijom. Takođe mogu nastati u slučaju vakuuma moći, kao što je to najčešće slučaj nakon državnih udara, revolucija ili kolapsa prethodnih političkih poredaka. Neki autoritarni režimi mogu pokazati stabilnost i efikasnost, posebno na kratkoročnom planu, zbog njihove sposobnosti za brzo donošenje odluka i implementaciju politika bez kašnjenja inherentnih demokratskim procesima. Međutim, te prednosti se često negativno odražavaju na ljudska prava i slobode.***

Na unutrašnjem planu, osnovni strah autoritarnih režima je demokratska promjena vlasti i tranzicija moći. Da bi djelovali preventivno, oni kreiraju unutrašnje hibridne prijetnje, izazivaju vještačke krize, manipulišu informacionim prostorom, a sredstvima prisile održavaju unutrašnju organizaciju vlasti. Na sličan način odnose se i prema spoljnim prijetnjama, pri čemu kao najveću opasnost percipiraju demokratske države i njihove vlade, dok proces demokratizacije u okruženju doživljavaju kao prijetnju za opstanak vlastitog sistema vrijednosti. Upečatljiv primjer je odnos Rusije prema Ukrajini.

Postoji širok spektar autoritarnih režima, koji se kreću od apsolutnih monarhija do vojnih hunti i jednopartijskih država. Njihove specifične karakteristike mogu se široko razlikovati u zavisnosti od kulturnih, istorijskih i geopolitičkih faktora. Nijesu svi autoritarni režimi u potpunosti lišeni određenih demokratskih elemenata. Na primjer, neki od njih mogu organizovati izbore, iako sa značajnim ograničenjima. Rezultate takvih neslobodnih i nedemokratskih izbornih procesa autoritarni režimi koriste kao uporište za dalje urušavanje liberalnih vrijednosti, a sve pod plaštom ubjedljive pobjede na izborima. Primjer erozije demokratskih tekovina i liberalnih vrijednosti možemo vidjeti u Mađarskoj, gdje se demokratski standardi urušavaju, a kao glavni izgovor se navodi očuvanje nezavisnosti i zaštita nacionalnih interesa.

Prema izvještaju Slobode u svijetu (Fridom haus) 38% procenata svjetske populacije živi u neslobodnim zemljama (Not Free Countries), što je najveći procenat od 1997. godine. Samo njih oko 20 odsto sada živi u slobodnim zemljama.[3]

U zavisnosti od tipologije, autoritarni režimi kreiraju procese koji se prividno podudaraju sa procesima u slobodnim demokratijama, a jedan od tih procesa je stvaranje pseudo-opozicionih partija koje služe kao primjeri živahne demokratije u zemlji, a suštinski su dekor vlasti za unutrašnju upotrebu. Pozadinski proces koji se uvijek odvija paralelno sa pseudo-demokratskim je obezbjeđivanje dugotrajne moći, odnosno promjene zakonskih ili ustavnih okvira koji omogućava dugotrajnost režima ili vladara. Primjer Vladimira Putina je eklatantan. Ruski predsjednik je amandmanima na Ustav stvorio uslove da se kandiduje na predsjedničkim izborima još dva puta, čime je obezbijedio da na mjestu predsjednika Rusije bude do 2036. godine. Uloga kvazi-opozicije u takvim prilikama je jasna, jer su amandmani na Ustav usvojeni jednoglasno. Stvarna opozicija u Rusiji, aktivisti i građani, bivaju zastrašeni i obeshrabreni za bilo koju vrstu aktivizma i onemogućava im se pristup medijima, a skoro svaki vid djelovanja sankcioniše se kao unutrašnji ekstremizam. Nakon invazije na Ukrajinu ruska Duma usvojila je niz zakona kojima se svako protivljenje specijalnoj vojnoj operaciji karakteriše kao izdaja, uz prijetnju zatvorske kazne. Namjere autoritarnih režima i strateški planovi se oslikavaju kroz odnos prema istaknutim opozicionim liderima i aktivistima u državi. Nakon aneksije Krima 2014. godine i građenja podrške za ekspanzionističke planove, Boris Nemcov, opozicioni lider i aktivista iz partije PARNAS ubijen je u Moskvi 2015. godine. Autoritarni režimi svaki vid samostalnog djelovanja percipiraju kao opasnost za svoju vladavinu i brutalno sijeku u korijenu svaki oblik političke ili građanske neposlušnosti.



**38%**

SVJETSKE POPULACIJE ŽIVI U NESLOBODNIM ZEMLJAMA

**20%**

SVJETSKE POPULACIJE ŽIVI U SLOBODNIM ZEMLJAMA

*Izvor: Izvještaj Slobode u svijetu 2022 (Fridom haus)*

## 1.2. **Instrumenti digitalnog autoritarizma**

U stručnoj literaturi koja se bavi tematikom zloupotrebe autoritarnih režima digitalnih informacionih tehnologija etablirao se termin digitalni autoritarizam, koji se odnosi na upotrebu digitalnih informacionih tehnologija radi nadzora, represije i manipulacije domaćeg i stranog stanovništva. Digitalna sfera pruža nove alate za održavanje moći, uključujući sofisticirane sisteme nadzora, automatsku kontrolu sadržaja i ciljane kampanje dezinformacija. Porast digitalnog autoritarizma podstaknut je takođe napretkom vještačke inteligencije, što omogućava efikasniju i sveprisutniju kontrolu nego ikada ranije.

Iako se ti napori događaju u digitalnom prostoru i duboko su umreženi, oni nijesu ograničeni na aktivnosti na društvenim mrežama. Digitalni autoritarizam koristi sve elemente informacionog prostora, uključujući vlasništvo nad me-

dijima i tehnološkim platformama, pritisak na poslovanje i oglašavanje i tradicionalne tehnike cenzure. Ipak, fokus ovog materijala će biti na aktivnostima autoritarnih režima koje se sprovode na društvenim mrežama za postizanje različitih strateških ciljeva.

Režimi mogu pratiti aktivnosti svojih građana, posebno onih koji su politički aktivni ili kritični prema vlasti, te koristiti te informacije kako bi suzbili neslaganje i kritiku. To može uključivati praćenje onlajn aktivnosti pojedinaca i korišćenje vještačke inteligencije za analizu objava na društvenim mrežama.

Takođe, te onlajn platforme se mogu koristiti za širenje propagande ili dezinformacija, oblikovanje narativa i stvaranje atmosfere straha. To može uključivati korišćenje lažnih identiteta na mrežama, automatizovanih bot naloga i trol farmi kako bi se pojačale određene poruke ili narativi, stvaranje i širenje lažnih vijesti ili ciljano oglašavanje (microtargeting) kako bi se dosegle određene demografske grupe sa prilagođenim porukama.

Manipulacija javnog mnjenja na platformama ima mnogo oblika, formi i naziva. Brojni termini su korišćeni za opisivanje niza aktivnosti u informacionom prostoru; hibridni rat, psihološki rat, aktivne mjere, lažne vijesti, dezinformacije, propaganda, koordinisano neautentično ponašanje, operacije informisanja/uticaja. Iako nijesu sinonimi, svi termini opisuju niz međusobno povezanih zlonamjernih aktivnosti, čiji je cilj da dovedu u zabludu ili da obmanu, u lokalnom ili globalnom informacionom prostoru.[4]

Za potrebe studije, koristićemo termin informacione operacije uticaja - IOU (information influence operations). IOU se odnosi na namjerno i organizovano nastojanje manipulacije ili uticaja na javno mnjenje, percepcije, vjerovanja ili ponašanja publike. Te operacije obično uključuju strateško i plansko korišćenje različitih komunikacionih kanala kako bi se oblikovali narativi, širile dezinformacije, podrivali demokratski procesi unutar i van zemlje, promovisali određeni politički, ekonomski i ideološki interesi, odnosno agende i degradirao integritet informacionog prostora.

Takođe, digitalni autoritarizam na društvenim mrežama može uključivati kažnjavanje političkih neistomišljenika, bilo pojedinaca i grupa putem onlajn uznemiravanja i javnog objavljivanja privatnih informacija (doxxing), ali i mjera hapšenja ili nasilja.

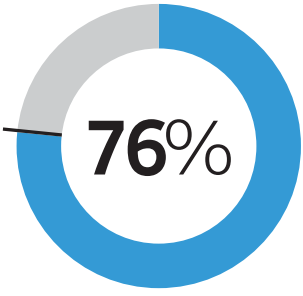
Određene vlade teže kreiranju onlajn prostora koji se mogu kontrolisati. Prema najnovijem izvještaju Fridom hausa, rekordan broj nacionalnih vlada blokirao je u 2022. godini vebsajtove sa političkim, društvenim ili vjerskim sadržajem. Time je direktno podrivano pravo na slobodno izražavanje i pristup informacijama. Većina blokiranja odnosila se na sajtove van zemlje.[5]

U tom smislu određeni nacionalni zakoni i rješenja predstavljaju dodatnu prijetnju slobodnom protoku informacija centralizacijom tehničke infrastrukture i primjenom represivnih propisa na platforme društvenih mreža i korisničke podatke, što omogućava cenzuru i filtraciju podataka. Napori Pekinga da izgradi i održi Veliki kineski zaštitni zid[6] pokrenuli su brojna pitanja kršenja privatnosti, sajber-bezbjednosti, lažnog propagandnog sadržaja i cenzure na mrežama. Sa druge strane, u širenju propagande i dezinformacija, uz pomoć

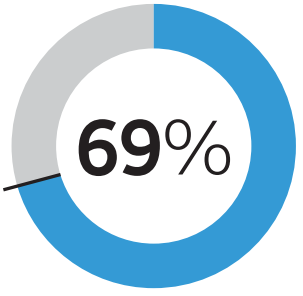
bot i trol mreža posebno je vješta ruska vlada. Autoritarni režimi također koriste AI rješenja da nadgledaju svoje građane, što olakšava identifikaciju, praćenje i ciljanje onih koji im se protive. Mogućnosti za korišćenje novih tehnologija za vršenje digitalnog nadzora i cenzure kontinuirano napreduju.

Digitalni autoritarizam na društvenim mrežama predstavlja razlog za sve veću zabrinutost usljed prodornosti i uticaja društvenih mreža na savremeni život, sa platformama kao što su Fejsbuk, Tviter, Instagram i druge koje igraju centralnu ulogu u oblikovanju javnog mnjenja i olakšavanju javnog diskursa.[7]

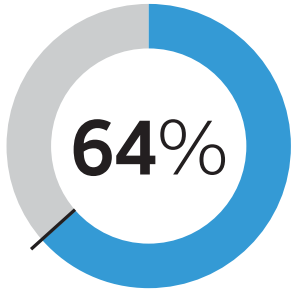
Prema izvještaju[8] Internet slobode 2022 (Fridom haus), preko 4.5 milijarde ljudi ima pristup internetu. Od toga:



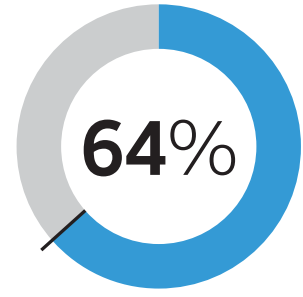

ŽIVI U ZEMLJAMA GDJE SU POJEDINCI HAPŠENI ZBOG OBJAVLJIVANJA POLITIČKOG, DRUŠTVENOG ILI VJERSKOG SADRŽAJA NA MREŽAMA



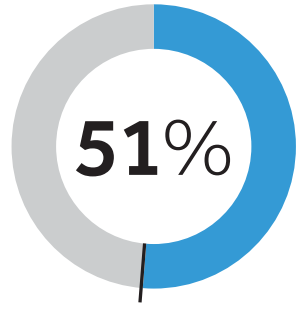

ŽIVI U ZEMLJAMA GDJE VLASTI MANIPULIŠU DISKUSIJAMA NA ONLAJN PLATFORMAMA



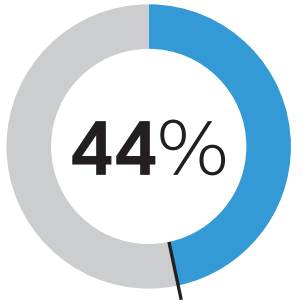

ŽIVI U ZEMLJAMA GDJE JE POLITIČKI, DRUŠTVENI I VJERSKI SADRŽAJ BIO BLOKIRAN




ŽIVI U ZEMLJAMA U KOJIMA SU POJEDINCI NAPADANI I UBIJANI ZBOG ONLAJN AKTIVNOSTI OD JUNA 2021. GODINE




ŽIVI U ZEMLJAMA GDJE JE PRISTUP DRUŠTVENIM MREŽAMA BIO PRIVREMENO ILI U POTPUNOSTI BLOKIRAN




ŽIVI U ZEMLJAMA GDJE VLAST GASE PRISTUP INTERNETU, ČESTO ZBOG POLITIČKIH RAZLOGA

# 2. Uspon društvenih mreža u digitalnom dobu

Kontinuirani rast društvenih mreža u posljednjih deset godina učinio je te platforme integralnim dijelom svakodnevice na globalnom nivou. Platforme poput Fejsbuka, Instagrama i Tvitera više se ne koriste isključivo za zabavu i komunikaciju, već imaju značajnu ulogu i u kreiranju i plasiranju informacija, marketingu, poslovnom povezivanju i političkoj komunikaciji.

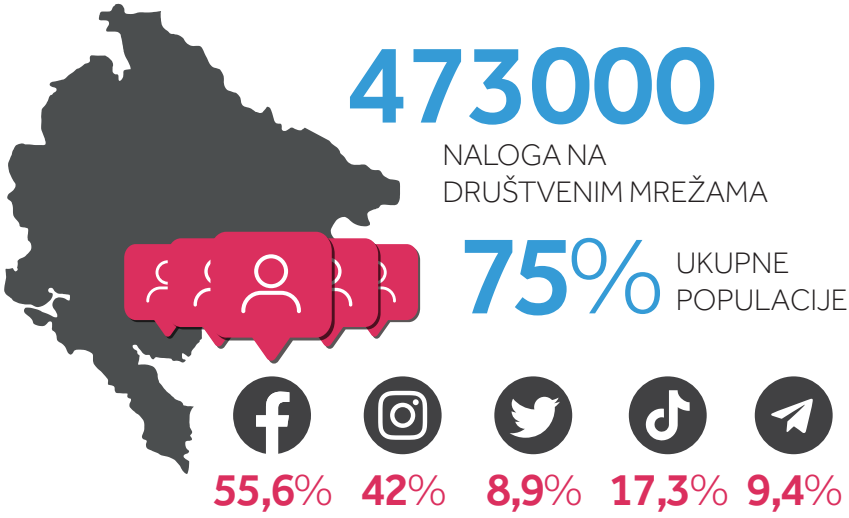
**Pandemija korona virusa je dodatno ubrzala promjene ka digitalnom i mobilnom medijskom i informacionom okruženju, sa potencijalnim dalekosežnim implikacijama za novinarstvo. Ipak, prema istraživanjima, kako u Crnoj Gori, tako i u svijetu, tradicionalni mediji još uvijek uživaju najveće povjerenje građana i odolijevaju sveprisutnim društvenim mrežama**

Pandemija korona virusa je dodatno ubrzala promjene ka digitalnom i mobilnom medijskom i informacionom okruženju, sa potencijalnim dalekosežnim implikacijama za novinarstvo. Ipak, prema istraživanjima, kako u Crnoj Gori, tako i u svijetu, tradicionalni mediji još uvijek uživaju najveće povjerenje građana i odolijevaju sveprisutnim društvenim mrežama.[9]

Fejsbuk je globalno društvena mreža sa najvećim brojem korisnika, ali je evidentan trend emigracije, pogotovo generacije Z (Zumeri – rođeni od sredine devedesetih do ranih 2010-ih) na više vizuelne platforme poput Instagrama i TikToka u posljednje tri godine. Telegram je takođe značajno porastao na nekim tržištima kao fleksibilnija alternativa Vocapu (WhatsApp).[10]

Procjenjuje se da, od 2023. godine, širom svijeta ima oko 4,76 milijardi korisnika društvenih mreža, što je 137 miliona više nego prethodne godine. Prema DataReportal podacima za 2023. godinu, 47% korisnika navodi da mreže primarno koriste radi komunikacije, 36% da ispuni svoje vrijeme, dok svaki treći korisnik, njih 34% koristi mreže za informisanje i čitanje vijesti.[11]

U januaru 2023. godine, u Crnoj Gori je bilo oko 473 hiljade naloga na društvenim mrežama, što je ekvivalent 75% ukupne populacije. Prema istraživanjima, 55,6% građana Crne Gore ima nalog na Fesjbuku, 42% na Instagramu, 17,3% na TikToku, 9,4% na Telegramu i 8,9% na Tviteru. Istraživanja[12] pokazuju da građani i građanke Crne Gore najveće povjerenje, kada je u pitanju izvor informacija, imaju u vijesti i informacije iz tradicionalnih medija, njih 57,8%. Povjerenje u vijesti i informacije koje dobijaju putem društvenih mreža ima njih 16,7%, među kojima Fejsbuk i Instagram uživaju najveće povjerenje kao izvor informacija.[13]




U biznis svijetu, društvene mreže su postale nezaobilazno sredstvo za marketing i oglašavanje. Kompanije koriste te platforme za direktnu interakciju sa svojim klijentima, promovisanje proizvoda i usluga i kreiranje uvida u navike potrošača putem različitih analitičkih alata. Uspon marketing usluga na tim platformama je još jedan dokaz značajne uloge društvenih mreža u oblikovanju ponašanja potrošača.

Iz društveno-političke perspektive, pomenute platforme takođe imaju značajnu ulogu. Korišćene su za mobilizaciju društvenih pokreta, od Arapskog proljeća do pokreta *Životi crnaca su važni* (Black lives matter). Platforme su omogućile građanima da izraze svoje stavove, dobiju podršku i organizuju proteste. Istovremeno, vlade i drugi akteri ih takođe mogu koristiti za širenje dezinformacija, propagande, manipulisanje javnim mnjenjem, miješanje u izbore i kontrolu protoka informacija.

I algoritmi društvenih mreža ojačavaju postojeće predrasude (confirmation bias) dok ograničavaju izloženost različitim i suprotnim tačkama gledišta, što

rezultira eho komorama (echo chambers) koje pojačavaju postojeće ideje dok ograničavaju izloženost drugim perspektivama. Na taj način je moguće još više polarizovati javno mnjenje i politički diskurs i doprinijeti nepovjerenju u institucije i demokratske procese.

U demokratskim zemljama, korišćenje društvenih mreža u političkim procesima postalo je uobičajeno. Političari, partije i aktivisti koriste ove platforme da se povežu sa biračima, podijele svoje stavove i generišu podršku. Od kraja 2020. godine, u Crnoj Gori je došlo je do proliferacije u upotrebi Tvitera od strane političara i javnih ličnosti, koji tu platformu koriste za direktnu komunikaciju sa javnošću, bilo putem tekstualnog ili audio formata, kroz popularne spejsove (Twitter space).

**Algoritmi za privlačenje pažnje, koji su u osnovi društvenih mreža, podstiču autoritarne prakse čiji je cilj širenje konfuzije, neznanja, predrasuda i podjela, čime se olakšava manipulacija i podriva demokratija**

*Ronald Dajbet*

Nasuprot tome, u mnogim autoritarnim režimima vladajuće strukture snažno cenzurišu i kontrolišu društvene mreže radi suzbijanja disidentskih glasova i održavanja moći. Primjer je Kina gdje je vlada zamijenila Gugl i Fejsbuk domaćim servisima kao što su Baidu i ViČet (WeChat), jer može regulisati informacije i prekinuti pristup međunarodnim platformama. U Rusiji je na snazi zakonodavstvo za povećanje kontrole nad internetom i onlajn sadržajem, čime se ograničava slobodan protok informacija.

Paraleno sa rastom autoritarnih praksi na mrežama, velike tehnološke platforme poput Fejsbuka monetizuju pažnju (attention economy)[14] i u sve većem obimu prikupljaju podatke od pojedinačnih korisnika, što se u stručnoj teoriji naziva model nadzornog kapitalizma (surveillance capitalism)[15]. I jedan i drugi model mogu imati snažne negativne implikacije po privatnost pojedinca i stvoriti prostor za autoritarne prakse. Kako je Ronald Dajbet rezimirao, algoritmi za privlačenje pažnje, koji su u osnovi društvenih mreža, podstiču autoritarne prakse čiji je cilj širenje konfuzije, neznanja, predrasuda i podjela, čime se olakšava manipulacija i podriva demokratija.[16]

Upotreba algoritama u pružanju medijskih i drugih usluga putem onlajn društvenih platformi ima direktne implikacije na demokratske procese. Zdrava demokratija je ona u kojoj građani učestvuju i donose slobodne i političke odluke na osnovu tačnih informacija, zasnovanih na provjerenim činjenicama i pouzdanim dokazima. Uloga društvenih mreža kao posrednika između korisnika i medija ih postavlja kao de fakto provajdere medijskog sadržaja. Obzirom na učestale neprofesionalne, neistinite i opasne sadržaje na društvenim mrežama, korisnici ne postaju samo izloženi, već posebno ranjivi na dezinformacije na mreži.

***Istraživanje Kembridž i Stanford univerziteta objavljeno 2015. godine u Zborniku radova Nacionalne akademije nauka SAD ukazalo je da Fejsbukovom algoritmu treba samo 10 lajkova neke osobe da je bolje pro-***

***cijeni od kolege na poslu, 70 da bolje procijeni od cimera, 150 da bolje procijeni od roditelja, sestre ili brata i 300 da bolje ocijeni osobu od supružnika.***[17]

Nakon nedavnih otkrića uzbunjivačice Frensis Haugen, jasno je da je Fejsbukov algoritam sortiranja i plasiranja vijesti na njuz fidu favorizovao sadržaj koji izaziva ljutnju i činio ga pet puta vidljivijim od sadržaja koji izaziva sreću. Teorija je bila jednostavna: objave sa mnogo vau, ljut/a, tužan/a i haha reakcija imale su tendenciju da zadrže korisnike više angažovanim i prisutnim na platformi, a zadržavanje korisnika je ključ poslovanja Fejsbuka. Na taj način, favorizovanje kontroverznih i polarizujućih objava je otvorilo vrata za više neželjenog sadržaja, kršeći Fesjbukove sopstvene uslove korišćenja. Interni dokumenti te kompanije, koji su procurili u javnost 2019. godine, potvrdili su da su objave koje su izazvale neku od gore naznačenih reakcija emotikonima češće uključivale dezinformacije, štetne vijesti i sadržaje upitnog i niskog kvaliteta. Promjena algoritma je, uprkos javnom značaju, bila onemogućena, budući da bi u krajnjoj računici dovela do manje upotrebe, manje klikova na oglase, odnosno, manju zaradu te kompanije.[18]

Takođe, kada razmatramo pitanje transparentnosti, problematična je i personalizacija sadržaja koja u kombinaciji sa profilisanjem i mikro-ciljanjem korisnika doprinosi stvaranju tzv. filter mejhura. U tim filter mjehurima su ljudi izloženi prekomjernoj količini vijesti ili stavova usklađenih s njihovim postojećim uvjerenjima. To dalje rezultira hermetičkim zatvaranjem korisnika u krug personalizovanih informacija shodno njihovim interesovanjima i uvjerenjima. Na taj način se ograničava izloženost alternativnim gledištima, stvarajući takozvane eho komore.

***U istraživanju Društvene mreže i novinarstvo u Crnoj Gori, koje je sproveo Medijski savjet za samoregulaciju (MMS) uz podršku UNESCO i EU, pokazalo se da ni novinarima ni urednicima nije bio najjasniji značaj i uloga algoritama. Od 20 intervjuisanih sagovornika, najveći broj njih nije razumio princip rada mreža, niti su mogli da dođu do smjernica ili uputstava o načinu korišćenja mreža.***[19]

Iako autoritarni režimi često mogu biti izvor informacionih operacija uticaja, uspjeh dezinformacione kampanje ne zavisi isključivo od njih. Mora postojati potražnja za lošim ili obmanjujućim informacijama koja odgovara ponudi. Stoga su potrebe emocionalne, vrjednosne ili ideološke validacije kod pojedinaca i grupa uparene sa algoritmima društvenih mreža. A one su, kao najsofisticiraniji sistemi isporuke informacija koje odgovaraju našim potrebama, važne za razumijevanje šire dinamike širenja dezinformacija u digitalnom okruženju.

Istraživanja pokazuju da u svim geografskim kontekstima, duboko polarizovana društva sa niskim povjerenjem u tradicionalne medije mogu biti podložnija tim psihološkim pokretačima koji stoje iza konzumiranja dezinformacija i lažnih vijesti.[20]

# 3. Autoritarni režimi i društvene mreže

Sve vlade, pa i one demokratske, imaju tendenciju da oblikuju javno mnjenje, iako različiti režimi to čine na različite načine u zavisnosti od okolnosti. Demokratski izabrane vlade tome pribjegavaju tokom zdravstvenih ili ekonomskih kriza ili u situacijama kada je potrebno da se održi javna podrška određenim osjetljivim politikama ili pitanjima. Nasuprot tome, autoritarni režimi redovno koriste cenzuru, nadzor i manipulaciju javnim mnjenjem o širokom spektru pitanja, a jedan od glavnih ciljeva jeste održavanje na vlasti. Prema izvještaju Internet slobode za 2022. godinu, zvaničnici u najmanje 53 zemlje su optužili, uhapsili ili zatvorili internet korisnike kao odgovor na kritički nastrojene objave na društvenim mrežama, dok su vlasti u najmanje 22 zemlje blokirale pristup društvenim mrežama i komunikacionim platformama.[21]

Društvene mreže se često zloupotrebljavaju jer su ljudi izloženi iskrivljenim informacijama najčešće bez njihovog znanja. Primjeri takvih praksi variraju od globalnih kampanja dezinformacija (npr. o korona virusu) koje vode zemlje poput Kine i Rusije.[22] U Bjelorusiji je vlada u kontekstu ruske agresije na Ukrajinu pojačala hapšenja blogera, onlajn aktivista i drugih korisnika izričući zatvorske kazne[23], a praktikuje se i miješanje u izborne procese drugih zemalja.

***Tokom posljednjih godina raste dostupnost naučne i stručne literature i izvještaja koji proučavaju i ukazuju na učestalost informacionih operacija uticaja u političke svrhe. Građa uključuje upotrebu političkih bot mreža za pojačavanje govora mržnje ili drugih tehnika manipulisanja sadržaja, nezakonito prikupljanje podataka ili mikro-ciljanje, kao i korišćenje trolova za suzbijanje političkog aktivizma ili slobode štampe.***[24]

U izvještaju Oksfordovog instituta za internet (Oxford Internet Intsitute) o organizovanim manipulacijama društvenim mrežama se ne ukazuje samo na rastuću sposobnost autoritarnih režima da iskoriste informacioni prostor unutar svojih granica, već i na pojavljivanje nekoliko država, koje su u stanju da sofisticirano koriste informacione operacije uticaja (IOU) van svojih geografskih granica. To su Kina, Indija, Iran, Pakistan, Rusija, Saudijska Arabija i Venecuela, od kojih su pet, prema izvještaju Fridom hausa za 2023. godinu, rangirane kao neslobodne (not free) a dvije kao djelimično slobodne (partly free).[25]

Istorijat institucionalizovanja modernih i visokotehnoloških napora za sprovođenje IOU počinje sa dugoročnim investicijama Rusije u nacionalističke kampove za omladinu, gdje su organizovani timovi preko društvenih mreža usmjeravali dezinformacije ka ruskim građanima koristeći popularni ruski sistem za blogovanje LiveJournal. Oni su predstavljali prethodnicu Agenciji za istraživanje interneta (IRA - Агентство интернет-исследований).[26] IRA, sa sjedištem u Sankt Peterburgu, koju je osnovao i finansirao Jevgenij Prigožin (vođa Vagner grupe), bavi se onlajn propagandom i uticajem na ruske poslovne i političke interese u zemlji i svijetu. Agencija je, od 2013. godine, koristila lažne naloge registrovane na mejnstrim društvenim mrežama, forumima i sajtovima medija širom svijeta da promoviše interese Kremlja u unutrašnjoj i spoljnoj politici, uključujući Ukrajinu, Zapadni Balkan i Bliski Istok. Ipak, javnost je tek nakon 2016. godine, usljed istrage o navodima o ruskom miješanju u američke predsjedničke izbore, dobila detaljne uvide u modus operandi te trol fabrike.

Da bi se razumjelo djelovanje Rusije kao autoritarnog režima na društvenim mrežama, potrebno je napraviti osvrt na sovjetsku medijsko-propagandnu doktrinu, odnosno propagandno obavještajni sistem aktivnih mjera (Active measures). Sistem je, po definiciji, obavještajni proizvod Sovjetskog KGB za širenje lažnih vijesti, dezinformacija i propagande preko radio stanica, novina i časopisa. Cilj im je bio da stavovi i aktuelna politika tadašnjeg SSSR budu prihvatljivi i izazovu afirmativne stavove stanovništva na Zapadu. Naslanjajući se na ovu praksu, a u novim geopolitičkim okolnostima, Valerij Gerasimov, načelnik Generalštaba Oružanih snaga Ruske Federacije, artikulisao je modernu rusku strategiju djelovanja, poznatu kao Gerasimovljeva doktrina, koja obuhvata upotrebu hakerskih usluga, instrumentalizaciju medija, kreiranje lažnih vijesti, curenje informacija, uz konvencionalna i asimetrična vojna sredstva.

**Iako je teško predstaviti kompletnu listu, poznato je da je i niz drugih autoritarnih sistema tokom protekle decenije počelo razvijati sopstvene internet timove s ciljem manipulisanja javnim mnjenjem na internetu. Neke od ovih zemalja uključuju Kinu i tzv. *50 Cent Army*, Venecuelu i Iran. Slični sistemi uspostavljeni su i u regionu Zapadnog Balkana, a aktivne su i privatne agencije koje za potrebe različitih vlada širom svijeta sprovode namjenske dezinformacione kampanje, najčešće u toku izbornih procesa.**

Društvene mreže se posmatraju kao novo bojno polje na kojem će zloupotreba informacija, obavještajno navođena strategija sa bot i trol farmama, lažnim vijestima i kreiranjem određenih narativa služiti u cilju amortizacije domaće i globalne javnosti spram bilo koje operacije ili politike koja može izazvati negodovanje.

Uprkos percepciji da se IOU oslanjaju isključivo na širenje i plasiranje neistina, stvarnost je nešto drugačija. Prema studiji Stenforda[27], jedna od ključnih taktika koje koriste Glavna obavještajna uprava glavnog štaba oružanih snaga Ruske Federacije (GRU) i Agencija za istraživanje interneta (IRA) je pranje narativa (narrative laundering), odnosno plasiranje određenog sadržaja u manje poznatom mediju. Zatim slijedi njegovo preuzimanje i konstantno ponavljanje u državnim medijima u cilju popularizacije. S tim je povezana i taktika pospješivanja (boosting), odnosno legitimizacija sadržaja kroz konstantno ponavljanje u medijima i na društvenim mrežama, u cilju stvaranja percepcije da određeni narativ zaista predstavlja popularno gledište većine. Načelo na kojem operacije uticaja počivaju je da informacije ne moraju biti tačne, već uvjerljive.

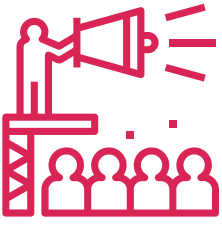
Iako je teško predstaviti kompletnu listu, poznato je da je i niz drugih autoritarnih sistema tokom protekle decenije počelo razvijati sopstvene internet timove s ciljem manipulisanja javnim mnjenjem na internetu. Neke od ovih zemalja uključuju Kinu i tzv. *50 Cent Army*[28], Venecuelu[29] i Iran[30]. Slični sistemi uspostavljeni su i u regionu Zapadnog Balkana[31], a aktivne su i privatne agencije koje za potrebe različitih vlada širom svijeta sprovode namjenske dezinformacione kampanje, najčešće u toku izbornih procesa.[32]

U studiji iz 2020. godine Prinston univerziteta Tracking Online Influence Efforts[33], naučnici su predstavili skup podataka koji obuhvata 76 inostranih i domaćih IOU u periodu 2011-2020. godine, pokrenutih od strane države ili vladajuće partije u autokratiji, sprovedenih u 30 zemalja. Rezultati su pokazali da je u tom periodu 64% informacionih operacija uticaja, usmjerenih ka inostranstvu, došlo iz Rusije, dostigavši vrhunac 2017. godine sprovođenjem 34 različite kampanje. Kina, Iran, Saudijska Arabija i UAE su zaslužni za ostatak aktivnosti.

# 4. Metode i tehnike

Autoritarni režimi koriste različite taktike na društvenim mrežama u cilju modeliranja stvarnosti u skladu sa vlastitim interesima. Metode mogu da variraju od upotrebe mreža bot i trol naloga, širenja lažnih ili obmanjujućih informacija kako bi se oblikovalo javno mnjenje i potisnuli disidentski glasovi, do ad-hominem targetiranja i uznemiravanja.

## 4.1. Propaganda i dezinformacije



Kontrola informacija i narativa se smatra ključnom za bezbjednost režima. U autoritarnom svijetu, sposobnost kontrole informacionog okruženja je od ključnog značaja, jer direktno utiče na spremnost građana da se pridruže opozicionim grupama, učestvuju u protestima i angažuju se u antirežimskim aktivnostima. To je oblast u kojoj Rusija, uz Kinu, igra vodeću ulogu. Kremlj preplavljuje kontrolisani onlajn prostor prorežimskim narativima, skrećući pažnju sa djelovanja vlasti, šireći vijesti koje podstiču konfuziju i neizvjesnost plasiranjem alternativnih narativa o događajima. Taj metod je korišćen i nakon invazije na Ukrajinu, u cilju ubjeđivanja domaće javnosti u ispravnost i opravdanost specijalne vojne operacije.

Mnogi autoritarni režimi imaju zajednički interes da jačaju svoj imidž na međunarodnom planu, ali i da pospješuju nepovjerenje u demokratiju i vladavinu prava uopšte. Diskreditacija demokratije kao modela upravljanja je cilj koji dijele svi autoritarni režimi, a mogućnosti su se znatno uvećale pojavom mreža. Stoga ne iznenađuje da su se Kina i Rusija zbližile u informacionom prostoru

nakon ruske agresije na Ukrajinu, što je dovelo do učestalog ponavljanja ruskih narativa u kineskim medijima i u obraćanjima njihovih zvaničnika s ciljem diskreditacije Zapada i otvorilo pitanje kineske neutralnosti u sukobu.[34] U empirijskom istraživanju Alijanse za osiguravanje demokratije iz 2023. godine prezentovan je podatak da je svaki od 50 tvitova kineskih diplomata i medija sa najviše dijeljenja na toj mreži pominjao NATO isključivo u negativnom kontekstu.[35] Ipak, postoje i raniji navodi i cijela dokumentacija o tajnim sastancima zvaničnika te dvije zemlje između 2017. i 2019. godine, s ciljem dijeljenja metoda i taktika za praćenje disidenata, kritičara i kontrolu interneta.[36]

Razvoj generativnih tehnologija će vjerovatno dodatno povećati kapacitet manipulisanja, kroz širu dostupnost dipfejk rješenja, što će otežati razlikovanje istinitog i lažnog digitalnog sadržaja. Mikrotargetiranje će omogućiti autokratama da prilagode sadržaj određenim pojedincima ili segmentima društva na sličan način kao što biznis svijet koristi demografske karakteristike i odlike ponašanja za prilagođavanje reklama i postizanje komercijalnih efekata. Adekvatna ilustracija dipfejk manipulacije u političke svrhe je zloupotreba identiteta ruske opozicije iz 2021. godine.[37] Za sada, mnogo češće od video materijala nailazimo na realistične fotografije kreirane putem AI, koje se uglavnom koriste za pravljene lažnih identiteta i naloga na društvenim mrežama.

U masovnom širenju propagande i dezinformacija, režimi često pribjegavaju korišćenju astroturfinga - taktike kojom se u javnosti nastoji stvoriti lažni privid široke podrške nekoj ličnost, organizaciji, ideji ili političkom potezu upotrebom trolova i bot mreža. Tim metodama se mreže bombarduju provladinim komentarima, objavama i heštegovima koji su u skladu sa odgovarajućim narativom vlasti, istovremeno diskreditujući ili napadajući one koji im se protive. Domet i efikasnost objava koje ti nalozi šire može biti poboljšana algoritmima društvenih mreža koje često promovišu sadržaj koji je popularan ili zanimljiv, bez obzira na njegovu istinitost. Međutim, mnoge platforme imaju sisteme za otkrivanje i njihovo uklanjanje, iako se često postavlja pitanje učinkovitosti.

Osim automatizovanih bot naloga čija kompleksnost varira, sve je češća upotreba naloga koje su kreirali i kojima upravljaju ljudi, kako bi mogli da učestvuju u razgovorima, objavljivanju komentara ili tvitova ili slanja privatnih poruka pojedincima.

***Nakon što je Ilon Mask preuzeo Tviter, pojačano je prisustvo bot i trol naloga ruske i kineske državne propagande na toj mreži, budući da je novi vlasnik ukinuo tim koji se bavio IOU. Ta jedinica je bila aktivna u detektovanju informacionih operacija i koordinisanih kampanja zemalja kao što su Rusija, Kina i Iran s ciljem da utiču na javno mnjenje i podriju demokratiju. Stoga je sada Tviter podložniji stranim manipulacijama i zloupotrebama, iako Mask tvrdi da je pod njegovim vođstvom mnogo manje dezinformacija na toj mreži.***[38]

Digitalni forenzički centar (DFC) je 2020. godine razotkrio veliku pro-kinesku bot mrežu povezanu sa vladajućom partijom iz Srbije, a koja je za cilj imala veličanje kineske medicinske pomoći povodom pandemije COVID-19, ali i prijateljstvo između dvije zemlje.[39] Iste godine, u javnom saopštenju Tvitera, navedeno je da je sa te platforme obrisano preko 8.000 naloga povezanih sa Srpskom naprednom strankom.[40]

# Kako uočiti bota?

Samo zato što se ponaša kao bot, ne znači da je bot. Ovi indikatori automatizovane ili koordinisane mrežne aktivnosti mogu pomoći, ali tražite kombinaciju znakova, ne samo jedan.

## NALOG:

- Nedavni datum kreiranja
- Nedostatak ličnih podataka
- Ukradena ili AI generisana profilna fotografija
- Polarizujuće riječi, haštagovi, linkovi ili emotikoni u biografiji
- Sumnjivo korisničko ime sa npr. mnogo brojeva

## SADRŽAJ:

- Tvitovanje na više jezika
- Uključivanje u više međunarodnih narativa
- Znaci automatizacije ili softvera za upravljanje naloga poput buff.ly
- Objavljivanje zapaljivih mimova i GIF-ova
- Haštag spamovanje
- Povremeni retvitovi van konteksta
- Pozivanje na  mali broj pouzdanih izvora vijesti
- Neprirodni način izražavanja

## AKTIVNOST:

- Veliki broj tvitova (više od 100 dnevno)
- Veliki procenat ritvitova (više od 80 posto)
- Kontinuirano objavljivanje u toku dana i noći
- Objavljivanje samo u određeno vrijeme
- Iznenadni porast aktivnosti ili promjena interesovanja

## MREŽA:

- Pratioci i praćenja su visoka ili identična
- Visok broj praćenja a bez pratioca
- Praćenje sumnjive mješavine izvora
- Povezan sa drugim sumnjivim nalozima
- Dupli nalozi
- Prethodno cirkulisanje sumnjivog sadržaja
- Prethodno prepoznati kao sumnjivi od strane drugih organizacija

Izvor: First Draft News

U finalnom kvartalnom izvještaju Mete za 2022. godinu, navodi se da je sa Fejsbuka obrisano više od 5000 naloga kao i izvjestan broj naloga na Instagramu, zbog kršenja pravila o koordinisanom neautentičnom ponašanju (coordinated inauthentic behavior). Ta mreža, koju je kontrolisala Srpska napredna stranka, imala je cilj da na prividno organski način predstavi ogromnu popularnost predsjednika Srbije i vladajuće stranke širom zemlje, kao i da izrazi podršku za poteze vlasti. Istovremeno, cilj je bio i diskreditacija opozicionih aktera na političkoj sceni. Za te aktivnosti utrošeno je najmanje 150.000 dolara.[41]

Sa druge strane, termin trol, u kontekstu društvenih mreža, odnosi se na pojedince ili naloge koji namjerno izazivaju neslogu, kontroverze ili negativne reakcije postavljanjem zapaljivog, polarizujućeg ili provokativnog sadržaja. U autoritarnim režimima trolovi koje sponzoriše država često se koriste da uznemiravaju, zastrašuju i diskredituju kritičare i opozicione ličnosti. To se najčešće postiže formiranjem armije trolova ili trol farmi, koje koordinisano djeluju i postavljaju određeni sadržaj s ciljem izazivanja reakcije publike. Primjeri se mogu naći i u Kini[42] i Iranu[43].

Kao što je već rečeno, informacione operacije uticaja nijesu ograničene na domaću sferu - često ciljaju i na stranu publiku u pokušaju da oblikuju međunarodnu percepciju i unaprijede geopolitičke interese režima. Kineske globalne IOU, na primjer, imaju za cilj promovisanje pozitivnog imidža zemlje i njene vlade, ali i umanjivanje važnosti pitanja ljudskih prava Ujgura, kao i forsiranje narativa koji su u skladu sa spoljnopolitičkim ciljevima Pekinga.

ProPublica je otkrila preko 10.000 lažnih Tviter naloga povezanih sa Komunističkom partijom Kine (KKP) uključenih u kampanju koordinisanog informacionog uticaja. Izvještaj je pokazao da su ti nalozi ciljali kineske disidente i pokušali da diskredituju proteste u Hong Kongu, uz kontinuirano objavljivanje dezinformacija o epidemiji korona virusa. [44]

Tokom 2019. godine u Hong Kongu su održani masovni protesti protiv prijedloga kineskog zakona o ekstradiciji, policijske burtalnosti i autoritarne vladavine. Pokrenuta je dezinformaciona kampanja na mrežama koja je bila usmjerena protiv protesta, na šta ukazuje i saopštenje Tvitera.[45] Uklonjeno je 936 naloga koji potiču iz Narodne Republike Kine, a koji su na kooridinisan način objavama pokušavali da kreiraju polarizaciju u društvu i podriju legitmitet i političku poziciju protesta u Hong Kongu. Pošto je Tviter blokiran u NR Kini, mnogi od tih naloga pristupili su Tviteru koristeći VPN. Međutim, neki nalozi su pristupali Tviteru sa određenih deblokiranih IP adresa koje potiču iz kontinentalne Kine. Nalozi koji su uklonjeni predstavljaju najaktivnije u pomenutoj kampanji i dio su veće mreže od približno 200.000 naloga.

Ipak, najpoznatiji primjer dolazi iz Rusije. Agencija za istraživanje interneta (IRA), ruska fabrika trolova, sa sjedištem u Sankt Peterburgu, povezana je sa ruskom vladom i zapošljava stotine plaćenih trolova koji preplavljuju društvene mreže proruskim sadržajem objavljenim pod lažnim indetitetima.[46]

Između 2013. i 2018. godine kampanje IRA-e na Fejsbuku, Instagramu i Tviteru dostigle su desetine miliona korisnika u Sjedinjenim Američkim Državama.


**MODUS OPERANDI IRA POČIVA NA ČETIRI STUBA[50]:**

**DISKREDITACIJA I NAPAD:** *američke institucije; kritičari Trampa; Demokratska partija na predsjedničkim izborima u SAD (2016) i na midterm izborima (2018); Emanuel Makron na francuskim izborima 2017; Hilari Klinton na predsjedničkim izborima u SAD 2016; Tereza Mej; američke vojne operacije na raznim lokacijama širom svijeta.*

**POLAZIRACIJA:** *američko društvo (na primjer, istovremeno podržavajući pokret Black Lives Matter i White Lives Matter), australijska politika; brazilska politika.*

**PODRŠKA:** *Desničarski pokreti u SAD; Alternativa za Nemačku (AfD) na njemačkim saveznim izborima (2017); referendum o Bregzitu; glasanje o nezavisnosti Katalonije; Donald Tramp na predsjedničkim izborima u SAD 2016.*

**PODRIVANJE I UMANJIVANJE PODRŠKE:** *aktivnosti usmjerene protiv Angele Merkel.*

Prema javno dostupnim podacima IRA je potrošila ukupno oko 100.000 dolara tokom dvije godine na reklame, što je zanemarljiv iznos s obzirom da su operativni troškovi IRA-e bili približno 1,25 miliona dolara mjesečno. Skoro 3.400 Fejsbuk i Instagram reklama koje je IRA kupila su takođe minorne u odnosu na preko 61.500 objava na Fejsbuku i 116.000 na Instagramu, uz 10 miliona tvitova koji su se širili pod maskom autentičnih korisničkih aktivnosti. Između 2015. i 2017. godine preko 30 miliona korisnika podijelilo je neke od lažnih objava sa Fesjbuka ili Instagrama sa svojim prijateljima i porodicom. Kako se navodi u izvještajima baziranim na osnovu Fejsbukovih podataka, aktivnosti IRA koje su širile dezinformacije o izbornom procesu i pospješivale podjele u društvu su dosegle mnogo više ljudi organski, nego putem plaćenih oglasa.[47]

Sadržaj se najčešće širi na način da alternativni ili mejnstrim mediji ili blogeri pod kontrolom države kreiraju dezinformacije i narative koje dalje šire bot i trol profili na svim kanalima, odnosno društvenim mrežama. Epilog je da pojedinci i grupe u digitalnoj sferi, bilo da su ideološki naklonjeni tom narativu ili samo spadaju u kategoriju korisnih idiota, dijele preuzete sadržaje. Na taj način organski podižu domet propagande, izlažući veliki broj ljudi istom sadržaju. U zavisnosti od lične ili grupne ideološke ili vrjednosne pozicije, ekstremno desni ili lijevi, blogeri ili teoretičari, uklapaju se u servirani narativ i dodaju svoje tvrdnje ili teze amplifikujući propagandu u korist kreatora.

Kako pokazuju podaci Fejsbuka dostavljeni Odboru za obavještajni rad Senata Sjedinjenih Američkih Država (SSCI) 2019. godine, jedna od stranica kreirana od IRA bila je i Crna Gora News Agency, usmjerena ka crnogorskoj javnosti. Cilj tih objava uglavnom je bio da diskredituju prozapadne subjekte i NATO.[48]

Kada je riječ o Crnoj Gori, političke partije strateški upotrebavaju bot naloge (kojima upravljaju ljudi) i trolove, a procjenjuje se da je 80% političkog sadržaja na društvenim mrežama i portalima njihovo djelo.[49]

## 4.2. **Nadzor**

Platforme društvenih mreža pružaju obilje podataka o aktivnostima i mišljenjima pojedinaca, što je postalo očigledno široj javnosti nakon afere Kembridž analitka.[51]

U aprilu 2018. godine, osnivač i izvršni direktor Fejsbuka Mark Zukenberg svjedočio je na dva kongresna saslušanja o ulozi svoje kompanije u skandalu Kembridž analitika, kada je otkriveno da je Fejsbuk izložio podatke blizu 87 miliona korisnika političkoj eksploataciji. Slučaj je eklatantan primjer kako se lični podaci sve više koriste da bi se uticalo na izborne ishode.

Jedna od primarnih metoda nadzora uključuje praćenje javnih objava i privatnih komunikacija na platformama društvenih mreža. Obzirom na obilje ličnih podataka i mišljenja koja se dijele na mrežama, te platforme pružaju bogat izvor informacija za režime koji žele da prate svoje građane. To varira od praćenja javnog raspoloženja i identifikovanja nezadovoljstava građana do izdvajanja pojedinaca koji izražavaju neslaganje ili protivljenje režimu. Istraživanja pokazuju, na primjer, da kineska vlada koristi digitalne alate za predviđanje događaja koji bi mogli da stvore žarišne tačke za nemire, a zatim preventivno primjenjuje represiju kako bi smanjila neslaganje prije nego što se nezadovoljstvo proširi[52].

***Ipak, najambiciozniji projekat masovnog nadzora i kontrole jeste kineski sistem socijalnog kredita, odnosno rejtinga, prema kojem svaki građanin ima numeričku vrijednost koja odražava njegov doprinos i korisnost za društvo u svim sferama života. Sistem počiva na velikoj količini ličnih podataka i proces je moguće sprovesti zahvaljujući oslanjanju građana na brojne onlajn i mobilne usluge. Ocjene mogu uticati na pristup određenim privilegijama kao što su putovanja, podizanje kredita, zapošljavanje i obrazovanje.***

SORM (Sistem za operativne istražne aktivnosti), sistem nadzora ruske vlade, prvobitno je razvio KGB za praćenje telefonskih poziva. Nadzor se proširio na internet kako bi pratili sadržaj mejlova, aktivnost pretraživanja interneta i druge digitalne podatke u okviru nove verzije poznate kao SORM-2. Do 2015. godine, ažurirana verzija — SORM-3 — obuhvatila je sve telekomunikacije. Prema ruskom zakonu, internet provajderi su obavezni da instaliraju SORM opremu koja omogućava ruskoj Federalnoj službi bezbjednosti (FSB) pristup svim podacima koji se dijele na mreži bez znanja ili kontrole kompanija o tome koji se podaci dijele i sa kim. SORM funkcioniše tako što u osnovi kopira sve tokove podataka na Internetu i telekom mrežama — šaljući jednu kopiju vladi, a drugu na željenu destinaciju.[53]

Uz pomoć vještačke inteligencije i mašinskog učenja, taj proces se može automatizovati i sprovoditi u velikim razmjerama, omogućavajući režimu da izgradi sveobuhvatne profile političkih stavova, ličnih veza i svakodnevnih rutina svojih građana.

S tim u vezi, postoje brojne rezerve kada je u pitanju korišćenje TikTok aplikacije van geografskih granica Kine. Sakupljanje podataka je norma za gotovo sve društvene mreže, ali pitanje koje se nameće jeste - ko ima pristup.

**U aprilu 2018. godine, osnivač i izvršni direktor Fejsbuka Mark Zukenberg svjedočio je na dva kongresna saslušanja o ulozi svoje kompanije u skandalu Kembridž analitika, kada je otkriveno da je Fejsbuk izložio podatke blizu 87 miliona korisnika političkoj eksploataciji. Slučaj je eklatantan primjer kako se lični podaci sve više koriste da bi se uticalo na izborne ishode.**

Kada je riječ o TikTok-u, česte su optužbe i navodi[54] da podaci globalnih korisnika završavaju u rukama Komunističke partije Kine (KPK), iako su to više puta demantovali iz te kompanije.[55]

Osim podataka o sadržaju, podaci o geolokaciji koji ostaju prilikom objavljivanja na mrežama su značajni za autoritarne režime. Putem njih može se pratiti kretanje pojedinaca ili grupa neistomišljenika i posebno je korisno za identifikaciju učesnika u protestima ili političkim skupovima.

## 4.3. Cenzura

Režimi često kontrolišu platforme društvenih mreža cenzurišući sadržaj koji je kritičan prema vladi ili koji dovodi u pitanje zvanični narativ. Ovo može uključivati blokiranje određenih korisnika, uklanjanje objava ili čak potpuno gašenje platformi.

Internet cenzura je možda najočigledniji način na koji autoritarni režimi koriste digitalne alate za represiju. Kina, na primjer, upravlja onim što je poznato kao Veliki zaštitni zid – trenutno najveći sistem cenzure na svijetu, zajednički poduhvat vlade, tehnoloških i telekomunikacionih kompanija koje rade zajedno na filtriranju sadržaja koje režim smatra štetnim.

Kina je osmu godinu zaredom bila najrepresivnija država na polju internet sloboda. Cenzura je pojačana tokom Olimpijskih igara u Pekingu 2022. godine i nakon što je teniska zvezda Peng Šuai optužila visokog zvaničnika Komunističke partije Kine (KPK) za seksualni napad. Vlada je nastavila da pooštrava kontrolu nad tehnološkim sektorom u zemlji, uključujući i nova pravila koja zahtijevaju da platforme koriste svoje sisteme za promovisanje ideologije KPK. Odvojeno, novinari, aktivisti za ljudska prava, pripadnici vjerskih i etničkih manjinskih grupa i ostali korisnici privedeni su zbog dijeljenja onlajn sadržaja, a neki su se suočili sa teškim zatvorskim kaznama.[56]

Posebno se obraća pažnja na izvještaje sa javnih skupova, partijskih sastanaka, kao i na vijesti o velikim praznicima. Zapravo, bilo kakvo veće okupljanje se smatra rizičnim, te su informacije o njima pod posebnom kontrolom. Ono na šta su kineski cenzori naročito osjetljivi su pokušaji povezivanja na inostrane društvene mreže poput Fejsbuka, Instagama ili Tvitera, te objavljivanje fotografija ili video zapisa sa političkom konotacijom.

Kineski ViČet primjenjuje automatsku cenzuru u realnom vremenu nad slikama koje se razmjenjuju putem čata. Kada se poruka pošalje od jednog korisnika drugom, ona prolazi kroz server kojim upravlja Tencent (matična kompanija ViČeta) koji otkriva da li poruka sadrži ključne riječi sa crne liste prije nego što se poruka pošalje primaocu.[57]

I sam tok istorije moguće je mijenjati takvim filtriranjem, a posebno su cenzurisani osjetljivi istorijski događaji koji se ne slažu sa zvaničnim državnim narativom. Informacije o protestu na Trgu Tjenanmen 1989. godine se ne mogu naći na Baidu Baike, kineskom ekvivalentu Vikipedije. Na pretragu termina 1989, dobijaju se samo dva rezultata: broj između 1988 i 1990 i naziv za kompjuterski virus. Svi ostali događaji iz 1989. su izbrisani iz evidencije, uključujući trenutak kada su vojnici Narodnooslobodilačke armije Kine otvorili vatru na civile u Pekingu nakon višemjesečnih studentskih protesta na Trgu Tjenanmen.[58]

***Tokom 1996. godine, kada je svega 150.000 Kineza bilo onlajn, Odlukom br. 159 Državnog savjeta eksplicitno se težilo stavljanju interneta pod državnu kontrolu. U posljednjih dvadeset godina, pravna i tehnička arhitektura Pekinga za veb cenzuru i nadzor dramatično je porasla. Iako je kineski predsjednik Si Đinping centralizovao kontrolu nad internetom 2013. godine (uglavnom kroz stvaranje Uprave za sajber prostor koja mu je odgovorna direktno) kineski internet prostor danas nadgleda preko šezdeset agencija sa ogromnom zakonskom i tehničkom sposobnošću da regulišu onlajn aktivnosti.***[59]

Osim Kine, Iran i Rusija nastoje da ograde građane od ostatka svijeta. Rusija je od usvajanja zakona o suverenom Internetu 2019. godine, konsolidovala svoju kontrolu nad infrastrukturom i intenzivirala blokiranje stranih platformi, VPN-ova i međunarodnih sajtova. Ostaje da se vidi koliko će vlada biti uspješna u postizanju tog cilja – zbog kombinacije političkih i posebno tehničkih faktora.[60] U Iranu, Nacionalna informaciona mreža centralizuje infrastrukturu pod državnom kontrolom, omogućavajući blokiranje skoro svih glavnih međunarodnih platformi i kontrolu domaćih komunikacijskih kanala.[61]

Pojedine države vrše sve veći pritisak na tehnološke kompanije da uklone sadržaj i podijele korisničke podatke, što se može vidjeti u izvještajima o transparentnosti koje objavljuju velike onlajn platforme. Javno dostupni podaci pokazuju da Fejsbuk, Gugl i Tviter najčešće dobijaju zahtjeve za uklanjanje sadržaja iz razloga nacionalne bezbjednosti, kritike vlasti i vjerskih uvreda. Između januara 2019. godine i juna 2020. godine samo tri zemlje koje se nalaze u prvih deset po broju zahtjeva za uklanjanje sadržaja iz navedenih razloga imaju punu slobodu interneta i kotiraju se kao demokratije – Ujedinjeno Kraljevstvo, Francuska i Njemačka.[62]

Tviter je primio 971 zahtjev od vlada i sudova, u periodu od 27. oktobra 2022. do 27. aprila 2023. godine. Zahtjevi su se kretali u rasponu od uklanjanja spornih objava do dostavljanja privatnih podataka za identifikaciju anonimnih naloga. Tviter je objavio da je u potpunosti ispunio zahtjeve u 808 i djelimično u 154 slučaja. Što se tiče devet zahtjeva, Tviter nije prijavio nikakav konkretan odgovor.

Ilon Mask je preuzeo Tviter obećavajući novu eru slobode govora i nezavisnosti od političkih pritisaka. Međutim, podaci pokazuju da je pod njegovom

**U Crnoj Gori je na dan parlamentarnih izbora 2016. godine ugašen pristup Vocap (WhatsApp) i Vajber (Viber) aplikacijama za komunikaciju zbog masovnog koordinisanog širenja negativnih poruka o navodnoj izbornoj krađi Demokratske partije socijalista, tada vladajuće partije, sa brojeva iz Kine i Velike Britanije[69]**

upravom, kompanija ispoštovala brojne zahtjeve za nadzor i cenzuru, posebno u zemljama kao što su Turska i Indija. U Indiji, koja mjesecima guši medije, novinare i kritičke glasove, Tviter je ispoštovao vladine zahtjeve za cenzurom sadržaja vezanog za BBC dokumentarac koji je bio veoma kritičan prema premijeru Narendru Modiju, a kojeg je u januaru blokirala indijska vlada. Iz te kompanije su se pravdali indijskim zakonima.[63] Prema izvještajima Reportera bez granica, sloboda štampe u Indiji je drastično opala, za osam poena u protekloj godini, i zemlja je bila na 150. mjestu na međunarodnoj listi.

Sa druge strane, u maju 2023. godine, dva dana prije izbora u Turskoj, Tviter je cenzurisao Erdoganove kritičare, što predstavlja ozbiljan presedan. Turska je zaprijetila da će onemogućiti pristup Tviteru u zemlji, ukoliko ne ukloni sadržaj sa nekoliko naloga.[64]

U godini prije Maskovog preuzimanja, stopa usklađenosti sa prijavama i zahtjevima vlada se kretala oko 50%. Nakon Maskovog preuzimanja, taj procenat se povećao na 83% (808 zahtjeva od ukupno 971). Naredbe se veoma razlikuju po obimu i predmetu, ali sve uključuju vladu koja traži od Tvitera da ili ukloni sadržaj ili otkrije informacije o korisniku.

***Iako Fejsbuk, Gugl i Tviter najčešće dobijaju zahtjeve za uklanjanje sadržaja iz razloga nacionalne bezbjednosti ili kritike vlasti, često dolazi i do pogrešnih poteza samih mreža, što rezultira direktnim kršenjem ljudskih prava. Fejsbuk (sada Meta) je priznao da je napravio greške u uklanjanju sadržaja u vezi sa protestima 2021. godine protiv iseljavanja Palestinaca iz njihovih domova u okrugu Šeik Jara u Jerusalimu. U eksternom izvještaju za potrebe Mete, u pomenutom slučaju, navodi se da su akcije uklanjanja sadržaja od strane Mete imala negativan uticaj na prava palestinskih korisnika na slobodu izražavanja, slobodu okupljanja, političko učešće i nediskriminaciju, a samim tim i na sposobnost Palestinaca da dijele informacije i uvide u njihova iskustva kako su se dogodila.[65] Navodi se i da je Meta brisala mnogo više objava o konkretnom slučaju na arapskom nego na hebrejskom jeziku. Takođe, prošlogodišnji izvještaj Amnesti internešnala (Amnesty International) ukazuje da su algoritmi te mreže podsticali širenje štetnog sadržaja protiv Rohinja muslimana u Mjanmaru, što je doprinijelo nasilju u stvarnom svijetu.***[66]

Sa napretkom AI, poboljšala se i sposobnost autokratija[67] da sprovode cenzuru. AI može da pregleda slike i tekst na sofisticirane načine, dozvoljavajući režimu da filtrira i blokira sadržaj koji se smatra nedozvoljenim.

Čak i ako takva cenzura ne da rezultate, autokratije imaju dodatnu liniju odbrane: mogu da ugase pristup internetu – u cjelini ili u djelovima – kako bi spri-

ječile građane da komuniciraju, organizuju se ili dijele poruke. Primjeri ove te taktike su brojni. Podsjećamo na primjere kada je ruska vlada koristila ciljano gašenje mobilnog interneta tokom antivladinih protesta u Moskvi 2019. godine ili kada je iranska vlada uspješno ugasila pristup internetu širom zemlje usred rasprostranjenih protesta u novembru 2019.[68]

U roku od nekoliko nedjelja nakon invazije na Ukrajinu Kremlj je blokirao Fejsbuk, Instagram i Tviter zbog ekstremizma, onemogućavajući stanovništvu pristup pouzdanim informacijama o ratu i ograničavajući njihovu mogućnost da se povežu sa korisnicima u drugim zemljama. Platforme su blokirane nakon što je iz Mete navedeno da će dozvoliti korisnicima društvenih mreža u Ukrajini da objavljuju poruke u kojima se poziva na nasilje protiv ruskog predsjednika Vladimira Putina i ruske vojske, kao i veličanje bataljona Azov. To predstavlja uspostavljanje dvostrukih standardna i kršenje sopstvenih pravila i politike koji se tiču govora mržnje. Najveće društvene mreže i tehnološke kompanije poput Fejsbuka (odnosno njegove matične kompanije Meta), Tvitera i Gugla su se priključile sankcijama EU protiv Sputnika i Raša Tudej (RT) i uklonile naloge tih medija sa njihovih platformi. Takve poteze su mnogi pozdravili, ali su istovremeno borci za slobodu govora, čak i unutar Rusije, upozorili na opasne posljedice pomenutih odluka, navodeći veću cenzuru u drugim nedemokratskim zemljama, dok se istovremeno onemogućuje pristup nezavisnim izvorima informacija. U fazi pisanja ove studije, nalozi ta dva ruska državna medija su dostupni na Tviteru.

Blokiranje platformi rezultiralo je većom upotrebom domaćih mreža – VK i Odnoklassniki. Yandex, popularni ruski pretraživač i pandan Gugla, prema javno dostupnim informacijama, dao je prioritet dezinformacijama i smanjio rezultate pretrage za sajtove koji su kritikovali invaziju. Vlada je takođe blokirala više od 5.000 vebsajtova, primorala medije da invaziju nazovu specijalnom vojnom operacijom i uvela zakon koji propisuje do 15 godina zatvora za one koji šire lažne informacije o sukobu.[70]

Uprkos činjenici da je internet cenzura zarobila digitalni prostor, milioni Rusa su se opredjelili za VPN servise i dark web kako bi zaobišli vladine restrikcije. Surfshark, VPN kompanija iz Litvanije, zabilježila je da je korišćenje njihovog VPN servera povećano za 3500% samo od početka invazije, 24. februara 2022. Najveći skok se dogodio 5. i 6. marta te godine, saopštila je kompanija, kada je Rusija najavila da će preduzeti mjere da blokira pristup Tviteru i Fejsbuku.[71]

U periodu epidemije korona virusa (2020-2021), brojni autoritarni režimi su uveli zakone pod maskom borbe protiv dezinformacija i infodemije.[72] Zemlje poput Irana, Rusije, Egipta, Venecuele, Bjelorusije, Kine i Kambodže preduzele su korake u borbi protiv opozicije i onih koji se ne slažu sa državnim narativom.[73] Tako je bloger iz Ruande osuđen na 10 godina zatvora zbog optužbi za podsticanje na građansku neposlušnost i širenje glasina, a u Bangladešu se medijski aktivista suočio sa zatvorskom kaznom do sedam godina zbog navodnog širenja lažnih vijesti protiv vlade.[74]

Nakon usvajanja novog restriktivnog zakona 2020. godine, kompanije kao što su Fejsbuk, Tviter i Jutjub bile su prinuđene da otvore kancelarije u Turskoj koje bi se pridržavale vladinih zahtjeva za uklanjanje sadržaja. Takođe, u okto-

bru 2021. godine, Turski parlament je usvojio zakon kojim je uvedena kazna zatvora do tri godine za pojedince za koje se smatra da promovišu lažne informacije na društvenim mrežama.[75] Osim, što omogućava državi da bude arbitar istinitosti, zakon zahtijeva od društvenih mreža da predaju lične podatke korisnika za koje se sumnja da šire lažne vijesti.[76]

## 4.4. **Uznemiravanje, zastrašivanje, diskreditacija**

Režimi mogu da koriste društvene medije da uznemiravaju, zastrašuju ili prijete kritičarima. To može uključivati doxxing (javno otkrivanje privatnih informacija o pojedincu), uznemiravanje na mreži ili čak prijetnje nasiljem. U izvještaju Oksfordovog internet instituta iz 2020. godine navodi se da su u pedeset devet zemalja pronađeni dokazi da se trolovi koriste za napad, doksovanje (doxxing) i uznemiranje političkih protivnika, aktivista ili novinara na društvenim mrežama. [77]

Osim što su kreirani za širenje dezinformacija i pospješivanje dometa državne propagande, bot i trol mreže mogu se usmjeriti na targetiranje pojedinaca ili grupa koji su kritičari režima.

Putem sredstava nadzora mreža mogu se identifikovati disidentski glasovi koji onda mogu biti meta uznemiravanja i na mreži i van mreže. Takav nadzor često ide ruku pod ruku sa zastrašivanjem, pri čemu režimi koriste zakone da bi suzbili slobodu govora i kaznili kritičare lišavanjem slobode, fizičkim i onlajn nasiljem.

# 5. Uticaj na demokratiju: razlozi za zabrinutost

Jedan od osnovnih stubova demokratije jeste slobodan protok pouzdanih i tačnih informacija. Danas se on uglavnom dešava onlajn, na platformama društvenih mreža koje su postale okosnica digitalnog informacionog ekosistema. Od 2016. godine je kroz više dokumentovanih slučajeva postalo evidentno da se tehnološki razvoj može efektivno i efikasno koristiti za degradaciju demokratskih sistema, vrijednosti i društava.

Informacione operacije uticaja su u velikoj mjeri omogućene algoritamskom dinamikom na koju se oslanjaju preporuke za sadržaj na društvenim mrežama, koji daju prioritet emocionalnom sadržaju koji će vjerovatno privući pažnju korisnika, zauzvrat promovišući senzacionalističke, često netačne informacije, dok istovremeno zaključavaju korisnike u eho komore, gdje se gubi dodir sa realnošću.[78] Razvoj generativnih tehnologija baziranih na vještačkoj inteligenciji, koje omogućavaju kreiranje realističnih audio, foto i video sadržaja će samo ubrzati taj trend.

Prethodna 2022. godina je obilježila šesnaestu uzastopnu godinu globalnog demokratskog pada.[79] Sa širenjem metoda, tehnika i pristupa za digitalni autoritarizam, nove tehnologije su upumpale novi život i osnažile autoritarizam i lidere koji svoju vladavinu održavaju na tim vrijednostima.

Razumijevanje i suočavanje sa digitalnim autoritarizmom ključni su kako za zaštitu individualnih sloboda, tako i za očuvanje integriteta demokratskih institucija i procesa.

## 5.1. Očuvanje demokratije i demokratskih vrijednosti

Digitalni autoritarizam predstavlja značajnu prijetnju demokratiji, što je vidljivo kroz brojne dokumentovane slučajeve miješanja autoritarnih režima u izbore u demokratskim državama, plasiranjem dezinformacija i stvaranjem podjela posredstvom platformi društvenih mreža. Takve prakse ne samo da mogu narušiti povjerenje u demokratske institucije i procese, već potencijalno mogu uticati na ishod izbora. Neki autoritarni režimi izvoze svoje prakse digitalnog autoritarizma u druge zemlje, utičući na taj način na globalne norme i standarde u vezi sa upravljanjem internetom i digitalnim pravima. Razumijevanje tih taktika i razvijanje efikasnih protivmjera je od ključnog značaja za očuvanje demokratije. Alate, tehnike i strategije digitalnog autoritarizma usvajaju u demokratskim zemaljama političke partije, interesne grupe i privatne kompanije na štetu javnog povjerenja, lične privatnosti i drugih građanskih sloboda.

Na suptilan i istovremeno direktan način autoritarne vlade koriste globalni informacioni prostor kako bi podrivale vrijednosti i institucije koje su u osnovi međunarodnog poretka zasnovanog na pravilima, diskreditujući ideju demokratije nastojeći da oslabe demokratske norme. Targetiranje demokratije za autoritarne režime je pitanje opstanka njihovih mehanizama upravljanja i vrijednosti za koje smatraju bi trebale biti u osnovi međunarodnog sistema u budućnosti.[80] Infodemija povezana sa pandemijom COVID-19 pružila je dalje mogućnosti za te sisteme da dodatno podstaknu podjele i međusobno se podrže u širenju narativa onda kada je to strateški korisno radi slabljenja demokratske kohezije. U širenju teorija zavjere o porijeklu virusa, kineski, iranski i ruski zvaničnici i mediji su međusobno retvitovali sadržaje koje su iznijele organizacije, mediji i nalozi povezani sa njihovim vladama.[81] Sa druge strane, talas populističkih ili neliberalno nastrojenih političkih partija i vođa u hibridnim režimima i demokratijama sve više preuzimaju pristup politici od autokratskih režima. Oni podrivaju institucije, odbacuju kritičare i iskorišćavaju digitalne platforme da bi širili propagandu i dezinformacije. Manipulišu političkim javnim mnjenjem i ne libe se da traže podršku i od ekstremnih grupa i aktera, kako u državi tako i van nje.

**Sloboda govora, sloboda okupljanja i pravo na privatnost su temeljna ljudska prava koja mogu biti ugrožena digitalnim autoritarizmom**

## 5.2. Zaštita ljudskih prava i sloboda

Sloboda govora, sloboda okupljanja i pravo na privatnost su temeljna ljudska prava koja mogu biti ugrožena digitalnim autoritarizmom. Internet je dugo vremena služio kao platforma za slobodu govora i slobodnu razmjenu ideja. Međutim, digitalni autoritarizam prijeti toj slobodi, budući da režimi mogu manipulisati onlajn diskursima, raspravama i suzbijati disidentske glasove. Sa pojavom sofisticiranih tehnologija nadzora, autoritarni režimi mogu pratiti aktivnosti svojih građana. To krši pravo na privatnost i može imati ozbiljne

posljedice na slobodu izražavanja, odnosno dovesti do autocenzure usljed straha. Osim toga, kroz zloupotrebu društvenih mreža, režimi mogu manipulisati javnim mnjenjem i podacima, kršeći pravo pojedinaca na pristup tačnim i nepristranim informacijama. Napredak AI omogućio je i efektivnije metode kontrole.  Rizik upotrebe novih tehnologija za potiskivanje ili kontrolu povećava se, posebno u vremenima društveno-političkih tenzija, izbora, protesta, demonstracija, oružanih sukoba ili drugih vrsta kriza, kao što je pandemija. Najizloženiji su branioci ljudskih prava i drugi aktivisti civilnog društva, uzbunjivači, nezavisni novinari, politička opozicija, kao i rasne i etničke manjine.

## 5.3. **Bezbjednost**

Taktike koje koriste digitalni autoritarni režimi, uključujući kampanje hakovanja, nadzora i dezinformacija, mogu predstavljati značajne bezbjednosne rizike. To može imati implikacije ne samo na pojedince, već i na kompanije, organizacije, pa  i vlade. Autoritarni režimi proširuju domet svojih digitalnih alata u inostranstvu, otvoreno povećavajući nadzor nad svojim, ali i građanima drugih zemalja.

## 5.4. **Informacioni integritet**

U razdoblju kada informacije u velikoj mjeri primamo putem društvenih mreža, širenje dezinformacija može imati ozbiljne posljedice: obmanjivanje javnosti, ometanje donošenja odluka na osnovu činjenica i pospješivanje postojećih podjela u društvu. Upotreba društvenih medija za širenje dezinformacija može imati značajan uticaj na javni diskurs u demokratijama, ali i na cjelokupno društvo, budući da podriva integritet odluka. To može dovesti do polarizacije i raslojavanja društva, što otežava postizanje konsenzusa i direktno utiče na sposobnost demokratskih društava da se efikasno suoče sa izazovima.

## 5.5. **Socijalna kohezija**

Digitalni autoritarizam često uključuje korišćenje zapaljivog sadržaja radi manipulacije javnim mnjenjem i stvaranja podjela. To može dovesti do povećane polarizacije i konflikta, čime se narušava socijalna kohezija. Autoritarni režimi mogu koristiti digitalne alate da bi uticali izvan svojih granica, oblikujući globalne narative i norme na načine koji služe njihovim geopolitičkim interesima. Takođe mogu izvoziti tehnologije nadzora i cenzure drugim zemljama, doprinoseći time globalnom širenju autoritarnih praksi.

# 6. Odgovori na izazov

Obezbjeđivanje slobode interneta je ključno za zaštitu demokratije, jer tehnologija treba da osnaži građane da donose odluke svjesno, na bazi činjenica, bez prisile ili manipulacije. Društvene mreže postale su značajne javne platforme sa ogromnom moći i odgovornošću da služe javnom dobru. Međutim, godinama unazad, uz krizu liberalnog demoratskog poretka, nailazimo na rastuće tendencije autoritarnih režima da zloupotrijebe tehnologiju za sopstvene potrebe, kako unutar, tako i van zemlje, direktno podrivajući demokratske procese širom svijeta.

Da bi se zaštitila demokratija u 21. vijeku, tehnološke kompanije, vlade i civilno društvo moraju da sarađuju na rješavanju problema manipulacije, zloupotreba i prikupljanja podataka. To zahtjeva multilateralnu i međusektorsku koordinaciju za promovisanje digitalne pismenosti, identifikaciju zlonamjernih aktera i sprječavanje i eksponiranje njihovog djelovanja koje krši ljudska prava, pravila digitalnih platformi i podriva procese unutar demokratija.

S tim u vezi, postoji široko rasprostranjeno mišljenje da tehnološke kompanije moraju da učine više kako bi spriječile informacione operacije uticaja, vodeći računa da svojim djelovanjem ne ograniče slobodu govora, odnosno ne krše osnovna ljudska prava.

Napori da se razotkriju dezinformacije i objelodane informacione operacije uticaja na platformama društvenih mreža postaju sve snažniji posljednjih godina, ali se u vezi sa tim otvaraju brojna pitanja primjene, dosljednosti i transparentnosti.[82]

Jedna od primarnih strategija koja koristi društvene mreže je upotreba algoritama mašinskog učenja za identifikaciju i označavanje potencijalno obmanjujućeg sadržaja.[83] Ti algoritmi mogu analizirati tekst, slike i video zapise u potrazi za dezinformacijama i teorijama zavjere. Neke platforme će u potpunosti ukloniti sporni sadržaj, dok će ga druge označiti kao potencijalno ob-

manjujući i smanjiti njegovu vidljivost. Ipak, biće potrebno određeno vrijeme da se algoritam dovoljno usavrši i istrenira za sve jezike podjednako kako bi efikasno prepoznavao i uklanjao sadržaj i sa našeg govornog područja.

Pored automatizovane detekcije, platforme poput Fesjbuka takođe su zaposlile timove za provjeru činjenica koji pregledaju označeni sadržaj, često u saradnji sa spoljnim organizacijama za fektčeking. Ako se utvrdi da je sadržaj lažan ili obmanjujući, može se označiti kao takav, pružajući korisnicima više konteksta i pomažući da se ograniči širenje neistina.[84]

Nakon dokumentovanih slučajeva u kojima je Fesjbuk služio kao posrednik za miješanje u izbore, ta i ostale platforme su posvetile više pažnje načelu transparentnosti. U kontekstu političkog marketinga, Fejsbuk je onemogućio plasiranje plaćenih političkih oglasa van matične zemlje finansijera reklame. Dodatno, javno dostupna postala je i biblioteka oglasa (Facebook Ads Library). Ona omogućava svima da pretražuju i gledaju aktivne i neaktivne oglase o društvenim pitanjima, izborima ili politici, a koji su pokrenuti na Fejsbuku ili Instagramu. Biblioteka sadrži detalje kao što su sadržaj oglasa, ko ga je platio, količinu potrošenog novca, broj dosegnutih ljudi i demografske podatke o tome ko je targetiran. Ta funkcija je posebno korisna za novinare, istraživače i sve zainteresovane zbog boljeg uvida u obim i prirodu političkog oglašavanja i onlajn kampanja. Takođe, omogućava regulatornim tijelima i istraživačima da prate tokove novca i identifikuju sa njima povezane trendove.[85]

***Meta, Tiktok, Tviter i Gugl godinama periodično objavljuju izvještaje transparentnosti (transparency reports). To su dokumenti koji omogućavaju uvid u različite aspekte njihovog poslovanja, posebno u oblastima koje se odnose na moderiranje sadržaja, vladine zahtjeve za korisničkim podacima i uklanjanjem sadržaja i sprovođenje standarda ili smjernica njihove zajednice (community standards).***

U tom kontekstu veoma su značajne mjere mreža koje tretiraju koordinisano neautentično djelovanje i informacione operacije uticaja kojima je cilj postizanje veće transparentnosti i autentičnosti. Nije dozvoljeno lažno predstavljanje, korišćenje lažnih naloga, vještačko neorgansko povećavanje popularnosti sadržaja kroz upotrebu bot mreža ili upuštanje u ponašanja koja vode drugim kršenjima standarda zajednice, odnosno pravila platformi. S tim u vezi, zainteresovani pojedinci, istraživači i mediji mogu pronaći javno dostupne podatke u kvartalnim izvještajima koje platforme objavljuju.[86] Da je velika trojka (Fejsbuk, Instagram i Tviter) podložna manipulacijama, pokazuje i podatak da su od 2018. godine označili i ukinuli preko 350 koordinisanih napora i informacionih operacija uticaja.[87] Ipak, veliki problem je dosljednost i efikasnost mjera u borbi protiv manipulacija i kooridinisanog ponašanja, budući da kupovina neautentične podrške na platformama ostaje jeftina i dostupna, a procenat identifikovanih i uklonjenih naloga, koji se koriste za takve operacije, se smanjuje.[88]

**Napori da se razotkriju dezinformacije i objelodane informacione operacije uticaja na platformama društvenih mreža postaju sve snažniji posljednjih godina**

Iako društvene mreže preduzimaju korake da podstaknu transparentnost i odgovornost, specifičnosti i učinkovitosti mjera mogu značajno da variraju od jedne do druge kompanije.[89] Otkako je Ilon Mask preuzeo Tviter, mnogi su ga optužili da podstiče širenje dezinformacije na platformi.[90] Kritika je uslijedila nakon što je Mask vratio ranije suspendovane ili zabranjene naloge, od kojih su neki bili čak i kažnjeni zbog širenja dezinformacija, teorija zavjere ili govora mržnje. Nerijetko, Mask na svom nalogu dijeli sadržaj upitne vjerodostojnosti.[91]

Osim društvenih mreža, Gugl ulaže napore u suzbijanju dezinformacija, izgradnji kapaciteta novinara i fact-checking udruženja. Nakon što je preko 80 fact-checking organizacija u januaru uputilo pismo[92] Jutjubu, ističući da je ta platforma jedan od glavnih kanala za širenje dezinformacija i teorija zavjere, što omogućava zloupotrebu platforme, Gugl (koji je vlasnik Jutjuba) je najavio donaciju od 13 milona dolara Međunarodnoj mreži za provjeru činjenica (IFCN), kojom će se finansirati formiranje Globalnog fonda za provjeru činjenica.[93]

Takođe, Gugl u kontinuitetu ažurira svoje algoritme za pretragu kako bi osigurao da se pouzdane informacije rangiraju više u rezultatima pretrage. Pored toga, kada korisnici pretražuju temu koja je netačna, Gugl pruža informacije od fact-checking organizacija pored rezultata pretrage. Kompanija sarađuje i sa spoljnim organizacijama kako bi se obezbijedila obuka i resursi za novinare i pružila podrška programima medijske pismenosti.

Pod pokroviteljstvom Evropske unije, niz kompanija i platformi je 2022. godine potpisalo Osnaženi kodeks u borbi protiv dezinformacija, s ciljem sprječavanja proliferacije lažnih vijesti, kao i povećanja transparentnosti i suzbijanja širenja botova i lažnih naloga.[94]

***Tviter je, na čelu sa Maskom, u maju 2023. godine napustio taj Sporazum,[95] pa je moderacija na Tviteru navodno uveliko smanjena, što je, kako pokazuju istraživanja, omogućilo povećano širenja dezinformacija. Tviter je ranije imao namjenski tim koji je radio na borbi protiv koordinisanih kampanja dezinformacija, ali stručnjaci i bivši zaposleni ističu da je većina njih dala ostavke ili je otpuštena.[96]***

Osim dobrovoljnog kodeksa, EU je donijela i Akt o digitalnim uslugama (Digital Service Act - DSA) – zakon koji će od avgusta 2023. godine pravno obavezivati kompanije da učine više u borbi protiv nelegalnog onlajn sadržaja. Akt, između ostalog, ima za cilj da podstakne pažljivije i transparentnije moderiranje sadržaja, poveća odgovornost platformi za informacije koje plasiraju i smanji dezinformacije. Potpuna primjena očekuje se sredinom februara 2024. godine. Dokument će obavezivati sve kompanije koje pružaju usluge u Evropskoj uniji bez obzira na to da li su osnovane na njenoj teritoriji ili ne. DSA predstavlja značajan iskorak, budući da je EU odlučila da preduzme korake u rješavanju problema širenja dezinformacija, govora mržnje i drugih protivzakonitih sadržaja putem društvenih mreža i velikih platformi za komunikaciju. Radi nadgledanja sprovođenja Akta, biće osnovana regulatorna Komisija koja će moći izricati sankcije – od novčanih kazni u iznosu od najviše 6 odsto globalnog prihoda kompanije, do privremene suspenzije pristupa platformi na nivou EU.[97]

Istovremeno, u fokusu će biti privatnost i zaštite podataka. Tako je Opšta uredba Evropske unije o zaštiti podataka (GDPR) uticala na uspostavljanje novih standarda koji se odnose na privatnost podataka i davanje korisnicima više kontrole nad njihovim ličnim podacima. Neke kompanije društvenih mreža su takođe promijnile svoja podešavanja privatnosti i prakse podataka kao odgovor na pritisak javnosti i regulatornu kontrolu.[98]

Nakon dvije godine rada i višemjesečnih pregovora, zakonodavci Evropske Unije su postigli dogovor i objavili Nacrt Zakona o vještačkoj inteligenciji. Uvidom u prijedloge akta, AI alati će biti klasifikovani prema njihovom percipiranom nivou rizika: od minimalnog do ograničenog, visokog i neprihvatljivog. Visokorizični AI sistemi uključuju one koji utiču na birače prilikom izbora i AI sisteme društvenih mreža za rangiranje i plasiranje sadržaja.[99] Pored navedenih, postoji i niz drugih relevatnih EU instrumenata u borbi protiv dezinformacija.

Osim internih napora kompanija i društvenih mreža, postoje organizacije posvećene borbi protiv dezinformacija i informacionih operacija uticaja na mreži. Riječ je o neprofitnim organizacijama, istraživačkim grupama i novinarskim organizacijama. One nadgledaju platforme društvenih mreža u potrazi za obmanjujućim sadržajem, izvještavaju o nalazima a nerijetko rade direktno sa platformama na rješavanju problema. Fejsbukova parcijalna dijeljenja podataka sa istraživačkim organizacijama poput DFRLab i Stanford Internet Observatory pomogla su da se podigne svijest o uticaju, dometu i načinu sprovođenja informacionih operacija koje realizuju brojni autoritarni režimi i akteri.

Ipak, na globalnom nivou postoji jasan disparitet u resursima između onih koji sprovode IOU i civilnog društva koje pokušava na njih da ukaže. Tim organizacijama nedostaju resursi za monitoring, analizu i suprotstavljanje malignim aktivnostima, a njihovo djelovanje je često usporeno ili otežano lokalnim političkim elitama koje i same šire dezinformacije. Važno je istaći da bi društvene mreže pojačanom saradnjom, transparentnošću i dijeljenjem podataka sa zainteresovanim stranama mogle efektivnije i dalekosežnije osvijetliti problem zloupotrebe mreža na različitim geografskim područjima.

Uprkos svim naporima, zloupotrebe na mrežama ostaju značajan izazov, pogotovo usljed nesrazmjerne primjene mjera na ne-engleskim govornim područjima.[100] Činjenica je i da količina sadržaja, globalni domet platformi i brzina kojom se dezinformacije mogu širiti doprinose složenosti ovog pitanja, što bi trebalo da obaveže mreže na proaktivnije djelovanje.

Još uvijek je rano govoriti da li će uključivanje EU i prepoznavanje problema doprinijeti rješavanju na međunarodnom planu, ali preduzete mjere predstavljaju važne korake, iako ostaje upitna implementacija na globalnom nivou.[101]

# 7. Zaključak

Sa porastom globalne upotrebe masovnih sredstava komunikacije u 21. vijeku, došlo je do zaokreta u načinu, brzini i mogućnostima razmjene informacija. Iako je početkom prethodne decenije vladalo uvjerenje o neminovnoj dezintegraciji autoritarnih režima, nakon nekoliko primjera upotrebe društvenih mreža u izvođenju značajnih društveno-političkih promjena, ta premisa se pokazala utopijskom i naivnom.

Sasvim suprotno, digitalni autoritarizam ukazao je na sposobnost pojedinih režima da se, ne samo adaptiraju, već i da preoblikuju ravnotežu moći između demokratija i autokratija, zloupotrebom društvenih mreža i iskorišćavanjem imanentnih slabosti demokratija da brzo i uniformno reaguju na rastuće izazove.

Predvodnici tog trenda su Rusija, Iran i Kina koje su razvile savremene metode kontrole, manipulacije, nadzora i cenzure prvo za potrebe unutar svojih geografskih granica, a zatim i za informacione operacije širom svijeta.

Propaganda i dezinformacije koje se šire na internetu i društvenim mrežama produbljuju društvenu polarizaciju, zaoštravaju etničke tenzije, raspiruju nacionalizam, slabe povjerenje javnosti u medije, novinarstvo, javne institucije, demokratske procese i vode ka krizi liberalne demokratije. Toj regresiji svjedoče i međunarodni izvještaji koji podvlače da internet i demokratija postaju sve više defanzivni i sve manje slobodni širom svijeta.

Motivacija za takvo djelovanje nije samo konsolidacija, kontrola i učvršćivanje vlasti, već jačanje imidža autoritarnih režima na međunarodnom nivou i pospješivanje nepovjerenja u demokratiju, vladavinu prava, kao i iskorišćavanje i jačanje postojećih društvenih, političkih i ekonomskih podjela. Diskreditacija tih vrijednosti i principa je direktno povezana sa opstankom pojedinih autoritarnih režima. S tim u vezi postoji rastući broj dokaza o koordinaciji i saradnji Moskve i Pekinga na širenju anti-zapadnih narativa i međusobnom preuzimanju taktika.

U sve većem broju zemalja prekidi mreže i druge represivne akcije koje ometaju pristup informacijama olakšane su naporima da se ostvari suverena kontrola odnosno suvereni internet. Određene zemlje su usvojile mjere za kontrolu protoka podataka i izolovanje domaćeg interneta sa globalne mreže. Na-

metanje novih ograničenja na prekogranični prenos i skladištenje podataka, kao i centralizovanje tehničke infrastrukture, omogućava vlastima potpunu kontrolu nad informacionim prostorom i sadržajem koji njihovi građani primaju, pogotovo u kontekstu domaćih i međunarodnih previranja. Takve prakse otvaraju prostor za kršenje osnovnih ljudskih prava, širenje nadzora, cenzure i lakši pristup korisničkim podacima kroz usvajanje rigoroznih zakona.

Iako se često može čuti da primarnu odgovornost snose društvene mreže, one ne mogu biti isključivo odgovorne, uprkos ulozi koju imaju u omogućavanju digitalnog autoritarizma. Bez obzira na nedosljednosti, te platforme su postale proaktivnije u identifikaciji i uklanjanju koordinisanog neautentičnog ponašanja koje potiče od državnih ili sa njima povezanih aktera. Posljednjih godina se kroz afirmaciju načela transparentnosti, putem javno dostupnih podataka, izvještaja i uvida u reklamiranje, radi na podizanju svijesti o postojanju i uticaju zloupotrebe mreža.

Evropska unija se, kao geopolitički važan akter, kroz nekoliko akata i dokumenata uključila aktivno pokušavajući doprinijeti rješavanju problema, primarno na nivou Evrope. Ipak, za konkretne rezultate novih zakonskih rješenja će biti potrebno dodatno vrijeme. Takođe, sve je više organizacija civilnog društva koje igraju značajnu ulogu u osvjetljavanju informacionih operacija uticaja kroz OSINT istraživanja.

Te aktivnosti bi trebale ispratiti nacionalne vlade predlaganjem novih zakona o zaštiti ličnih podataka, koji će biti ažurirani za digitalno doba, što bi otežalo svim akterima da pristupe podacima pojedinaca i da ih koriste za informacione operacije uticaja. Osim toga, bezbjednosni sektor svake države bi mogao ostvariti konkretnu saradnju i razmjenu informacija sa platformama o operacijama autoritarnog uticaja i drugim akcijama koje ciljaju na demokratski integritet unutar samih država.

Demokratije su godinama kasnile u osmišljavanju sveobuhvatnih odgovora na ove kompleksne izazove. Kao što su trendovi koji su doveli do informacione i krize liberalne demokratije pokazali, imperativ je da odgovor bude višedimenzionalan. Stoga bi kombinacija javno-privatnog partnerstva, medija i civilnog sektora trebala imati opredjeljujuću ulogu u budućem definisanju i sprovođenju uniformnog odgovora. U međuvremenu, autoritarni režimi će nastaviti da pritiskaju, bez obzira da li su demokratije u stanju da pronađu efikasan odgovor ili ne.[102]

Iz svega izloženog, nameće se zaključak da je najbolji način za suprostavljanje autoritarizmu svake vrste da se njeguju, brane i afirmišu demokratske vrijednosti, vladavina prava, slobodni i fer izbori, sloboda govora, kao i nezavisnost i profesionalnost medija. Ako demokratije ne uspiju da odbrane sopstvene tekovine, principe i interese sa jednakom odlučnošću kojom ih autoritarni režimi napadaju, digitalni autoritarizam će postati nova normalnost.

# 8. Reference


**1** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**2** Putin calls for balanced assessment of Stalin, 03.12.2009, Reuters, Dostupno na:https://www.reuters.com/article/idUSGEE5B21J6

**3** Repucci, S, Slipowitz, A, Freedom in the world 2022 The Global Expansion of Authoritarian Rule, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-03/FITW_World_2022_digital_abridged_FINAL.pdf

**4** Kalathil, S, The Evolution of Authoritarian Digital Influence: Grappling with the New Normal, National Defense University Press, News Article View (ndu.edu), Dostupno na: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=DJRX5DRHKfqeXbyt6et98w%3D%3D

**5** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**6** Trajković, I, Kineski digitalni zid za suvereni državni internet, 25.07.2022, Al Jazeera, Dostupno na: https://balkans.aljazeera.net/news/technology/2022/7/25/kineski-digitalni-zid-za-suvereni-drzavni-internet

**7** Wong, B, Bottorff, C, Top Social Media Statistics And Trends Of 2023, 18.05.2023, Forbes, Dostupno na: https://www.forbes.com/advisor/business/social-media-statistics/#:~:text=In%202023%2C%20an%20estimated%204.9,5.85%20billion%20users%20by%202027

**8** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**9** EU citizens trust traditional media most, new Eurobarometer survey finds, 12.07.2022, European Parliament, Dostupno na: https://www.europarl.europa.eu/news/en/press-room/20220704IPR34401/eu-citizens-trust-traditional-media-most-new-eurobarometer-survey-finds

**10** Newman N, Fletcher, R, Robertson, C, Eddy, K, Nielsen, R, Digital News Report 2022, Reuter Institute and University of Oxford, Dostupno na: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf

**11** Kemp, S, Digital 2023: Global Overview Report, 26.12.2023, Datareportal, Dostupno na: https://datareportal.com/reports/digital-2023-global-overview-report

**12** Tradicionalni mediji dominantno oblikuju politička uvjerenja crnogorskih građana, 29.05.2023, CeMI, Dostupno na: https://cemi.org.me/me/post/tradicionalni-mediji-dominantno-oblikuju-politicka-uvjerenja-crnogorskih-gradana-1090

**13** Medijska pismenost i građani Crne Gore Istraživanje javnog mnjenja, maj 2023, Digitalni forenzički centar, https://dfcme.me/wp-content/uploads/Istrazivanje-javnog-mnjenja-2023-2.pdf

**14** The Attention Economy Why do tech companies fight for our attention?, 17.08.2021, Center for Humane Technology, Dostupno na: https://www.humanetech.com/youth/the-attention-economy

**15** Kavenna, J, Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy', 4.10.2019, Guardian, Dostupno na: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

**16** Deibert, R, The Road to Digital Unfreedom: Three Painful Truths About Social Media, Januar 2019, Journal of Democracy, Dostupno na: https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/

**17** Quenqua, D, Facebook Knows You Better Than Anyone Else, 19.01.2015, The New York Times, Dostupno na: https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html

**18** Algoritmom do informacije ili profita?, 15.11.2022, Digitalni forenzički centar, Dostupno na: https://dfcme.me/algoritmom-do-informacije-ili-profita/

**19** Spaić,A, Vujović, R, Petričević, P, Jovićević, I, Društvene mreže I novinarstvo u Crnoj Gori, Medijski savjet za samoregulaciju, Dostupno na:https://www.medijskisavjet.me/images/sampledata/dokumenti/Drus%CC%8Ctvene_mrez%CC%8Ce_i_novinarstvo_u_CG.pdf

**20** Woolley, S, Joseff, K, DEMAND FOR DECEIT: How the Way We Think Drives Disinformation, Januar 2020, National Endowment for Democracy, Dostupno na: https://www.ned.org/wp-content/uploads/2020/01/Demand-for-Deceit.pdf

**21** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**22** Standish, R, Study Shows How Russian, Chinese Disinformation About COVID-19 Evolved During The Pandemic, 02.12.2021, Radio Free Europe, Dostupno na: https://www.rferl.org/a/russia-china-covid-disinformation-campaigns/31590996.html

**23** Freedom of the Net 2022. Belarus, Freedom House, Dostupno na: https://freedomhouse.org/country/belarus/freedom-net/2022

**24** Bradshaw, S, Bailey, H, Howard, P, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, Dostupno na: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

**25** Ibid.

**26** Howard, P, Lie Machines How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives, Yale University Press, Dostupno na: https://yaleboooks.yale.edu/book/9780300250206/lie-machines/

**27** Diresta, R, Grossman, S, Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019, Stanford Internet Observatory Cyber Policy Center, Dostupno na: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf

**28** Lau, J, Who Are the Chinese Trolls of the '50 Cent Army'?, 07.10.2016, Voice of America, Dostupno na: https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html

**29** Kelly, S, Truong, M, Shahbaz, A, Earp, M, White, J, Manipulating Social Media to Undermine Democracy, Freedom House, Dostupno na: https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

**30** Khameneh, A, The Scorched-Earth Tactics of Iran's Cyber Army, 21.03.2023, Weird, Dostupno na: https://www.wired.com/story/iran-cyber-army-protests-disinformation/

**31** Milivojević, A, Castle: Kako srpska vlast manipuliše razumom, a građani za to još i plaćaju, 18.06.2020, Balkan Insight, Dostupno na: https://balkaninsight.com/sr/2020/06/18/castle-kako-srpska-vlast-manipulise-razumom-a-gradani-za-to-jos-i-placaju/

**32** Kirchgaessner, S, Ganguly, M, Pegg, D, Cadwalladr, C, Burke, J, Revealed: the hacking and disinformation team meddling in elections, 15.02.2023, The Guardian, Dostupno na: https://

www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

**33** Martin, D, Shapiro, J, Ilhardt, J, Trends in Online Influence Efforts, 2020, Empirical Studies of Conflict, Dostupno na: https://esoc.princeton.edu/publications/trends-online-influence-efforts

**34** Bodnar, J, Schafer, B, Soula, E, A Year of Disinformation: Russia and China's Influence Campaigns During the War in Ukraine, 24.02.2023, GMF Alliance for Securing Democracy, Dostupno na: https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/

**35** ibid.

**36** Belovodyev, D, Soshnikov, A, Standish, R, Exclusive: Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship, 05.04.2023, Radio Free Europe, Dostupno na: https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html

**37** Roth, A, European MPs targeted by deepfake video calls imitating Russian opposition, 22.04.2021, The Guardian, Dostupno na: https://www.theguardian.com/world/2021/apr/22/european-mps-targeted-by-deepfake-video-calls-imitating-russian-opposition

**38** Atanesijan, G, Društvene mreže I lažne vesti: Ruske trolove nema ko da kontroliše na Tviteru, 19.04.2023, BBC News na srpskom, Dostupno na: https://www.bbc.com/serbian/lat/svet-65285088

**39** DFC otkriva: Sa koronom stigla i mreža bot profila u Srbiju, 13.04.2020, Digitalni forenzički centar, Dostupno na: https://dfcme.me/nova-mreza-bot-profila/

**40** Twitter Removes Thousands Of Accounts 'Promoting' Serbian Ruling Party, 02.04.2020, Radio Free Europe, Dostupno na: https://www.rferl.org/a/serbia-twitter-vucic-sns-serbian-progressive-party/30526199.html

**41** Nimmo, B, Franklin, M, Agranovich, D, Hundley, L, Torrey, M, DETAILED REPORT: Quarterly Adversarial Threat Report, Februar 2023, Meta, Dostupno na: https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf

**42** Waddell, K, 'Look, a Bird!' Trolling by Distraction, 27.01.2017, The Atlantic, Dostupno na: https://www.theatlantic.com/technology/archive/2017/01/trolling-by-distraction/514589/

**43** Deck, Andrew, A million-strong troll army is targeting Iran's #MeToo activists on Instagram, 29.06.2022, Rest of world, Dostupno na: https://restofworld.org/2022/troll-army-targeting-irans-metoo-activists-instagram/

**44** Kao, J, Shuang Li, M, How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus, 26.03.2020, ProPublica, Dostupno na: https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

**45** Information operations directed at Hong Kong, 19.08.2019, Twitter blog, Dostupno na:

**46** Maynes, C, Inside the Internet Research Agency: a Mole Among Trolls, 17.04.2018, Voice of America, Dostupno na: https://www.voanews.com/a/inside-the-internet-research-agency-a-mole-among-trolls/4352107.html

**47** Howard, P, Ganesh, B, Liotsiou, D, The IRA, Social Media, and Political Polarization in the United States, 2012-2018, Computational Propaganda Research Project, Dostupno na: https://www.intelligence.senate.gov/sites/default/files/documents/The-IRA-Social-Media-and-Political-Polarization.pdf

**48** DiResta, R, Grossman, S, Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019, 12.11.2019, Stanford Freeman Spogli Institute for International Studies, Dostupno na: https://fsi.stanford.edu/publication/potemkin-think-tanks

**49** MREŽE BOTOVA I TROLOVA U CRNOJ GORI (1): VOJNICI NA ZADATKU, 21.09.2022, Centar za istraživačko novinarstvo Crne Gore, Dostupno na: https://www.cin-cg.me/mreze-botova-i-trolova-u-crnoj-gori-1-vojnici-na-zadatku/

**50** Martin, D, Shapiro, J, Ilhardt, J, Trends in Online Influence Efforts, 05.08.2020, Scholar Princeton, Dostupno na: https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_onli-

ne_influence_efforts_v2.0_aug_5_2020.pdf

**51** Klajnmen, Z, Afera Fejsbuk-Kembridž analitika: Šta sve znamo do sada, 21.03.2018, BBC News na srpskom, Dostupno na: https://www.bbc.com/serbian/lat/svet-43475183

**52** Qin, B, Strömberg, D, Wu, Y, Why Does China Allow Freer Social Media? Protests versus Surveillance and

Propaganda, Journal of Economic Perspectives, Dostupno na:https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.1.117

**53** Polyakova, A, Meserole, C, Exporting digital authoritarianism The Russian and Chinese models, Avgust 2019, Brookings, Dostupno na: https://www.brookings.edu/research/exporting-digital-authoritarianism/

**54** Milmo, D, TikTok's ties to China: why concerns over your data are here to stay, 8.11.2022, The Guardian, Dostupno na: https://www.theguardian.com/technology/2022/nov/07/tiktoks-china-bytedance-data-concerns

**55** Shepardson, D, TikTok CEO: App has never shared US data with Chinese government, 22.03.2023, Reuters, Dostupno na: https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/

**56** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**57** Kenyon, M, WeChat Surveillance Explained, 07.05.2020, The Citizen Lab, Dostupno na: https://citizenlab.ca/2020/05/wechat-surveillance-explained/

**58** Moore, M, Tiananmen Massacre 25th anniversary: the silencing campaign, 18.05.2014, The Telegraph, Dostupno na: https://www.telegraph.co.uk/news/worldnews/asia/china/10837992/Tiananmen-Massacre-25th-anniversary-the-silencing-campaign.html

**59** Polyakova, A, Meserole, C, Exporting digital authoritarianism The Russian and Chinese models, Avgust 2019, Brookings, Dostupno na: https://www.brookings.edu/research/exporting-digital-authoritarianism/

**60** Sherman, J, Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior, 12.07.2021, Atlantic Council, Dostupno na: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

**61** Iran's National Information Network, 9.11.2012, The citizen lab, Dostupno na: https://citizenlab.ca/2012/11/irans-national-information-network/

**62** Clarke, L, Swindells, K, How social media companies help authoritarian governments censor the internet, 09.06.2021, The New Statesman, Dostupno na: https://www.newstatesman.com/science-tech/2021/06/how-social-media-companies-help-authoritarian-governments-censor-internet

**63** India ban on BBC Modi documentary 'imperils press freedom', 25.12.2023, Aljazeera, Dostupno na: https://www.aljazeera.com/news/2023/1/25/india-banning-bbc-documentary-on-modi-attack-on-press-freedom

**64** Kagubare, I, Klar, R, Twitter's restriction of Turkish election content sparks fear of precedent, 25.05.2023, The Hill, Dostupno na: https://thehill.com/policy/technology/4019109-twitters-turkey-election-sparks-criticism/

**65** Biddle, S, FACEBOOK REPORT CONCLUDES COMPANY CENSORSHIP VIOLATED PALESTINIAN HUMAN RIGHTS, 21.09.2022, The Intercept_, Dostupno na: https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/

**66** MYANMAR: FACEBOOK'S SYSTEMS PROMOTED VIOLENCE AGAINST ROHINGYA; META OWES REPARATIONS, 29.09.2022, Amnesty International, Dostupno na: https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

**67** Brandom, R, Twitter is complying with more government demands under Elon Musk,

27.04.2023, Rest of world, Dostupno na: https://restofworld.org/2023/elon-musk-twitter-government-orders/#:~:text=In%20its%20first%20six%20months,the%20previous%20twelve%20months%20combined.&text=The%20data%2C%20drawn%20from%20Twitter's,requests%20from%20governments%20and%20courts.

**68** Frantz, E, Kendall-Taylor, A, Wright, J, Digital Repression in Autocracies, Mart 2020, V – Dem Institute, Dostupno na: https://www.v-dem.net/media/publications/digital-repression17mar.pdf

**69** Vlada: Gašenje Vibera na dan izbora nije neustavno, 28.03.2017, FOS media, Dostupno na: https://fosmedia.me/arhiva/infos/drustvo/vlada-gasenje-vibera-na-dan-izbora-nije-neustavno

**70** Shahbaz, A, Funk, A, Vesteinsson, K, Freedom on the Net 2022 Countering an Authoritarian Overhaul of the Internet, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

**71** Perrett, C, Russia's internet censorship is forcing citizens to turn to the dark web and VPNs for news and social media, 17.03.2022, Insider, Dostupno na: https://www.businessinsider.com/what-happens-social-media-and-news-go-dark-in-russia-2022-3

**72** Wiseman, J, Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges, 3.10.2020, International Press Institute, Dostupno na: https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/

**73** Shahbaz, A, The Rise of Digital Authoritarianism, Freedom House, Dostupno na: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

**74** ibid.

**75** Freedom of the world 2023 Turkey, Freedom House, Dostupno na: https://freedomhouse.org/country/turkey/freedom-world/2023

**76** Hubbard, B, Timur, S, Turkey Allows Jail Terms for What It Deems 'Fake News', 14.10.2022, The New York Times, Dostupno na: https://www.nytimes.com/2022/10/14/world/europe/turkey-jail-fake-news.html

**77** Bradshaw, S, Bailey, H, Howard, P, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Research Project, Oxford Internet Institute, University of Oxford, Dostupno na: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf

**78** Mantellassi, F, Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy, 16.02.2023, Geneva Centre for Security Policy, Dostupno na: https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and

**79** Freedom in the World 2022 The Global Expansion of Authoritarian Rule, Feburar 2020, Freedom House, Dostupno na: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

**80** Kalathil, S, The Evolution of Authoritarian Digital Influence Grappling with the New Normal, National Defense University, Dostupno na: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=DJRX5DRHKfqeXbyt6et98w%3D%3D

**81** ibid.

**82** Kornbluh, K, Goodman, E, Weiner, E, Safeguarding Digital Democracy - Digital Innovation and Democracy Initiative Roadmap, Mart 2020, The German Marshall Fund of the United States, Dostupno na: https://www.gmfus.org/sites/default/files/Safeguarding%2520Democracy%2520against%2520Disinformation_v7.pdf

**83** Mosseri, A, Working to Stop Misinformation and False News, 07.04.2017, Meta, Dostupno na: https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news#:~:text=If%20the%20fact%2Dchecking%20organizations,appear%20lower%20in%20News%20Feed.

**84** Meta's Third-Party Fact-Checking Program, Meta, Dostupno na:https://www.facebook.com/formedia/mjp/programs/third-party-fact-checking

**85** Ad Library, Meta, Dostupno na: https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=ME&media_type=all

**86** Coordinated Inauthentic Behavior, Meta, Dostupno na: https://about.fb.com/news/tag/coordinated-inauthentic-behavior/

**87** Pamment, J, Victoria Smith, Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online, Jul 2022, NATO Strategic Communications Centre of Excellence, Dostupno na: https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244

**88** Fredheim, R, Sebastian Bay, Anton Dek, Martha Stolze, Tetiana Haiduchyk, Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation, 03.03.2023, NATO Strategic Communications Centre of Excellence, Dostupno na: https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/272

**89** Tobin, A, Varner, M, Angwin, J, Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up, 28.12.2017, ProPublica, Dostupno na: https://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes

**90** 'Stamp of approval': Twitter's Musk amplifies misinformation, 19.04.2023, France 24, Dostupno na: https://www.france24.com/en/live-news/20230419-stamp-of-approval-twitter-s-musk-amplifies-misinformation

**91** Lee, K, Elon Musk, in a Tweet, Shares Link From Site Known to Publish False News, 30.10.2022, The New York Times, Dostupno na: https://www.nytimes.com/2022/10/30/business/musk-tweets-hillary-clinton-pelosi-husband.html

**92** Milmo, D, YouTube is major conduit of fake news, factcheckers say, 12.01.2022, The Guardian, Dostupno na: https://www.theguardian.com/technology/2022/jan/12/youtube-is-major-conduit-of-fake-news-factcheckers-say

**93** Ma, O, Feldman, B, How Google and YouTube are investing in fact-checking, 29.11.2022, Google blog, Dostupno na: https://blog.google/outreach-initiatives/google-news-initiative/how-google-and-youtube-are-investing-in-fact-checking/

**94** The 2022 Code of Practice on Disinformation, European Commission, Dostupno na: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

**95** Thierry Breton, Twitter, 26.05.2023, Dostupno na: https://twitter.com/ThierryBreton/status/1662194595755704321?s=20

**96** Spring, M, Twitter insiders: We can't protect users from trolling under Musk, 06.03.2023, BBC News, Dostupno na: https://www.bbc.com/news/technology-64804007

**97** Pitanja i odgovori: Akt o digitalnim uslugama*, 25.04.2023, Evropska komisija, Dostupno na: https://ec.europa.eu/commission/presscorner/detail/hr/QANDA_20_2348

**98** Шта је Општа уредба о заштити података?, Google, Dostupno na: https://support.google.com/google-ads/answer/7687725?hl=sr

**99** AI Act: a step closer to the first rules on Artificial Intelligence, 11.05.2023, European Parliament, Dostupno na: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence#:~:text=AI%20systems%20with%20an%20unacceptable,behaviour%2C%20socio%2Deconomic%20status%2C

**100** Marinescu, D, Facebook's Content Moderation Language Barrier, 08.09.2021, New America, Dostupno na: https://www.newamerica.org/the-thread/facebooks-content-moderation-language-barrier/

**101** Engler, A, The EU AI Act will have global impact, but a limited Brussels Effect, 08.06.2022, Brookings, Dostupno na: The EU AI Act will have global impact, but a limited Brussels Effect (brookings.edu)

**102** Kalathil, S, The Evolution of AuthoritarianDigital Influence Grappling with the New Normal, National Defense University, Dostupno na: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_33-50_Kalathil-2.pdf?ver=DJRX5DRHKfqeXbyt6et98w%3D%3D

## IMPRESUM

**IZDAVAČ:** Digitalni forenzički centar
**GLAVNA I ODGOVORNA UREDNICA:** Azra Karastanović
**AUTORI:** Milan Jovanović i DFC tim
**DIZAJN I PRIPREMA ZA ŠTAMPU:** Ana Đurković
**TIRAŽ:** 80 primjeraka
**ŠTAMPA:** Piccolo Print Podgorica

CIP - КАТАЛОГИЗАЦИЈА У ПУБЛИКАЦИЈИ
НАЦИОНАЛНА БИБЛИОТЕКА ЦРНЕ ГОРЕ, ЦЕТИЊЕ

ISBN 978-9940-817-08-4
COBISS.CG-ID 22499332

Ovaj projekat finansira Ambasada SAD u Podgorici. Mišljenja, nalazi, zaključci ili preporuke koji su ovdje izneseni su stav autora i ne odražavaju nužno stav Stejt dipartmenta/Vlade SAD.

www.dfcme.me DFCMNE DFCME DFCMEDOTME

DFC
DIGITALNI FORENZIČKI CENTAR