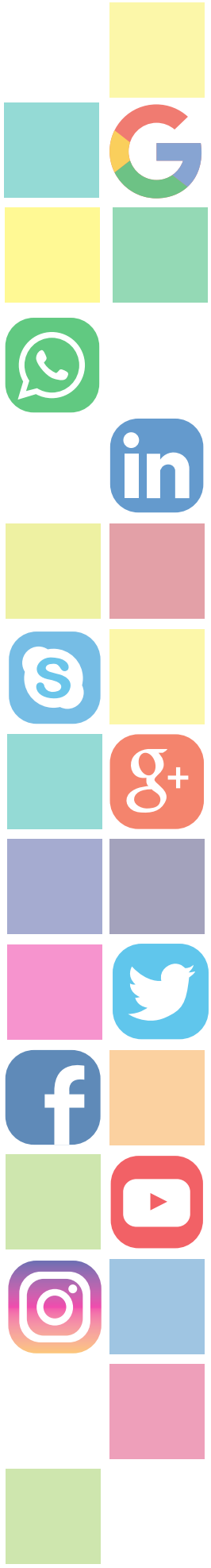
FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK
SERBIA

MEDIJI I NOVE POLITIKE UPRAVLJANJA INTERNETOM

SLOBODA IZRAŽAVANJA I MEDIJSKE SLOBODE U DIGITALNOM OKRUŽENJU



Dokument je nastao u okviru projekta *Gde je mesto medija u novim politikama upravljanja internetom?* koji je podržala Fondacija za otvoreno društvo, Srbija i bavi se mapiranjem trendova, praćenjem postojeće domaće zakonske regulative, međunarodnih inicijativa i dobrih praksi, kao i rizika koji ugrožavaju medijske slobode u digitalnom okruženju. Dokument donosi i preporuke regulacije/samoregulacije u oblastima gde se presecaju medijske politike sa politikama upravljanja internetom.

Autor: Tanja Maksić

Urednik: Dragana Žarković Obradović

Saradnici: Lada Vučenović i Milica Milić

Beograd, 2020

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

Stavovi i informacije iznete u dokumentu isključiva su odgovornost BIRN-a i ne izražavaju stavove Fondacije za otvoreno društvo, Srbija.

SADRŽAJ

I MEDISJKE POLITIKE U DIGITALNOM OKRUŽENJU

Svakog dana, 4,48 milijardi ljudi (ili 58% svetske populacije) koristi internet. Najveći svetski pretraživač Google dobije 40 hiljada upita svake sekunde, a popularna društvena mreža za razmenu video sadržaja YouTube ima 7 miliona sati pregleda na dan. Korisnici provedu 950 miliona sati na aplikaciji Facebook.

Statistički podaci iz Srbije govore da naši građani u velikoj meri prate globalne trendove. Podaci Republičkog zavoda za statistiku (2019. godina) pokazuju da u Republici Srbiji preko 3,81 miliona pojedinaca koristi internet. Od toga, njih 70% ima naloge na društvenim mrežama. Uređaj koji se najčešće koristi za pristup internetu van kuće ili posla je mobilni telefon, a internet se u najvećoj meri koristi za traženje informacija, slanje onlajn poruka (putem Skype-a, Viber-a, WhatsApp-a, Messanger-a i sl.), slušanje muzike i učešća na društvenim mrežama.

TOP 5 INTERNET PORTALA PO BROJU KORISNIKA
(podaci za oktobar 2020.)

Blic · a! · Kurir · Telegraf · Mondo

→ Preko **2 MILIONA KORISNIKA** i više miliona **pregledanih stranica**

→ Vreme provedeno na ovim sajtovima meri se **STOTINAMA GODINA**

Gemius Audience (audience.rs)

INTERNET je 2019. godine dnevno koristilo **72%** građana Srbije

TELEVIZIJU je pratilo **69%**

RADIO STANICE slušalo **37%**

ŠTAMPU pratilo **30%**

U starosnoj grupi od **15 do 65** godina:

- ▸ **68,2%**
- ▸ **59,8%**
- ▸ **43,6%**

▸ **15,4%** građana prati ▸ oko **500.000** naloga ▸ oko **300.000** neaktivno **50.000** pripadaju „botovima" koji su tu da podrže svog ili napadnu protivničkog lidera

Podaci IPSOS-a (uvid UNS-a)

Kako pokazuju gore navedeni podaci, **internet je dramatično promenio našu svakodnevicu** i način na koji komuniciramo, **pristupamo sadržaju i razmenjujemo informacije**. Jednako snažno je uticao i na medije. Digitalno okruženje kreira novi medijski ekosistem u kom se menja način proizvodnje, plasiranja i distribucije medijskog sadržaja u odnosu na tradicionalne medijske sisteme.

Ovim dokumentom, prvim u nizu, **BIRN pokreće debatu o transformativnom uticaju internet i digitalnih tehnologija na razvoj medija**. Serijom izveštaja ispitaće se status medijskih sloboda u digitalnom prostoru; otvorenost, inkluzivnost i pristup informacijama; kao i ekonomska održivost medija i novi biznis modeli.

Veliki deo promena koje su uslovljene tehnološkim inovacijama dolaze iz najrazvijenijih zemalja (naročito SAD gde se nalazi sedište najvećih tehnoloških kompanija poput Google-a, Facebook-a, Amazon-a, Twitter-a i sl.) ali ove promene podjednako utiču na medije u manje razvijenim društvima. Upravo zato je važno da donosioci odluka i medijska industrija manje robusnih sistema shvate promene koje suštinski transformišu medijsko okruženje i da učestvuju u postavljanju novih standarda profesije.

Ovi transformativni procesi treba da se baziraju na principima otvorenog interneta; integriteta i verodostojnosti medija koji su i u novom, digitalnom okruženju, čuvari javnosti i otvoreni forumi za društvene debate; neguju pluralitet mišljenja i nesmetan protok informacija; ekonomski održivih medija koji imaju dovoljno znanja i kapaciteta da prate trendove i uvode inovacije.

U praksi, ipak nije tako, jer **internet i digitalni prostor sve više postaju mesto gde se sloboda izražavanja i medijske slobode susreću sa brojnim izazovima i problemima** – algoritamsko i platformsko usmereno informisanje dovodi do toga da se ljudi informišu u zatvorenim krugovima svojih istomišljenika ili poznanika (tzv. news bubbles), količina i brzina širenja dezinformacija je tolika da ponekad ozbiljno ugrožava društveni dijalog, mediji, a posebno mali, lokalni, teško monetizuju svoj sadržaj i dosadašnji biznis modeli ne obezbeđuju njihovu održivost, a resursima kojima raspolažu, teško mogu da prate trendove.

Covid 19 pandemija koja je izbila ove godine takođe je imala značajan uticaj kako na celo društvo, tako i na medije. Ova društvena kriza pokazala je vrednost tačnog, proverenog i istinitog informisanja za zaštitu zdravlja građana, ali ujedno i ogolila mnoge slabosti medijskog sistema, od finansijske nezavisnosti do raznih mehanizama za pritisak, suzbijanje slobodnog protoka informacija, manipulaciju podacima i sl. U trenucima kada se veliki broj životnih aktivnosti (od informisanja, različitih poslovnih procesa do obrazovanja) odvija isključivo onlajn, važno je da se u ovom prostoru ponašamo odgovorno kao korisnici, ali ujedno i da razumemo prednosti i mane digitalnog prostora, te adekvatno reagujemo u slučajevima kršenja prava.

Upravo zato, BIRN nudi ovaj i naredne izveštaje kao početnu tačku za dalje razgovore unutar same novinarske profesije, ali i medijskoj industriji i industriji oglašavanja, civilnom društvu i biznis sektoru, kao i donosiocima odluka.

Dodatno, BIRN će kroz ovaj projekat doprineti **novom promišljanju razvoja medijskih politika, jer će na njih presudno uticati i načini na koje se promišlja i implementira politika regulacije interneta**. Iako su debate o pitanjima regulacije interneta globalne i neke od gorućih tema brojnih svetskih javnih foruma, naši izveštaji prevashodno će imati u vidu lokalni kontekst, ograničenja i mogućnosti domaće medijske scene. Izveštajima se mapira trenutno stanje, relevantne politike i zakonodavni okvir, kao i ključni akteri koji aktivno rade na politikama upravljanja internetom.

POD POLITIKAMA UPRAVLJANJA INTERNETOM[1] (engl. Internet governance) podrazumeva se komplementarni set programa, normi, zajedničkih principa, zakona i procedura, koje primenjuju vlada, privatni sektor, civilno društvo i IT zajednica, a koje zajedno oblikuju evoluciju i upotrebu interneta.

Razvoj medija i politike upravljanja internetom prepliću se na raskrsnici mnogih važnih pitanja, ali čini se da mediji ne učestvuju u punom kapacitetu u ovim društvenim debatama. Nedostatak znanja i kompetencija samo je deo problema, uz koji treba dodati i nedostatak resursa, kao i činjenicu da mnoge politike u vezi sa upravljanjem internetom ostaju na nivou tehničkih, a da se dimenzija ljudskih prava (time i slobodan protok informacija, sloboda izražavanja i sl.) zanemaruje.

Nedostatak domaćih medijskih politika ogleda se i u tome što su one usmerene na tradicionalne modele regulacije te nisu prilagođene digitalnom okruženju.

Izveštajima će se dati predlog za unapređenje tih politika, najpre, u svetlu primene nove medijske strategije (*Strategije unapređenja javnog informisanja 2020-2025.*) i izmene medijskih zakona koji će neminovno slediti, ali i u svetlu primene drugih, relevantnih strategija i zakona (na primer, strategije primene veštačke inteligencije, unapređenja digitalnih veština, informacione bezbednosti i sl.) kao i dodatne samoregulacije medijske profesije i industrije.

[1] Videti, na primer, definiciju UNESCO https://en.unesco.org/themes/internet-governance

II SLOBODA MEDIJA U DIGITALNOM OKRUŽENJU – KONTEKST

Internet i društveni mediji nesumnjivo su uticali na demokratizaciju i proširenje granica slobode izražavanja, ujedno i medijskih sloboda. Na nivou proširenja ljudskih prava i sloboda internet je doprineo novim mogućnostima za kreiranje i uređivanje sadržaja, a samim tim i nove mogućnosti za proširenje informisanosti, znanja i kreativnosti; nove mogućnosti za organizovanje i mobilizaciju različitih društvenih grupa; nove mogućnosti za inoviranje i generisanje ekonomske aktivnosti, inovacija i razvoja.

Otvorena, dinamična i interaktivna priroda interneta omogućava širokom krugu korisnika da budu kreatori, ko-kreatori ili urednici sadržaja, ne samo njegovi „pasivni" konzumenti. Za razliku od tradicionalnih, centralizovanih, hijerarhijski uspostavljenih medijskih sistema, internet i digitalni mediji izgradili su potpuno novi medijski sistem, zasnovan na interaktivnosti, konvergentnosti, mobilnosti, brzini i instant objavi vesti, inovacijama.

> „Internet nije samo medij, već potpuno novo medijsko okruženje... Možda ima smisla govoriti i dalje o novim medijima kao sasvim novoj, na internetu zasnovanoj generaciji medija, koja gradi novu medijsku ekologiju. Uz njih živimo u medijskom prostoru koji je radikalno drugačiji od onoga koji je postojao do kraja 20. veka i u kojem se svaki novi medij pojavljivao kao pojedinačni – štampa, radio, film ili televizija. Digitalnom revolucijom gradi se medijski drugačije organizovani svet. On odgovara novom, umreženom društvu, u kome se taj virtuelni internet prostor integriše sa realnim prostorom i utoliko se granice između realnog i virtuelnog sveta gotovo ukidaju".[2]

Razvoj digitalnih tehnologija otvorio je nove mogućnosti za komunikaciju, ali je stvorio i nove oblike kršenja prava na slobodu izražavanja, kao i nove oblike pritiska na novinare i medijske organizacije.

Podaci monitoringa SHARE Fondacije pokazuju ukupno 232 različite povrede prava novinara, istraživačkih novinara i onlajn medija i platformi (u periodu od 2014. do januara 2020. godine) u Srbiji.

Promene u regulatornom okviru treba da odgovore upravo na ove izazove i probleme kojima se umanjuju medijske slobode i slobode izražavanja, imajući u vidu specifičnosti i strukturne promene koje donosi digitalno okruženje. Promene u regulativi mogu se pratiti i na globalnom planu, promenama u EU direktivama, ali i na nivou nacionalnih država.

U Srbiji novi regulatorni ciklus pokrenut je usvajanjem nekoliko strateških dokumenata koji postavljaju temelje regulacije onlajn prostora – informacione bezbednosti, digitalnih veština, razvoja veštačke inteligencije, e-uprave i otvorenih podataka, medija i razvoja sistema informisanja.

[2] Snježana Milivojević, „Šta je novo u novim medijima", Peščanik (2017), https://pescanik.net/sta-je-novo-u-novim-medijima/

Što se tiče same slobode medija i informisanja, koja je glavni predmet ovog izveštaja, ona se nominalno štiti domaćim zakonodavstvom, bez obzira na to da li se radi o onlajn ili oflajn medijima. *Aktuelni Zakon o javnom informisanju i medijima* navodi u svojim prvim članovima[3] da je javno informisanje slobodno te da ne podleže niti jednom obliku cenzure. Istim zakonom garantuje se zaštita medijskog pluralizma, slobodan protok i razmena informacija, kao i uređivačka autonomija medija.

Suprotno zakonu i proklamovanim demokratskim principima, sloboda medija u Srbiji je u poslednjih nekoliko godina u stalnom padu, što pokazuju brojna domaća i međunarodna istraživanja. Na primer, *Indeks* koji prati organizacija Reporteri bez granica (Reporters without borders) beleži da medijske slobode u Srbiji ugrožavaju agresivne kampanje protiv istraživačkih novinara koje sprovode provladini mediji; veze između političara i medija; činjenicu da vlasti tolerišu lažne vesti; nedostatak pluralizma i sl.[4] Sličan zaključak stoji i u izveštaju organizacije Freedom House[5], ali i u izveštajima Evropske komisije i institucija Evropske unije koje prate medijske slobode kao deo „paketa reformi" u procesu pridruživanju Srbije Uniji.

Reporteri bez granica analizirajući situaciju medijskih sloboda u Srbiji naglašavaju da one postoje uglavnom na onlajn platformama, skoncentrisane u okviru rada istraživačkih novinarskih centara.

> „Mi se krećemo internetom kao po svojoj šumi, koristimo ga do krajnjih granica, učimo kako da budemo atraktivni u sajber svemiru i tu objavljujemo ono što smo istražili".
>
> **Branko Čečen, direktor CINS-a**

Medijska strategija mapira nekoliko ključnih mesta ugrožavanja slobode medija (novinara i medijskih radnika) u digitalnom prostoru: Informaciona bezbednost (mera 1.4 Strategije), Presretanje elektronskih komunikacija (mera 1.3 Strategije), Bezbednost novinara u onlajn okruženju (mera 1.2 Strategije). Ovim pitanjima treba dodati i ona koja se tiču nesmetanog protoka informacija i upravljanja medijskim sadržajem, a obuhvataju algoritamsko moderiranje sadržaja, širenje dezinformacija, „trolovanje" i sl.

[3] Zakon o javnom informisanju i medijima („Službeni glasnik RS" br. 83/2014, 58/2015 i 12/2016 - autentično tumačenje), članovi 1 do 6

[4] Indeks medijskih sloboda za Srbiju organizacije Reporteri bez granica za 2019. godinu dostupan je ovde https://rsf.org/en/serbia

[5] Izveštaj ove organizacije za 2019. godinu dostupan je ovde https://freedomhouse.org/report/freedom-world/2019/serbia

III SVE VEĆI BROJ PRITISAKA I NAPADA NA NOVINARE: INFORMACIONA BEZBEDNOST I ZAŠTITA IZVORA U DIGITALNOM OKRUŽENJU

POD INFORMACIONOM BEZBEDNOŠĆU SE PODRAZUMEVA reagovanje na bezbednosne rizike povezane sa upotrebom informaciono-komunikacionih tehnologija, koja uključuje bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca.

Kako su mediji i novinari korisnici tehnologija, čitav spektar bezbednosnih rizika deo je i ove profesije.

Bezbednost novinara i medijskih radnika, medijskih sajtova i tehnike koja je neophodna za novinarski rad, uz bezbedan javni prostor za društvenu debatu, jedan je od osnovnih postulata prava na izražavanje i informisanje. Ovaj postulat primenjuje se jednako i u oflajn i u onlajn sferi, tradicionalnim i onlajn medijima.

Praksa, ipak, pokazuje drugačiju tendenciju.

„U odnosu na broj svih zabeleženih napada (pritisci i ozbiljniji napadi), gotovo 30% zabeleženih se vrši u onlajn prostoru. Kada je reč o verbalnim pretnjama, u 34% slučajeva to se čini preko različitih društvenih mreža i medija koji funkcionišu na internetu (Facebook, Twitter, Instagram, portali, veb-stranice, forumi). Od ukupnog broja predmeta koji su se u 2018. i 2019. godini našli pred tužilaštvima (73 predmeta), 29 predmeta se odnose na ugrožavanje bezbednosti novinara kroz različite oblike onlajn napada (preko 39% od ukupnog broja).“

Iz izveštaja *Kritične tačke SĆF*

Društvene mreže i internet platforme sve češće postaju mesto za upućivanje pretnji i različitih vrsta pritisaka usmerenih ka novinarima i medijskim radnicima. Postoji čitav spektar pretnji i pritisaka koji variraju od tehničkih napada, podsticanja grupnih napada, targetiranje drugim napadačima, ugrožavanje privatnosti, uznemiravanje, nanošenje uvreda, proganjanje i sl., kojima redakcije i mediji mogu da budu izloženi, a tek mali deo ovih napada bude adekvatno procesuiran.

Ugrožavanje bezbednosti novinara za posledicu ima povećan nivo cenzure i autocenzure, i čitav niz problema od psiholoških do pritiska da se određene osetljive teme pokrenu i istraže, što ukupno vodi do snižavanja kvaliteta informisanja.

STALNA RADNA GRUPA ZA BEZBEDNOST NOVINARA

(Izveštaji o postupanju javnih tužilaštava u vezi sa krivičnim delima izvršenim na štetu novinara u vezi sa njihovom bezbednošću)

▸ **PERIOD JANUAR 2019 – MART 2020.**

UKUPAN BROJ POSTUPAKA ZA DATI PERIOD 64 POSTUPKA

25 POSTUPAKA VODI TUŽILAŠTVO ZA VISOKOTEHNOLOŠKI KRIMINAL
Ugrožavanje sigurnosti (čl. 138 st. 3 KZ)

1 POSTUPAK VODI TUŽILAŠTVO ZA VISOKOTEHNOLOŠKI KRIMINAL.
Rasna i druga diskriminacija (čl. 387 KZ)

Postojećim zakonodavstvom nije prepoznat ni čitav spektar pritisaka kojima su svakodnevno izloženi mediji i novinari. Kako bi odgovor države i nadležnih institucija bio adekvatniji, potrebno je izmeniti odgovarajuće zakone, najpre, Krivični zakonik.

„Krivični zakonik nije prilagođen savremenim tehnologijama i jako je teško da se procesuiraju lica koja vrše krivična dela putem interneta, naročito putem društvenih mreža. Policija i tužilaštvo najčešće ove pretnje u onlajn sferi tretiraju kao krivična dela koja se gone po privatnoj tužbi, što znači da novinar kojem se preti mora sam da sazna identitet lica koje mu preti, pa tek ako sazna identitet da opet samostalno pokrene krivični postupak, zastupa optužbu... drugim rečima nema nikakvu pomoć države. Upravo u tom smislu bi trebalo menjati Krivični zakonik i Zakonik o krivičnom postupku kako bi država pomogla novinarima bar kada je u pitanju prikupljanje dokaza i identifikacija lica koja prete preko društvenih mreža“

Veljko Milić, advokat, član UO NDNV
i član Stalne radne grupe za bezbednost novinara.

PREPORUKE ZA UNAPREĐENJE REGULATORNIH I SAMOREGULATORNIH MEHANIZAMA, POTENCIJALNI PRAVCI DELOVANJA:

- **Inicirati izmene Krivičnog zakonika i Zakona o krivičnom postupku tako da one prepoznaju krivična dela na štetu novinara i medijskih radnika koja dolaze iz digitalne sfere, u mnogo većoj meri nego što je slučaj sa postojećim pravilima;**
- **Unaprediti sistem prevencije, prepoznavanja i prijavljivanja napada, kroz kreiranje obuka i vodiča za medije i novinare kako bi se kroz sistem edukacije povećala svest i znanje o digitalnoj bezbednosti.**

III a. POSTOJEĆI MEHANIZMI ZAŠTITE NOVINARA I NJIHOVA (NE)EFIKASNOST

Informaciona bezbednost u RS regulisana je *Strategijom informacione bezbednosti*[6] (koja ističe krajem ove godine) i relevantnim zakonom[7]. Mediji nisu prepoznati kao deo „kritične infrastrukture" koja se štiti ovim regulatornim okvirom.

Osim toga, Zakonom je ustanovljen Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT) u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), a dodatno su formirani i sektorski CERT-ovi koji se bave posebnim segmentima i sektorima društva. **Posebni CERT koji se bavi prevencijom i zaštitom bezbednosti za medije i civilno društvo vodi SHARE Fondacija**[8].

SHARE CERT je registrovan 2017. godine i do sada je pružio više od 50 saveta prilikom incidenata u IKT sistemima. Vrste slučajeva sa kojima se tim SHARE Fondacije susretao variraju, od tipičnih primera onesposobljavanja servisa (Distributed Denial of Service - DDoS), preko ubacivanja malicioznog koda, "brute force" napada na delove sajta, targetiranja ranjivih elemenata sajtova (npr. ankete) do potpunog onemogućavanja korišćenja naloga (npr. društvene mreže, mejl nalozi).

Medijskom strategijom predviđeno je u meri 1.4 da **Nacionalni CERT, kao i posebni CERT-ovi, prate bezbednost novinara i reaguju po potrebi, kao i da učestvuju u održavanju obuka za medije i medijske radnike, a sve u cilju prevencije i bolje zaštite od takvih napada**.

Novinarima i medijima, osim CERT-a, na raspolaganju je još jedan mehanizam za prijavljivanje ugrožavanja sigurnosti, pretnji i pritisaka koje dolaze iz onlajn sfere, a to je Stalna radna grupa za bezbednost novinara koja je formirana na osnovu aktivnosti za Akcioni plan za pregovaračko poglavlje 23 još decembra 2016. godine[9].

Stalna radna grupa se u određivanju prema slučajevima napada na novinare u najvećoj meri vodi Krivičnim zakonikom[10] koji u članu 138. prepoznaje osobe koje se bave javnim informisanjem kao one kojima se može ugroziti sigurnost.

Jedna od glavnih prepreka identifikaciji identiteta lica koje ugrožavaju bezbednost onlajn i prikupljanju digitalnih dokaza je saradnja sa globalnim kompanijama koje vode Google i društvene mreže (Facebook i Twitter, kao najčešće zastupljene).

[6] Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine, „Službeni glasnik RS", br. 55/05, 71/05 – ispravka, 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US i 44/14

[7] Zakon o informacionoj bezbednosti, „Službeni glasnik RS", broj 6/16

[8] Više informacija je ovde https://www.sharecert.rs/

[9] Memorandum o osnivanju Stalne radne grupe potpisalo je 7 medijskih udruženja (Udruženje novinara Srbije, Nezavisno udruženje novinara Srbije, Nezavisno društvo novinara Vojvodine, Asocijacija nezavisnih elektronskih medija, Asocijacija onlajn medija, Društvo novinara Vojvodine, Asocijacija medija) i Republičko javno tužilaštvo i MUP. Memorandumom je, između ostalog, predviđeno hitno postupanje MUP-a i RJT-a u slučajevima napada na novinare i medijske radnike, određivanje kontakt tačaka i koordinaciju ovih institucija i udruženja, kao i formiranje registra za praćenje slučajeva. Pored Memoranduma, Stalna radna grupa izrađuje godišnje planove rada kojima se mapiraju aktivnosti koje doprinose sprovođenju Memoranduma.

[10] Krivični zakonik RS, Sl. glasnik RS, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019

Na primer, Google, u svom Izveštaju[11] navodi da se najveći broj zahteva koje ova kompanija dobija od različitih državnih institucija i agencija odnosi na uklanjanje sadržaja koji urušava nacionalnu bezbednost, a zatim i sadržaj u vezi sa klevetom, zaštitom autorskih prava, privatnošću i bezbednošću.

Google u istom izveštaju navodi da ova kompanija razmatra svaki zahtev državnih organa pojedinačno, a da u pojedinim slučajevima zahteva i sudski nalog. Nema, međutim, detaljnije objašnjenih kriterijuma za postupanje po ovim zahtevima. Izveštaj Facebook-a[12] za Srbiju za period jul – decembar 2019. pokazuje da su državne institucije (uključujući i policiju, tužilaštvo i sl.) ovoj kompaniji uputili ukupno 182 zahteva (od toga 155 u vezi sa pravnim poslovima, poput tužbi i sl., kao i 27 hitnih zahteva) u vezi sa 334 naloga korisnika ove mreže, kao i da je kompanija u 76% zahteva odgovorila pozitivno na ove zahteve te dostavila tražene podatke.

Zamajac novom promišljanju regulatornog okvira koji bi dao adekvatniji odgovor na ovaj problem očekuje se kroz rad novoformirane radne grupe, formirane pri kancelariji Zaštitnika građana[13]. Mandat ove radne grupe je **uspostavljanje Platforme za evidenciju slučajeva ugrožavanja bezbednosti i pritisaka na novinare i druge medijske aktere**, u kojoj će se evidentirati svaki pojedinačni slučaj ugrožavanja bezbednosti i svaki oblik pritiska na lica koja obavljaju poslove od javnog značaja u oblasti informisanja u vezi sa poslovima koje obavljaju.

Trenutno, u okviru ove inicijative funkcioniše radna grupa koja ima zadatak da definiše pojam „pritiska“ na novinare i medije, koja će se u velikoj meri oslanjati na NUNS-ovu bazu napada i pritisaka. Dodatno, radna grupa treba da osmisli projekte i osigura novac koji će garantovati održivost same Platforme.

Platforma koja treba da bude formirana u našoj zemlji u velikoj meri oslanjaće se na iskustva slične onlajn baze koja funkcioniše na nivou Saveta Evrope.[14]

[11] Google Transparency report dostupan je ovde https://transparencyreport.google.com/government-removals/overview?hl=en_US
[12] https://transparency.facebook.com/government-data-requests/country/RS
[13] Sporazum o uspostavljanju Platforme za evidenciju slučajeva ugrožavanja bezbednosti i pritisaka na novinare i ostale medijske aktere potpisala je Kancelarija Zaštitnika građana u partnerstvu sa 10 medijskih i novinarskih udruženja i sindikata medijskih radnika.
[14] Platforma SE je dostupna ovde https://www.coe.int/en/web/media-freedom

PREPORUKE ZA UNAPREĐENJE REGULATORNIH I SAMOREGULATORNIH MEHANIZAMA, POTENCIJALNI PRAVCI DELOVANJA:

- **Podsticanje neposredne saradnje sa kontakt tačkama u okviru mehanizma Stalne radne grupe za bezbednost novinara kako bi se osigurala neophodna hitnost u postupanju, a time i efikasnije prikupljanje digitalnih dokaza i identifikacija napadača;**
- **Nova platforma koja će pratiti pretnje i pritiske na novinare i medije u okviru inicijative Zaštitnika građana treba, već u osnovama svom angažmana, da prepozna i jasno navede specifičnosti pretnji i pritisaka koje dolaze iz onlajn sfere;**
- **Kroz mehanizam CERT sistema unaprediti bezbednost u infrastrukturi onlajn medija u Srbiji, kao i adekvatno procesuiranje napada ukoliko do njih dođe.**
- **Intenzivirati međunarodnu saradnju sa vodećim društvenim mrežama, jer su upravo društvene mreže glavni kanal upućivanja nedozvoljenih pretnji i pritisaka. Bolje iskoristiti instrumente međunarodne politike (na primer, kroz radne grupe OEBS-a, Saveta Evrope i sl.) i učešće na internacionalnim forumima za intenziviranje ove saradnje.**

III b. PRAĆENJE, NADZOR I ZAŠTITA IZVORA

Zahvaljujući savremenim tehnologijama, video nadzoru, praćenju komunikacija putem elektronskih uređaja i sl., komunikacije novinara mogu biti, ovlašćeno ili neovlašćeno, presretnute. Problem je utoliko veći jer **ne postoji dovoljna transparentnost u korišćenju sredstava nadzora, niti kontrolni mehanizmi koji će sprečiti zloupotrebu, dalju analizu ili dalje korišćenje, ovako prikupljenih podataka**.

Ovakva okolnost ne samo da ugrožava bezbednost i privatnost samih novinara, već i njihovih izvora. Osim na dokumentima i podacima, novinarski tekstovi zasnivaju se i na prikupljanju informacija od nezavisnih i kompetentnih izvora. **Većina istraživačkih novinarskih priča kojima se otkrivaju slučajevi „krupne" korupcije počivaju upravo na poverljivim informacijama izvora ili uzbunjivača**.

Zakonom, ali i profesionalnim i etičkim standardima profesije, novinari su dužni da ovakvim izvorima obezbede anonimnost i čuvaju njihovu tajnost.

Trenutni pravni okvir obezbeđuje pravo čuvanja novinarske tajne (Član 52 *Zakona o javnom informisanja i medijima*) i propisuje da novinar nije dužan da otkrije izvor informacije, osim u slučajevima kad je reč o podacima koji se odnose na krivična dela za koje je zaprećena kazna zatvora od najmanje pet godina. Dodatno, Član 41 (Zaštita izvora informacija) Krivičnog zakonika pruža zaštitu novinarima i urednicima, te oni ukoliko ne otkriju identitet izvora informacija, ne mogu se krivično goniti.

Trendovi pokazuju (a oni su naročito vidljivi u zemljama malog demokratskog kapaciteta, poput Srbije) da će **nadzor, uz već postojeće mehanizme finansijske kontrole i uticaja na ekonomsku održivost medija, biti jedan od najefikasnijih sredstava kontrole medija**.

„Kada smo objavili prvo istraživanje u KRIK-u naši novinari počeli su da sreću ljude ulicom koji ih prate, fotografišu… Osim što su tabloidi pisali da smo 'soroševci', 'strani plaćenici' bilo je i transkripata naših telefonskih razgovora i komentarisanja radnih verzija naših tekstova, a koji nisu objavljeni".

Dragana Pećo, novinarka portala KRIK na debati UNS-a[15].

Nekoliko primera iz poslednje dve godine svedoči o tome. U toku februara 2020. godine novinska agencija Tanjug, TV Pink kao i nekoliko drugih medija prenelo je izjavu ministra Aleksandra Vulina kao reakciju na autorski tekst bivšeg ministra odbrane Dragana Šutanovca iz magazina Nedeljnik. Problem sa pomenutom izjavom je u tome što navedeni autorski tekst nikada nije objavljen u Nedeljniku, niti u bilo kom drugom mediju[16]. Ovaj slučaj otvorio je pitanje prisluškivanja novinara i nadzora njihovih elektronskih komunikacija. U toku vanrednog stanja zbog pandemije korona virusa, uhapšena je Ana Lalić, novinarka portala nova.rs. Policija je privela novinarku nakon što je Klinički centar Vojvodine obavestio tužilaštvo i policiju da je svojim tekstom uznemirila javnost i naštetila ugledu te zdravstvene ustanove. Tom prilikom, policija je uzela njen laptop i mobilne telefone na kojima se nalazila celokupna njena prepiska sa izvorima[17]. U toku 2019. godine, uz burnu reakciju javnosti, oslobođen je pritvora Aleksandar Obradović, glavni izvor za istraživačku priču o umešanosti Branka Stefanovića, oca ministra policije, u trgovinu oružjem, poslu koji za račun interesa privatne firme stvara gubitak državnoj firmi Krušik[18].

Problem neovlašćenog nadzora i pristupa komunikacijama novinara detektovan je i u Medijskoj strategiji, mera 1.3, u kojoj se navodi:

Problem je utoliko veći, ako sami državni organi neovlašćeno pristupaju sadržini komunikacije ili zadržanim podacima. Izmenama Zakona o elektronskim komunikacijama iz 2014. godine uvedena je obaveza za operatore i nadležne organe da dostavljaju statističke evidencije o zadržanim podacima. Javno dostupni podaci pokazuju da se ni posle izmena zakona nije smanjila frekvencija pristupa od strane državnih organa, pa je tako utvrđeno da su državni organi, tokom 2015. godine, samo kod jednog operatora pristupili 300.845 puta, u 2016. godini 293.244 puta, a u 2017. godini čak 381.758 puta. Među tih nekoliko stotina hiljada (samostalnih) pristupa, mogli su da se nađu i novinari, čija bi komunikacija mogla da bude kompromitovana, a izvor ugrožen.

Medijska strategija, mera 1.3

Pomenuti *Zakon o elektronskim komunikacijama*[19] u članu 128 navodi da su operateri dužni da zadrže podatke o elektronskim komunikacijama (praćenje i utvrđivanje izvora komunikacije; utvrđivanje odredišta komunikacije; utvrđivanje početka, trajanja i završetka komunikacije; utvrđivanje vrste komunikacije; identifikaciju terminalne opreme korisnika; utvrđivanje lokacije mobilne terminalne opreme

[15] http://uns.org.rs/desk/UNS-news/95160/potrebno-je-formirati-jaku-komisiju-koja-ce-istraziti-aferu-vulinge-jt-video.html
[16] https://www.danas.rs/drustvo/nedeljnik-odakle-ministru-vulinu-tekst-iz-nedeljnika-koji-nikada-nije-objavljen/
[17] https://www.raskrikavanje.rs/page.php?id=Ana-Lalic-Prepiska-sa-izvorima-mi-je-u-telefonima-koji-mi-jos-nisu-vraceni-637
[18] https://javno.rs/vest/uzbunjivac-obradovic-za-birn-zeleo-sam-da-se-sazna-istina-o-krusiku
[19] Zakon o elektronskim komunikacijama Sl. glasnik RS, br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon

korisnika), kao i da pristup zadržanim podacima nije dopušten bez pristanka korisnika, osim na određeno vreme i na osnovu odluke suda.

Bez obzira na ove odredbe, a prema rečima Đorđa Krivokapića[20] iz SHARE Fondacije, **policija i srodne službe mogu da pristupaju elektronskoj komunikaciji direktno u meri u kojoj žele, što je pokazatelj da u ovoj oblasti nema vladavine prava, ali ni poverenja građana u institucije**.

U odgovoru na ovaj problem, sami novinari i mediji moraju konstantno unapređivati svoje znanje, alate i sisteme zaštite, jer je to jedan od ključnih preduslova zaštite osetljivih, privatnih podataka i podataka o izvorima u digitalnoj sferi[21]. Sa druge strane, država mora da obezbedi sistemsku transparentnost i odgovornost u pogledu politika o zadržavanju podataka i nadzor (uključujući masovni i ciljani nadzor), kao i da unapredi politike zaštite novinarskih izvora i politike zaštite privatnosti tako da odgovaraju digitalnom dobu.

Medijska strategija (*Strategija razvoja javnog informisanja u RS 2020-2025*), na primer, regulatornog odgovora na ovaj problem predviđa izmenu medijske regulative i regulative koja uređuje oblast elektronskih komunikacija kako bi se uredila oblast zaštite novinarskih izvora, propisivanjem elemenata ovog prava; ali i izmene krivičnog zakonodavstva u cilju uvođenja krivičnopravne zaštite tajnosti novinarskih izvora i izmenom regulative (*Zakonika o krivičnom postupku*), definisanje novinara kao lica koja su zbog dužnosti čuvanja profesionalne tajne oslobođena od dužnosti svedočenja ukoliko bi svojim iskazom povredili dužnost čuvanja profesionalne tajne.

PREPORUKE ZA UNAPREĐENJE REGULATORNIH I SAMOREGULATORNIH MEHANIZAMA, POTENCIJALNI PRAVCI DELOVANJA:

- **Izmene *Zakona o elektronskim komunikacijama* treba da iznova definišu i ograniče krug prava za zakonito presretanje elektronske komunikacije, jer ova praksa nije u skladu sa pravilima zaštite privatnosti;**
- **Sami novinari i mediji treba da prošire znanja u vezi sa digitalnom bezbednošću i bezbednošću komunikacija, kao i da izrade i uvedu sigurnosne protokole u svoj svakodnevni rad kako bi zaštitili sebe i svoje izvore.**

[20] Gostovanje na televiziji N1 http://rs.n1info.com/SciTech/a595473/Krivokapic-Podaci-iz-elektronskih-komunikacija-dostupni-drzavnim-organima.html

[21] Jedan od korisnih resursa može biti i publikacija Share Fondacije https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic_bezbednost_organizacija_u_digitalnom_okruzenju.pdf

IV VESTI KOJIMA NE TREBA DA VERUJETE: BORBA PROTIV DEZINFORMACIJA

Tokom pandemije Kovida-19 u Centralnoj i Jugoistočnoj Evropi (uključujući i Srbiju), više od polovine slučajeva kršenja digitalnih prava povezano je sa propagandom, dezinformacijama, neistinama i objavljivanjem neproverenih informacija, pokazuju nalazi monitoringa koje su sproveli BIRN i SHARE Fondacija[22].

Dramatičan porast broja dezinformacija u vreme krize pokazuje da se radi o značajnom društvenom problemu koji utiče na kvalitet javnog informisanja i koje je ugroženo namernim, masovnim i sistematičnim širenjem dezinformacija.

POD POJMOM LAŽNIH VESTI (termin preuzet iz engleskog fake news) podrazumeva se objavljivanje netačnih ili obmanjujućih informacija u formi vesti.

Lažne vesti mogu imati nekoliko pojavnih oblika, od satire i parodije, do glasina, propagande i dezinformacija koje podrazumevaju namerno i sistematično širenje lažnih vesti. Širenje dezinformacija posebno je povezano sa trendom politike post-istine, info ratovima i mešanjem u izborne procese u jednoj zemlji.

Posledice širenja dezinformacija mogu biti tolike da ugroze čitave demokratske procese u pojedinim zemljama, kako vrlo slikovito pokazuje slučaj Cambridge Analytica, gde je dezinformacijama targetirana publika putem društvenih mreža, koristeći pre svega neautorizovan pristup ličnim podacima, a sa ciljem da se utiče na ishod referenduma (Brexit) u Velikoj Britaniji.

Osim društvenih mreža, koje su posebno istaknute kao platforme za širenje dezinformacija, treba imati u vidu i druge tehnologije kao što su servisi za direktne poruke (direct messaging platforms), deep fake video materijal, botovi (automated software, bots), i sl.

Od širenja dezinformacija nisu pošteđeni ni uobičajeni kanali komunikacije kao što se televizijske stanice, mediji, veb sajtovi. U velikom broju slučajeva pojedini mediji mogu biti i generatori ove vrste sadržaja. Projekat *Raskrikavanje*[23] istraživačkog portala Krik pokazuje da su **tabloidi posebno problematičan izvor informisanja, jer objave više desetina lažnih vesti u svojim medijima** – u vrhu liste su Informer, Alo i Srpski telegraf.

Koliko brzo napreduju tehnike širenja toliko brzo treba da reaguju institucije. **U Srbiji trenutno nema regulatornog okvira za borbu protiv dezinformacija.** Ovaj pojam se spominje jednom u delu Medijske strategije u kom se navodi da „Promena preferencija publike i tehničke mogućnosti dovele su i do negativnih pojava koje se ogledaju u širenju govora mržnje ili dezinformacija (engl. fake news)".

[22] Izveštaj dostupan na https://javno.rs/analiza/vise-od-160-slucajeva-krsenja-digitalnih-prava-tokom-pandemije-kovida-19

[23] https://www.raskrikavanje.rs/kesformisanje/

„Sistem sveobuhvatnog monitoringa je neizvodljiv, jer je nemoguće oformiti dovoljno veliki tim koji bi proverio sve što u Srbiji objavljuju mejnstrim mediji, a kamoli svi registrovani i fantomski mediji. Vreme za proveru teksta najčešće je višestruko duže od vremena koje je bilo potrebno da se tekst napiše, što znači da bi sveobuhvatni monitoring zahtevao više uposlenih nego što je novinara u Srbiji".

Stefan Janjić, urednik portala FakeNews Tragač

Set mera koji je osmišljen Medijskom strategijom (u glavi 5. strategije) podrazumeva aktivnosti koje nisu regulatorne, već se kreću u pravcu unapređenja medijske pismenosti, samoregulacije i sl.

U Srbiji, kao deo samoregulatornih praksi, od ove godine Facebook je pokrenuo zvanično partnerstvo sa Istinomerom i agencijom France-Presse (AFP)[24] u suzbijanju dezinformacija na ovoj društvenoj mreži. Ove dve organizacije će proveravati sadržaj i skenirati lažne vesti i informacije na srpskom jeziku koje se objavljuju na ovoj društvenoj mreži. Stvarni efekat ovakvog partnerstva tek treba da se vidi, ali ideja vodilja je da kada se neka priča oceni kao neistinita, Facebook umanjuje njenu vidljivost i distribuciju, označava sadržaj kao dezinformaciju i onemogućava reklamiranje stranicama koje učestalo šire lažne vesti[25].

Otežavajuća okolnost za suštinsku borbu protiv dezinformacija u Srbiji predstavlja i činjenica da one nekad dolaze i iz samog vrha vlasti, kao i da su deo šire javne kampanje i obračuna sa političkim protivnicima ili kritičarima vlasti.

„Ne možemo zaboraviti da pojedinci iz vlasti zapravo predstavljaju pokretač brojnih dezinformacija, da svesrdno podržavaju propagandni program i ne razumeju medije. Takva situacija ne može ulivati poverenje građanima da će u borbu protiv dezinformacija država ući sa čistim namerama. To me sve navodi da je bolje da se koliko - toliko ta priča zadrži unutar profesije i na nivou samoregulacije".

Vesna Radojević, urednica portala Raskrikavanje

U aprilu ove godine, društvena mreža Twitter uklonila je više od osam hiljada profila koji su u prethodnom periodu isključivo služili „promociji vladajuće stranke u Srbiji i njenog lidera". Na zvaničnom profilu kompanije saopšteno je da „Krajem prošle godine, identifikovali smo niz povezanih naloga uključenih u koordinisanu akciju namenjenih promociji vladajuće partije u Srbiji i njenog lidera. Ovakvo delovanje je u suprotnosti sa našim propisima i predstavljaju nameran pokušaj ugrožavanja slobode javnog izražavanja ".

[24] https://www.istinomer.rs/arhiva/saopstenja/istinomer-medju-novim-fejsbukovim-partnerima-u-borbi-protiv-dezinformacija/
[25] https://www.facebook.com/business/help/2593586717571940?id=673052479947730

PREPORUKE ZA UNAPREĐENJE REGULATORNIH I SAMOREGULATORNIH MEHANIZAMA, POTENCIJALNI PRAVCI DELOVANJA:

- Osmisliti inovativna i efikasna samoregulatorna, koregulatorna i regulatorna rešenja u borbi protiv dezinformacija koje narušavaju pluralitet mišljenja i negativno utiču na javno mnjenje, kvalitet javne debate i narušavaju poverenje u medije. U osmišljavanju ovih pravila intenzivirati konsultacije sa EU i harmonizaciju sa evropskom praksom;
- Kampanje medijske pismenosti treba podržavati i učiniti vidljivim što većem broju korisnika;
- U izveštavanju voditi se preporukama i Etičkim kodeksom novinara, te uložiti napor u dodatnu proveru izvora i tačnost informacija.
- Dodatno ojačati kapacitete Saveta za štampu kao jedinog samoregulatornog tela koje se bavi primenom Etičkog kodeksa novinara Srbije, između ostalog i u domenu istinitosti izveštavanja i širenjem dezinformacija.

V INFORMACIJE IZ CRNE KUTIJE: ALGORITAMSKO UPRAVLJANJE SADRŽAJEM

Svaki digitalni trag, sadržaj koji je objavljen na internetu ili profilima na društvenim mrežama, obrađuje se u tzv. crnim kutijama veštačke inteligencije ili algoritama[26].

POD ALGORITMOM SE PODRAZUMEVA skup operacija potrebnih za rešavanje nekog zadatka koja se izvršavaju po tačno određenom redosledu.

Svaki algoritam se sastoji od početka (ulaz) i kraja (izlaz), dok se između nalaze elementi koji sadrže definisani put ka rešenju zadatka.

„Unutar tih nevidljivih zidova, u svakom trenutku algoritmi odlučuju koja će se informacija pojaviti u našoj infosferi, koliko i koji vaši prijatelji će videti vašu objavu, koja vrsta sadržaja će postati deo vaše realnosti, a šta će biti cenzurisano ili obrisano. Negde duboko ispod slojeva algoritamskih mašina, mogu se kriti novi oblici mogućih kršenja ljudskih prava, novi oblici eksploatacije i mehanizama manipulacije, koji u velikoj meri utiču na milijarde ljudi svakoga dana".

SHARE LAB[27]

Algoritmi imaju sveobuhvatan uticaj na slobodu izražavanja i na medijske slobode. Oni utiču na naše celokupno informaciono okruženje („AI svuda") te regulišu vidljivost sadržaja; algoritamski vođene aplikacije odlučuju sa kojim publikama sadržaj komunicira; upravljaju pretragom podataka (ovo je naročito važno u svetlu korporativnog monopola nad internet pretraživačima, poput Google-a); algoritamska personalizacija omogućava targetiranje korisnika sadržajem koji može dovesti do efekta tzv. „informacijskog balona" (engl. information bubble) i komuniciranja u krugu istomišljenika, učvršćivanju postojećih predrasuda (engl. information bias) itd.

Nedostatak transparentnosti, nedostatak perspektive ljudskih prava i nedostatak zakonske obaveze pri korišćenju ili promeni algoritama glavni su nedostaci algoritamskih informacionih sistema.

„Uz neke izuzetke, ustanovili smo da kompanije uglavnom nisu otkrile dovoljno informacija o silama koje oblikuju naše informaciono okruženje. Facebook, Google i Twitter ne skrivaju činjenicu da oni koriste algoritme za oblikovanje sadržaja, ali manje predočavaju kako algoritmi zapravo rade, koji faktori utiču na njih i kako

[26] Algoritam predstavlja skup operacija potrebnih za rešavanje nekog zadatka koja se izvršavaju po tačno određenom redosledu.

[27] https://resursi.sharefoundation.info/sr/resource/nematerijalni-rad-i-prikupljanje-podataka-algoritamska-fejsbuk-fabrika/

korisnici mogu koristiti algoritme da prilagode svojim potrebama“[28].

Imajući u vidu značaj razumevanja i transparentnosti u radu algoritama, ali i velike mogućnosti za njihovu zloupotrebu, Savet Evrope je 2018. godine usvojio Preporuku o medijskom pluralizmu i transparentnosti vlasništva nad medijima – uloga internet posrednika u kreiranju i distribuciji (medijskog) sadržaja ostvaruje uticaj na raznovrsnost i transparentnost kao osnove demokratskog društva.

Predlog iznet u Preporukama je da automatsko donošenje odluka, koje rukovodi distribucijom informacija, bude unapređeno tako da građani imaju pristup najvećoj mogućoj raznolikosti onlajn sadržaja. Selektivna izloženost određenom sadržaju kao i ograničenja koja iz ove situacije proističu mogu da dovedu do još veće polarizacije društva.

Za razumevanje informacionog okruženja i upravljanje medijskim sadržajem važno je razlikovati dva tipa algoritama:

1) **algoritmi za oblikovanje sadržaja**. Ovi sistemi „uparuju“ sadržaj sa korisnikom i određuju sadržaj koji svaki pojedinačni korisnik vidi na mreži, uključujući korisničke ili „organske“ postove i plaćene oglase. Facebook-ov News Feed, Timeline na Twitter-u ili preporučeni sadržaj na YouTube-u su neki od primera ovih algoritama;

2) **algoritmi za moderaciju sadržaja**, tj. za uklanjanje sadržaja koji krše pravila samih kompanija i društvenih mreža. Ovakvi algoritmi su naučeni da, bez interakcije sa ljudima, uklone sadržaj koji je štetan ili opasan. Ovi algoritmi najbolje rade kada imaju na raspolaganju jednostavna i jasna pravila za detektovanje ovakvog sadržaja. Međutim, algoritmima je i dalje teško da prepoznaju sadržaj koji ima elemente nasilja, mržnje ili pogrešne informacije, a da one i kao takve imaju značaja za javno informisanje i javnost. U ovakvim slučajevima, intervencija moderatora je ključna i odluka o ukidanju sadržaja ne može se prepustiti isključivo veštačkoj inteligenciji.

U odnosu na prvi tip, i način na koji promena u radu algoritama može da utiče na domet sadržaja i rad medija, najbolje oslikavaju rezultati šestomesečnog eksperimenta kompanije Facebook (eksperiment je osim u Srbiji, sproveden još u Slovačkoj, Kambodži, Boliviji i Gvatemali), koja je u toku 2017. godine odlučila da razdvoji *news feed* tako da odvoji postove „korisnika“ od plaćenih „stranica“, među kojima su se našle i stranice medija i istraživačkih centara. Stranice „korisnika“ bile su smeštene u primarni *news feed*, što je rezultiralo time da je vidljivost medijskih tekstova i objava dramatično pala (procene pojedinih medija variraju od 50% do 80%)[29], što je dalje uticalo i na protok informacija, javnu debatu i samu održivost medija[30].

Pod pritiskom javnosti, regulatora i medijskog sektora koji doživljava duboku ekonomsku krizu i krizu biznis modela podstaknutu upravo delovanjem društvenih mreža, kompanije poput Facebook-a i Google-a, najavljuju promene u algoritmima i rangiranju sadržaja. Algoritmi Facebook-a u Google-a favorizovali su i nagrađivali medijske sadržaje koji su atraktivni, proizvode brze reakcije, a od sada bi trebalo da daju prednost sadržajnim, argumentovanim vestima i tekstovima.

Najavljeno je da će Fejsbuk unaprediti način rangiranja vesti u okviru njuz fida, kako

[28] Iz izveštaja *Its not just a content, its a business model: Democracys Online Speech Challenge* https://www.
to-the-black-box

[29] https://www.cima.ned.org/blog/facebooks-explore-feed-experiment-threatens-independent-voices-serbia/

[30] https://www.nytimes.com/2017/11/15/opinion/serbia-facebook-explore-feed.html

bi se dao prioritet originalnom, relevantnom i činjeničnom izveštavanju[31]. Kompanija je sarađivala sa medijskim izdavačima da se što preciznije definiše šta je 'originalna vest' kako bi algoritmi bustovali originalne priče i pomogli korisnicima tokom pretrage. Promene algoritma, za sada, biće primenjene samo na vesti, i to samo na engleskom jeziku, sa nadom da će u budućnosti biti proširene i na druge jezike. Najavljena promena u algoritmu je mali, ali konkretan potez koji je FB povukao kako bi umanjio uticaj i širenje dezinformacija.

U odnosu na drugi tip algoritama i automatskog uklanjanja sadržaja, baza BIRN-a i SHARE Fondacije pokazuje ukupno 24 slučaja algoritamskog blokiranja i uklanjanja sadržaja[32]. Od svih slučajeva, tri su uključivala novinske kuće (Južne vesti, BIRN i Danas), dok je dodatnih sedam slučajeva uključivalo novinare i blogere.

Analiza slučajeva pokazuje da je kršenje autorskih prava osnova za uklanjanje sadržaja u šest slučajeva. Pitanja autorskih prava i intelektualne svojine od suštinske su važnosti za očuvanje integriteta novinarskog rada i održivog modela poslovanja. Algoritamska uklanjanja na osnovu kršenja autorskih prava obično se rešavaju isključivanjem monetizacije sadržaja ili deljenjem prihoda od sadržaja (kakav je bio slučaj sa Južnim vestima) između medija i nosioca autorskih prava.

Kriterijumi za algoritamsko uklanjanje osetljivijih tema su mnogo manje transparentni, ali i dalje presudno važni kada je reč o informisanju javnosti. Kao što pokazuju i ostali prijavljeni slučajevi u bazi podataka BIRN-a i SHARE fondacije, drugi osnovi za uklanjanje sadržaja uključuju kršenje privatnosti i sadržaja koji je algoritam prepoznao kao štetan, što obično uključuje kontroverzne teme kao što je spor Kosova i Srbije, slučaj silovanja Romkinje, presude Haškog tribunala o ratnim zločinima, itd. Sve su to važne teme za javnu raspravu i ukupni demokratski diskurs, ali kako one obično donose kontroverzu i visoko polarizovana gledišta u društvu, često se prijavljuju administratorima[33].

Na domaćoj medijskoj sceni gotovo da nije bilo nikakve debate o algoritamskom upravljanju sadržajem.

Medijska strategija samo u jednom delu analize stanja pominje algoritme u kontekstu izazova sa kojima se suočavaju mediji u digitalnom dobu:

> „Publici u digitalnom okruženju potrebna su i digitalna prava, koja podrazumevaju zaštitu privatnosti korisnika (uključujući tu i pravo na zaborav), informacionu bezbednost, blokiranje reklama i transparentnost rada algoritama, i dr. Promena preferencija publike i tehničke mogućnosti dovele su i do negativnih pojava koje se ogledaju u širenju govora mržnje ili dezinformacija (engl. fake news)".

Strategija ne podrazumeva izmene regulative kao odgovor na prepoznate probleme, već kao rešenje nudi medijsku pismenost, ali i istraživanja i proširenje baze znanja, saradnju sa relevantnim domaćim i međunarodnim institucijama, kao i debatu i dijalog različitih zainteresovanih strana.

Ulogom algoritama i veštačke inteligencije mnogo detaljnije se bavi *Strategija razvoja*

[31] https://www.axios.com/facebook-algorithm-original-reporting-e127c8b7-c749-4120-a65e-239b55d18758.html
[32] https://monitoring.bird.tools/data?category=Blocking%20and%20filtering%20of%20content
[33] Više o uklanjanju sadržaja na društvenim mrežama dostupno je ovde https://gfmd.info/gfmd-content/uploads/2020/11/DC-Sustainability-Annual-Report-2020-FINAL.pdf

veštačke inteligencije u Republici Srbiji[34]. Ova strategija u okviru posebnog cilja 5 (Etična i bezbedna primena veštačke inteligencije) propisuje i posebne mere poput zaštite ličnih podataka, zaštitu korisnika od diskriminacije i obezbeđivanje odgovornog razvoja veštačke inteligencije, gde svaka od ovih mera ima implikacije i na informisanje i medijske slobode.

Ipak, navedene mere u okviru strategije nisu do kraja razvijene, pa je prilika i da se medijski sektor uključi aktivnije u ovu debatu i predloži rešenja koja bi bila u skladu sa standardima ljudskih prava u ovoj oblasti.

PREPORUKE ZA UNAPREĐENJE REGULATORNIH I SAMOREGULATORNIH MEHANIZAMA, POTENCIJALNI PRAVCI DELOVANJA:

- **Medijski sektor treba da postane aktivni učesnik u debatama o razvoju veštačke inteligencije i algoritama, jer njihova upotreba utiče na slobodan protok informacija i moderaciju i upravljanje sadržajem. Medijski sektor naročito treba da bude uključen u razvoj etičkih standarda, kako je predviđeno nacionalnom *Strategijom razvoja veštačke inteligencije u RS*;**
- **Detaljno se upoznati sa *Kodeksom dobre prakse*, uslovima za korišćenje platformi i servisa, mehanizama za prijavu povreda prava, analizirati podatke iz izveštaja o transparentnosti, te koristiti i druge alate koji su već dostupni, javni i na raspolaganju novinarima i medijima;**
- **Prilagoditi etičke i profesionalne standarde novoj realnosti, te na taj način zaštititi svoje korisnike.**

[34] http://www.mpn.gov.rs/wp-content/uploads/2019/11/1-Nacrt-strategije-razvoja-ve%C5%A1ta%C4%8Dke-inteligencije-u-Republici-Srbiji-za-period-2020.-2025.-godine.pdf

ANEKS I

Komparativne prakse evropskih zemalja: regulacijom protiv dezinformacija

Komparativne prakse zemalja EU pokazuju sličnu tendenciju. Na primer, Evropska unija je kreirala *Akcioni plan za borbu protiv dezinformacija* u decembru 2018[35]. Ovaj plan predviđa četiri stuba aktivnosti: 1. *Unapređenje kapaciteta evropskih institucija da detektuju, analiziraju, razotkriju dezinformacije* (podrazumeva dodatne resurse u vidu eksperata za pretrage podataka i analizu procesiranja relevantnih podataka, kao i dodatni monitoring medija i razvoj softvera koji mogu da istražuju, analiziraju, objedinjuju velike količine digitalnih podataka); 2. *Jačanje koordiniranog i zajedničkog/udruženog odgovora na dezinformacije* (uspostavljanje sistema brzog uzbunjivanja će omogućiti upozorenja na kampanje dezinformacija u realnom vremenu); 3. *Mobilisanje privatnog sektora da se bavi dezinformacijama* (onlajn platforme, oglašivači, oglašivačka industrija imaju ključnu ulogu u rešavanju problema dezinformisanja. Evropska komisija je 2018. godine objavila *Kodeks dobre prakse o suzbijanju dezinformacija* koji su potpisale vodeće onlajn platforme i obavezale se da sprovedu neophodne akcije); 4. *Podizanje svesti građana i jačanje društvene rezilijentnosti* (neophodno je razumeti kako i zašto građani, a nekad i cele zajednice, padaju pod uticaj narativa dezinformacija i definisati objašnjenje i odgovor na ovaj fenomen. Evropska komisija će: organizovati medijske kampanje; kreirati timove istraživača i *fact-checkers*, koji poznaju lokalno digitalno okruženje, da detektuju i obelodane dezinformacije na različitim platformama; povećati nivo medijske pismenosti).

I vodeće zemlje Evrope poput Nemačke, Velike Britanije i Francuske aktivno rade na osmišljavanju nacionalnog regulatornog okvira koji bi odgovorio na problem nekontrolisanog širenja dezinformacija.

Francuska je predstavila okvir za regulaciju društvenih mreža[36] koji se oslanja na pet osnovnih stubova: prvi, na očuvanje slobode izražavanja, kao i preduzetničkih sloboda; drugi, na obaveze samih platformi koje treba da osiguraju transparentnost u priređivanju sadržaja (content curation), sprovođenju pravila mreže i zaštita integriteta korisnika; treći, informisan dijalog između vlade, civilnog društva i zainteresovanih strana; četvrti, formiranje nezavisne regulatorne institucije; i peti, saradnja na nivou EU.

Nemački Bundestag je usvojio Zakon o izvršenju na društvenim mrežama (tzv. Zakon o Fejsbuku)[37] koji je stupio na snagu 1. oktobra 2017. godine. U skladu sa odredbama ovog zakona, platforme društvenih mreža koje prime više od sto žalbi na nezakonite sadržaje u toku kalendarske godine, u obavezi su da podnesu zvanični izveštaj svakih šest meseci koji će biti objavljen u Službenom glasniku. Takođe, ovi izveštaji moraju biti vidljivi i lako dostupni i na njihovim matičnim sajtovima. Svu odgovornost za obradu žalbi snose društvene mreže, i moraju da obezbede procedure koje transparentne i efikasne. Sve procedure moraju biti lako dostupne korisnicima. Vrlo je jasno definisana odgovornost i obaveza platformi

[35] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[36] http://thecre.com/RegSM/wp-content/uploads/2019/05/French-Framework-for-Social-Media-Platforms.pdf
[37] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

kada je u pitanju postupanje po žalbama, pa tako moraju da: 1. Uklone ili blokiraju nelegalan sadržaj po dobijanju žalbe; 2. U slučaju uklanjanja, sadržaj se zadržava kao dokaz i skladišti u skladu sa EU direktivama; 3. Postupanje po žalbama mora da se prati na mesečnom nivou i da bude pod nadzorom rukovodstva/menadžmenta. Bilo kakvi organizacijski nedostaci moraju biti odmah uklonjeni. Menadžment društvenih mreža mora redovno da obezbedi zaposlenima zaduženim za procesuiranje žalbi obuku i programe podrške na nemačkom jeziku, ne manje od jednom u šest meseci; 4. Društvene mreže su u obavezi da imenuju osobu odgovornu za saradnju sa institucijama Savezne Republike Nemačke. Takođe, na onlajn platformama jasno mora biti naznačen i vidljiv kontakt odgovorne osobe.

Za razliku od prethodne pravne prakse, gde su operateri mreža, pod pretnjom kazne morali da obrišu sadržaje, nova rešenja ih obavezuju da prijave sporne tekstove, snimke ili slike, ali i da Saveznoj kriminalističkoj službi (BKA) proslede podatke kao što su login, IP adresa ili broj porta korisnika, i to pre nego što se utvrdi postojanje osnovne sumnje da je počinjeno krivično delo[38].

Pod pritiskom javnosti i evropskih regulatora, onlajn platforme i društvene mreže usvojile su tzv. *Kodeks dobre prakse* (*Code of Practice on disinformation*)[39], skup

Šta nudi onlajn crno tržište?

Crno tržište za manipulaciju društvenim medijima ima u ponudi tri segmenta - lako pristupačno otvoreno tržište, dark web i oflajn usmeno tržište, kao neformalne kanale za kupovinu lajkova, šerova, komentara, naloga, pretplatnika/sabskrajbera. Uprkos postojanju uslova korišćenja društvenih medija, industrija nudi trgovinu reakcijama na društvenim medijima, a i dalje je legalna u većini zemalja, koji znatno utiču na formiranje javnog mnjenja.

Koji alati su dostupni na crnom tržištu?

Lažni nalozi (fake accounts) – bazičan je alat koji omogućava manipulaciju reakcijama na DM (share, likes, comments, itd.) Cena u velikoj meri zavisi da li su registrovani automatski, manualno ili hakovani. Postoji niz drugih elemenata koji diktiraju tržišnu vrednost:

- **Provera naloga** (account verification) – može biti putem broja mobilnog telefona ili mejl naloga, verifikovani nalozi su skuplji, zato što ih je teže detektovati. Takođe, postoje i različiti stepeni verifikacije.

[38] Novine koje donosi nemački Zakon o izvršenju na društvenim mrežama naišao je na brojne kritike. Recimo Article 19, međunarodna organizacija koja se bavi ljudskim pravima, izrazila je duboku zabrinutost da naznačeni zakon ugrožava slobodu izražavanja i daje opasan primere vladama drugih zemalja da intenzivnijom primenom krivičnih odredbi guše kritički stav i ozbiljno utiču na r*ad novinara i boraca za ljudska prava.*

[39] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

- **Sadržaj** (content) – što više sadržaja je kreirano za lažni nalog, autentičnije će izgledati, u zavisnosti od zadatka koji treba da obavi, verodostojnost sadržaja naloga može se smatrati manje ili više poželjnom. Tržište nudi napredne usluge – naloge pravljene po meri, do te mere sofisticirane da ih je gotovo teško detektovati kao lažne.

- **Starost naloga** (account age) – za poverenje i kredibilitet bitna je i starost naloga, dostupne su različite varijante u rasponu od nekoliko dana do sedam godina starosti.

Manipulacija društvenom/socijalnom metrikom (Manipulating Social Mertics) dostupna je za sve velike platforme društvenih medija (u obliku – share, likes, comments) i koriste se različiti alati: automatizovani lažni nalozi, specijalne „freelance" platforme (koje u većini slučajeva angažuju ljude iz zemalja u razvoju), „razmena lajkova", gde se korisnicima nude lajkovi u zamenu za njihove, zlonamerni softveri koji funkcionišu bez dozvole korisnika. U ponudi se može pronaći i trending content na platformama kao što je YouTube.

Izvor: NATO Strategic Communications Center of Excellence i Singularex mapirali su tržište alata i usluga za manipulaciju na društvenim medijima