Preoblikovanje izborne kampanje korištenjem društvenih medija u Crnoj Gori

- Analytical Paper –

CeMI
CENTRE FOR MONITORING AND RESEARCH

IFES
International Foundation for Electoral Systems

CENTRE FOR MONITORING AND RESEARCH

International Foundation for Electoral Systems

PREOBLIKOVANJE IZBORNE KAMPANJE KORIŠTENJEM DRUŠTVENIH MEDIJA U CRNOJ GORI

- Analytical Paper –

Septembar 2020

PREOBLIKOVANJE IZBORNE KAMPANJE KORIŠTENJEM DRUŠTVENIH MEDIJA U CRNOJ GORI

- Analytical Paper –

Izdavač:
Centar za monitoring i istraživanje CeMI
Bul. Josipa Broza 23A
e-mail: info@cemi.org.me
www.cemi.org.me

Urednica:
Teodora Gilić

Autori:
Milica Zrnović
Ivan Vukčević
Vladimir Simonović

CENTRE FOR MONITORING AND RESEARCH

International Foundation for Electoral Systems

Ovaj dokument je objavljen u okviru Facebook Pilot projekta koji sprovodi Centar za monitoring i istraživanje (CeMI), u saradnji i uz finansijaku podršku Međunarodne Fondacije za izborne sisteme (IFES).

Sadržaj

Uvod

Internet se često definiše kao jedno od najvećih dostignuća modernog čovjeka, koje je brzo postalo vitalni aspekt našeg života. Ono nam omogućava pristup ogromnoj količini informacija i usluga i omogućava nam povezivanje i komunikaciju, ne samo sa ljudima koje poznajemo, već i sa velikim brojem nepoznatih ljudi širom svijeta. Internet se nastavlja ubrzano razvijati i njegov uticaj na svaki dio našeg života ne može se potcijeniti.

Upravo, ne bi se trebalo čudi što je evolucija Interneta vidljiva i u političkoj sferi. Tokom proteklih nekoliko godina, napravljene su značajne promjene u načinu na koji politički kandidati, organizacije i partije vode svoje izborne kampanje. Nekada su se kampanje održavale na javnim mjestima, sa onoliko ljudi koliko je moglo da popuni sale. Kasnije su kampanje evoluirale uključujući bilborde, spotove na radio stanicama, TV reklame, štampane oglase, itd. Danas je upotreba društvenih medija jedna od glavnih pokretačkih snaga političkih kampanja i izbora. Društveni mediji su brzo postali jedan od glavnih alata nekih od najuticajnijih političkih partija i subjekata i imali su veliki uticaj na to kako kandidati organizuju i strukturiraju svoje kampanje.

Imajući to u vidu, u poslednjih nekoliko godina sve je veća zabrinutost zbog štetnih sadržaja i nasilnih aktivnosti koje se posebno dijele na društvenim mrežama tokom izbornog perioda. Te aktivnosti uključuju lažne profile, neželjeni sadržaj, diskreditaciju oponenata, lažne vijesti, itd. Moramo biti svijesni da prijetnje ne samo društvenim medijima, već cjelokupnoj informacionoj i komunikacionoj infrastrukturi mogu ugroziti privatnost i integritet korisnika i uticati na druge aspekte našeg svakodnevnog života. Stoga su pouzdanost i sigurnost mreža, informacionih sistema i usluga od suštinskog značaja za ekonomske i društvene aktivnosti, posebno za funkcionisanje društva u cjelini.

U Crnoj Gori, Direkcija za informatičku bezbjednost i odgovor na kompjuterske incidente (CIRT) identifikovala je trend rasta broja prijavljenih internet i sajber incidenata (npr. uskraćeni pristup sistemu i ličnim podacima, razne mrežne prevare, itd.), kao i sofisticiranost samih napada. Incidenti s prijavljeni od strane javnog i privatnog sektora. U 2013. godini zabilježena su 22 incidenta, u 2014 - 42, 2015 - 132, 2016 - 163, 2017 - 385. Ukupan broj prijavljenih incidenata u periodu od 2013-2017 bio je 744, od čega se 17,2% odnosilo na zloupotrebe profila na društvenim mrežama i 5,65% na neprikladne sadržaje na Internetu[1].

U svjetlu Parlamentarnih izbora 2020. godine u Crnoj Gori, ovaj analitički paper ima za cilj pružanje opšteg pregleda nacionalnog pravnog okvira koji se odnosi na društvene medije i sajber sigurnost, kao i sagledavanje zakona koji regulišu društvene medije u drugim zemljama. Konačne preporuke i zaključci zasnovani su na nalazima analize sprovedene u svrhu pripreme i izrade ovog dokumenta.

[1] *Strategija sajber bezbjednosti Crne Gore 2018-2021, Decembar 2017*

1. Pravni i institucionalni okvir koji se odnosi na društvene medije u Crnoj Gori

Pravni okvir

Kada je riječ o društvenim medijima i regulatornom okviru koji se odnosi na korišćenje Interneta u Crnoj Gori, ne postoji zakon koji isključivo uređuje ovu oblast i bavi se pitanjima u vezi sa društvenim mrežama.

Neki od pravnih akata koje je ovdje važno pomenuti i koji regulišu sajber prostor i bezbjednost, kao i elektronske medije, komunikaciju i trgovinu su sljedeći:

1. Zakon o potvrđivanju Konvencije o računarskom kriminalu (Budimpeštanska konvencija)
2. Ustav Crne Gore
3. Krivični zakonik
4. Zakonik o krivičnom postupku
5. Zakon o informacionoj sigurnostiy
6. Zakon o elektronskim medijima
7. Zakon o elektronskim komunikacijama
8. Zakon o elektronskoj trgovini

Ostali akti koje je ovdje važno pomenuti su takođe:

- Strategija sajber bezbjednosti Crne Gore 2013 - 2017
- Strategija sajber bezbjednosti Crne Gore 2018 - 2021

Shodno Ustavu Crne Gore[2] potpisani i ratifikovani međunarodni dokumenti i ugovori, kao i prihvaćena pravila i standardi međunarodnog prava, imaju primat nad nacionalnim zakonodavstvom i sprovode se direktno kada uređuju drugačije od nacionalnih zakona. Dakle, mnoge međunarodne i evropske konvencije koje se bave materijom računarske bezbjednosti, kriminala ili slično, a koje je potpisala Crna Gora, prenose se u nacionalni zakon i neposredno se primjenjuju putem zakona nakon njihove ratifikacije.

Budimpeštanska konvencija Savjeta Evrope (Konvencija o računarskom kriminalu)[3] stupila je na snagu 2010. godine za Crnu Goru. Konvencija računarski kriminal definiše kao širok spektar djela - od širenja virusa, neovlašćenog pristupa računarskoj mreži, piraterije, pornografije i upada u bankarske sisteme, zloupotrebe platnih kartica ali i druga krivična djela koja uključuju upotrebu računara. Nadalje, Konvencija definiše kao krivično djelo akitivnosti povezane sa kršenjem autorskih i sličnih prava.

Crna Gora je takođe 2010. godine ratifikovala **Dodatni protokol uz Budimpeštansku konvenciju**[4] koji se odnosi na kriminalizaciju djela rasističke i ksenofobne prirode počinjena putem računarskih sistema, a iste je godine stupio na snagu u Crnoj Gori.

[2]Ustav Crne Gore („Sl. list CG", br. 1/2007 i 38/2013 - Amandmani I-XVI)
[3]Konvencija o računarskom kriminalu (Budimpeštanska konvencija), Savjet Evrope, 2001
[4]Dodatni protokol uz Budimpeštansku konvenciju koji se odnosi na kriminalizaciju djela rasističke i ksenofobne prirode počinjena putem računarskih sistema, Savjet Evrope, 2003

U skladu sa Konvencijom i njenim protokolom, **Crnogorski Krivični zakonik**[5] propisuje sankcije za skup aktivnosti, definisanih kao krivična djela, koja su direktno ili indirektno povezana sa sajber prostorom i sadržajem kreiranim na Internetu. **Član 370** definiše krivična djela koja izazivaju nacionalnu, rasnu i vjersku mržnju i predviđa da će svako ko javno podstiče na nasilje ili mržnju prema grupi ili članu grupe koja je određena na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti, kazniće se zatvorom od šest mjeseci do pet godina (stav 1). Ista sankcija propisana je za svakoga ko javno odobrava, negira postojanje ili značajno umanjuje težinu krivičnih djela genocida, zločina protiv čovječnosti i ratnih zločina učinjenih protiv grupe ili člana grupe koja je određena na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti, na način koji može dovesti do nasilja ili izazvati mržnju prema grupi lica ili članu takve grupe, ukoliko su ta krivična djela utvrđena pravosnažnom presudom suda u Crnoj Gori ili međunarodnog krivičnog suda(stav 2). Prilog „javno" dozvoljava tumačenje, uključujući mogućnost povezivanja tih krivičnih djela sa Internetom i online svijetom. Takođe, krivična djela udruživanje radi protivustavne djelatnosti (član 372) i pripremanje djela protiv ustavnog uređenja i bezbjednosti Crne Gore (član 373) omogućavaju tumačenje da se ta krivična djela mogu vršiti na Internetu[6].

Član 443 Krivičnog zakonika definiše krivična djela rasne i druge diskriminacije predviđajući da svako ko na osnovu razlike u rasi, boji kože, nacionalnosti, etničkom porijeklu ili nekom drugom ličnom svojstvu krši osnovna ljudska prava i slobode zagarantovane opšteprihvaćenim principima međunarodnog prava i potvrđenim međunarodnim ugovorima od strane Crne Gore, kazniće se zatvorom od šest mjeseci do pet godina (stav 1) i svako ko širi ideje o superiornosti jedne rase nad drugom ili promoviše rasnu mržnju, ili podstiče na rasnu ili drugu diskriminaciju kazniće se zatvorom od tri mjeseca do tri godine (stav 3).

Zakonik o krivičnom postupku[7] predviđa mjere za borbu protiv dječije pornografije na Internetu. Iako su ove mjere opšte odredbe koje se tiču postupaka prema maloljetnicima, Zakonik predviđa hitnost postupka, kao i isključenje javnosti, kada je riječ o tim djelima.

Zakon o informacionoj bezbjednosti[8] definiše pojam i mjere informacione bezbjednosti, odnosno fizičke zaštite, kao i zaštite podataka i informacionog sistema. Takođe predviđa da je Direkcija za informatičku bezbjednost i odgovor na kompjuterske incidente (CIRT) nadležni organ za prevenciju i zaštitu od računarskih bezbjednosnih incidenata na internetu i ostalih rizika bezbjednosti informacionih sistema državnih organa, pravnih i fizičkih lica u Crnoj Gori.

Zakon o elektronskim medijima[9] uređuje prava, obaveze i odgovornosti pravnih i fizičkih lica koja obavljaju djelatnost proizvodnje i pružanja audio-vizuelnih medijskih usluga (AVM usluga), usluga elektronskih publikacija putem elektronskih komunikacionih mreža nadležnosti, status i izvori finansiranja Agencije za elektronske medije sprječavanje nedozvoljene medijske koncentracije, podsticanja medijskog pluralizma i druga pitanja od značaja za oblast pružanja AVM usluga, u skladu s međunarodnim konvencijama i standardima (čl. 1).

Zakonom o elektronskim komunikacijama[10] uređuje se način upravljanja i korišćenja elektronskih komunikacionih mreža, uslovi i način obavljanja djelatnosti u oblasti elektronskih komunikacija, kao i druga pitanja od značaja iz ove oblasti (čl. 1). U Poglavlju XI, zakonom su propisane mjere i aktivnosti koje operater treba da preduzme u cilju zaštite elektronskih komunikacija i sprječavanja njihove zloupotrebe. Između ostalog, operaterima daje nadležnost

[5]Krivični zakonik Crne Gore ("Sl. list RCG", br. 70/2003, 13/2004 i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, 49/2018 i 3/2020)
[6]Izvještaj Savjeta Evrope, Montenegro Media Sector Inquiry with Recommendations for Harmonization with the Council of Europe and European Union standards, Savjet Evrope, 2017
[7]Zakonik o krivičnom postupku („Sl. list CG", br. 57/09)
[8]Zakon o informacionoj bezbjednosti ("Sl. list CG", br. 014/10 i 040/16)
[9]Zakon o elektronskim medijima ("Sl. list CG", br. 46/2010, 40/2011, 53/2011, 6/2013, 55/2016, 92/2017, 82/2020)
[10]Zakon o elektronskim komunikacijama („Sl. list CG", br. 40/2013)

da upozore ili privremeno blokiraju korisnički račun u slučaju da postoje dokazi da je korisnik poslao neželjenu poštu ili u slučaju zloupotrebe naloga elektronske pošte (član 179). Ako korisnik nastavi da zloupotrebljava elektronsku poštu, operater može trajno izbrisati korisnički račun raskine pretplatnika i raskinuti pretplatnički ugovor. Ako treća osoba zloupotrebi elektronsku poštu, korisnik je odgovoran samo ukoliko nije postupio u skladu sa upozorenjima operatera za preduzimanje mjera zaštite. Takođe, u slučaju prevare ili zloupotrebe iz djelokruga Zakona o elektronskim komunikacijama, operater ima obavezu da na zahtjev Agencije za elektronske komunikacije i poštanske usluge ili na sopstvenu inicijativu - u tom slučaju uz prethodno pribavljenu saglasnost Agencije - blokira pristup određenim brojevima i uslugama (član 145).

Zakon o elektronskoj trgovin[i11] definiše pojam „usluga informacionog društva" kao „uslugu koja se pruža na razdaljinu uz naknadu putem elektronske opreme za obradu i skladištenje podataka, na lični zahtjev korisnika, a posebno internet prodaja robe i usluga, nuđenje podataka na internetu, reklamiranje posredstvom interneta, elektronski pretraživači, kao i omogućavanje traženja podataka i usluga koje se prenose elektronskom mrežom, obezbjeđivanje pristupa mreži ili skladištenje podataka korisnika"(čl. 3).

Zakon predviđa da davalac usluge informacionog društva nije dužan pregledati podatke koje je skladištio, prenio ili učinio dostupnim, niti ispitivati okolnosti koje bi upućivale na nedopušteno djelovanje korisnika. Davalac usluga informacionog društva mora obavijestiti nadležni državni organ ako utvrdi da postoji osnovana sumnja da korišćenjem njegove usluge korisnik preduzima nedopuštene aktivnosti i ako postoji osnovana sumnja da je korisnik njegove usluge pružio nedopušteni podatak. Davalac usluga informacionog društva dužan je, na osnovu odgovarajućeg sudskog, odnosno upravnog akta, predočiti sve podatke na osnovu kojih se može preduzeti otkrivanje ili gonjenje počinilaca krivičnih djela, odnosno zaštita prava trećih lica(član 22).

Prva **Strategija sajber bezbjednosti Crne Gore 2013 - 2017**[12] sadrži sedam ključnih strateških ciljeva sa svrhom definisanja institucionalne i organizacione strukture na polju sajber bezbjednosti u državi, zaštite kritične informatičke infrastrukture u Crnoj Gori, jačanja kapaciteta i odgovora na incidentne situacije, te javno-privatno partnerstvo, kao i podizanje nivoa svijesti u društvu i zaštite na Internetu. Strategija je takođe predviđala uspostavljanje Nacionalnog savjeta za sajber bezbjednost, savjetodavnog tijela Vlade, osnovanog 2017. godine koje nadgleda sprovođenje Strategije sajber bezbjednosti, i lokalnih CIRT-ova, čiji je cilj jačanje sajber infrastrukture na lokalnom nivou.

Strategija sajber bezbjednosti Crne Gore 2018 - 2021[13] nastavak je prethodne strategije i definiše osam ciljeva za unaprjeđenje Nacionalne sajber strategije za Crnu Goru u periodu od 2018 - 2021. Oslanjanje na evropske i evroatlantske koncepte, jačanje međuinstitucionalne, regionalne, međunarodne saradnje i partnerstva javnog i privatnog sektora, zaštita podataka i edukacija u oblasti sajber bezbjednosti fokus su Strategije u narednim godinama.

Institucionalni okviri

Kada je u pitanju institucionalni okvira, slično zakonodavnom okviru, ne postoji nacionalni organ sa isključivim nadležnostima u oblasti regulacije društvenih medija.

Sljedeće institucije imaju suštinsku ulogu kada je riječ o bezbjednosti informacionog sistema i zaštiti prava korisnika u vezi sa elektronskim medijima, komunikacijama i trgovinom:

[11] *Zakon o elektronskoj trgovini („Sl. list CG", br, 80/04)*
[12] *Strategija sajber bezbjednosti Crne Gore 2013 – 2017, Jul 2013*
[13] *Strategija sajber bezbjednosti Crne Gore 2018-2021, Decembar 2017*

1. Ministarstvo javne uprave (Nacionalni CIRT)
2. Ministarstvo unutrašnjih poslova / Uprava policije
3. Agencija za elektronske medije (AEM)
4. Agencija za elektronske komunikacije i poštanske usluge

Direkcija za informatičku bezbjednost i odgovor na kompjuterske incidente (CIRT) je centralni organ na državnom nivou formiran u okviru Ministarstva za informaciono društvo i telekomunikacije radi izvještavanja o sajber incidentima. Sa organizacione tačke gledišta, CIRT je danas dio Ministarstva javne uprave. Tim koordinira aktivnosti za smanjenje rizika od računarskih incidenata, kao i odgovora na računarske incidente u slučaju da se dese. Pored toga, posvećen je podizanju svijesti i edukaciji o tome kako prepoznati sajber prijetnje i sajber kriminal. Posljednjih godina kreiran je **31 lokalni CIRT tim**, zadužen za saradnju sa članovima nacionalnog CIRT-a po pitanjima zaštite od računarskih bezbjednosnih incidenata na internetu. Kada je u pitanju privatni sektor, kreirano je sedam CIRT timova u okviru kompanija Crnogorski Telekom, Telenor, M:tel, Wireless Montenegro, Telemach, M-kabl i Societe Generale Montenegro Banka.[14]

U okviru **Ministarstva unutrašnjih poslova** i Odsjeka za borbu protiv organizovanog kriminala i korupcije, formirana je Grupa za borbu protiv visokotehnološkog kriminala koja se bavi pitanjem visokotehnološkog kriminala (djelima kompjuterskog kriminala, dječijom pornografijom, zloupotrebom kreditnih kartica i autorskih prava). **Uprava policije Crne Gore**, **Forenzički centar**, nadgleda sprovođenje Krivičnog zakonika u odnosu na sajber kriminal. Od 2013. postoji sistematizovani tim za testiranje računara i mobilnih telefona.[15]

Agencija za elektronske medije (AEM) prati usklađenost pružalaca usluga elektronskih medija u skladu sa Zakonom o elektronskim medijima i odgovorna je za sprovođenje uredbe koja se odnosi na elektronske publikacije - web stranice uredničkog oblika i/ili portali koji sadrže elektronske verzije štampanih medija i/ili informacije iz medija na način dostupan široj javnosti bez obzira na njihov obim. Agencija je nadležna za izdavanje odobrenje za emitovanje programa putem digitalnog ili analognog zemaljskog, kablovskog, internetskog ili satelitskog prenosa audio-vizuelnih medijskih usluga. Internetsko emitovanje putem globalne informatičke mreže izričito je isključeno iz režima licenciranja i ne podliježe obavezi pribavljanja odobrenja (član 98. stav 2. Zakona o elektronskim medijima).

Agencija za elektronske komunikacije i poštanske usluge odgovorna je za zaštitu interesa korisnika, rješavanje sporova na tržištu elektronskih komunikacija i nadzor nad radom operatera (član 11. Zakona o elektronskim komunikacijama). Agencija je, zajedno sa organom nadležnim za zaštitu ličnih podataka, odgovorna za propisivanje uslova za sprječavanje i suzbijanje zloupotrebe i prevara povezanih sa pružanjem usluga elektronske pošte, uključujući SMS i MMS.

Crnogorsko zakonodavstvo nudi i **sudski mehanizam** za zaštitu ljudskih prava i osnovnih sloboda. Prema Ustavu Crne Gore i Zakonu o sudovima[16], svako ima pravo da se obrati sudu radi ostvarivanja svojih prava (član 3).

U krivičnim predmetima **Osnovni sud** je nadležan da u prvom stepenu sudi za krivična djela za koja je zakonom propisana kao glavna novčana kazna ili kazna zatvora do deset godina, bez obzira na to da li je djelo izvršeno u mirnodopskim uslovima, za vrijeme vanrednog stanja, neposredne ratne opasnosti ili ratnog stanja. Takođe, u građanskim predmetima Osnovni sud je u prvom stepenu nadležan za odlučivanje u sporovima iz lično-pravnih odnosa, kao i u sporovima povodom ispravke ili odgovora za informaciju sadržanu u medijima i o zahtjevima povodom povrede ličnih prava učinjenih u medijima.

[14]Idem
[15]Idem
[16]Zakon o sudovima („Sl. list CG", br. 011/15)

Legislativa takođe predviđa **vansudske mehanizme** za zaštitu prava i sloboda. Član 56. Ustava propisuje da svako ima pravo obraćanja **međunarodnim organizacijama** radi zaštite svojih prava i sloboda zajemčenih Ustavom. Takođe, čl. 57 predviđa pravo obraćanja d**ržavnom organu ili organizaciji koja vrši javna ovlašćenja** i pravo na odgovor.

2. Društveni mediji i zloupotreba državnih resursa tokom izbora

Kako su društveni mediji postali sve važnije sredstvo tokom izborne kampanje, presudno je pronaći načine za monitoring kršenja pravila kampanja koje se mogu dogoditi u ovom prostoru.[17] Imajući u vidu da tokom političkih kampanja na društvenim mrežama, u državama gdje su strategije kampanje manje istaknute, političke stranke i kandidati vjerovatno neće prekoračiti finansijska ograničenja upotrebom Facebook-a i sličnih platformi.[18] Pored toga, politički subjekti na društvenim mrežama mogu počiniti i druga kršenja koja mogu predstavljati zloupotrebu državnih resursa.[19] Naime, društveni mediji su korisno sredstvo za dokumentovanje kršenja, poput upotrebe službenih vozila ili kancelarija tokom kampanja.

Ovo se posebno odnosi na zloupotrebu institucionalnih resursa, odnosno „nenovčanih materijalnih i kadrovskih resursa dostupnih državi, uključujući javne medije i druge alate za komunikaciju."[20] Konkretno, zloupotreba javnih medija, zvaničnih naloga na društvenim medijima i radnog vrijemena državnih službenika, kao i njihovih ličnih naloga na društvenim mrežama tokom kampanje, predstavljaju primjere zloupotrebe institucionalnih resursa. S tim u vezi, međunarodna zajednica istakla je važnost zakonskog i regulatornog okvira za sprječavanje određenih zloupotreba povezanih sa institucionalnim resursima države i očuvanja nepristrasnosti i profesionalnosti državne službe.[21]

Kada je riječ o institucionalnim resursima i korišćenju službenih i ličnih naloga na društvenim mrežama, u Crnoj Gori postoji set pravila i principa koje je propisala Vlada CG.

Naime, Vlada Crne Gore je 2018. godine usvojila **Komunikacionu strategiju 2018-2020**[22] koja definiše ključne teme/kampanje, kao i ciljeve komunikacije Vlade sa građanima. U okviru Strategije, Crnogorska Vlada je osnovala **Komisiju za implementaciju komunikacione strategije**.

Komisija je 2019. objavila Pravila o komunikacijama[23]. Dokument je sastavljen od 11 poglavlja i 20 pravila koja detaljno opisuju procedure planiranja aktivnosti i objava, definisanja ključnih poruka, usvajanja komunikacionih planova, odgovora na medijske upite, organizacije konferencija za medije, upravljanja nalozima na društvenim medijima i kriznog komuniciranja.

Konkretno, **Poglavlje 9 i pravilo 13** se bave pitanjem upravljanja nalozima na društvenim mrežama. Predviđa se da evidenciju o aktivnosti ministarstava na društvenim medijima i registar sa imenima i kontakt podacima administratora vodi Služba za odnose s javnošću Vlade Crne Gore – Biro za online komunikaciju i koordinaciju.

[17]Training in Detection and Enforcement (TIDE): Political Finance Oversight Handbook, International Foundation for Electoral Systems (IFES), (Magnus Ohman ed.), 2013
[18]Idem
[19]Idem
[20]Idem
[21]Joint Guidelines for Preventing and Responding to Misuse of Administrative Resources during Electoral Process, Venice Commission and OSCE/ODIHR, 2016
[22]Komunikaciona strategija 2018 – 2020, Vlada Crne Gore, 2018
[23]Pravila o komunikacijama, Komisiju za implementaciju komunikacione strategije, Vlada Crne Gore, 2019

Biro, uz saglasnost rukovodioca Službe za odnose s javnošću Vlade Crne Gore, administrira zvanične naloge Vlade na društvenim medijima, dok ministarstva i organi uprave određuju jednog ili više administratora koji su odgovorni za upravljanje zvaničnim nalozima institucije na društvenim medijima.

Poglavlje 9 pruža tačne informacije o tome koje podatke treba da sadrži zvanična objava na društvenim mrežama, kao i da se podaci označeni stepenom tajnosti i informacije izvan nadležnosti organa ne objavljuju.

Kada je riječ o interakciji sa korisnicima, budući da svi sadržaji objavljeni na zvaničnim nalozima Vlade i organa uprave mogu biti protumačeni kao zvaničan stav Vlade, komentari i druge objave korisnika mogu se ukloniti ukoliko se odnose na: tajne podatke, klevetničke ili netačne informacije i nezakonite inicijative; uvrijedljive i neprimjerene zahtjeve; te pitanja koja zadiru u tuđe nadležnosti.

Poglavlje 10 obuhvata smjernice za privatno korišćenje društvenih medija za državne službenike i namještenike. U okviru ovog poglavlja, pravilo 14 predviđa da se stavovi državnih službenika saopšteni putem društvenih medija smatraju javnom komunikacijom, na isti način kao i stavovi izraženi na javnim skupovima ili u tradicionalnim medijima. Shodno tome, principi Etičkog kodeksa moraju se primjenjivati i na ponašanje državnog službenika ili namještenika na društvenim medijima.

Naime, **Etički kodeks**[24] propisuje da se „van radnog vremena službenik ne smije ponašati na način koji ima negativan uticaj na ugled državnog organa" (član 5). Takođe, „prilikom iznošenja stavova državnog organa i ličnih stavova, službenik je dužan da čuva ugled državnog organa i lični ugled. U javnim nastupima u kojima ne predstavlja državni organ, službenik ne smije iznositi podatke iz djelokruga državnog organa ili poslova svog radnog mjesta, koji bi mogli narušiti ugled državnog organa i povjerenje građana u rad državnog organa" (čl. 8). Smjernice predviđaju da se ovo posebno odnosi na privatne objave sa službenih putovanja, iz radnog prostora, učešća na događajima u kojima službenik ili namještenih predstavlja državni organ i svim drugim službenim aktivnostima u okviru i van radnog vremena, kao i u vezi sa iznošenjem ličnih političkih stavova o dešavanjima u zemlji i inostranstvu. Nepoštovanje ovih pravila povlači disciplinsku odgovornost.

Nadalje, **Zakon o državnim službenicima i nameštenicima**[25] propisuje da državni službenik, odnosno namještenik vrši poslove politički neutralno i nepristrasno, u skladu sa javnim interesom, i dužan je da se uzdržava od javnog ispoljavanja svojih političkih uvjerenja (čl. 9).

Činjenicu da su ljudski resursi od presudne važnosti tokom predizborne kampanje prepoznaje i **Zakon o izboru odbornika i poslanika**[26] koji propisuje da javni funkcioneri koje imenuje ili postavlja Vlada Crne Gore i koje bira ili imenuje lokalna samouprava, državni službenici i namještenici ne mogu učestvovati u izbornoj kampanji, niti mogu javno izražavati svoje stavove povodom izbora, u radnom vremenu, odnosno dok su na dužnosti. Takođe, policijski službenici i pripadnici Agencije za nacionalnu bezbjednost ne smiju učestvovati u izbornoj kampanji na bilo koji način (čl. 50a).

Pored toga, državnim funkcionerima i funkcionerima lokalne samouprave je zabranjeno da, u vrijeme izborne kampanje, svoje medijske nastupe u ulozi državnog ili drugog javnog funkcionera zloupotrijebe i iskoriste za reklamiranje ili reklamiranje izborne liste i/ili njenog izbornog programa (čl. 51a, st. . 2).

[24]Etički kodeks („Sl. list CG", br. 050/18)
[25]Zakono državnim službenicima i namještenicima ("Sl. list CG", br. 2/2018 i 34/2019)
[26]Zakono izboru odbornika i poslanika ("Sl. list RCG", br. 16/2000, 9/2001, 41/2002, 46/2002, 45/2004, 48/2006, 56/2006 i "Sl. list CG", br. 46/2011, 14/2014, 47/2014, 12/2016, 60/2017 i 10/2018)

3. Političko oglašavanje na internetu tokom perioda kampanje: iskustva sa izbora 2016. i 2018. godine

Prema podacima od januara 2020. godine, u Crnoj Gori postoji 1,2 miliona mobilnih telefonskih veza, 464,7 hiljada internet korisnika (74% ukupne populacije), od čega je 390 hiljada prisutno na društvenim mrežama (62% ukupne populacije).[27]

Uz ovaj trend prisutnosti populacije na internetu, koji svake godine raste, nije iznenađujuće što su društveni mediji postali centralni dio strategija kampanje političkih partija u Crnoj Gori. Međutim, ovaj trend nije jedinstven samo za Crnu Goru, već predstavlja globalni izazov.

Naime, glavni izazovi političke kampanje na internetu su manipulacije poput stvaranja iluzije masovne podrške ili popularnosti određenih subjekata u cilju ostvarivanja, odnosno pridobijanja istinske podrške, širenja dezinformacija/lažnih vijesti/pogrešnih informacija. Pored toga, postojanje alata poput praćenja tema koje su u trendu, kao i filtera i algoritama na internetu, korisnicima se pružaju informacije na koje veoma vjerovatno da će reagovati, što na kraju može dovesti do smanjenja raznolikosti mišljenja u njegovoj okolini.

Društvene mreže, između ostalih mogućnosti, izbornim akterima nude mogućnost plaćanja svojih oglasa i odabira obima, starosne strukture, pola, te lokacije svoje publike. Na taj način, čak i ako birači ne prate političke subjekte, na njih će se uticati i biće izloženi političkom sadržaju koji se pojavljuje na svakoj web stranici.

Birači imaju pravo da prate političke subjekte na internetu, kao i njihov rad i aktivnosti kako bi prikupili informacije i napravili slobodan i informisan izbor. Međutim, sve veći pritisci tokom izbora i pomenuta propaganda na internetu mogu uticati na odluku birača da ne bude prisutan na mreži. Kao posljedica, mogu im nedostajati relevantne informacije potrebne za slobodan i informisan izbor, ili mogu odlučiti da uopšte ne glasaju. Istraživanje je pokazalo da ne izlaganje argumentima o politizovanim pitanjima smanjuje snagu mišljenja birača i njihovu namjeru da djeluju.[28]

Kada je u pitanju korišćenje društvenih medija i mreža tokom Parlamentarnih izbora 2016. i Predsjedničkih izbora 2018. u Crnoj Gori, rastući trend upotrebe interneta i društvenih medija u svrhe političke kampanje, kao i neke ilegalne aktivnosti, bili su prilično vidljivi.

Parlamentarni izbori 2016

Tokom Parlamentarnih izbora u Crnoj Gori 2016. godine, izborna kampanja je sprovedena na standardne načine: skupovi, posjete od vrata do vrata, bilbordi, oglašavanje u tradicionalnim i društvenim medijima, kao i debate. Glavna tema izbora 2016. bila je pristupanje Crne Gore NATO-u.[29]

Što se tiče društvenih medija, izbore 2016. godine karakteriše blokiranje aplikacija za razmjenu poruka, Viber i WhatsApp, nekoliko sati tokom izbornog dana i prije toga. Naime, Agencija za elektronske komunikacije i poštanske usluge naložila je operaterima elektronskih komunikacija da privremeno zabrane upotrebu WhatsApp i Vibera zbog zaštite korisnika od primanja neželjenih obavještenja i neželjene pošte (čl. 178 Zakona o elektronskim komunikacijama).[30] Agencija je obavijestila operatere o prijavljenim slučajevima širenja „nezakonitog marketinga"

[27]Digital 2020: Montenegro, Datareportal, Januar 2020
[28]Digital Democracy Project, Research Memo 7, Public Policy Forum, Oktobar 2019
29OSCE/ODIHR, Međunarodna misija za posmatranje izbora Crna Gora - Parlamentarni izbori 2016, Preliminarni nalazi i zaključci, oktobar 201630Izvještaj Savjeta Evrope: Analiza medijskog sektora u Crnoj Gori sa preporukama za usklađivanje sa standardima Savjeta Evrope i Evropske Unije, decembar 2017

na mrežama i pozvala ih da usvajanjem adekvatnih mjera spriječe potencijalnu neželjenu komunikaciju.[31] Prema nekim medijskim člancima, privremeno gašenje aplikacija za razmjenu poruka bilo je vodeća tema na društvenim mrežama o izborima.[32]

Parlamentarne izbore 2016. obilježilo je i hapšenje 20 ljudi, uključujući državljane Srbije, kao i Ruske državljane i bivše državne zvaničnike, te crnogorske opozicione lidere za koje se sumnjalo da planiraju da izvrše politički motivisane oružane napade na državu. Slučaj je završio pred Višim sudom u Podgorici, a osumnjičeni su procesuirani i sankcionisani kaznom zatvora za krivična djela terorizma i stvaranje kriminalne organizacije. Stranke su uložile žalbu na odluku Višeg suda u Podgorici i postupak se trenutno nastavlja pred Apelacionim sudom.

Ruski državljani umješani u krivično djelo osuđeni su na 15 i 12 godina zatvora, lideri opozicije po pet godina zatvora, a penzionisani general srpske policije na osam godina zatvora, dok su pripadnici krajnje desničarskih političkih organizacija iz Srbije osuđen na po sedam godina zatvora. Ostala lica angažovana u stvaranju kriminalne organizacije osuđena su na kaznu zatvora u trajanju od 1 do 3 godine u skladu sa propisanim zakonskim sankcijama za djela koja im se stavljaju na teret.[33]

Od važnosti je napomenuti da se najveći broj prijavljenih sajber incidenata koji se tiču prevara putem Interneta dogodio upravo u 2016. godini, dok se najviše incidenata povezanih sa zloupotrebama profila na društvenim mrežama i incidentima u vezi sa neželjenim sadržajem na Internetu dogodilo u 2016., kao i u 2015. godini.[34]

Predsjednički izbori 2018

Političke kampanje tokom Predsjedničkih izbora u Crnoj Gori 2018. bile su uglavnom vidljive preko bilborda, ali kampanja se odvijala i kroz skupove i sastanke sa biračima, posjete od vrata do vrata, oglašavanje u tradicionalnim medijima, kao i na društvenim mrežama.

Glavne teme kampanja odnosile su se na zapošljavanje, strane investicije, migracije, bezbjednost i lokalna i opštinska pitanja, vladavinu prava i EU integracijama, a prisutne su bile i kritike opozicije prema dugogodišnjoj vladajućoj stranci takođe.[35] Kako se kampanja fokusirala na pojedince, a ne na političke ideologije ili politike kandidata, kandidati su su povremeno koristili diskriminatorsku, uvrijedljivu ili nacionalističku retoriku.[36]

Međutim, tokom kampanje za Predsjedničke izbore 2018. godine poštovane su osnovne slobode, posebno jednak pristup javnim mjestima, javnom emiteru i besplatno vrijeme emitovanja, kao i slobode javnog okupljanja, kretanja i udruživanja.[37] Prema izvještajima, Agencija za elektronske medije nije primila nijednu žalbu koja se odnosi na medije.[38]

Iako ne postoje tačni podaci o političkom oglašavanju na internetu tokom izbornog perioda 2016. i 2018. godine, strategije kampanje političkih partija i istraživanja javnog mnjenja pokazale su sve veći značaj društvenih medija za buduće izbore. Naime, istraživanje javnog mnjenja, sprovedeno 2017. godine prije izbora, pokazalo je da je za birače televizija i dalje primarni izvor vijesti, dok upotreba interneta raste tokom godina kako društveni mediji imaju sve širi domet.[39]

[31]Idem
[32]WhatsApp i Viber blokirani na dan izbora u Crnoj Gori, Advox Global Voices, oktobar 2016
[33]Svi optuženi za 'državni udar' proglašeni krivim, Radio Slobodna Evropa, maj 2019
[34]Strategija sajber bezbjednosti Crne Gore 2018-2021, decembar 2017
[35]OSCE/ODIHR, Međunarodna misija za posmatranje izbora Crna Gora – Predsjednički izbori 2018, Preliminarni nalazi i zaključci, april 2018
[36]Idem
[37]Crna Gora - Predsjednički izbori 2018, Misija ODIHR-a za posmatranje izbora, Konačni izvještaj, jun 2018
[38]Idem

Iako međunarodna zajednica pozdravlja napredak koji je Crna Gora postigla u oblasti slobode izražavanja i medija, mediji bi trebalo da aktivno prate kampanje na nepristrasan i profesionalan način, umjesto da se oslanjaju na izvještavanje koje su dostavile političke partije.[40] Kada se radi o govoru mržnje, javni govor mržnje, te drugi oblici mržnje i dalje zabrinjavaju imajući u vidu da ipak ima netolerantnih političkih izjava, naročito za vrijeme izbora, kao i komentara koji sadrže uvrijedljiv jezik, uvrede i govor mržnje prema drugim grupama (nacionalnim manjinama, LGBTQI populaciji).[41]

S tim u vezi, posljednji izbori u regionu jasno ukazuju na sve veću ulogu internet alata i društvenih medija tokom političkih kampanja. Uzimajući u obzir kontekst pandemije COVID-19, dok je većina tradicionalnih sredstava političke kampanje ograničena, vrlo je vjerovatno da će se kampanja na Parlamentarnim izborima 2020. godine, kao i na budućim izborima u Crnoj Gori, odvijati pretežno na društvenim mrežama.

[39]Istraživanje javnog mnjenja, CISR-IPSOS, oktobar 2017
[40]Crna Gora - Parlamentarni izbori 2016, Posmatračke misije (OSCE/ODIHR), Konačni izvještaj, januar 2017
[41]Izvještaj Evropske Komisije za borbu protiv rasizma i netrpeljivosti (ECRI) o Crnoj Gori, peti ciklus procesa monitoringa, septembar 2017

4. Uporedna praksa

Internet i društveni mediji izuzetno su široki koncepti, pa ih je gotovo nemoguće regulisati u svim njegovim segmentima, pogotovo što se ova oblast preklapa sa spektrom osnovnih ljudskih prava, uključujući pravo na slobodu izražavanja i mišljenja. Međutim, pitanje je postoji li mogućnost kontrole ove oblasti jer smo svjedoci mnogih slučajeva zloupotreba, kršenja i neprimjerenih sadržaja koji se svakodnevno stvaraju.

S tim u vezi, mnoge države širom svijeta preduzele se određene mjere u smislu usvajanja pravnih akata i propisa kojima se nacionalnim vlastima, državnim organima i medijima dodeljuju posebne nadležnosti u pogledu kontrole i sprječavanja zloupotreba i nasilja na internetu. Ovo iz razloga što su mnogi zakoni o medijima praktično neprimjenljivi u digitalnom svijetu.

Cilj ovog poglavlja koji se bavi uporednom analizom jeste dati pregled nacionalnih praksi vezanih za društvene medije i sajber prostor širom svijeta. Primjeri, odnosno države predstavljene u nastavku, odabrane su na osnovu njihovih povećanih napora u oblasti regulisanja društvenih medija kako bi zaštitili osnovna ljudska prava i slobode građana na internetu.

Glavni zaključci:

- Razvoj prakse regulisanja i monitoringa društvenih medija još uvijek traje.
- Svaka se država suočava sa različitim prijetnjama u odnosu na računarski kriminal i zloupotrebe na internetu, pa je potreban jedinstveni pristup - prilagođen svakoj državi pojedinačno.
- Zakonska rješenja mogu dati veću kontrolu države nad onim što se kreira i dijeli na internatu, međutim, to može dovesti do cenzure i kršenja osnovnih ljudskih prava kao što je sloboda izražavanja u online prostoru.
- Sprovođenje reformi, u smislu uvođenja novih zakonskih okvira koji se odnose na društvene medije, može potrajati duže, a njegova efikasnost i uticaj mogu biti dovedeni u pitanje, imajući u vidu da se tehnologija razvija brzim tempom.
- Postojeći domaći zakoni bi trebali biti ažurirani u skladu sa razvojem tehnologija kako bi se riješilo pitanje zloupotreba na društvenim medijima.
- Treba potencirati jačanje kapaciteta, odnosno primjenu novih metodologija monitoringa koje će koristiti državne institucije kada su u pitanju društveni mediji.
- **Treba promovisati unaprjeđenje saradnje između državnih organa, kao i njihove saradnje sa privatnim i OCD sektorom (višestranački pristup) u ovoj oblasti.**

Njemačka

U decembru 2019. godine **Njemačka je usvojila Državni ugovor o modernizaciji medijskog zakonodavstva (Državni ugovor o medijima (MStV))**[42] koji bi trebao stupiti na snagu u septembru 2020. godine. Ovim Ugovorom, Njemačka istovremeno primjenjuje izmijenjenu **Direktivu Evropskog Parlamenta i Savjeta 2018/1808/EU**[43] u vezi sa pružanjem audio-vizuelnih medijskih usluga s obzirom na promijenljive tržišne uslove.

Novi Ugovor o medijima proširuje svoj obim i uključuje platforme društvenih medija, pretraživače i video portale, podvrgavajući ih nezavisnom, nevladinom nadzoru od strane njemačkih medijskih uprava (Landesmedienanstalten). Uvedene su dvije značajne obaveze: obaveza transparentnosti i zabrana diskriminacije. Obaveza transparentnosti tiče se algoritamske transparentnost, odnosno jasnu prezentaciju kriterijuma prema kojima se predstavlja sadržaj, kao i najavu promijena tih kriterijuma, dok se odredba o diskriminaciji u suštini odnosi na zabranu diskriminacije određenih novinarskih i uredničkih ponuda. Nedostaci Ugovora su nedovoljno razrađeni detalji poput nedovoljno definisanih standarda za razlikovanje odgovarajućeg od neprimjerenog sadržaja, već društvene platforme imaju potpunu slobodu procjene u skladu sa svojim standardima, kao i to ko sve potpada u grupi medijskih posrednika.

Izmijenjena Direktiva o audio-vizuelnim medijskim uslugama, kao i novi Ugovor o modernizaciji medijskog zakonodavstva takođe su razlozi da Federalna Vlada pripremi Zakon o izmjenama i dopunama **Zakona o mrežama (NetzDG)**[44]. Postojeći NetzDG stupio je na snagu 2017. godine, stavljajući društvene mreže u obavezu da suzbiju govor mržnje i druge ekstremističke poruke na svojim digitalnim platformama. Međutim, u junu 2020. njemački Parlament usvojio je izmjene kojima se proširuje NetzDG, zahtijevajući od kompanija da uklone sav sadržaj koji je nezakonit[45] u roku od 24 sata od njegovog upozorenja, uz propisane novčane kazne ukoliko ne postupe u skaldu sa tim. Zakon dozvoljava rok do sedam dana da kompanije odluče o sadržaju koji je označen kao uvrijedljiv, ali koji možda neće sadržati jasne element klevete ili podstrekavanja na nasilje. Takođe, Zakon uvodi obavezu izvještavanja sa platformi (svakih šest mjeseci kompanije će morati javno da prijave broj pritužbi koje su primile i kako su postupale sa njima), što takođe zahtijeva da određene vrste „krivičnog sadržaja" prijave Kancelariji Savezne kriminalističke policije.

Izmjene Zakona NetzDG i dalje traju. Međutim, glavne novine zakona su: ojačana prava korisnika, jednostavniji kanali za izvještavanje, pojednostavljeno postupanje po podnijetim zahtjevima, prošireni kriterijumi za transparentno izvještavanje.

[42]Državni ugovor o medijima (MStV), 2020

[43]Direktiva Evropskog Parlamenta i Savjeta 2018/1808/EU o izmjeni Direktive Savjeta 2010/13/EU, Evropski Parlament i Savjet, novembar 2018

[44]Zakon o mrežama (Netzdurchsetzunggesetz, NetzDG), (Federalni sl. list I, p. 3352 ff., oktobar 2017)

[45]U okviru pododijeljka 1 NetzDG-a definisani su različiti oblici nezakonitog sadržaja koji se odnose na reklame, emitovanje, televizijsku prodaju, itd.

Francuska

Po uzoru na Njemačku, Francuska je takođe usvojila **Zakon br. 2020-766**[46] čiji je cilj suzbijanje sadržaja koji podstiču na mržnju na internetu 24. juna 2020. godine, kojim se zahtijeva da društvene platforme uklanjaju ilegalne sadržaje poput govora mržnje na osnovu rase, nacionalnosti, pola, invaliditeta, ili seksualne orjentacije u roku od 24 sata. Pored toga, sadržaji povezani sa terorizmom ili dječjom pornografijom moraju se ukloniti u roku od jednog sata, u suprotnom će date kompanije biti kažnjene velikim novčanim iznosima. Društveni mediji moraju, na godišnjem nivou, prijavljivati ukupan broj ilegalnog sadržaja, dok će za svako prikrivanje podataka biti kažnjeni. Zakon je odobren takođe i zbog širenja dezinformacija u vezi sa COVID-19.

Jaki zakoni protiv govora mržnje već su postojali u Francuskoj, često sa krivičnim sankcijama, ali ta pravila, uspostavljena prije pojave društvenih medija, imaju malo uticaja na internet.

Velika Britanija

Iako se krivično zakonodavstvo Ujedinjenog Kraljevstva primenjuje na internet aktivnosti na isti način kao i na aktivnosti van interneta, u avgustu 2018. godine, Kraljevsko tužilaštvo objavilo je smjernice o prestupima na društvenim mrežama.[47]

Pored toga, 2019. godine zakonodavci su pripremili nacrt **Zakona o povredama na internetu**[48] koji bi ograničio dijeljenje određenog nasilnog i ekstremističkog sadržaja na internatu. Jasno je rečeno da zakonodavni okviri Velike Britanije nisu postavljeni dovoljno široko i da su neophodne promjene u vezi sa regulacijom oblasti društvenih mreža.

Novi regulatorni okvir obuhvatio bi kompanije društvenih medija, forume za javnu raspravu, maloprodaje koji korisnicima omogućavaju da kupuju proizvode na internetu, neprofitne organizacije, web stranice za razmijenu podataka i ostale provajdere. Monitoring sadržaja treba da vrši nezavisni regulator. Ovdje se predlaže da se ojača uloga organa koji su do sada bili uključeni u nadgledanje medijskih i radio sadržaja. Predlaže se da same platforme jasno definišu šta se podrazumijeva pod dozvoljenim, a šta zabranjenim sadržajem i da ove smjernice budu jasno predstavljene nadležnom organu koji će ovo nadgledati.

Međutim, zakon je još uvijek u radnoj verziji i kritikovan je, a izražena je zabrinutost da bi mogao uticati na slobodu izražavanja na internetu, dovesti do povećane cenzure i uklanjanja sadržaja koji nisu nezakoniti.
Kada je reč o institucionalnom okviru u Velikoj Britaniji, mnogi organi imaju ulogu vezano za određene vrste aktivnosti na internetu, npr. Ofcom, Uprava za konkurenciju i tržište, Uprava za standarde oglašavanja, Kancelarija komesara za informacije i Uprava za finansijsko ponašanje.[49]

Evropska Unija

Direktiva Evropskog Parlamenta i Savjeta **2018/1808/EU** o izmjeni Direktive Savjeta 2010/13/EU[50] proširuje pravila na usluge društvenih medija, koje su postale važan alat za razmjenu informacija, zabavu i obrazovanje, uključujući pružanje pristupa programima i video zapisima koje kreiraju korisnici.

[46]Zakon n° 2020-766 (JORF no. 0156)
[47]Social Media - Guidelines on prosecuting cases involving communications sent via social media, UK Crown Prosecution Service, avgust 2018
[48]Online Harms White Paper, april 2019
[49]House of Commons, Social Media Regulation, Briefing Paper, Number 8743, februar 2020
[50]Direktiva 2018/1808/EU o izmjeni Direktive Savjeta 2010/13/EU, Evropski Parlament i Savjet, novembar 2018

Pitanje - koje društvene mreže treba da budu obuhvaćene ovom Direktivom - riješeno je konstatacijom da su društvene mreže sve ono čija je glavna svrha pružanje mogućnosti postavljanja programa i video zapisa. Ako je objavljivanje video sadržaja i dijeljenje zaseban dio usluge koju pruža određena društvena mreža, onda Direktiva reguliše samo taj dio. Video zapisi koji su dio sadržaja elektronskih novina i animiranih slika poput GIF-ova nisu obuhvaćeni ovom Direktivom. Direktiva 2018/1808/EU ne reguliše ne-ekonomske aktivnosti poput audio-vizuelnih sadržaja na privatnim web stranicama i nekomercijalnim zajednicama od interesa. Ova Direktiva navodi deset alata koje bi provajderi video zapisa trebali da koriste kako bi ispunili zahtjeve koji se odnose na zaštitu maloljetnika od neprimjerenog sadržaj. Ovi alati se odnose na uslove kao što su verifikacija starosti, roditeljska kontrola i mogućnost usvajanja još strožih pravila za provajdere video usluga.

Međutim, ove mjere ne predstavljaju preveliki teret za provajdere, jer su to već neke od mjera koje se već primjenjuju. Ključna novina je da će provajderi video zapisa biti podložni medijskoj regulativi i moraće da se registruju. Pored toga, ova Direktiva zahtijeva da se 30% ponude mora sastojati od evropskog sadržaja.

Direktiva o bezbjednosti mreže i informacionih sistema (NIS Direktiva) 2016/1148 Evropskog Parlamenta i Savjeta,[51] usvojena 2016. godine, odnosi se na mjere za visok zajednički nivo bezbjednosti mrežne i informacionih sistema širom Unije. Direktivom je osnovana Grupa za saradnju koja podržava i olakšava stratešku saradnju, diskusije i razmjenu dobrih praksi između država članica u vezi sa bezbjednošću mreže i informacionih sistema. Takođe, predviđa da uslovi koji se odnose na bezbjednost i obavještavanje treba da se primjenjuju i na operatere osnovnih usluga, kao i na pružaoce digitalnih usluga, kako bi se promovisala kultura upravljanja rizikom i osiguralo da se izvještava o najtežim incidentima.

Savjet Evrope

Preporuka **CM/Rec(2018)2** Komiteta ministara državama članicama o ulogama i odgovornostima internet posrednika,[52] usvojena je 2018. godine i poziva države da stvore bezbjedno internet okruženje u kojem sve strane, i korisnici i platforme, znaju svoja prava i obaveze. U okviru dokumenta, pretraživači i društveni mediji su definisani kao internetski posrednici.

Savjet predlaže jačanje mehanizama samoregulacije i koregulacije. Naime, Preporuka nameće obavezu država u pogledu zaštite i promocije ljudskih prava i osnovnih sloboda u digitalnom okruženju, kao i odgovornosti internet posrednika u pogledu poštovanja ljudskih prava i osnovnih sloboda koje države imaju za cilj da obezbijede.

Odredbe koje se odnose na državne vlade navode da one mogu da se miješaju u internet sadržaj samo ako je to regulisano zakonom i na način koji je u skladu sa tim zakonom. Pored toga, obim vladinih ovlašćenja mora biti jasno naveden kako bi se spriječile moguće zloupotrebe. Od vlada se traži da verifikuju da li ove platforme imaju jasne i efikasne mehanizme za uklanjanje neadekvatnog sadržaja. Od pružaoca usluga potrebna je veća transparentnost u smislu ograničavanja sadržaj. Pri ograničavanju sadržaja mora biti jasno navedeno na kojoj pravnoj osnovi je dati sadržaj ograničen. Jedno od pitanja koje je izuzetno problematično i koje treba regulisati je pitanje botova, to su nalozi koji se algoritamski kontrolišu i oponašaju aktivnost ljudskih korisnika, ali funkcionišu mnogo bržim tempom. Pružaoci usluga moraju omogućiti detaljne informacije o tome kako funkcionišu algoritamski i automatizovani alati. Da bi vlada mogla da kontroliše određeni algoritam, ona mora da posjeduje sveobuhvatne informacije koje mogu biti u suprotnosti sa nekim od osnovnih ljudskih prava.

[51]Direktiva o bezbjednosti mreže i informacionih sistema (NIS Direktiva) 2016/1148, Evropski Parlament i Savjet, jul 2016
[52]Preporuka CM/Rec(2018)2 Komiteta ministara državama članicama o ulogama i odgovornostima internet posrednika, Savjet Evrope, mart 2018

Štaviše, prilikom implementacije Preporuke, države i posrednici su dužni da ispunjavaju svoje odgovornosti u pogledu poštovanja ljudskih prava u skladu sa O**snovnim principima Ujedinjenih Nacija o poslovanju i ljudskim pravima**[53] **i Preporukom CM/Rec (2016)3** Komiteta ministara državama članicama o ljudskim pravima i poslovanju. [54]

Kada je reč o društvenim medijima i sadržajima na internatu, Savjet Evrope pruža državama članicama niz preporuka, od kojih je važno pomenuti: Preporuka CM/Rec(2016)5 o slobodama na internetu,[55] Preporuka CM/Rec(2016)1 o promociji i zaštiti prava na slobodu izražavanja i prava na privatni život u odnosu na neutralnost mreže,[56] Preporuka CM/Rec(2015)6 o slobodnom, prekograničnom protoku informacija na Internetu,[57] Preporuka CM/Rec(2014)6 o Vodiču o ljudskim pravima za korisnike Interneta,[58] Preporuka CM/Rec(2012)3 o zaštiti ljudskih prava u odnosu na pretraživače,[59] Preporuka CM/Rec(2012)4 o zaštiti ljudskih prava u odnosu na usluge društvenih mreža,[60] itd.

SAD

U SAD-u ne postoje federalni ili državni zakoni koji izričito regulišu društvene medije i sadržaje na internetu. Trenutni pravni okvir sastoji se od **Ustava Sjedinjenih Američkih Država (Prvi amandman)**[61] **i poglavlje 230 Zakona o pristojnosti komunikacija iz 1996 (CDA)**.[62]

Naime, Prvi amandman pruža zaštitu od državnih postupaka kada pojedinci tvrde da su time prekršena njihova prava na slobodu govora na internetu. Prvi amandman generalno štiti slobodu govora, ali se njegova zaštita ne primjenjuje na isti način u svim slučajevima jer se svaka vladina uredba koja utiče na sadržaj objavljen na društvenim medijima ne bi analizirala na isti način. Međutim, Prvi amandman ne zabranjuje regulisanje ponašanja. Postupanje privatnih kompanija regulisano je poglavljem 230 Zakona o pristojnosti komunikacija. CDA je poznat kao najvažniji zakon koji štiti slobodu izražavanja na internetu. Međutim, poglavlje 230 pruža širok imunitet pružaocima interaktivnih računarskih usluga, uključujući društvene medije. Poglavlje 230 pruža imunitet od bilo koje tužbe kojom se traži da se pružalac usluge smatra odgovornim za objavljivanje informacija koje je kreirao pružalac informativnog sadržaja, efikasno štiteći web stranice društvenih medija od odgovornosti za postavljanje sadržaja. Takođe, daje imunitet web stranicama koje preduzimaju „dobronamjerne mjere" kako bi ograničile pristup sadržaju koji provajder ili korisnici smatraju nepristojnim, razvratnim, raskalašenim, prljavim, pretjerano nasilnim, uznemiravajućim ili na bilo koji drugi način neprikladnim.

U 2019. godini predstavljen je Zakon o odvraćanju od pristrasnog algoritma,[63] u skladu sa kojim bi se bilo koji društveni mediji, koji koristi algoritme za upravljanje sadržajem bez dozvole ili znanja korisnika, mogao legalno smatrati izdavačem, a ne platformom, čime se uklanja imunitet predviđen poglavljem 230 CDA. Takođe, predstavljen je i Zakon o ukidanju podrške za internetsku cenzuru,[64] koji bi zahtijevao da društveni mediji moraju pokazati Federalnoj komisiji za trgovinu (FTC) da su njihove prakse upravljanja sadržajem bile politički neutralne, kako bi im se odobrio imunitet u skladu sa poglavljem 230 CDA. Međutim, nijedan od navedenih zakona nije usvojen. Najnoviji pokušaj je dvostranački zakon - Zakon o ukidanju nasilnog i širokog zanemarivanja interaktivnih tehnologija (EARN IT)[65] koji je predstavljen u martu 2020. Cilj ovog zakona je sprječavanje dječje pornografije, putem čega će se oslabiti imunitet predviđen poglavljem 230 CDA i ograničiti šifrovanje, zahtijevajući od kompanija da slijede niz „najboljih praksi" ili će u protivnom izgubiti imunitet shodno poglavlju 230 zbog optužbi za dječiju pornografiju.

[54] *Preporuka CM/Rec (2016)3, Savjet Evrope, mart 2016*
[55] *Preporuka CM/Rec(2016)5, Savjet Evrope, april 2016*
[56] *Preporuka CM/Rec(2016)1, Savjet Evrope, januar 2016*
[57] *Preporuka CM/Rec(2015)6, Savjet Evrope, april 2015*
[58] *Preporuka CM/Rec(2014)6, Savjet Evrope, april 2014*
[59] *Preporuka CM/Rec(2012)3, Savjet Evrope, april 2012*
[60] *Preporuka CM/Rec(2012)4, Savjet Evrope, april 2012*
[61] *Ustav Sjedinjenih Američkih Država, Prvi amandman*
[62] *Zakon o pristojnosti komunikacija, 47 Američki zakonik, Poglavlje 230 - Zaštita od privatnog blokiranja i pregled uvrijedljivog sadržaja*
[63] *Biased Algorithm Deterrence Act, H.R.492 — 116th Congress (2019-2020), 2019*
[64] *Ending Support for Internet Censorship Act, S.1914 — 116th Congress (2019-2020)*
[65] *EARN IT Act, S.3398 — 116th Congress (2019-2020), 2020*

Imajući u vidu predstavljeni pravni okvir, u SAD-u, pravima korisnika na društvenim medijima prvenstveno upravljaju privatne politike koje kreiraju sami pružaoci informacionih usluga i kompanije.

Meksiko

Pored gore predstavljenih pravnih pokušaja da se regulišu društveni mediji i zaštite prava korisnika, Meksiko je posebno zanimljiv slučaj za ovo poglavlje koje se bavi uporednom praksom jer daje primjer regulisanja društvenih medija kroz upotrebu nacionalnih taktika za odvraćanje od korupcije.

Naime, Vrhovno Odjeljenje Izbornog suda Meksika potvrdilo je presudu koju je donelo Regionalno Odjeljenje Izbornog suda u Montereju[66] kojom je poništio izbore na jednom biračkom mjestu tokom parlamentarnih i lokalnih izbora održanih u Meksiku 2015. godine. U presudi se navodi da su poništeni rezultati izbora sa jednog biračkog mjesta jer je guverner prekršio nepristrasnost i fer izbora time što je njegovo učešće u izborima postalo javno poznato.[67] Guverner je objavio fotografije na svom ličnom Twitter nalogu, što je podijeljeno na zvaničnoj web stranici Vlade, uključujući i njega kako putuje na biračka mjesta sa kandidatima. Fotografije objavljene na društvenim mrežama korišćene su kao dokaz koji sugeriše kršenje nepristrasnosti i zloupotrebu državnih resursa.[68]

Na ovaj način predstavljena je drugačija perspektiva kako regulisati društvene medije. Nadalje, ovaj primjer pokazuje da nisu svi aspekti zloupotrebe na društvenim mrežama regulisani (ili bi trebali biti) regulisani određenim zakonom, već su aktivnosti državnih organa i njihova sposobnost da koriste društvene medije kao sredstvo za monitoring kršenja presudni, posebno tokom izbora i predizborne kampanje.

[66] *Electoral Tribunal of Mexico, Case PAN v. PRI (SM JIN 0035 2015)*
[67] *Idem*
[68] *Idem*

Zaključci i preporuke

Na osnovu analize pravnog i institucionalnog okvira, kao i iskustava sa izbora u 2016. i 2018. godini u Crnoj Gori, očigledno je da su neophodna dalja unaprjeđenja u pogledu zaštite prava građana i osnovnih sloboda na internetu.

Sa razvojem i napretkom u oblasti informacione tehnologije, pružaoci internet usluga takođe trpe sajber napade na svoju infrastrukturu. Međutim, ne postoji koordinirani odgovor, kao što su sigurni kanali komunikacije na nacionalnom nivou, u cilju riješavanja takvih situacija. Još jedan značajan problem je što u Crnoj Gori ne postoji definisan način praćenja ili evidentiranja malicioznog protoka podataka koji ulaze u zemlju.

Analizom uporedne prakse pokazalo se da postoje razni pokušaji za regulisanje širenja nezakonitih i štetnih sadržaja na društvenim medijima, kao i za zaštitu sajber prostora širom svijeta. Međutim, različita institucionalna i pravna, kao i kulturna pozadina svake države u velikoj mjeri određuju koji mehanizmi i propisi najbolje odgovaraju, kako bi se osiguralo puno uživanje i zaštita digitalnih prava korisnika, tj. građana. Na primjer, iako je Njemačka dala veliki doprinos u pogledu odgovornosti medijskih posrednika, zahvaljujući visokom stepenu nezavisnosti medija u državi, nije vjerovatno da bi se isti mehanizam mogao primijeniti u drugim zemljama ili državama članicama EU gdje je nivo nezavisnosti medija niži.

Ipak, potreba za regulisanjem oblasti interneta i sajber prostora ostaje neophodnost savremenog svijeta s ciljem sprječavanja mogućih zloupotreba i kršenja osnovnih sloboda i ljudskih prava korisnika. U nastavku je dat kratak pregled nekih ključnih preporuka koje proističu iz analize.

Ključne preporuke

Za javni sektor:

- Odredbe o ograničenjima državnih službenika i namještenika o učestvovanju u kampanjama tokom obavljanja dužnosti ili mandata u cilju održavanje nepristrasnosti i političke neutralnosti, bi mogle biti eksplicitno ažurirane kako bi se riješilo pitanje upotreba državnih i privatnih naloga na društvenim mrežama.
- Nacionalne vlasti mogu razmotriti unaprjeđenje domaće taktike za borbu protiv korupcije kako bi se regulisala upotrebu društvenih medija, posebno tokom izbora i političkih kampanja.
- Usvojiti više kooperativni način prilikom formiranja mehanizama za podršku rizičnim korisnicima, na koordiniran način sa pristupom više zainteresovanih strana, koji bi mogao uključivati podršku fizičke sigurnosti, pravnu podršku, podizanje svijesti i digitalnu podršku.
- Proširivanje aktivnosti obuke službenika za sprovođenje zakona i pravosuđa o zločinima iz mržnje, krivičnim djelima na internetu, računarskim kriminalom, sprovođenjem seminara/konferencija/kurseva o međunarodnim standardima i sudskoj praksi u vezi sa zaštitom digitalnih prava, kao i za sprovođenje efikasnih istraga u vezi sa krivičnim djelima na internetu.

Za OCD i medije:

- Jačati vještine digitalne pismenosti građana, posebno mlađe populacije, kroz formalno i neformalno obrazovanje s ciljem edukacije, informisanja i senzibilizacije mladih o bezbjednosti informacionog sistema, internet rizicima, zloupotrebama i načinu zaštite svojih prava i sloboda, naročito tokom izbornog procesa
- Sprovesti informativnu kampanju za podizanje svijesti javnosti o oglasima na internetu, manipulacijama, kršenjima prava korisnika na internetu i mehanizmima zaštite.

Literature

1. Biased Algorithm Deterrence Act, H.R.492 — 116th Congress (2019-2020), 2019
2. Crna Gora - Parlamentarni izbori 2016, Posmatračke misije (OSCE/ODIHR), Konačni izvještaj, januar 2017
3. Crna Gora - Predsjednički izbori 2018, Misija ODIHR-a za posmatranje izbora, Konačni izvještaj, jun 2018
4. Digital 2020: Montenegro, Datareportal, Januar 2020
5. Digital Democracy Project, Research Memo 7, Public Policy Forum, Oktobar 2019
6. Direktiva Evropskog Parlamenta i Savjeta 2018/1808/EU o izmjeni Direktive Savjeta 2010/13/EU, Evropski Parlament i Savjet, novembar 2018
7. Direktiva o bezbjednosti mreže i informacionih sistema (NIS Direktiva) 2016/1148, Evropski Parlament i Savjet, jul 2016
8. Dodatni protokol uz Budimpeštansku konvenciju koji se odnosi na kriminalizaciju djela rasističke i ksenofobne prirode počinjena putem računarskih sistema, Savjet Evrope, 2003
9. EARN IT Act, S.3398 — 116th Congress (2019-2020), 2020
10. Electoral Tribunal of Mexico, Case PAN v. PRI (SM JIN 0035 2015)
11. Ending Support for Internet Censorship Act, S.1914 — 116th Congress (2019-2020)
12. Etički kodeks („Sl. list CG", br. 050/18)
13. House of Commons, Social Media Regulation, Briefing Paper, Number 8743, februar 2020
14. Istraživanje javnog mnjenja, CISR-IPSOS, oktobar 2017
15. Izvještaj Evropske Komisije za borbu protiv rasizma i netrpeljivosti (ECRI) o Crnoj Gori, peti ciklus procesa monitoringa, septembar 2017
16. Izvještaj Savjeta Evrope: Analiza medijskog sektora u Crnoj Gori sa preporukama za usklađivanje sa standardima Savjeta Evrope i Evropske Unije, decembar 2017
17. Joint Guidelines for Preventing and Responding to Misuse of Administrative Resources during Electoral Process, Venice Commission and OSCE/ODIHR, 2016
18. Komunikaciona strategija 2018 – 2020, Vlada Crne Gore, 2018
19. Konvencija o računarskom kriminalu (Budimpeštanska konvencija), Savjet Evrope, 2001
20. Krivični zakonik Crne Gore ("Sl. list RCG", br. 70/2003, 13/2004 i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, 49/2018 i 3/2020)
21. Ohman, M. (Ed.), Training in Detection and Enforcement (TIDE): Political Finance Oversight Handbook, International Foundation for Electoral Systems (IFES), 2013
22. Online Harms White Paper, april 2019
23. OSCE/ODIHR, Međunarodna misija za posmatranje izbora Crna Gora – Parlamentarni izbori 2016, Preliminarni nalazi i zaključci, oktobar 2016
24. OSCE/ODIHR, Međunarodna misija za posmatranje izbora Crna Gora – Predsjednički izbori 2018, Preliminarni nalazi i zaključci, april 2018
25. Osnovni principi Ujedinjenih Nacija o poslovanju i ljudskim pravima,
26. Pravila o komunikacijama, Komisiju za implementaciju komunikacione strategije, Vlada Crne Gore, 2019
27. Preporuka CM/Rec (2016)3, Savjet Evrope, mart 2016
28. Preporuka CM/Rec(2012)3, Savjet Evrope, april 2012
29. Preporuka CM/Rec(2012)4, Savjet Evrope, april 2012

30. Preporuka CM/Rec(2014)6, Savjet Evrope, april 2014
31. Preporuka CM/Rec(2015)6, Savjet Evrope, april 2015
32. Preporuka CM/Rec(2016)1, Savjet Evrope, januar 2016
33. Preporuka CM/Rec(2016)5, Savjet Evrope, april 2016
34. Preporuka CM/Rec(2018)2 Komiteta ministara državama članicama o ulogama i odgovornostima internet posrednika, Savjet Evrope, mart 2018
35. Social Media - Guidelines on prosecuting cases involving communications sent via social media, UK Crown Prosecution Service, avgust 2018
36. Strategija sajber bezbjednosti Crne Gore 2013 – 2017, Jul 2013
37. Strategija sajber bezbjednosti Crne Gore 2018-2021, Decembar 2017
38. Svi optuženi za 'državni udar' proglašeni krivim, Radio Slobodna Evropa, maj 2019
39. Ustav Crne Gore („Sl. list CG", br. 1/2007 i 38/2013 - Amandmani I-XVI)
40. Ustav Sjedinjenih Američkih Država, Prvi amandman
41. WhatsApp i Viber blokirani na dan izbora u Crnoj Gori, Advox Global Voices, oktobar 2016
42. Zakon n° 2020-766 (JORF no. 0156)
43. Zakon o mrežama (Netzdurchsetzunggesetz, NetzDG), Federalni sl. list I, p. 3352 ff., oktobar 2017
44. Zakon o elektronskim komunikacijama („Sl. list CG", br. 40/2013)
45. Zakon o elektronskim medijima ("Sl. list CG", br. 46/2010, 40/2011, 53/2011, 6/2013, 55/2016, 92/2017, 82/2020)
46. Zakon o elektronskoj trgovini („Sl. list CG", br, 80/04)
47. Zakon o informacionoj bezbjednosti ("Sl. list CG", br. 014/10 i 040/16)
48. Zakon o pristojnosti komunikacija, 47 Američki zakonik, Poglavlje 230 - Zaštita od privatnog blokiranja i pregled uvrijedljivog sadržaja
49. Zakon o sudovima („Sl. list CG", br. 011/15)
50. Zakonik o krivičnom postupku („Sl. list CG", br. 57/09)
51. Zakono državnim službenicima i namještenicima ("Sl. list CG", br. 2/2018 i 34/2019)
52. Zakono izboru odbornika i poslanika ("Sl. list RCG", br. 16/2000, 9/2001, 41/2002, 46/2002, 45/2004, 48/2006, 56/2006 i "Sl. list CG", br. 46/2011, 14/2014, 47/2014, 12/2016, 60/2017 i 10/2018)


CeMI