

# Smjernice za promatranje izbornih kampanja na društvenim mrežama



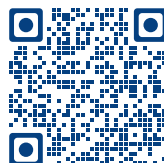
Smjernice za promatranje  
izbornih kampanja na  
društvenim mrežama

Ovaj dokument je izvorno objavljen u izdanju OESS-ova Ureda za demokratske institucije i ljudska prava 2021. godine, na engleskom jeziku, pod nazivom „Guidelines for Observation of Election Campaigns on Social Networks“. Hrvatska verzija je prijevod, pripremljen i objavljen u sklopu projekta Podrška izborima na Zapadnom Balkanu, financiranog od strane Europske unije, uz financijsku potporu Austrijske državne agencije za razvoj. U slučaju nedosljednosti, konzultirajte izvornik na engleskom jeziku. Za više informacija o projektu i pristup biblioteci projekta, posjetite: <http://www.osce.org/odihr/wb>



Funded by  
the European Union

With funding  
from the  Austrian  
Development  
Agency



Nakladnik: OESS-ov Ured za demokratske institucije i ljudska prava (ODIHR)  
Ul. Miodowa 10  
00-251 Varšava  
Poljska

[www.osce.org/odihr](http://www.osce.org/odihr)

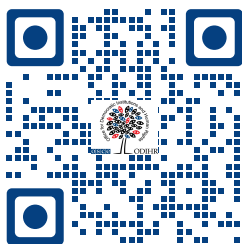
© OSCE/ODIHR 2023

Sva prava pridržana. Sadržaj ove publikacije može se slobodno koristiti i umnožavati u obrazovne i druge nekomercijalne svrhe pod uvjetom da se uz takvu uporabu OESS/ODIHR navede kao izvor.

ISBN 978-83-66690-98-1

Dizajn: Dejan Kuzmanovski

Naslovnica, Poglavlje 2, Poglavlje 3, Poglavlje 4, Poglavlje 5, Poglavlje 6,  
Poglavlje 7: OESS/Dejan Kuzmanovski



# Kazalo

<b>Predgovor</b>	<b>5</b>
<b>1. Uvod</b>	<b>7</b>
1.1. Svrha smjernica	8
1.2. Društvene mreže i mediji	10
<b>2. OEES- ova stajališta i druge međunarodne obveze, standardi i načela</b>	<b>14</b>
<b>3. Opća obilježja izbornih kampanja na društvenim mrežama</b>	<b>20</b>
3.1 Sadržaj i aktivnost	21
a. Poticanje na mržnju, netrpeljivost ili nasilje	23
b. Netolerantna, agresivna i negativna retorika	26
c. Manipulativne informacije	27
d. Rješavanje problema manipulativnih informacija	29
3.2 Političko oglašavanje i oglašavanje tijekom kampanje	37
a. Odgovori na oglašavanje na internetu	39
3.3 Zaštita privatnosti podataka	42
<b>4. ODIHR-ov pristup promatranju i procjeni izbornih kampanja na društvenim mrežama</b>	<b>46</b>
4.1 Misija procjene potreba	47
4.2 Promatračka misija	47
4.3 Izrada preporuka	49
<b>5. Uloga političkog analitičara u promatranju i procjeni izborne kampanje na društvenim mrežama</b>	<b>52</b>
5.1 Procjena pravnog okvira	54
a. Sadržaj na internetu	54
b. Političko oglašavanje i oglašavanje tijekom kampanje	55
c. Zaštita privatnosti podataka	56
5.2 Promatranje i procjena aktivnosti tijekom kampanje	58
a. Izbor platformi	60
b. Izbor korisničkog računala	61
c. Prikupljanje informacija	63

5.3 Promatranje i procjena političkog oglašavanja i oglašavanja tijekom kampanje	65
a. Transparentnost oglašavanja	65
b. Zahtjevi u vidu izvještavanja	67
c. Kampanja koju vodi treća strana	68
<b>6. Nadzor</b>	<b>70</b>
6.1 Nadzor nad sadržajem	71
6.2 Nadzor nad političkim oglašavanjem i oglašavanjem tijekom kampanje	73
6.3 Nadzor nad zaštitom privatnosti podataka	74
<b>7. Izazovi i prilike za kvantitativnu procjenu</b>	<b>78</b>
7.1 Metodološka ograničenja	78
7.2 Podaci iz vanjskih izvora	81
a. Alati za praćenje društvenih medija (Web-Listening) i sustavno učitavanje podataka (Data Scraping)	82
b. Pristup podacima <i>big-tech</i> kompanija	83
c. Provjeravatelji činjenica	85
<b>Aneks I – Relevantni međunarodni dokumenti</b>	<b>88</b>
<b>Aneks II – Glosar relevantnih termina</b>	<b>94</b>

# Predgovor

Internet je javnosti omogućio raširen pristup informacijama, između ostalog i pristup tijekom izbornih razdoblja, te pružio alat za široku političku raspravu i sudjelovanje u njoj. S pojavom stranica za društveno umrežavanje na internetu, izborne kampanje ušle su u novu eru komunikacija. Politički diskurs odmakao se od jednostranog prenošenja informacija, prema multilateralnom interaktivnom sustavu u kojem birači na raspolaganju imaju otvorene kanale za iznošenje mišljenja. Rasprava o utjecaju društvenih mreža na birače i izborne procese u posljednje je vrijeme privukla dosad neviđenu pozornost javnosti. Prije nego što se pozabavimo detaljima ove rasprave, važno je razumjeti da je digitalna kampanja tek još jedna metoda kojom se izborni kandidati i drugi akteri koji sudjeluju u izborima koriste kako bi privukli potporu ili komunicirali s biračima. Kao takva, ona treba biti podložna međunarodno priznatim standardima i načelima slobodnog i pravednog vođenja kampanje.

Stranice društvenih mreža pružaju prostor biračima za veće neposredno sudjelovanje u kampanjama i pritom izbornim kandidatima omogućavaju bolju mobilizaciju njihove potpore. Istodobno, korištenje društvenih mreža, posebice tijekom izbornih kampanja, sa sobom nosi širok dijapazon izazova. Neki od njih predstavljaju prijetnju ostvarivanju i zaštiti temeljnih sloboda i ljudskih prava, kao i ukupnom integritetu izbornog procesa.

Internetske komunikacijske tehnologije konstantno se razvijaju, a krajolik i popularnost različitih platformi društvenih mreža redovito se mijenjaju u sve rigidnije reguliranom okruženju. *Big-tech* kompanije, kao vlasnici društvenih mreža, počele su uvoditi promjene u načinu na koji funkcioniraju i postupaju s internetskim sadržajem. Mnoge od tih inicijativa mogu potencijalno dovesti do pozitivnog razvoja, kao što je povećana transparentnost, sprječavanje zlouporabe privatnih podataka ili zaštita specifičnih prava ili kategorija korisnika od uznemiravanja, ali one također često mogu onemogućiti pristup i primjenu temeljnih sloboda. U ovom kontekstu, jedna od pojava koja najviše zabrinjava je što platforme podliježu pritisku nekih vlada da uklone legitiman sadržaj i korisničke profile koji se kritički odnose prema vlasti, često bez mogućnosti pravne zaštite. Tamo gdje su *big-tech* kompanije ustale u obranu slobode govora, ponekad su izložene sve većem regulatornom pritisku, što uključuje i prijetnje da će izgubiti pristup tržištu.

Ured za demokratske institucije i ljudska prava (ODIHR) Organizacije za sigurnost i suradnju u Europi (OESS) razvio je sistematičnu i sveobuhvatnu metodologiju za promatranje izbora i procjenu izbornih procesa. Dok je procjena izborne kampanje već središnji aspekt ODIHR-ove opće metodologije za promatranje izbora, ove Smjernice konkretno se bave kampanjama koje se vode na društvenim mrežama. One sadrže smjernice za ODIHR-ove promatrače i koristan su alat za druge međunarodne i građanske promatračke organizacije u vezi s važnim načelima i međunarodnim dobrim praksama u vezi s ovom temom. Smjernice mogu pomoći i državama članicama OESS-a u njihovim nastojanjima da adekvatno odgovore na izazove koji proizlaze iz aktivnosti kampanja na internetu tijekom izbornog procesa.<sup>1</sup>

*Matteo Mecacci*  
*Direktor ODIHR-a*

---

<sup>1</sup> ODIHR se opredijelio da će redovito razmatrati i usavršavati svoju metodologiju promatranja izbora, u skladu s relevantnim zadacima koje mu postavljaju države članice OESS-a <https://www.osce.org/mc/23209> (Ministerial Council Decision 19/06)



# 1. UVOD

Društvene mreže pojedincima i skupinama omogućavaju izražavanje mišljenja, sudjelovanje u dijalogu i neposredno komuniciranje s političkim akterima i institucijama, kao i da postanu aktivni sudionici u izbornoj kampanji.<sup>2</sup> Globalno, korištenje društvenih mreža dodatno je pojačalo kritički angažman birača i potaknulo pojavu i organizaciju velikih skupina i društvenih pokreta. Društvene mreže postale su ključne za napredak u pogledu izražavanja i ostvarivanja temeljnih sloboda time što su birače od pasivnih primatelja informacija pretvorile u aktivne sudionike koji doprinose sadržaju javne rasprave. Društvene mreže uvelike su promijenile političke kampanje, bilo da se radi o načinu na koji ih kandidati koriste kao platforme za prezentiranje svojih politika i raspravu s biračima o njima, kao alate za političko oglašavanje, ili za prikupljanje i obradu osobnih podataka birača.

S druge strane, korištenje društvenih mreža na izborima, i šire u politici, može sa sobom nositi cijeli niz izazova i prijetnji. Neki od njih uključuju širenje manipulativnog sadržaja; pokušaje pojedinih država da ograniče pristup određenim temeljnim slobodama na internetu; neopravdanu kriminalizaciju sadržaja i aktivnosti; samovoljno blokiranje ili ukidanje pristupa mrežama; i selektivno prezentiranje, brisanje ili skrivanje sadržaja koji bi mogao djelotvorno izolirati određene skupine birača u uske informacijske silose ili, takozvane, ‘eho komore’. Drugi tipovi izazova povezani su sa zlouporabom osobnih podataka za oglašavanje i izborni inženjering, strano miješanje u izbore i politički diskurs, i sve veće korištenje botova i trolova s ciljem uspostavljanja javne agende i oblikovanja mišljenja birača, kao i za mobilizaciju ili onemogućavanje izlaska birača na izbore. Takve prakse, bilo da ih promoviraju države, big-tech kompanije, različite interesne skupine ili pojedinci, štetne su za demokratski izborni proces i mogu umanjiti povjerenje javnosti u izbore.<sup>3</sup>

Prepoznajući prijetnje koje predstavljaju neki od ovih izazova, posebice porast različitih tipova manipulativnog sadržaja, *big-tech* kompanije sve više nastoje suzbiti širenje takozvanih ‘dezinformacija’ i drugih zlouporaba koje potiču

---

2 Smjernice koriste termin „društvene mreže“ u smislu internetskih platformi koje pružaju višesmjernu interakciju putem sadržaja koji generiraju korisnici. Ova definicija slična je onima koje su korištene u [Zajedničkom izvješću](#) Europske komisije Vijeća Europe za demokraciju putem vladavine prava (Venecijanska komisija) i Uprave za informacijsko društvo i akciju protiv kriminala Glavne uprave za ljudska prava i vladavinu prava (DGI), o digitalnim tehnologijama i izborima; i [Smjernicama](#) instituta International IDEA za izradu kodeksa ponašanja tijekom izbora na društvenim medijima iz 2019.

3 Drugi glavni problemi povezani su s *decentraliziranom* ili *transnacionalnom* prirodom društvenih mreža i s ograničenjima u pogledu primjenjivosti i djelotvornosti zakonskih i pravosudnih radnji, kao i mogućnosti učinkovitog pravnog lijeka, koje iz toga proizlaze.

okruženje koje ne doprinosi provođenju demokratskih izbora. Za rješavanje pitanja takvih tipova sadržaja, u suradnji s vladama ili međunarodnim organizacijama razvijeni su zajednički zakoni, po kojima su se *big-tech* kompanije obvezale da će identificirati ili razriješiti značajna pitanja pouzdanosti sadržaja, transparentnosti prilikom oglašavanja i zaštite podataka. Neki od tih zakona predviđaju brisanje nezakonitog sadržaja ili oglasa, dok je u nekim zemljama korisnike potrebno obavijestiti kad su predmetom mikrociljanja (eng. *micro targeting*).

## 1.1 Svrha smjernica

Ove pojave, kako pozitivne tako i negativne, otvorile su brojna pitanja poštivanja temeljnih ljudskih prava u sferi interneta. Iako su neke države članice OESS-a pokušale regulirati neke aspekte interneta u domaćem zakonodavstvu, praksa je pokazala da su smisleni, sveobuhvatni i najučinkovitiji odgovori oni koji se provode multilateralno, kroz akcije koje prepoznaju prekograničnu prirodu društvenih mreža. U tom pogledu, Ujedinjeni narodi, OESS i druge regionalne organizacije poput Vijeća Europe ili Europske unije, pokrenule su inicijativu kojom ističu potrebu primjenjivanja zaštite ljudskih prava i temeljnih sloboda na jednak način na internetu kao i u stvarnom svijetu. Tako je pristup internetu i korištenje društvenih mreža tijekom izbora postalo ključno područje interesa u kontekstu međunarodnog i građanskog promatranja izbora.

Iako je vođenje kampanja na internetu globalno u porastu i uključuje cijeli niz aktivnosti i metoda, od kojih se neke često koriste izvan razdoblja službene kampanje i nastavit će se razvijati, ove Smjernice ne obuhvaćaju sve aspekte aktivnosti na internetu u kontekstu izbora. Također, ove Smjernice ne nastoje dati definiciju, razliku ili procjenu različitih tipova manipulativnog sadržaja (namjernu netočnu informaciju, eng. *disinformation*, zlonamjernu informaciju, eng. *malinformation*, ili nenamjernu netočnu informaciju, eng. *misinformation*) i ne daju naputke o tome treba li socijalne mreže smatrati odgovornima za sadržaj. U ovom kontekstu posebno je važno spomenuti da ne postoji jedinstveni pristup i da države članice OESS-a imaju suverena prava u reguliranju funkcioniranja društvenih platformi i ponašanja u vlastitim izbornim kampanjama na internetu, u skladu s međunarodno dogovorenim obvezama, standardima i načelima, te vlastitim političkim opredjeljenjima.

Cilj ovih Smjernica je dati okvir, uglavnom namijenjen izbornim promatračima, pomoću kojeg će na odgovarajući način procijeniti utjecaj ključnih aspekata kampanje na internetu na sveukupni integritet izbornog procesa i izborne kampanje. Ti aspekti uključuju aktivnosti kandidata na internetu, širenje specifičnih tipova sadržaja relevantnih za izborni proces, političko

oglašavanje i oglašavanje tijekom kampanje, te zaštitu privatnih podataka. Smjernice su razvijene uz izvanproračunsku potporu i dio su ODIHR-ovih nastojanja kontinuiranog poboljšanja svoje metodologije te povećanja sposobnosti promatranja određenih, specijaliziranih aspekata izbora.

U skladu s ODIHR-ovom metodologijom promatranja izbora, svaka procjena regulatornog okvira i prakse glede vođenja kampanje, uključujući i vođenje kampanje na društvenim mrežama, treba se vršiti na temelju priznatih obveza, standarda i načela sadržanih u relevantnim međunarodnim dokumentima.<sup>4</sup> Procjena treba uzeti u obzir pravni okvir koji se odnosi na vođenje kampanje na internetu, koji će se vjerojatno stalno i brzo mijenjati i širiti. Uslijed toga, svaki slučaj promatranja i procjenjivanja provođenja izbora na internetu neminovno sadrži ograničenja, te će se način na koji međunarodni izborni promatrači pristupaju ovoj temi nastaviti mijenjati.

Bitno je da politički analitičari, koji imaju sveukupnu odgovornost za procjenu izborne kampanje, uključujući i one na društvenim mrežama, budu u stanju kontekstualizirati ono što se događa na internetu i utvrditi korelacije unutar ukupnog ambijenta kampanje. S obzirom na razna pitanja koja na internetu treba promatrati, politički analitičari u procjeni izborne kampanje na društvenim mrežama trebaju surađivati s drugim ključnim članovima tima. Potencijalna područja preklapanja i modusi suradnje razrađeni su u nastavku.

Smjernice su strukturirane na sljedeći način:

- ♦ Uvod u vođenje kampanje na društvenim mrežama, koji uključuje pregled razlika i preklapanja između društvenih mreža i tradicionalnih medija;
- ♦ Analiza OESS-ovih stajališta i drugih međunarodnih obveza, standarda i načela relevantnih za vođenje izborne kampanje na internetu;
- ♦ Opis općih karakteristika vođenja kampanje na društvenim mrežama i ključnih područja reguliranja i procjene: internetski sadržaj i aktivnosti, političko oglašavanje i zaštita privatnosti podataka;
- ♦ ODIHR-ov pristup promatranju i procjeni vođenja kampanje na društvenim mrežama;
- ♦ Uloga političkog analitičara u promatranju i procjeni vođenja kampanje na društvenim mrežama;

---

4 Između ostalog, to uključuje [Opću deklaraciju o ljudskim pravima](#) (UDHR) iz 1948.; [UN-ov Međunarodni pakt o građanskim i političkim pravima](#) (ICCPR) iz 1966.; [Europsku konvenciju za zaštitu ljudskih prava i temeljnih sloboda](#) (ECHR) iz 1950. i [OESS-ov Kopenhaški dokument](#) iz 1990.

- ♦ Analiza važnosti učinkovitog nadzora internetskog sadržaja, političkog oglašavanja i zaštite podataka;
- ♦ Predstavljanje nekih prilika i ključnih metodoloških ograničenja za kvantitativni monitoring.

Smjernice se bave ODIHR-ovim pristupom promatranju i procjeni izbornih kampanja isključivo na društvenim mrežama. ODIHR-ova metodologija ukupnog promatranja i procjene izbornih kampanja koja uključuje tradicionalne oblike vođenja kampanje obrađena je u Priručniku za promatranje izbornih kampanja i političkih okruženja, objavljenom zajedno s ovim Smjernicama. Smjernice se bave društvenim mrežama kao entitetima koji se značajno razlikuju od tradicionalnih medija (televizije i tiska), njihovih internetskih verzija, kao i specijaliziranih informativnih portala, koji se procjenjuju u odnosu na međunarodne obveze u vezi s medijima, standardima i stajalištima, te stoga ostaju u djelokrugu rada medijskih analitičara tijekom izbornih promatračkih aktivnosti.<sup>5</sup> Elementi po kojima se društvene mreže razlikuju od tradicionalnih medija opisane su u sljedećem odjeljku.

U kontekstu OESS-a nisu razrađena specijalizirana stajališta u vezi s društvenim mrežama, a kampanje na internetu moraju ispuniti iste standarde koji se promjenjuju na ukupno vođenje izborne kampanje. Zbog nepostojanja konkretnih stajališta i standarda, te kako bi se bolje razumjeli izazovi koje predstavlja budući razvoj u domeni interneta, ove Smjernice nude definicije i citate iz brojnih izvješća vjerodostojnih međunarodnih organizacija, a koje su relevantne za države članice OESS-a. Dok će područje društvenih mreža sasvim izvjesno nastaviti tempo brzog razvoja i veoma je vjerojatno da će se pojavljivati nove platforme, u vrijeme pisanja Smjernica, u OESS-ovu području se tijekom izbornih kampanja najčešće koriste sljedeće društvene mreže: *Facebook, Instagram, Twitter, YouTube, Odnoklasniki i Vkontakte*. Alati za prenošenje poruka, kao što su *WhatsApp, Messenger, Telegram* ili drugi, mogu igrati važnu ulogu u širenju informacija, pogotovo tijekom izbornih razdoblja, međutim, oni nisu predmet ovih Smjernica ponajviše zbog njihove zatvorene prirode i manjka transparentnosti za promatranje, kao i zbog drugih pitanja glede poštivanja privatnosti i zaštite podataka članova tih skupina.

## 1.2 Društvene mreže i mediji

Pitanje prirode društvenih mreža – treba li ih shvaćati kao medij, kako često korišteni termin ‘društveni medij’ implicira, ili kao nešto drugo – i dalje je predmet javne i akademske rasprave. Očito je da društvene mreže služe kao medij komunikacije i razmjene informacija. Štoviše, služe za sličnu svrhu

<sup>5</sup> Za više o ODIHR-ovoj izbornoj metodologiji, vidi [Election Observation Handbook \(Sixth Edition\)](#), a za izbornu kampanju, vidi [Handbook for Observation of Political Environment and Election Campaign](#).

– razmjenu informacija, i teže postići sličan cilj – informirati javnost.<sup>6</sup> Međutim, u posljednje vrijeme sve je veći konsenzus o tome da društvene mreže doista jesu kreacija sui generis i da postoje mnogi aspekti koji ih odvajaju od tradicionalnih i internetskih medijskih organizacija. Neki od tih aspekata su:

- ♦ **Sadržaj:** U kontekstu tradicionalnih i internetskih medija, medijske organizacije i profesionalni novinari su ti koji kreiraju većinu sadržaja, dok je produkcija sadržaja na društvenim mrežama disperzirana, i uglavnom su konzumenti ti koji ga oblikuju i šire.
- ♦ **Uređivačka politika:** Uređivačka politika jedan je od temelja funkcioniranja i djelovanja medija. S druge strane, izuzmu li se algoritamske postavke koje kreiraju *big-tech* kompanije, društvene mreže nemaju jasne standarde uređivačke politike te se vodi rasprava o nivou odgovornosti koju bi one morale snositi za sadržaj produciran i dijeljen na njihovim platformama.
- ♦ **Angažman:** Društvene mreže veoma su difuzne informacijske platforme, gdje svatko može sudjelovati u razgovoru u realnom vremenu. Tradicionalni mediji uspostavljeni su hijerarhijski, a informacije općenito teku u jednom smjeru – od medijske organizacije ka širokoj javnosti.
- ♦ **Multimedijalnost:** Društvene mreže dozvoljavaju korištenje različitih tipova sadržaja u istom prostoru i u isto vrijeme: tekst, fotografije ili grafike, video i audio. Tradicionalni mediji obično imaju uže mogućnosti u pogledu prezentacije, iako i internetski mediji mogu integrirati različite tipove komunikacije.
- ♦ **Vrijeme:** Komunikacija na društvenim mrežama je trenutačna, dok tradicionalni mediji općenito rade po prethodno uspostavljenom rasporedu. Internetski mediji su fleksibilniji, ali i oni pokazuju tendenciju ograničenosti na prethodno uspostavljene vremenske okvire, dok je komunikacija na njima u realnom vremenu i dalje iznimka, a ne pravilo.
- ♦ **Trošak:** Kada se radi o produkciji sadržaja, tradicionalni i internetski mediji u usporedbi s društvenim mrežama najčešće zahtijevaju znatno veće troškove, uključujući materijalne i ljudske resurse, koji iziskuju prihod sredstava kako bi se omogućilo kontinuirano funkcioniranje.
- ♦ **Prikupljanje privatnih podataka:** Iako tradicionalni mediji često koriste različite tehnike za mjerenje svog rejtinga ili popularnosti programa, poput anketa javnog mnijenja ili mjernih uređaja, koji povremeno mogu

---

<sup>6</sup> Zbog ovih preklapanja između tradicionalnih medija i društvenih mreža, izvjestan broj međunarodnih standarda, obveza, načela i političkih stajališta u vezi sa slobodom izražavanja i pristupom informacijama primjenjiv je na obje kategorije. ODIHR-ova metodologija za promatranje medija može se naći u [Handbook on Media Monitoring for Election Observation Missions](#).

prikupiti određenu količinu osobnih podataka, jedan od ključnih aspekata funkcioniranja društvenih mreža (i drugih platformi utemeljenih na internetu te internetskih medija) je stalno prikupljanje privatnih podataka njihovih korisnika. Tip, količina, obrada, korištenje i trgovanje privatnim podacima korisnika, posebice u svrhu izbora, postalo je jedno od najkontroverznijih pitanja u vezi s funkcioniranjem društvenih mreža.

Prepoznavši promjene na području masovnih komunikacija, **Vijeće Europe**, međunarodna organizacija za ljudska prava koja u svojem članstvu broji 47 od 57 država članica OEES-a, razradila je **šest kriterija** za zajedničko razumijevanje pojma medija u državama članicama, te treba li društvenim mrežama dati specifična prava glede medija i dodijeliti im određene odgovornosti.<sup>7</sup> U toj Preporuci zapaža se da „stupanj do kojeg se kriteriji ispunjavaju omogućuje prepoznavanje predstavlja li novi komunikacijski servis medij ili ukazuje na to da može vršiti posredničku ili pomoćnu aktivnost na medijskim servisima“. Ova Preporuka dalje navodi da „se posrednici [...] mogu razlučiti od medija budući da ispunjavaju neke od tih kriterija [...], ali obično ne ispunjavaju neke od ključnih kriterija, kao što su uređivačka kontrola ili svrha. Međutim, oni često igraju bitnu ulogu, što im može dati znatnu moć u pogledu dometa i kontrole ili nadzora nad sadržajem. Shodno tome, [oni] mogu lako preuzeti aktivnu ulogu u uređivačkim procesima u sredstvima masovne komunikacije. Države članice ih stoga trebaju pažljivo razmotriti prilikom kreiranja politika glede medija i posebnu pozornost posvetiti svojim vlastitim pozitivnim i negativnim obvezama koje proizlaze iz članka 10. Europske konvencije o ljudskim pravima.“

Ti kriteriji (navedeni masnim slovima) koji su dopunjeni skupom pokazatelja (navedениh u zagradama) su: (i) **Namjera djelovanja u svojstvu medija** (samooznačavanje medijem; metode rada tipične za medij; opredijeljenost za profesionalne medijske standarde; praktična rješenja za masovno komuniciranje); (ii) **Svrha i osnovni ciljevi medija** (proizvodnja, prikupljanje ili širenje medijskih sadržaja; rad na aplikacijama ili platformama dizajniranim za olakšavanje interaktivne masovne komunikacije – na primjer, društvene mreže; animiranje i davanje prostora za javnu raspravu i politički dijalog; oblikovanje i utjecanje na javno mnijenje; promicanje vrijednosti; olakšavanje nadzora i povećanje transparentnosti i odgovornosti; nuđenje obrazovanja, razonode, kulturnog i umjetničkog izražavanja; kreiranje radnih mjesta; generiranje prihoda; periodično obnavljanje i ažuriranje sadržaja); (iii) **Uređivačka kontrola** (uređivačka politika; uređivački proces; moderiranje; uređivački tim); (iv) **Profesionalni standardi** (predanost; procesi usklađivanja; žalbeni procesi; potvrđivanje prerogativa, prava ili privilegija); (v) **Doseg i širenje informacija** (stvarno širenje; masovna komunikacija u svojoj ukupnosti; resursi za informiranje javnosti); (vi) **Očekivanja javnosti** (raspoloživost; pluralizam i raznolikost; pouzdanost; poštivanje profesionalnih i etičkih standarda; odgovornost i transparentnost).

7 Vidi Preporuku CM/Rec(2011)7 o novom pojmu medija Odbora ministara Vijeća Europe..





## 2.

# OESS-ova STAJALIŠTA I DRUGE MEĐUNARODNE OBVEZE, STANDARDI I NAČELA

Države članice zasad nisu utvrdile zasebna stajališta u pogledu korištenja interneta i društvenih mreža. Međutim, u posljednjem desetljeću bilo je udruženih nastojanja s raznim međunarodnim organizacijama, uključujući Vijeće Europe, za utvrđivanje temeljnih načela i standarda za korištenje tehnologija na izborima. Vođenje izborne kampanje na društvenim mrežama treba poštivati iste uvjete kao i tradicionalno vođenje kampanje i stoga mora ispuniti iste obaveze, stajališta i standarde koji se primjenjuju na druge metode vođenja kampanje. OESS-ova stajališta – s kojima su se države članice



OESS-a složile u Kopenhaškom dokumentu 1990., i kasnija OESS-ova stajališta i ministarske odluke – definiraju načela u vezi s demokratskim izborima, bez obzira na metodu kampanje koja se koristi. Općenito gledano, ova načela nalažu da se kampanja treba voditi u slobodnom i pravičnom okruženju, uz poštivanje temeljnih sloboda, a države trebaju osigurati potrebne uvjete za natjecanje kandidata pod jednakim uvjetima.

Prilikom procjene zakonodavstva i praksa vođenja kampanja na društvenim mrežama, treba uzeti u obzir sljedeće obveze, standarde, načela i stajališta što su ih potpisale države članice OESS-a u različitim međunarodnim dokumentima:

**1. Sloboda izražavanja i pravo na mišljenje bez uplitanja** – temeljno ljudsko pravo, neodvojivo od svakog demokratskog društva, u kontekstu izbora osigurava pravo kandidata na iznošenje svojih gledišta i pravo birača na pristup raznovrsnim informacijama i donošenje utemeljene odluke prilikom izbora kandidata.<sup>8</sup> Suštinski element ove slobode je pravo na mišljenje bez tuđeg uplitanja, što znači da svi građani, kao i udruge, uključujući političke stranke, moraju imati slobodu posjedovanja vlastitih gledišta i njihova slobodnog prenošenja drugima.<sup>9</sup> Interpretativni izvori zapažaju da: „birači trebaju biti u stanju formirati mišljenja neovisno, slobodni od nasilja ili prijetnje nasiljem, prisile, navođenja ili manipulativnog uplitanja bilo koje vrste“.<sup>10</sup> Istodobno, sloboda izražavanja ima neka ograničenja. Ona uključuju: „svako zagovaranje nacionalne, rasne ili vjerske mržnje koja predstavlja poticanje na diskriminaciju, netrpeljivost ili nasilje“.<sup>11</sup>

i. **Pristup informacijama i internetu** – pravo na slobodu izražavanja blisko je vezano uz ostvarivanje drugih prava, kao što je pristup informacijama.<sup>12</sup> Iako u međunarodnom pravu još uvijek nije priznato kao

8 UDHR i ICCPR jamče pravo na slobodu mišljenja i izražavanja. Njihova neophodnost u svakom demokratskom društvu je dalje potvrđena u Općim komentarima br. 25 i 34 koje je izdao UN-ov Odbor za ljudska prava. Brojni drugi sporazumi štite slobodu izražavanja, kao što su [Međunarodna konvencija o ukidanju svih oblika rasne diskriminacije \(ICERD\)](#); i [Konvencija o pravima osoba s invaliditetom \(CRPD\)](#).

9 Vidi članak 19.1 ICCPR-a. I [OESS-ov Kopenhaški dokument](#) iz 1990. i [Konvenciju o ljudskim pravima i temeljnim slobodama \(CHR\)](#) Zajednice neovisnih država (CIS) iz 1995., redom u člancima 9.1 i 11(1), prepoznaju da svatko ima pravo na slobodu izražavanja i da to pravo mora uključivati slobodu izražavanja, primanja i prenošenja informacija i ideja, bez uplitanja javnih tijela i bez obzira na granice.

10 Vidi Odbor za ljudska prava Ujedinjenih naroda (UN) [Opći komentar br. 25](#).

11 To je zabranjeno po ICCPR-u. Nadalje, sve druge zabrane mogu se primijeniti na (1) poštivanje prava ili ugleda drugih i (2) zaštitu nacionalne sigurnosti ili javnog reda i mira, ili javnog zdravlja ili morala. U svim slučajevima, prije nametanja bilo kakvih ograničenja temeljnih prava, uključujući slobodu izražavanja, treba provesti takozvani trostruki test pravne utemeljenosti, potrebe i razmjernosti, što znači da svako ograničenje (1) mora biti jasno utvrđeno zakonom uz mogućnost pravnog lijeka; (2) mora se jasno opravdati gore navedenim iznimnim okolnostima; i (3) mora biti razmjerno interesima koje namjerava zaštititi.

12 Vidi Odbor za ljudska prava Ujedinjenih naroda [Opći komentar br. 34](#).

ljudsko pravo, Vijeće za ljudska prava UN-a (HRC) pozvalo je države na promicanje univerzalnog pristupa internetu i priznavanje ljudska prava u kibernetičkom prostoru.<sup>13</sup> Pristup internetu kao temeljno pravo također se promiče u nekoliko OEES-ovih i UN-ovih zajedničkih deklaracija o slobodi izražavanja i interneta.<sup>14</sup> Na razini država, neke države članice OEES-a priznale su u svom nacionalnom zakonodavstvu pristup internetu kao temeljno pravo.<sup>15</sup>

- ii. **Načelo mrežne neutralnosti** – suštinski povezano s pravom na pristup internetu, ovo načelo zahtijeva jednako tretiranje sveukupnog prometa podataka.<sup>16</sup> Mrežna neutralnost znači da je korisnicima interneta potrebno omogućiti korištenje bilo koje aplikacije ili pristup bilo kojem servisu po vlastitom izboru i da tim prometom ne upravljaju, ne postavljaju prioritete ili ne diskriminiraju mrežni operateri.<sup>17</sup> Sukladno načelu mrežne neutralnosti u kontekstu izbora, pružatelji internetskih usluga ne smiju namjerno blokirati, usporavati, umanjivati važnost ili diskriminirati određeni tip internetskog sadržaja.

**2. Nediskriminacija** – nalaže da svi pojedinci bez obzira na rasu, boju kože, spol, jezik, religiju, političko ili drugo mišljenje, nacionalnost ili društveno podrijetlo, imovinu, rođenje ili drugi status trebaju biti jednako tretirani.<sup>18</sup> U kontekstu izbora i kampanja na internetu, ovo se u velikoj mjeri odnosi na korištenje diskriminatornog jezika protiv birača ili kandidata koji pripadaju određenim zajednicama i skupinama. Nadalje, poštivanje ovog načela treba se procjenjivati u odnosu na negativnu praksu algoritama nekih *big-tech*

13 Rezolucije UN HRC-a iz 2012. i 2016. o promicanju, zaštiti i ostvarivanju ljudskih prava na internetu potvrdile su „da neka prava [...] izvan interneta moraju također biti zaštićena na internetu, posebno sloboda izražavanja“ i pozivaju na „usvajanje nacionalnih javnih politika glede interneta čiji je cilj univerzalni pristup i ostvarenje ljudskih prava“.

14 Vidi zajedničke deklaracije UN-a, OEES-a i Organizacije američkih država (OAS): *Sloboda izražavanja i internet* (2011); *Univerzalnost i pravo na slobodu izražavanja* (2014); *Sloboda izražavanja i „lažne vijesti“, dezinformiranje i propaganda* (2017); *Neovisnost medija i raznolikost u digitalnom dobu* (2018); *Izazovi slobode izražavanja u idućem desetljeću* (2019) i *Sloboda izražavanja i izbori u digitalnom dobu* (2020).

15 U trenutku pisanja ovih Smjernica ova lista uključuje: Estoniju, Finsku, Francusku, Grčku i Španjolsku.

16 Na globalnoj razini, mrežna neutralnost zagovara se u Zajedničkoj deklaraciji UN-a, OEES-a i OAS-a iz 2011. o *Slobodi izražavanja i internetu*. Odbor ministara Vijeća Europe navodi da načelo mrežne neutralnosti „osnažuje puno ostvarivanje i uživanje prava na slobodu izražavanja“. Vidi također *Uredbu EU-a iz 2015., Standarde za slobodan, otvoren i inkluzivan Internet* Međuameričke komisije o ljudskim pravima, i *Zajednički izvješće* Venecijanske komisije iz 2019. i Direkcije za informacijsko društvo i Djelovanje protiv kriminala Glavne uprave za ljudska prava i vladavinu prava (DGI), o Digitalnim tehnologijama i izborima. Vidi također *Izvješće* posebnog izvjestitelja UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja iz 2017.

17 Vidi također *OEES-ov Media Freedom on the Internet Guidebook* iz 2016. i *Deklaraciju Odbora ministara Vijeća Europe o mrežnoj neutralnosti* iz 2010.

18 Međunarodno pravo određuje da svatko treba biti tretiran jednako pred zakonom i uživati jednaku zakonsku zaštitu. Vid ICERD; CRPD; ICCPR i Opći komentar br. 28; OAS ACHR; EU CFR; CIS CHR.

kompanija i pretraživača koji sistematično diskriminiraju ili umanjuju važnost sadržaja i rezultata pretrage u odnosu na specifične skupine i zajednice. Države članice OESS-a su se u Kopenhaškom dokumentu iz 1990. izjasnile da će osigurati uvjete pod kojima je građanima dozvoljeno „natjecanje za političku ili javnu dužnost, pojedinačno ili kao predstavnici političkih stranaka ili organizacija, bez diskriminacije“.

**3. Jednakost prilika** – jednaki uvjeti su suštinski dio pravičnog natjecanja.<sup>19</sup> Okviri izbornih kampanja, za tradicionalno ili internetsko vođenje kampanje, trebaju pružiti priliku svim kandidatima i drugim kvalificiranim akterima za slobodno izražavanje svojih gledišta na jednakoj osnovi i bez neopravdanog ograničavanja. Svi kandidati na izborima trebaju imati iste prilike predstaviti svoju kandidaturu, trebaju podlijevati istim pravilima kojima se uređuje korištenje internetskog prostora za kampanju, i ostvarivati isti pristup društvenim mrežama. Nekoliko OESS-ovih stajališta sadržanih u Kopenhaškom dokumentu iz 1990. konkretno poziva na jednak tretman i pravične prilike za natjecanje, uključujući stavke 7.6 i 7.7.<sup>20</sup>

**4. Načelo transparentnosti**– u samoj je srži procjene političkog financiranja i financiranja kampanje.<sup>21</sup> Stoga je to ključni element kada se radi o promatranju kampanja, pogotovo u pogledu objavljivanja izvora financiranja i iznosa koje su potrošili kandidati, političke stranke i treće strane na internetu. U kontekstu društvenih mreža, načelo transparentnosti također je relevantno kada se radi o moderiranju internetskog sadržaja (primjerice, kako se određeni tip sadržaja promovira, njegov značaj umanjuje ili se uklanja s određene platforme). Provedba načela transparentnosti i dalje predstavlja izazov i često može biti onemogućena zbog transnacionalne i decentralizirane

---

19 Vidi također ICCPR; CRPD; ACHR; CFR; CIS CHR; Opći komentar br. 25; Preporuku Odbora ministara o financiranju političkih stranaka 1516(2001) iz 2001. Vijeća Europe, i Kodeks dobre prakse u izbornim pitanjima iz 2002. Članak 10. Konvencije o standardima demokratskih izbora, pravima birača i slobodama u državama članicama Zajednice nezavisnih država radi osiguranja pravednih izbora nalaže „jednake mogućnosti za svakog kandidata ili svaku političku stranku (koaliciju) za sudjelovanje u izornoj kampanji, uključujući pristup masovnim medijima i telekomunikacijskim sredstvima“.

20 U stavu 7.6 OESS-ova Kopenhaškog dokumenta iz 1990., države članice izjasnile su se da će „političkim strankama i organizacijama pružiti potrebna pravna jamstva kako bi im se omogućilo međusobno natjecanje na temelju jednakog tretmana pred zakonom i od strane vlasti“, a u stavku 7.7 da će „dati dozvole da se vođenje političke kampanje obavlja u pravičnom i slobodnom ozračju u kojoj administrativno djelovanje, nasilje i zastrašivanje ne sprječavaju stranke i kandidate u slobodnom predstavljanju svojih gledišta i kvalifikacija, niti birače sprječavaju u stjecanju informacija i raspravljanju o tome“.

21 Konvencija Ujedinjenih naroda protiv korupcije (UNCAC) iz 2003., navodi da svaka država potpisnica Konvencije također treba razmotriti poduzimanje odgovarajućih mjera za „povećanje transparentnosti financiranja kandidatura za izabranu javnu dužnost“. Drugi međunarodni standardi obuhvaćeni su u Preporuci (2003)4 Odbora ministara Vijeća Europe državama članicama i Preporuci 1516 (2001) Parlamentarne skupštine Vijeća Europe (PACE). Vidi također članke 7. i 12. Konvencije o standardima demokratskih izbora, pravima birača i slobodama u državama članicama Zajednice nezavisnih država (CIS).

prirode društvenih mreža i mogućnosti anonimnosti korisnika mreže, te uslijed ograničenih mehanizama provedbe.<sup>22</sup>

**5. Zaštita podataka** – odnedavno je postala temeljno načelo u javnoj raspravi o utjecaju društvenih mreža na politička i izborna zbivanja. Privatne kompanije (big-tech platforme, trgovci (brokeri) podacima, ali i kandidati) obrađuju velike količine osobnih podataka prikupljenih iz anketa, javnih evidencija, aktivnosti na internetu, komercijalnih i drugih izvora. Ti se podaci često koriste za ciljano vođenje kampanje, oglašavanje, slanje izravnih poruka i procjenu naklonosti birača. Međunarodno pravo pruža zaštitu od „svojevoljnog nezakonitog miješanja u [...] privatnost, obitelj, dom ili prepisku“ i obvezuje države na „osiguravanje da informacije koje se tiču privatnog života osobe ne dospiju u ruke osoba koje nisu zakonom ovlaštene primati, obrađivati ili koristiti te informacije“.<sup>23</sup> Zaštita ovog prava također je ugrađena u mnoge regionalne instrumente, uključujući OESS-ov Kopenhaški dokument iz 1990.<sup>24</sup> Pravo na privatnost jednako se primjenjuje na internetu i izvjestan broj instrumenata poziva na veću zaštitu podataka na internetu.<sup>25</sup>

**6. Sloboda okupljanja i sloboda udruživanja** – koje štite UDHR i ICCPR kao i OESS-ov Kopenhaški dokument iz 1990.<sup>26</sup> Druga regionalna tijela, poput Vijeća Europe i njegove Europske konvencije o ljudskim pravima (ECHR) ili CIS-a, također štite ili jamče slobode mirnog okupljanja i udruživanja.<sup>27</sup> Digitalne tehnologije donijele su nove prilike za ostvarivanje tih sloboda uveliko proširivši mogućnosti pojedinaca, političkih pokreta i skupina civilnog društva za organiziranje i mobiliziranje, povezivanje s drugim skupinama i koordiniranje svojih aktivnosti te okupljanje u okruženju interneta bez

---

22 Manjak transparentnosti naveden je kao glavni nedostatak u moderiranju sadržaja i reguliranju koje vrše *big-tech* kompanije. Vidi [Izvjешće UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja iz 2019.](#) Vidi također [Zajedničku deklaraciju UN-a, OESS-a i OAS-a iz 2011.](#)

23 Vidi ICCPR i [Opći komentar br. 16](#) Odbora za ljudska prava UN-a.

24 [OESS-ov Kopenhaški dokument](#) iz 1990. zahtijeva od država osiguravanje pristupa informacijama i zaštitu privatnosti.

25 Vidi [Rezoluciju Opće skupštine UN-a o pravu na privatnost u digitalnoj eri, Konvenciju 108](#) Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka; [Preporuku \(20012\)/4](#) Odbora ministara Vijeća Europe o zaštiti ljudskih prava na servisima društvenih mreža i [Preporuku \(2016\)/5](#) o slobodi na internetu.

26 U [OESS-ovu Kopenhaškom dokumentu](#) iz 1990., države članice izjasnile su se da će štiti temeljne slobode koje imaju središnje mjesto u provođenju demokratskih izbora, uključujući mirno okupljanje (stav 9.2) i udruživanje (stav 9.3). Nadalje, stav 7.6 osigurava „pravo pojedinaca i skupina na udruživanje u vlastite političke stranke“, a stavak 7.7 osigurava „provođenje političkih kampanja u slobodnoj i pravičnoj atmosferi“ u kojoj „nasilje i zastrašivanje ne sprječavaju stranke i kandidate u slobodnom iznošenju svojih gledišta i kvalifikacija, niti sprječavaju birače u informiranju ili raspravljanju i glasovanju oslobođene od straha od odmazde“

27 Vidi članak 11. [ECHR-a](#) i članak 12. [Povelje Europske unije o temeljnim pravima](#) (CFR) iz 2000. Vidi također članak 12. [CIS CHR-a](#).

neopravdanog fizičkog uplitanja trećih strana ili vlada.<sup>28</sup> I Opća skupština UN-a i UN HRC naglasili su da države imaju obvezu zaštititi slobodu okupljanja i udruživanja na internetu.<sup>29</sup> Iako se okupljanje „općenito shvaća kao fizičko okupljanje ljudi, što uključuje i slobodu okupljanja“, UN HRC prepoznaje da se zaštita ljudskih prava, koja uključuje pravo na okupljanje, „može primijeniti i na slične interakcije na internetu“.<sup>30</sup>

**7. Pravo na učinkoviti pravni lijek** – u kontekstu izbora, zahtijeva od država uspostavu pravila i procedura koje će biračima, kandidatima i drugim sudionicima u izborima omogućiti upućivanje žalbi zbog kršenja njihovih prava u vezi s izborima putem učinkovitog sustava rješavanja sporova.<sup>31</sup> U kontekstu internetske izborne kampanje, ovo pravo nalaže da tijela odgovorna za rješavanje sporova tijekom izbora osiguraju učinkovite i pravodobne pravne lijekove za kršenje prava birača, kandidata ili drugih sudionika u izborima na internetu, uključujući kršenja koja vrše društvene mreže i big-tech kompanije, kao što su moderiranje i uklanjanje sadržaja, pitanja zaštite podataka ili političkog oglašavanja i oglašavanja tijekom kampanje.

Za implementaciju i poštivanje navedenih sloboda i prava u kontekstu vođenja izborne kampanje na društvenim mrežama koje su u vlasništvu nekoliko *big-tech* kompanija, relevantne su **UN-ove Smjernice o poslovnom sektoru i ljudskim pravima** (UN Guiding Principles on Business and Human Rights). Ovaj dokument bavi se primjenom ljudskih prava u kontekstu djelovanja transnacionalnih korporacija i drugih poslovnih subjekata i sadrži tri opća skupa načela: (i) postojeće obveze država članica u vezi s poštivanjem, zaštitom i ostvarivanjem ljudskih prava i temeljnih sloboda; (ii) uloga poslovnih subjekata kao specijaliziranih društvenih tijela koja vrše specijalizirane funkcije, od kojih se zahtijeva poštivanje svih primjenjivih zakona i poštivanje ljudskih prava; i (iii) potreba usklađenosti prava i obveza s odgovarajućim i učinkovitim pravnim lijekovima u slučaju njihova kršenja. U vezi s ovim načelima, dokument navodi da je „cilj ili funkcija zakona zahtijevati od poslovnih subjekata poštivanje ljudskih prava“ i da „poslovni subjekti moraju poštivati ljudska prava“.<sup>32</sup>

28 Vidi [Izvjješće](#) iz 2019. posebnog izvjestitelja UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja i [Izvjješće o enkripciji i anonimnosti](#) iz 2018.

29 Vidi [Rezoluciju](#) Opće skupštine UN-a o promicanju i zaštiti ljudskih prava i temeljnih sloboda, uključujući prava na mirno okupljanje i slobodu udruživanja; i UN HRC-ovu [Rezoluciju](#) o promicanju, zaštiti i ostvarivanju ljudskih prava na internetu.

30 Vidi [Rezoluciju](#) UN HRC-a o promicanju i zaštiti ljudskih prava u kontekstu mirnih prosvjeda.

31 Vidi članak 2.3 ICCPR-a; članak 13. ECHR-a; stavak 5.10 OESS-ova [Kopenhaškog dokumenta](#) iz 1990. i članak 6. CIS CHR-a.

32 Vidi [UN-ove Smjernice o poslovnom sektoru i ljudskim pravima](#) iz 2011.



### 3.

## OPĆE KARAKTERISTIKE IZBORNIH KAMPANJA NA DRUŠTVENIM MREŽAMA

Vođenje kampanja na društvenim mrežama često je jedina metoda koja se koristi tijekom cijele izborne kampanje. Golema količina informacija na društvenim mrežama i izazovi koji proizlaze iz njihove globalne i decentralizirane prirode dovode do toga da je potpuno praćenje nepraktično i neizvodljivo. Iako se ODIHR-ovim pristupom promatranju i procjeni vođenja kampanje na internetu bavimo u sljedećem poglavlju i to na temelju pristupa država članica OESS-a i drugih međunarodnih organizacija reguliranju i

rješavanju vođenja kampanje na društvenim mrežama, ovo poglavlje nudi prikaz sljedećih ključnih karakteristika:

1. Sadržaj i aktivnost na internetu;
2. Digitalno političko oglašavanje i oglašavanje tijekom kampanje; i
3. Pravila u pogledu zaštite podataka birača.<sup>33</sup>

### 3.1 SADRŽAJ I AKTIVNOST

Sadržaj koji generira (ili kreira) korisnik je bilo koji sadržaj, kao što su tekst, snimak glasa, video, slike ili njihova kombinacija, koji kreira pojedinac ili skupina korisnika društvene mreže. Zbog svoje 'organske' prirode, *big-tech* kompanije i mnoge države i međunarodne organizacije ovaj tip sadržaja tretiraju različito od sadržaja koje kreiraju komercijalne robne marke i, odnedavno, sadržaja koje kreiraju političke stranke, kandidati, institucije i organizacije civilnog društva. Treći tip sadržaja, koji se razlikuje od prethodne dvije kategorije, jeste sadržaj koji kreiraju takozvani 'influenseri' na društvenim mrežama.<sup>34</sup>

U OESS-ovoj regiji postoje mnogi nacionalni i međunarodni pokušaji reguliranja sadržaja i aktivnosti na internetu, što uključuje i izborna razdoblja. U tom procesu, države članice trebaju uzeti u obzir potrebne elemente zaštite prava na slobodu izražavanja i drugih temeljnih prava. Pored konvencionalnog shvaćanja ovog prava kao prava na posjedovanje i izražavanje različitih političkih gledišta, što je od ključnog značaja za slobodno vođenje izbornih kampanja, sloboda izražavanja povremeno također može uključivati ili se odnositi na govor koji se može smatrati duboko uvredljivim, te na informacije ili ideje koje mogu uvrijediti, šokirati ili uznemiriti.<sup>35</sup>

Ponekad se mogu nametnuti neka ograničenja slobode izražavanja, ali samo u skladu s međunarodnim obvezama i standardima i onda kad takvo izražavanje uključuje poticanje na nasilje, netrpeljivost, mržnju, diskriminaciju ili druge tipove ekstremno agresivne ili netolerantne retorike i informacijskog

33 *Internetski sadržaj u vezi s kampanjom* i bilo kakva ograničenja koja se nametnu na njega tijesno su povezana sa slobodom izražavanja, pravom na pristup internetu, nediskriminacijom i načelom transparentnosti i mrežne neutralnosti; *političko oglašavanje i oglašavanje tijekom izbora* uglavnom je povezano s načelima transparentnosti, jednakosti prilika i nediskriminacije; aspekt koji se tiče *zaštite podataka* u vezi je s pravom na privatnost i transparentnost.

34 'Influenser' na društvenoj mreži u kontekstu izbora je osoba ili vlasnik korisničkog računa koji aktivno širi politički sadržaj i ima sposobnost utjecanja na određene birače ili kategorije birača kada se radi o formiranju njihova mišljenja i izbora. Iako je fenomen 'influensera' uglavnom aktivan u komercijalnom svijetu, postaje sve relevantniji i u političkoj i izbornoj komunikaciji na društvenim mrežama.

35 Vidi *Opći komentar br. 34* i Europski sud za ljudska prava (ECTHR) *Obrazloženje o slobodi izražavanja i informiranja*.

nereda.<sup>36</sup> U pogledu reguliranja i ograničavanja slobode izražavanja i mišljenja na internetu, UN HRC navodi da su dozvoljena samo ograničenja u pogledu konkretnog sadržaja usklađena sa zaštitom i promicanjem ljudskih prava, te da su generičke zabrane isključene.<sup>37</sup> U OESS-ovoj regiji ta je praksa pokazala da je cilj država članica regulirati ili ograničiti tri opće kategorije sadržaja i govora koji:

- sadrže elemente poticanja na mržnju ili nasilje;
- su netolerantni, agresivni ili uvrjedljivi; i
- u novije vrijeme, sadržaje koji su manipulativnog karaktera s namjerom nanošenja štete ili predstavljaju ono što se često naziva dezinformacijom.<sup>38</sup>

Iako su slučajevi govora koji sadrži navedene elemente prisutni i javljaju se i mimo izbornih razdoblja, postaju intenzivniji naročito tijekom izbornih kampanja. Korištenje ovog tipa govora može imati negativan utjecaj na birače, bilo da ih obeshrabri u sudjelovanju u izborima ili utječući na njihovo pravo na formiranje mišljenja o različitim političkim pitanjima bez uplitanja ili ih pogrešno informirajući o nekim tehničkim i činjeničnim vidovima izbornog procesa, čime se u konačnici umanjuje povjerenje javnosti u ukupan politički i izborni proces.

Ključni izazovi za države članice OESS-a u raspravi o reguliranju internet-skog sadržaja i njegovu utjecaju na temeljne slobode, osobito na slobodu izražavanja, povezani su s *nedostatkom zajedničkih definicija i shvaćanja* temeljnih koncepata, kao što su poticanje, mržnja ili ‘namjerne dezinformacije’, kao i *uloge i odgovornosti društvenih mreža* (ili *big-tech* kompanija kao njihovih vlasnika) u širenju sadržaja. Pored ovih pitanja, također se javljaju kritike glede nedosljedne sudske prakse, čak i u okviru iste jurisdikcije. Važno je primijetiti da praksa pokazuje kako je tumačenje značenja ovih koncepata, ili utjecaja i odgovornosti društvenih mreža, predmet dugih sudskih procesa u kojima sudjeluju kompleksni akteri, te se o njima odlučuje od slučaja do slučaja.<sup>39</sup>

36 Nadalje, kao što stoji u [ICCPR-u](#), svako ograničenje mora ispuniti trostruki test pravne utemeljenosti, potrebe i razmjernosti.

37 Vidi [Opći komentar br. 34. Izvješće](#) iz 2011. godine, UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, mjere „blokiranja predstavljaju nepotrebna ili nerazmjerna sredstva za postizanje željenog cilja, budući da često nisu dovoljno ciljane i dovode do toga da širok spektar sadržaja mimo onoga što se smatra nezakonitim postane nedostupnim.”

38 OESS-ov predstavnik za slobodu medija (RFoM) dobio je od država članica OESS-a mandat za davanje ranih upozorenja i brzih odgovora na ozbiljno nepoštivanje propisa u pogledu slobodnih medija i slobode izražavanja. Iako bavljenje medijskim sadržajem nije u samoj srži mandata OESS-ova RfoM-a, ova pitanja mogu biti od interesa iz nekoliko razloga te je stoga RFoM o tome objavio niz izjava i izvješća. Vidi [web-stranicu](#) OESS RFoM-a.

39 Vidi [Bazu podataka o govoru mržnje](#) Europskog suda za ljudska prava (ECtHR).



U odsustvu zajedničkog shvaćanja pojmova, ODIHR-ovi promatrači trebaju se suzdržati od davanja definicija, klasifikacija ili karakterizacija određenih događaja ili aktivnosti koje su zapazili u vezi s ovim konceptima. ODIHR-ovi promatrači svoja nastojanja trebaju usmjeriti na procjenu utjecaja ovih zlouporaba na izborni proces, a ta procjena treba se temeljiti na relevantnim međunarodnim obvezama, standardima, načelima i stajalištima glede demokratskih izbora.

Nakon dvije bitne presude Europskog suda za ljudska prava (ECtHR), definirano je, i sada se primjenjuje, pet kriterija prilikom razmatranja slučajeva odgovornosti prenositelja sadržaja koje generira korisnik: (i) kontekst i sadržaj spornih komentara; (ii) odgovornost autora komentara; (iii) mjere koje poduzimaju operateri internet stranice i ponašanje pogođene strane; (iv) posljedice komentara na pogođenu stranu; i (v) posljedice za podnositelje žalbi. U predmetu **Delphi AS protiv Estonije**, ECtHR je utvrdio da je dotični posrednik odgovoran za ekstremnu prirodu sadržaja koje je generirao korisnik, te je presudio da posrednici trebaju snositi odgovornost, pogotovo u slučajevima koji uključuju poticanje na nasilje ili 'govor mržnje', pritom naglašavajući profesionalni i komercijalni karakter informativnih platformi.

U predmetu **Magyar Tartalomszolgáltatók Egyesülete (MTE) i Index.hu Zrt protiv Mađarske**, koji se tiče uvreda i vulgarnih komentara, ali ne i nekog oblika 'govora mržnje' niti izravnih prijetnji protiv pojedinaca, ECtHR je potvrdio da informativni portali, u pravilu, moraju preuzeti dužnosti i odgovornosti, međutim, zbog specifične prirode interneta, te dužnosti i odgovornosti mogu se do izvjesnog stupnja razlikovati od onih tradicionalnih izdavača, osobito u pogledu sadržaja koji objavljuje treća strana. Najvažnije je da je ECtHR naveo da bi utvrđivanje objektivne odgovornosti internetskih stranica, samo stoga što dozvoljavaju nefiltrirane komentare koji mogu predstavljati kršenje zakona, zahtijevalo „pretjeranu i neprovedivu predostrožnost koja može dovesti do podiranja prava na prenošenje informacija na internetu“, a uzeo je u obzir i negativne posljedice mišljenja da su posrednici odgovorni za komentare treće strane.<sup>40</sup>

## a. Poticanje na mržnju, neprijateljstvo ili nasilje

Općenito gledano, međunarodni sporazumi zabranjuju poticanje na mržnju, diskriminaciju, netrpeljivost i nasilje, ali ne postoji konsenzus oko značenja i jasnoće definicije 'govora mržnje'.<sup>41</sup> Međutim, definiciju tog koncepta na

<sup>40</sup> ECtHR dalje zapaža da „takva odgovornost može imati predvidive negativne posljedice na okruženje komentara internetskog portala [...] Za Sud, te posljedice mogu imati, neposredno ili posredno, učinak smanjenja slobode izražavanja na internetu“.

<sup>41</sup> Vidi ICCPR, koji od država zahtijeva zabranu „zagovaranja nacionalne, rasne ili vjerske mržnje koja predstavlja poticanje na diskriminaciju, netrpeljivost ili nasilje“ kao i „svakog zagovaranja rata“.

regionalnoj su razini ponudile organizacije poput Vijeća Europe.<sup>42</sup> Ukupno gledano, u svim regijama OEES-a mnogi su državni zakoni i dalje nejasni i ne definiraju ključne pojmove kao što su ‘mržnja’ ili ‘poticanje’; preširoka tumačenja onoga što predstavlja ‘govor mržnje’ mogu otvoriti mogućnosti ograničavanja govora u nezakonite svrhe.<sup>43</sup>

Nepostojanje jasnih definicija dovodi do nedosljednog usvajanja i provedbi propisa u regiji OEES-a. Međutim, budući da su države članice OEES-a svjesne kakvu prijetnju po javni život predstavlja širenje ovakvih problema, „odlučile su se za zauzimanje čvrste javne pozicije protiv govora mržnje i drugih oblika agresivnog nacionalizma, rasizma, šovinizma, ksenofobije, antisemitizma i nasilnog ekstremizma, kao i slučajeva diskriminacije na temelju religije ili vjerovanja“, te su „svjesne važnosti borbe protiv zločina iz mržnje, koji mogu biti potaknuti rasističkom, ksenofobnom i antisemitskom propagandom na internetu“.<sup>44</sup> Iako većina država članica OEES-a ima zakone koji ograničavaju određene oblike govora, „postoje izražene razlike između zakona o govoru mržnje u različitim zemljama, [a] uobičajena kritika na račun zakona o govoru mržnje je da zadiru u slobodu govora ili postaju kazna za mišljenja ili stajališta, a ne za djela“.<sup>45</sup>

**UN-ova Strategija i akcijski plan za djelovanje protiv govora mržnje** obuhvaćaju tri razine nezakonitog i zakonitog izražavanja.<sup>46</sup> Na *višoj razini* su „neposredno i javno poticanje na genocid“ i „zagovaranje nacionalne, rasne ili vjerske mržnje što predstavlja poticanje na diskriminaciju, netrpeljivost ili nasilje“, zabranjeni u međunarodnom pravu. Na *srednjoj razini*, izvjesni oblici ‘govora mržnje’ mogu biti zabranjeni, ali samo ako ograničenja navedena u zakonu uvažavaju legitimni cilj (npr., poštivanje prava drugih, ili zaštitu javnog reda) i ako su potrebna i razmjerna. Na *nižoj razini*, zakonska ograničenja ne treba nametati na širenje zakonitog izražavanja koje je, primjerice, uvrjedljivo, šokantno i zabrinjavajuće. (Vidi u nastavku Piramidu govora mržnje koju je izradila organizacija Article 19). Strategija također utvrđuje UN-ov pristup i odgovore na slučajeve govora mržnje, koje treba procjenjivati na temelju šest kriterija utvrđenih

42 Odbor ministara Vijeća Europe naveo je da pojam ‘govor mržnje’ obuhvaća sve oblike izražavanja koji šire, potiču, promiču ili opravdavaju rasnu mržnju, ksenofobiju, antisemitizam ili druge oblike mržnje utemeljene na netoleranciji, uključujući netoleranciju izraženu kroz agresivni nacionalizam i etnocentrizam, diskriminaciju i neprijateljstvo prema manjinama, migrantima i osobama imigrantskog podrijetla. Vidi posebnu [web-stranicu](#) Vijeća Europe o ‘govoru mržnje’.

43 Međunarodni ugovor koji se eksplicitno bavi oblicima izražavanja koji se mogu tumačiti kao ‘govor mržnje’ je ICERD. Prema ICERD-u, države nisu obvezne kriminalizirati ‘govor mržnje’, iako mogu postojati neke zabrane. Godine 2013., Odbor za eliminaciju rasne diskriminacije, ekspertno tijelo koje prati ICERD, objašnjava u svojem *Općem komentaru br. 35* da kriminalizaciju „treba ograničiti na ozbiljne slučajeve, koji se mogu dokazati izvan razumne sumnje, dok manje ozbiljne slučajeve treba rješavati sredstvima koja nisu kaznenopravna, uzimajući u obzir, između ostalog, prirodu i opseg utjecaja na ciljane osobe i skupine“.

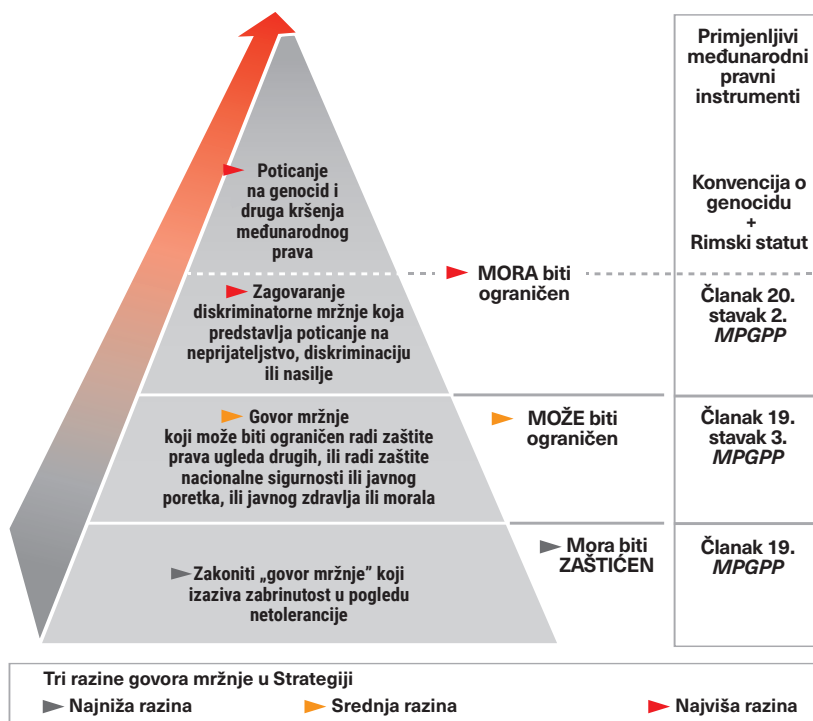
44 Vidi [Odluku Ministarskog vijeća 10/06](#) iz Porta i [Odluku Ministarskog vijeća 04/03](#) iz Maastrichta.

45 Vidi RFoM-ov [Neslužbeni dokument o propagandi i slobodi izražavanja](#) iz 2015. i [ODIHR-ov Hate Crime Laws, A Practical Guide](#) iz 2009..

46 Vidi [Strategiju i akcijski plan o govoru mržnje UN-a](#) iz 2020.

u testu donjeg praga definiranom u Rabatu.<sup>47</sup> U provedbi Strategije, UN zapaža da: a. treba kriminalizirati samo poticanje na diskriminaciju, neprijateljstvo ili nasilje koje ispunjava svih šest kriterija; b. manje ozbiljni oblici poticanja ili 'govora mržnje' (tj. oni koji ne ispunjavaju svih šest kriterija) trebaju biti predmet ograničenja temeljenih na građanskom ili administrativnom zakonu ili odgovora javne politike; i c. javna osuda govora mržnje, odgovornost za napade na osobe koje ostvaruju svoja prava slobode izražavanja, i ubrzano donošenje mjera javne politike vezanih uz promicanje različitosti mogu biti posebno važni neposredno nakon što se dogodi incident govora mržnje ili poticanja, te kada eskaliraju tenzije u društvu.

### Piramida govora mržnje prema organizaciji Article 19.<sup>48</sup>



IZVOR: Članak 19, Objašnjenje „govora mržnje”: Priručnik, str. 19.

47 **Akcijski plan iz Rabata**, inicijativa Visokog povjerenika Ujedinjenih naroda za ljudska prava o zabrani zagovaranja nacionalne, rasne ili vjerske mržnje što predstavlja poticanje na diskriminaciju, neprijateljstvo ili nasilje, sugerira visoki prag za definiranje ograničenja slobode izražavanja, poticanja na mržnju i primjenu članka 20. ICCPR-a. Tu se navodi šestodijelni test praga koji treba ispuniti kako bi neka izjava predstavljala kazneno djelo: (i) društveni i politički kontekst, (ii) status govornika, (iii) namjera poticanja javnosti protiv neke ciljane skupine, (iv) sadržaj i oblik govora, (v) doseg širenja i (vi) vjerojatnost izazivanja štete, koja uključuje njezinu neminovnost.

48 Article 19 je međunarodna organizacija za ljudska prava koja se bavi pitanjima slobode izražavanja i pristupa informacijama. Vidi [Article 19, 'Hate Speech' Explained: A Toolkit](#).

S pojavom društvenih mreža, korištenje različitih oblika vulgarnog, štetnog, neprijateljskog ili čak nezakonitog sadržaja postalo je veoma vidljivo, pogotovo tijekom izbornih razdoblja. Prema međunarodnom pravu, ekstremne mjere, kao što su politika blokiranja, gašenje interneta ili kriminalizacija suparničkih političkih stajališta na internetu, treba primjenjivati samo u iznimnim slučajevima otvoreno nezakonitog sadržaja ili diskursa koji nije zaštićen pravom na slobodu izražavanja.<sup>49</sup> U svim drugim slučajevima treba primijeniti alternativne alate, kao što su obrazovanje, protugovor i promocija pluralizma.<sup>50</sup>

Unatoč mnogim nastojanjima, inicijativama i javnim kampanjama za rješavanje pitanja 'govora mržnje', brojne međunarodne organizacije izvještavaju da su mnogi pojedinci, skupine i zajednice i dalje meta mržnje i diskriminacije na internetu. Diskriminatorne prakse, poticanje na nasilje i 'govor mržnje' nisu ograničeni na rasizam i ksenofobiju, već mogu poprimati i oblike seksizma, antisemitizma, islamofobije, mizoginije, homofobije i druge oblike.<sup>51</sup> Iako internetske platforme biračima dozvoljavaju slobodno dijeljenje informacija i mišljenja, također otvaraju vrata neprimjerenim komentarima, kao što su seksističke i druge diskriminatorne opaske.<sup>52</sup> Uznemiravanje na internetu može dovesti do isključivanja određenih skupina iz političkog i izbornog natjecanja, posebice žena kao kandidatkinja koje u nekim kontekstima mogu biti glavna meta takvog govora.<sup>53</sup>

## b. Netolerantna, agresivna i negativna retorika

U nekim kontekstima, izborne kampanje mogu postati emocionalno nabijene, pri čemu kandidati ili birači koriste agresivniju retoriku. U regiji OESS-a, jedan dio država članica usvojio je i provodi odredbe u domeni interneta koje su kopija propisa i ograničenja osmišljenih za konvencionalne načine vođenja kampanje i tradicionalne medije, uključujući kaznene zakone o kleveti. Općenito gledano, kazneni zakoni o kleveti, kao i njihova primjena i zloporaba od strane političara ili drugih javnih ličnosti predstavljaju kršenje

49 Ovo uključuje ratnu propagandu i zagovaranje mržnje što predstavlja poticanje na nasilje, izravno i javno poticanje na genocid i dječju pornografiju, pod uvjetom da je pravosudno tijelo utvrdilo postojanje nezakonitosti sadržaja.

50 Vidi [Izvjješće](#) iz 2019. UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja.

51 Vidjeti PACE-ovu [Rezoluciju 2144 \(2017\)](#) o Dokidanju kibernetičke diskriminacije i govora mržnje na internetu.

52 Vidi [Studiju DGI \(2017\)](#)<sup>10</sup> Vijeća Europe o medijima, izborima i rodnim pitanjima.

53 Interparlamentarna unija (IPU) – PACE iz 2018. u svojoj je [studiji](#) pokazala da su žene članice parlamenta u Europi vjerojatnija meta internetskih napada. [Studija](#) iz 2016. koju je provelo isto tijelo utvrdila je da su „društveni mediji postali glavno mjesto na kojem se psihološko nasilje – osobito u obliku seksističkih i mizoginih opaski, ponižavajućih slika, *mobbinga*, zastrašivanja i prijetnji – vrši protiv parlamentarki“.

međunarodnih standarda.<sup>54</sup> Nadalje, sankcije za klevetu ili uvredu moraju biti razmjerne kršenju prava ili ugleda drugih. Mjere koje su ove države usvojile trebaju uzeti u obzir sve moguće učinkovite i odgovarajuće dobrovoljne pravne lijekove koje mediji ponude i pogođene osobe prihvate.

**Europski sud za ljudska prava** je u dvjema povijesnim presudama presudio da je „sloboda izražavanja [...] primjenjiva ne samo na 'informacije' ili 'ideje' koje su prihvatljive i smatraju se neuvredljivim ili nevažnim, već i na one koje vrijeđaju, šokiraju ili uznemiravaju državu ili bilo koji sektor stanovništva“ a potrebne su za postojanje „pluralizma, tolerancije i otvorenosti bez kojih nema demokratskog društva“. Sud je također primijetio da su „ograničenja u pogledu onog što predstavlja prihvatljivu kritiku [...] veća za političare koji djeluju u javnom svojstvu“, koji „neizbježno i svjesno sebe izlažu većem nadzoru i od strane novinara i šire javnosti kad su u pitanju njihove riječi i djela“.<sup>55</sup> Iako su obje presude donesene u vrijeme prije pojave društvenih mreža, ECtHR je nedavno ponovo potvrdio da je „njegova sudska praksa [vezana uz] članak 10. u potpunosti primjenjiva na Internet“.<sup>56</sup>

### c. Manipulativne informacije

Debata o zajedničkom shvaćanju pojmova i razvoju jedinstvene terminologije za prethodno obrađena pitanja i dalje traje, ali ove zlouporabe u javnoj sferi postoje već prilično dugo i države imaju iskustva u njihovu rješavanju, te su kao takve te zlouporabe često podložne strogim regulatornim standardima. S druge strane, fenomen manipulativnog sadržaja na internetu (najčešće korišteni termin je 'dezinformacija'), koji postaje posebice izražen u razdoblju kampanje, predstavlja veći izazov za reguliranje i često može imati odlučujuće ili štetne učinke na izborne procese i ishode.<sup>57</sup> Zbog nepostojanja jasnih regulatornih standarda koji odgovaraju novim izazovima koji proizlaze iz svijeta interneta i njegove globalne prirode, kao i zbog potencijala za veliko širenje koji karakteriziraju društvene mreže, u nekim je kontekstima

54 Vidi [web-stranicu](#) OEES-ova RFoM-a o kleveti. UN-ov Odbor za ljudska prava u [Općem komentaru br. 34](#) potvrdio je da sve države „trebaju razmotriti dekriminalizaciju klevete, i da, u svakom slučaju, primjena kaznenog zakona treba biti prihvatljiva samo u najozbiljnijim slučajevima te da zatvor nikada nije odgovarajuća kazna“. [Zajednička deklaracija](#) UN-a, OEES-a i OAS-a iz 2020. poziva države na ukidanje kriminalizacije klevete i njezinu zamjenu odgovarajućim građanskopravnim propisima o kleveti.

55 Vidi ECtHR-ove predmete [Handyside protiv Ujedinjenog Kraljevstva](#) (1976) i [Lopes Gomes da Silva protiv Portugala](#) (2000).

56 Vidi ECtHR-ova [Obrazloženja o slobodi izražavanja i informiranja](#).

57 Iako ne postoji univerzalno prihvaćena definicija informacija manipulativnog sadržaja, neke organizacije pokušale su izraziti razliku između različitih tipova informacijskog nereda, kao što su: (1) *Dezinformacije*: lažne ili obmanjujuće informacije kojima je namjera učiniti štetu; (2) *Misinformacije*: lažne informacije koje nisu kreirane kako bi se učinila šteta; (3) *Malinformacije*: informacije utemeljene na realnosti koje se dijele s namjerom izazivanja štete. Fokus ovih Smjernica je na procjeni utjecaja različitih tipova manipulativnog sadržaja na integritet izbornog procesa i vođenje izbornih kampanja, a ne nastoje dati terminološko objašnjenje i razliku između ovih koncepata.

širenje i proliferacija ovog tipa sadržaja postalo sve izraženije i uzrokuje zabrinutosti za ukupni integritet izbornog procesa.

Različiti tipovi manipulativnog sadržaja na internetu, pogotovo dezinformacije, mogu biti štetni za demokratski proces i mogu negativno utjecati na provođenje istinski demokratskih izbora. Budući da se ovaj tip sadržaja često koristi s ciljem obmanjivanja birača ili podriivanja povjerenja javnosti u izborni proces, on ograničava pravo birača na formiranje mišljenja bez neopravdanog uplitanja te smanjuje njihovu sposobnost odabira na temelju pune informiranosti. Šire gledano, ovaj tip sadržaja može se također uplitati u pravo na slobodu od nezakonitih napada na čast i ugled, budući da se često odnosi na konkretnog pojedinca, političku ili javnu osobu, i osmišljen je kako bi naudio njezinu ili njegovu ugledu, a kada je usmjeren protiv određenih skupina u društvu, kao što su migranti ili određene skupine nacionalnih manjina i potiče mržnju, nasilje ili diskriminaciju, može opstruirati načelo nediskriminacije, kako je definiran u ICCPR-u. Istodobno, slaba regulativa i/ili odgovori na planu politika, kako *big-tech* tvrtki tako i tijela vlasti, mogu također imati štetan utjecaj na zaštitu temeljnih prava, pogotovo prava na slobodu izražavanja. Preširoka ograničavanja manipulativnog sadržaja i dezinformacija mogu dovesti do ograničavanja legitimnog govora.<sup>58</sup>

Države članice OESS-a odlučile su se za osiguravanje uvjeta za izborne procese u skladu s demokratskim standardima i načelima, i time imaju odgovornost osigurati okruženje za izbore u kojem nema manipulativnog sadržaja i u kojem su birači slobodni formirati svoja mišljenja bez neopravdanog uplitanja. Prema tome, države članice imaju odgovornost i obvezu baviti se fenomenom dezinformacija. Decentralizirana, disperzirana i ekstrateritorialna priroda društvenih mreža, teškoće u identificiranju počinitelja uslijed anonimnosti korisnika i često neučinkoviti odgovori pravosuđa uslijed nepostojanja jurisdikcijske ovlasti, potaknuli su brojne vlade na rješavanje ovog problema putem multilateralnih inicijativa i suradnje u kojoj sudjeluju i nedržavni akteri, poput civilnog društva, medija i *big-tech* tvrtki.

**Izvešće UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja** iz 2021. razmatra prijetnje po ljudska prava, demokratske institucije i izborne procese koje predstavljaju dezinformacije. Izvešće prepoznaje kompleksnosti i izazove koje predstavljaju dezinformacije u digitalnom dobu, i smatra da su odgovori država i kompanija problematični, neadekvatni i štetni po ljudska prava. Izvešće poziva na višedimenzionalne odgovore više aktera koji su čvrsto utemeljeni na okviru međunarodnih ljudskih prava i poziva *big-tech* kompanije na razmatranje svojih poslovnih modela, a države na rekalkibriranje svojih odgovora na

58 **Zajednička deklaracija** UN-a, OESS-a i OAS-a iz 2017. naglašava da neki oblici manipulativnog sadržaja mogu štetiti ugledu i privatnosti pojedinca, ili potaknuti na nasilje, diskriminaciju ili netrpeljivost protiv skupina u društvu koje je moguće identificirati. Međutim, u Deklaraciji se zaključuje da su „opće zabrane širenja informacija utemeljenih na nejasnim ili dvosmislenim idejama, uključujući ‘lažne vijesti’ ili ‘neobjektivne informacije’, nekompatibilnes međunarodnim standardima u pogledu ograničavanja slobode izražavanja [...] i trebaju biti ukinute“. Nadalje, **Zajednička deklaracija iz 2020.** o izborima u digitalnom dobu daje argumente protiv blokiranja i gašenja interneta, kao i protiv preširokih ili dvosmislenih zakona o dezinformaciji.

dezinformacije jačanjem uloge slobodnih, neovisnih i raznovrsnih medija, ulaganjem u medijsku i digitalnu pismenost, osnaživanjem pojedinaca i ponovnom izgradnjom povjerenja javnosti. Specifično za izbore, izvješće prepoznaje da se kampanje dezinformiranja koriste „na veoma vidljive načine s ciljem podriivanja prava na slobodne i pravične izbore [i] teže utjecati na izbore“. Izvješće zaključuje da je zbog fenomena dezinformacije „lako – ali opasno – izgubiti iz vida vrijednost koju digitalna tehnologija nudi demokraciji, održivom razvoju i ljudskim pravima, ili ključni značaj prava na slobodu mišljenja i izražavanja u toj jednadžbi. Zato su pokušaji borbe protiv dezinformacija kroz podriivanje ljudskih prava kratkovidni i kontraproduktivni. Pravo na slobodu mišljenja i izražavanja nije dio problema, već je cilj i sredstvo u borbi protiv dezinformacija.“<sup>59</sup>

#### **d. Rješavanje problema manipulativnih informacija**

##### *i. Odgovori država*

Uz nepostojanje jasne definicije i konsenzusa o tome što predstavlja informaciju manipulativnog sadržaja, zbog čega je smanjena učinkovitost odgovora na njih, jedan od ključnih izazova s kojim se suočava većina država članica OESS-a je rješavanje i reguliranje manipulativnih sadržaja na način koji poštuje ljudska prava i temeljne slobode, kao i načela zakonitosti, potrebe i razmjernosti.<sup>60</sup> Pristup utemeljen na ljudskim pravima zahtijeva ne samo izravno fokusiranje na dezinformacije, već i na njihov negativni utjecaj. Treba uvesti adekvatne dugoročne politike unaprjeđivanja digitalne pismenosti i provoditi kampanje za podizanje svijesti sudionika u izborima, umjesto isključivo zakonodavnih i regulatornih rješenja koja bi mogla negativno utjecati na temeljna prava koja uključuju i slobodu izražavanja.

Iako države članice OESS-a imaju pozitivnu obvezu osiguravanja jednakih uvjeta svim kandidatima te osiguravanja prava birača, što je sastavni dio međunarodnih i regionalnih instrumenata, nema jedinstvenog rješenja za izazove koje predstavlja manipulativni sadržaj.<sup>61</sup>

<sup>59</sup> Vidi *Izvješće UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja* iz 2021.

<sup>60</sup> Vidi *Rezoluciju 44/12 UN HRC-a o slobodi mišljenja i izražavanja* iz 2020.

<sup>61</sup> Prema članku 2. *ICCPR-a*, države su glavni nositelji dužnosti koja podrazumijeva obvezu poštivanja, zaštite i ostvarivanja ljudskih prava i imaju pozitivnu obvezu osigurati provedbu tih prava. U kontekstu dezinformacija, države se trebaju suzdržati od uplitanja u pravo na formiranje mišljenja i imaju obvezu osigurati da se drugi akteri, poput poslovnih subjekata, u to pravo ne upliću, kao i obvezu proaktivnog plasiranja informacija od javnog interesa u javnu domenu i promicanja pluralnih i raznolikih izvora informacija, što uključuje i medijsku slobodu.

Globalno se mogu identificirati četiri pristupa kojima se države služe u rješavanju problema dezinformacija i manipulativnog sadržaja, među kojima su i oni koje provode države članice OESS-a:

- (i) Primjena relevantnih odredbi postojećeg građanskog, kaznenog i administrativnog prava i drugih zakona koji reguliraju medije, izbore i borbu protiv klevete, čak i ako ti zakoni, usvojeni u doba prije interneta, ne odražavaju uvijek aktualna tehnološka dostignuća;
- (ii) Usvajanje novih zakona kojima se uvode sankcije društvenim mrežama koje šire lažne vijesti, obično kroz nametanje novčanih kazni i naredbi za uklanjanje informacija prepoznatih kao lažnih;
- (iii) Suradnja s izbornim tijelima i internetskim platformama kako bi se osiguralo dobro informirano biračko tijelo, bilo metodom identifikacije i blokiranja lažnih vijesti, osiguravanjem resursa za provjeru činjenica koji će služiti općoj javnosti, ili masovnim objavljivanjem istinitih vijesti tijekom razdoblja izbora i izvan njega; i
- (iv) Primjena širih i dugoročnih politika s ciljem obrazovanja građana o opasnostima koje predstavljaju lažne vijesti.<sup>62</sup>

U cijeloj OESS-ovoj regiji, nekoliko država usvojilo je zakone koji nameću odgovornost posrednika u plasmanu sadržaja koje generira korisnik. Takav pristup nailazi na kritiku relevantnih organizacija za ljudska prava kao pristup koji nije u potpunosti usklađen s međunarodnim standardima, a države se poziva na izbjegavanje prenošenja odgovornosti na kompanije kao subjekte koji će presuđivati o sadržaju. Pridavanje ove vrste obveze i odgovornosti privatnim kompanijama, daje im ovlast korporativnog prosuđivanja vrijednosti ljudskih prava, često na štetu ostvarivanja sloboda od strane korisnika.<sup>63</sup> Druge države članice OESS-a usvojile su neregulatorne mjere, uključujući, primjerice, izradu profesionalnih kodeksa, uspostavu vijeća za medije, imenovanje javnih radio-televizijskih organizacija ili uspostavu specijaliziranih jedinica za borbu protiv informacijskog nereda, nastojanja na planu samoregulacije samih medijskih kuća i programe medijskog opismenjanja.<sup>64</sup>

62 Vidi [Izvjješće Kongresne knjižnice o Inicijativama za suzbijanje lažnih vijesti u odabranim zemljama](#) iz 2019.

63 Vidi [UN HRC-ov Doprinis parlamenata radu vijeća za ljudska prava i njegovo opće redovito izvješće](#). Vidi također [Zajedničke deklaracije UN-a, OESS-a i OAS-a iz 2017. i 2020.](#) u kojima se ponovo potvrđuje da se posrednici nikad ne smiju smatrati odgovornima za sadržaj koji šire, osim ako specifično ne interveniraju u taj sadržaj ili propuste izvršiti zakonski obvezujuću naredbu da se on ukloni iako za to imaju tehničke kapacitete. Nadalje, obje deklaracije pozivaju *big-tech* kompanije na zauzimanje pristupa utemeljenog na ljudskim pravima prilikom reguliranja sadržaja, te na implementiranje UN-ovih [Smjernica o poslovnom sektoru i ljudskim pravima](#).

64 Za detaljan pregled studija slučaja iz pojedinih država, vidi [OESS-ov report on disinformation iz 2019.](#)



## ii. Big-Tech kompanije

Privatne kompanije prilikom moderiranja i reguliranja sadržaja trebaju primjenjivati pristup utemeljen na ljudskim pravima, međutim, važno je naglasiti da one nemaju iste obveze u pogledu ljudskih prava kao države. Kao odgovor na povećani javni pritisak i nakon brojnih kontroverzi u vezi s masovnim i široko rasprostranjenim informacijama manipulativnog sadržaja koje su ponekad vodile u netrpeljivost i nasilje, kao i na zlouporabu privatnih podataka, uključujući zlouporabu u političke svrhe i u svrhe kampanje, koje su možda imale odlučujući utjecaj na ishod izbora, nekoliko big-tech kompanija usvojilo je skup mjera za rješavanje ovih izazova.<sup>65</sup> Nadalje, kao što je prethodno navedeno, neke od država usvojile su propise kojima su izravnu obvezu i odgovornost prenijele na *big-tech* kompanije kao odgovorne posrednike sadržaja koji generiraju korisnici. Međutim, pokušaji izbjegavanja odgovornosti od strane privatnih subjekata i financijske sankcije ponekad mogu dovesti do uklanjanja zakonitog i legitimnog sadržaja bez prilike za ulaganje žalbe.

Iako samoreguliranje može biti pozitivno rješenje, ono se općenito provodi na dobrovoljnoj osnovi. Uz pitanja glede *big-tech* kompanija koje djeluju kao subjekti koji presuđuju o sadržaju, ostala su pitanja u vezi s oslanjanjem internetskih platformi na automatsko označavanje ili uklanjanje sadržaja i nedovoljnu transparentnost u pogledu standarda i procesa prilikom ograničavanja sadržaja. Korištenje softvera umjetne inteligencije za uklanjanje sadržaja nema kapacitete za kontekstualnu procjenu i predstavlja očite rizike za pretvaranje u radnje koje nisu u skladu sa zakonskim okvirom o ljudskim pravima. Kao opće pravilo, svaka politika koja ograničava sadržaj mora biti jasna, objektivna, lako dostupna i razumljiva, a korisnici trebaju biti promptno obaviješteni u slučaju bilo koje radnje koja se provodi protiv njihova sadržaja.<sup>66</sup>

**Big-tech kompanije** na raspolaganju imaju cijeli raspon mogućnosti, osim brisanja ili uklanjanja web-stranica i korisničkih računa. Te mjere mogu uključivati:

65 Promjene koje su neke big-tech kompanije uvele osmišljene su uglavnom kao odgovor na zabrinutost javnosti, između ostalog i na zabrinutost međuvladinih organizacija, kao što je EU. Uz pravila koja se tiču moderiranja sadržaja, nove politike uključuju dodatna jamstva za zaštitu privatnih podataka korisnika i mjere usmjerene na transparentnost političkog oglašavanja. Usvojeni skup mjera sačinjen je u skladu s odlukom big-tech kompanija o primjenjivanju EU-ova **Kodeksa o suzbijanju dezinformacija** (koji ćemo kasnije razmotriti u ovim Smjernicama). Iako je primijećen izvjestan napredak u kontekstu EU, „izvješća pokazuju da je potrebno daljnje djelovanje u drugim područjima kako bi se povećala pouzdanost online ekosustava i zaštita korisnika“. Nadalje, jedna od ključnih kritika na račun *big-tech* kompanija tiče se činjenice da su, bez obzira na njihovo globalno prisustvo i doseg, politike zaštite podataka, moderiranja sadržaja i transparentnog političkog oglašavanja i oglašavanja tijekom kampanje neujednačene u različitim zemljama, uključujući i one iz OEES-ove regije.

66 Vidi **Zajedničku deklaraciju** UN-a, OEES-a i OAS-a iz 2017.

- brisanje sadržaja,
- ograničavanje njegove viralnosti,
- naznačavanje njegova podrijetla,
- suspendiranje relevantnog korisnika ili organizacije koja je sponzor tog sadržaja,
- uvođenje rejtinga kako bi se pokazalo da neka osoba koristi zabranjeni sadržaj,
- privremeno ograničavanje sadržaja dok ga tim ne pregleda,
- sprječavanje korisnika u unovčavanju svojeg sadržaja,
- ometanje razmjene sadržaja, dodavanje upozorenja i oznaka na sadržaj,
- pružanje pojedincima više mogućnosti blokiranja drugih korisnika,
- smanjenje širenja sadržaja,
- ometanje *botova* i koordiniranog neautentičnog sadržaja,
- nametanje ograničenja u pogledu geolokacije, i promicanje protuporuka.<sup>67</sup>

### *iii. Nastojanja međunarodne zajednice*

Nekoliko UN-ovih institucija i agencija posvećuje značajnu pozornost fenomenu širenja informacija manipulativnog sadržaja. Konkretno navodeći utjecaj dezinformacija na izbore, glavni tajnik UN-a u svojem je izvještaju Općoj skupštini iz 2019. godine, naveo da korištenje interneta u kontekstu izbora, „bilo kao sredstva za poticanje na sudjelovanje u izborima, bilo kao alata za širenje dezinformacija i govora mržnje, otvara kompleksna pitanja [...] Paralizirajuća sumnja da se bilo kojom informacijom ili diskursom može manipulirati – i erozija povjerenja koja proizlazi iz toga – nalazi u samoj srži izazova koji za demokraciju predstavlja internet. Među ostalim mjerama, naglašava se važnost izgradnje otpornosti društava na širenje lažnog i mrzi-lačkog sadržaja, veće transparentnosti javnog diskursa i vođenja dijaloga u kojem sudjeluje više sudionika s ciljem pronalaska odgovora na izazove u pogledu politika.“ Nadalje, uz ovu i već spomenute deklaracije i izvješća posebnog izvjestitelja UN-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, Organizacija Ujedinjenih naroda za obrazovanje, znanost i kulturu (UNESCO) izdala je nekoliko publikacija glede šireg pitanja informacijskog nereda i njegova utjecaja na izborne procese.<sup>68</sup>

<sup>67</sup> Vidi *Izvješće* iz 2019. UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja.

<sup>68</sup> Vidi *Priručnik za obrazovanje i edukaciju novinara* iz 2018., *Izbori i mediji u digitalnom dobu* iz 2019. i izvješće Komisije za istraživanje širokopojsnog pristupa *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression* iz 2020.

U kontekstu OESS-a, OESS RfOM izdao je nekoliko dokumenata o pitanjima slobode izražavanja na internetu.<sup>69</sup> Nadalje, u suradnji s UN-ovim i OAS-ovim izvjestiteljima o slobodi izražavanja, OESS RfOM izdao je nekoliko zajedničkih deklaracija u vezi s informacijskim neredom, uključujući Zajedničku deklaraciju o slobodi izražavanja i izborima u digitalnoj eri, donesenu 2020. godine.<sup>70</sup>

**Zajednička deklaracija** iz 2020. godine prepoznaje „bitnu ulogu koju sloboda izražavanja i informiranja, slobodni, neovisni i raznoliki mediji i slobodan i dostupan Internet igraju u osiguravanju slobodnih i pravednih izbora“, te da različiti tipovi informacija manipulativnog sadržaja „mogu zaoštriti i čak generirati tenzije u vezi s izborima“. Deklaracija poziva „sve stranke i kandidate na izbjegavanje namjernog korištenja izjava ovog tipa s ciljem povećanja svojih izbornih šansa, prepoznavši važnu ulogu koju neovisni izborni regulatori igraju u rješavanju ovih oblika govora i u promicanju pristupa informacijama“ te izražava zabrinutost zbog prakse od strane država „usvajanja zakona koji [...] neopravdano ograničavaju slobodu izražavanja“. Zajednička deklaracija sadrži i skup preporuka državnim i nedržavnim akterima, uključujući *big-tech* kompanije, čiji je cilj zaštita slobode izražavanja na internetu.

**Zajednička izjava** iz 2021. godine potvrđuje „kako političari i državni službenici imaju važnu ulogu u oblikovanju medijske agende, javne rasprave i mišljenja“ i izražava „zabrinutost zbog sve veće učestalosti ‘govora mržnje’ na internetu i izvan njega, dezinformacija i opasne retorike protiv medija, branitelja ljudskih prava i skupina izloženih riziku od diskriminacije, kao i okrivljivanja istih, koje dolazi i od političara i državnih službenika, što ograničava slobodu izražavanja, čime se smanjuje raznolikost informacija i ideja u društvu i obmanjuju građani. Nadalje, Zajednička izjava iz 2021. godine osuđuje „povećan broj javnih priopćenja nekih političara i državnih službenika koja su netolerantna i izazivaju podjele, negiraju utvrđene činjenice, napadaju novinare i branitelje ljudskih prava zbog ostvarivanja svoga prava na slobodu izražavanja i nastoje potkopati demokratske institucije“, te ponavlja, „Države imaju pozitivnu obvezu stvoriti okružje koje omogućuje slobodu izražavanja i pravo na informacije“. Slično prethodnoj izjavi, radi zaštite slobode izražavanja, Zajednička izjava iz 2021. godine daje niz preporuka državama i nedržavnim sudionicima, kao i političkim strankama, političarima i visokim državnim dužnosnicima.

Brojne druge međuvladine institucije kao i međunarodne mreže i organizacije civilnog društva unutar OESS-ove regije pozivaju na pristup koji uključuje više aktera i zajedničku odgovornost svih zainteresiranih strana radi uspostave djelotvornih mehanizama transnacionalne suradnje u rješavanju problema informacija manipulativnog sadržaja. Ove regionalne inicijative od temeljnog su značaja u rješavanju problema ovog tipa informacija,

69 Vidi OESS RfOM-ov [Social Media Guidebook](#) iz 2013., [OESS-ov Media Freedom on the Internet: An OSCE Guidebook](#) iz 2016. i [Review of International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media](#) iz 2019.

70 Vidi [Zajedničku deklaraciju UN-a, OESS-a i OAS-a](#) iz 2020.

uključujući i one tijekom izbornih razdoblja, čije stvaranje i širenje nadilazi državne granice i jurisdikcije. Ova zajednička nastojanja na planu traženja odgovora na ove pojave posebno su relevantna i zato što im je cilj odgovoriti na izazove koji proizlaze od već raširene informacije manipulativnog sadržaja čija je namjera izazvati štetu po društvo, utjecati na demokratske procese ili ishode izbora.

Dok se većina ovih inicijativa na širi način bavi informacijama manipulativnog sadržaja i njihovim negativnim utjecajem na cjelokupni društveni i demokratski razvoj, neke od njih prepoznaju i bave se specifičnim utjecajem ovog tipa sadržaja na izborne procese. Njihova nastojanja u rješavanju problema manipulativnog sadržaja opsežnija su u pristupu te uključuju ne samo sugestije ili preporuke u vezi s kreiranjem sadržaja, moderiranjem, širenjem i drugim aspektima tih aktivnost, već i sugestije ili preporuke u vezi sa zaštitom privatnosti podataka i transparentnošću u političkom oglašavanju i oglašavanju tijekom kampanje. Stoga je većina inicijativa koje postoje u OESS-ovu području spomenutih u ovom dijelu relevantna i za sljedeća poglavlja Smjernica koja se bave političkim oglašavanjem i zaštitom podataka.

Nekoliko institucija Vijeća Europe također se bavi pitanjem širenja manipulativnog sadržaja tijekom i izvan izbornih razdoblja i ulogom koju društvene mreže imaju u sprječavanju njegovog širenja. Godine 2020., Odbor ministara usvojio je Preporuku o utjecaju algoritamskih sustava na ljudska prava, a 2018. godine Preporuku o ulogama i odgovornostima posrednika na internetu.<sup>71</sup> PACE je zagovarao uključivanje medijske pismenosti u školske nastavne planove, potporu projektima podizanja svijesti i ciljanim edukacijama radi promicanja kritičkog korištenja društvenih mreža, online medija i potporu edukaciji profesionalnih novinara.<sup>72</sup> Specifično za izborne procese, 2020. godine Venecijanska komisija usvojila je Načela korištenja digitalnih tehnologija usklađena s temeljnim pravima.<sup>73</sup>

71 Vidi [Preporuku CM/Rec\(2020\)/1](#) i [Preporuku CM/Rec\(2018\)/2](#) koja priznaje nadzorne i uređivačke uloge raznih platformi i poziva države da im dodijele odgovarajuće odgovornosti. [CM/Rec\(2018\)/2](#) preporučuje državama uvođenje zakona i propisa primjenjivih na posrednike u djelotvornoj zaštiti ljudskih prava i temeljnih sloboda korisnika, te da bi posrednici na internetu trebali imati sličnu odgovornost poštivanja međunarodnih standarda ljudskih prava. Preporuka također navodi da su transparentnost, inkluzivnost, nadzor i učinkoviti pravni lijekovi ključni za moderiranje sadržaja na platformama u skladu s ljudskim pravima. Vidi također Deklaraciju Odbora ministara o manipulativnim mogućnostima algoritamskih procesa iz 2019. koja naglašava „potrebu procjene regulatornih okvira u vezi s političkim komuniciranjem i izbornim procesima kako bi se zaštitila pravednost i integritet izbora izvan interneta i na njemu u skladu s uspostavljenim načelima“.

72 Vidi PACE-ovu [Resolution on online media and journalism: challenges and accountability](#) iz 2017.

73 Vidi [Principles for a fundamental rights-compliant use of digital technologies in electoral processes](#) iz 2020.

Ova **Načela** naglašavaju „potrebu za pristupom usklađenim s ljudskim pravima; ljudska prava i temeljne slobode moraju se prevesti u digitalno okruženje“. Ovaj dokument zapaža da internet „utječe na to kako ljudi komuniciraju, ponašaju se i formiraju vlastita mišljenja, [i] preobrazio je načine na koje je moguće oblikovati javno mnijenje, ali je također ponudio sredstva za iskrivljavanje stvarnosti u dosad neviđenom opsegu [...] Zloupotreba digitalne tehnologije radi manipuliranja činjenicama, širenja dezinformacija na strateški, koordiniran način, provođenja nadzora prikupljanjem informacija od građana i o njima, i radi angažiranja skupina političkih aktera utjecala je na građansko povjerenje u demokratske institucije i vladavinu prava.“ Ovi izazovi „prijete sveukupnom demokratskom procesu i moraju se oprezno analizirati u kontekstu izbornih kampanja [i] problema koji nastaju kada tehnologija prestane biti konkurentna prednost i postane prijetnja integritetu izbora, ograničavajući time pravo na slobodne izbore.“ Načela prepoznaju da „digitalne tehnologije utječu na različite načine, kako pozitivne tako i negativne, na različite tipove demokracije [i] na sve faze izbornih procesa, te značajno povećavaju broj aktera u kampanji, bez obzira na broj stranaka.“

Ovaj dokument iznosi **osam načela** koja se bave širim aspektima korištenja novih tehnologija u izbornim procesima, kao što su privatnost podataka, kibernetička sigurnost i izborne kampanje na društvenim mrežama:

**Načelo 1** – Načela slobode izražavanja koja podrazumijevaju robusnu javnu debatu moraju biti primijenjena u digitalnom okruženju, pogotovo tijekom izbornih razdoblja.

**Načelo 2** – Tijekom izbornih kampanja, kompetentno i neovisno tijelo za upravljanje izborima (EMB) ili pravosudno tijelo treba imati ovlasti zatražiti od privatnih kompanija uklanjanje jasno definiranih sadržaja treće strane s interneta, na temelju zakona o izborima i u skladu s međunarodnim standardima.

**Načelo 3** – Tijekom izbornih razdoblja, otvoren internet i mrežna neutralnost trebaju biti zaštićeni.

**Načelo 4** – Osobni podaci trebaju biti učinkovito zaštićeni, posebno tijekom ključnog razdoblja izbora.

**Načelo 5** – Integritet izbora mora se sačuvati putem periodične provjere pravila i propisa o političkom oglašavanju i odgovornosti posrednika na internetu.

**Načelo 6** – Integritet izbora mora se zajamčiti prilagodbom specifičnih međunarodnih propisa novom tehnološkom kontekstu i razvijanjem institucionalnih kapaciteta za borbu protiv kibernetičkih prijetnji.

**Načelo 7** – Treba ojačati okvir za međunarodnu suradnju i suradnju između javnog i privatnog sektora.

**Načelo 8** – Treba promovirati usvajanje samoregulatornih mehanizama.

EU je 2018. godine uspostavila Stručnu skupinu na visokoj razini čija je svrha pružanje savjeta o inicijativama na planu politika za borbu protiv dezinformacija.<sup>74</sup> Strategija EU-a ne predviđa regulatornu intervenciju, već je poglavito usmjerena na višedimenzionalni pristup koji uključuje samoregulatorni Kodeks dobre prakse, provjeru činjenica, korištenje umjetne inteligencije i medijsku pismenost.<sup>75</sup> Inicijative sadržane u Kodeksu prakse, Akcijski plan protiv dezinformacija i kasnije praćenje provedbe obveza koje su preuzele *big-tech* kompanije u vezi s Kodeksom, specifično su usmjereni na zaštitu integriteta izbora za Europski parlament.<sup>76</sup>

EU smatra da je prijetnja koja dolazi od širokih kampanja dezinformacija „glavni izazov za Europu i da zahtijeva koordinirani odgovor zemalja EU-a, institucija EU-a, društvenih mreža, informativnih medija i građana EU-a“. Kao odgovor na te prijetnje, Komisija EU-a razradila je više inicijativa za rješavanje problema dezinformacija, a među njima su:

- Kodeks prakse o dezinformacijama – za izradu seta samoregulatornih standarda koji bi važili za cijeli svijet;
- Europski opservatorij za digitalne medije – koji okuplja provjeritelje činjenica, pripadnike akademske zajednice i druge relevantne aktere u pružanju potpore kreatorima politika;
- Akcijski plan o dezinformacijama – s ciljem povećanja kapaciteta EU-a i suradnje u borbi protiv dezinformacija;
- Europski akcijski plan za demokraciju – za izradu smjernica za utvrđivanje obaveza i odgovornosti internetskih platformi u borbi protiv dezinformacija;
- Komunikacija o ‘rješavanju problema internetskih dezinformacija: europski pristup’ – prikupljanje alata za rješavanje problema širenja dezinformacija i osiguravanje zaštite vrijednosti EU-a;
- Program praćenja i izvještavanja o virusu COVID-19, koji su realizirale potpisnice Kodeksa prakse – kojem je cilj djelovati kao mjera za postizanje transparentnosti kako bi se osigurala odgovornost za rješavanje problema dezinformacija;

74 Svih 27 članica EU-a su države članice OESS-a. Vidi [Završno izvješće stručne skupine na visokoj razini](#). Vidi također [Rezoluciju 2016/2030\(INI\)](#) o strateškoj komunikaciji EU-a s ciljem suprotstavljanja propagandi.

75 Vidi [Izvješće o odgovaranju na dezinformacije: europski pristup](#) iz 2018. Samoregulatorni [Kodeks dobre prakse u suzbijanju dezinformacija](#) iz 2018. uključio je *Facebook*, *Google* i *Twitter*, u svibnju 2019. godine pridružio se i *Microsoft*, a u lipnju 2020. *TikTok* je postao 16. potpisnik Kodeksa. Novi Kodeks prakse, za koji se očekuje da će biti predstavljen 2021., namjerava pojačati okvir za suradnju i pomaknuti se u smjeru suregulatornog instrumenta, kako je to utvrđeno [Zakonom o digitalnim uslugama EU-a](#).

76 Vidi [Procjena Kodeksa dobre prakse u suzbijanju dezinformacija](#) Europske komisije koja sadrži ključne nalaze procjene provedbe i učinkovitosti Kodeksa koji je sastavila Europska komisija, uključujući prakse ciljano sastavljene sa svrhom zaštite integriteta izbora za Europski parlament. Vidi također [Izborni izvješće Europske komisije iz 2019.](#) koje nadopunjuje konkretna stajališta u pogledu transparentnosti političkog oglašavanja na internetu

- Europska mreža suradnje na izborima – mreža predstavnika tijela vlasti država članica nadležnih za izborna pitanja, koja pruža praktičnu razmjenu mišljenja o temama relevantnim za osiguravanje slobodnih i pravednih izbora, što uključuje zaštitu podataka, kibernetičku sigurnost, transparentnost i podizanje svijesti.<sup>77</sup>

Godine 2019, OAS je objavio Vodič za osiguravanje slobode izražavanja u vezi s namjernim dezinformacijama u kontekstu izbora kojim se „uspostavlja konceptualni okvir za bavljenje fenomenom širenja namjerno pogrešnih informacija, i uključuje preporuke državama [članicama OAS-a] i drugim akterima koji mogu pozitivno utjecati na borbu protiv lažnih informacija. Ovaj Vodič sistematizira međuameričke standarde ljudskih prava kojim bi se države trebale voditi u svojim odgovorima na ove pojave, te prezentira određeni broj preporuka namijenjenih različitim sudionicima u izborima, uključujući države članice OAS-a i razne državne institucije, *big-tech* kompanije, političke stranke, medije i novinare, provjeravatelje činjenica, oglašivačke kompanije koje trguju podacima korisnika, te sveučilišta i istraživačke centre.<sup>78</sup>

#### *iv. Inicijative civilnog društva*

Inicijative civilnog društva igraju važnu ulogu u osnaživanju i informiranju birača, podizanjem svijesti javnosti i sprječavanjem širenja različitih tipova manipulativnog sadržaja. Mnoge organizacije civilnog društva djeluju kao dio širih mreža koje također prate internetski sadržaj, općenito ili tijekom izbornih razdoblja. Nekoliko država članica OESS-a institucionalizirale su mreže za provjeru podataka, u suradnji s novinarima, civilnim društvom, *big-tech* kompanijama i znanstvenom zajednicom, s ciljem prepoznavanja i razotkrivanja viralnih misinformacija i borbe protiv lažnih vijesti.<sup>79</sup>

### **3.2 POLITIČKO OGLAŠAVANJE I OGLAŠAVANJE TIJEKOM KAMPANJE**

Političko oglašavanje i oglašavanje tijekom kampanje okosnica je svih demokratskih i kompetitivnih izbora.<sup>80</sup> Kako bi doprli do birača i tražili njihovu potporu, kandidati moraju imati slobodu vođenja kampanje, uključujući i plaćeno oglašavanje na internetu. Kada se radi o reguliranju političkog

<sup>77</sup> Vidi web-stranice Europske komisije o [Dezinformacijama](#) i o [Europskoj mreži suradnje u području izbora](#).

<sup>78</sup> Vidi OAS-ov [Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts](#) iz 2019.

<sup>79</sup> Vidi Izvješće o [informacijskom neredu iz 2017](#). Vijeća Europe, koje sadrži popis nekih inicijativa glede provjere činjenica.

<sup>80</sup> Za sveobuhvatnu ODIHR-ovu metodologiju financiranja stranaka i kampanje, vidi ODIHR-ov [Handbook for the Observation of Campaign Finance](#) i [Guidelines on Political Party Regulation](#).

oglašavanja i oglašavanja tijekom kampanje, obvezatno je slijediti nekoliko ključnih načela:

- sva temeljna prava moraju biti poštovana, uključujući pravo na slobodu izražavanja i na formiranje i posjedovanje mišljenja;
- zaštita jednakosti prilika i očuvanje pravičnih izbornih procesa zahtijeva osiguravanje izjednačene utakmice i zaštitu kampanje od uzurpiranja od strane političkih interesa;
- reguliranje mora osigurati transparentnost i povećati odgovornost kako bi se biračima omogućilo biranje na temelju potpune informiranosti;
- prava na privatnost birača moraju se poštovati u svakom trenutku, a to je područje koje je postalo osobito relevantno s pojavom internetskog oglašavanja.

Općenito gledano, pravila koja važe za političko oglašavanje na internetu trebaju odgovarati ili odražavati regulaciju tradicionalnih formi vođenja kampanje. Da bi se osigurala transparentnost i jednake prilike, okviri za političko oglašavanje trebaju sadržavati limite na donacije, uključujući i priloge u robi ili uslugama, a troškovi oglasa na društvenim mrežama trebaju biti podložni ukupnom ograničavanju troškova, zahtjevima za izvještavanjem i objavljivanjem informacija, dok se mehanizmi nadzora i sankcioniranja trebaju proširiti na oglašavanje na društvenim mrežama. Kao što je to slučaj u nedigitalnom svijetu, političko oglašavanje na internetu treba biti podložno zahtjevima u pogledu označavanja, pri čemu se, između ostalog, trebaju uspostaviti jasna pravila za identificiranje sponzora.

Vođenje kampanje treće strane i kampanje o 'političkom pitanju' sve su relevantniji na internetu. Internetsko okruženje naročito je pogodno za aktivizam treće strane zbog decentralizirane prirode internetske komunikacije i lakoće dopiranja do velikih segmenata izborne baze uz relativno nizak trošak. Vođenje kampanje treće strane ili kampanje o nekom 'političkom pitanju' treba biti podložno istim načelima transparentnosti i odgovornosti kao i kad se radi o tradicionalnim oblicima vođenja kampanje.

Značajno pitanje u ovoj raspravi je često nejasna linija između informacija koje su proizvedene kao 'organski sadržaj' i oglašavanja. Dok su ove prve zaštićene slobodom izražavanja i ne smiju biti regulirane, osim u iznimno opravdanim slučajevima, ove druge mogu i, u skladu s međunarodnim standardima, trebaju biti podložne pravilima o transparentnosti. Iako pristupi političkom oglašavanju i oglašavanju tijekom kampanje variraju, većina država članica OESS-a definira ih kroz odgovore na pitanja jesu li materijal ili poruka plaćeni, koliki im je obujam, doseg, učestalost, tj., sistematična distribucija, koji im je namjeravani cilj i je li im namjera povećavanje ili umanjene potpore za konkretne političke opcije.



Međutim, u nekim slučajevima izborni akteri mogu se odlučiti na korištenje društvenih mreža za širenje poruka naizgled 'organskog sadržaja' u kojima se kandidati podržavaju ili kritiziraju. Kad se to odvija na organiziran način, postavlja se pitanje treba li takva nastojanja tretirati kao širenje 'organskog sadržaja' ili kao oglašavanje. Iako se ovo ne tiče samo društvenih mreža, često je na njima izraženije, s obzirom na mogućnost za pojačavanje, širi doseg i lakoću kojom se ti sadržaji mogu širiti.

U svjetlu širokog spektra tehničkih mogućnosti koje nude internet i društvene mreže, razni akteri mogu doprijeti do specifičnih skupina birača svojim 'organskim' ili plaćenim sadržajem zahvaljujući osobnim podacima korisnika koje prikupljaju big-tech tvrtke ili drugi akteri, uključujući kompanije specijalizirane za brokering podataka.<sup>81</sup> Iako ove tehnike takozvanog (mikro)ciljanja nužno ne krše međunarodne standarde, sve je više pokušaja uvođenja regulativa s ciljem osiguravanja informiranosti birača o tome da je ono što na internetu vide plaćeno i da su oni specifično odabrani da vide taj sadržaj, uključujući i razlog zbog kojeg je to učinjeno i tko je to učinio. Slično tome, takozvano 'pojačavanje' sadržaja, koje na umjetan način uz plaćanje povećava doseg u javnosti, zamagljuje liniju između pružanja informacija i vođenja kampanje. Tu se također javlja i sve veća zabrinutost glede mogućnosti algoritama za stavljanje u privilegirani položaj specifičnih kategorija sadržaja, čime u konačnici mogu poremetiti jednake šanse u izbornim kampanjama. Aspekt koji se tiče zaštite podataka, a koji je usko vezan uz političko oglašavanje i oglašavanje tijekom kampanje, kao i uz kreiranje ukupnog sadržaja, njegovim pojačavanjem i širenjem, pogotovo u vezi s takozvanim kampanjama dezinformiranja, obrađen je kasnije u ovim Smjernicama.

### a. Odgovori na internetsko oglašavanje

Posljednjih godina mnogi akteri zabrinuti su da internetsko političko oglašavanje i oglašavanje tijekom kampanje služi za remećenje jednakih prilika te da nekim kandidatima daje neopravdanu prednost. Zbog te bojazni raste i potreba za potpuno transparentnim i odgovornim vođenjem političkog oglašavanja na internetu, uključujući i njegove troškove i sponzorstvo, ograničenja na donacije i ulogu kampanje treće strane ili one 'o političkim pitanjima' koja se vodi na društvenim mrežama. Različite tehnike plaćenih kampanja, uključujući (mikro)ciljanje birača, sve su više predmet regulacija koje uvode nacionalna ili supranacionalna tijela, kao i praćenja od strane organizacija civilnog društva.

<sup>81</sup> (Mikro)ciljanje tijekom kampanje i političko (mikro)ciljanje obično se sastoji od prikupljanja osobnih podataka, korištenja tih podataka za identificiranje skupina birača koji imaju zajedničke interese ili stajališta, i koji su vjerojatno podložni određenoj poruci, te slanje poruka specifično oblikovanih ili prilagođenih tim skupinama.

## *i. Odgovori država*

Mnoge države članice OESS-a rješavale su pitanje sve učestalijeg vođenja kampanje na internetu povećanjem transparentnosti u pogledu financiranja kampanje. Pritom su se ili implicitno oslonile na postojeće okvire unutar kojih se odvija tradicionalno oglašavanje, ili su osmislile nove propise specifično vezane uz domenu interneta.

Kao što je već spomenuto, regulatorni modeli u državama članicama OESS-a međusobno se uvelike razlikuju. Dok neki modeli sadrže opće zabrane ili ograničenja na političko oglašavanje na radiju i televiziji te takva ograničenja proširuju na kampanje vođene na internetu, drugi sadrže zabrane koje se samo djelomice primjenjuju na internet. U skladu s dobrom praksom, sve veći broj država članica OESS-a u kojima je dozvoljena kampanja na internetu, zahtijeva eksplicitno označavanje oglasa kao takvima, slično materijalima za kampanju koji se izlažu na otvorenom ili oglasima na tradicionalnim medijima. Kandidati su također obvezni podnijeti izvješće o svojim troškovima na internetu, jednako kao što prikazuju troškove izvan interneta. Kako bi se dodatno povećala transparentnost, novousvojeni zakoni u nekim državama obvezuju internetske platforme na objavu cijena oglasa prije početka kampanje i/ili podnošenje izvješća ili objavljivanje transparentno raščlanjenih prihoda od prodaje političkih oglasa.

S ciljem rješavanja pitanja vođenja kampanje treće strane i kampanje o 'političkom pitanju', neke države članice OESS-a uvele su širu regulativu te zahtijevaju objavljivanje informacija o sponzorima svih politički relevantnih oglasa; u drugim državama, postojeća pravila proširena su na cjelokupni sadržaj koji se tiče rasprave od općeg interesa, čime se osigurava obuhvaćanje pravilima širokog političkog konteksta. Ukupno gledano, praksa pokazuje da je upravo u području kampanje koju vodi treća strana i one o 'političkom pitanju', kao i ciljanju birača na društvenim mrežama, primjena pravila uspostavljenih za kampanje u tradicionalnim medijima najmanje učinkovita. Dio zemalja sve više prepoznaje te nedostatke, i sve je veći korpus propisa usmjerenih specifično na domenu interneta s ciljem uvođenja transparentnosti u političko oglašavanje.

## *ii. Big-Tech kompanije*

Pošto su pod sve većim pritiskom korisnika i u svjetlu sve veće kontrole koju provode vlade, neke *big-tech* kompanije počele su uvoditi mjere s ciljem jačanja transparentnosti političkog oglašavanja i oglašavanja u okviru političke kampanje na internetu, dok su se neke platforme povukle iz političkog oglašavanja. Iako su platforme počele potvrđivati identitet donatora i oglašivača te objavljivati iznose njihovih priloga, i dalje su prisutni mnogi nedostaci,

kao što je provjera sponzora putem nesavršenog sustava samoopredjeljenja. Važna je činjenica da se neke novouvedene mjere bave vidovima plaćenog političkog sadržaja, iako još uvijek nisu rasvijetljene mutne prakse (mikro) ciljanja i 'pojačavanja' sadržaja, pa *big-tech* kompanije trenutačno koriste različite pristupe na različitim tržištima. Nadalje, neke su platforme manje otvorene kad se radi o objavljivanju informacija o kampanjama koje vode treće strane ili kampanjama o nekom 'političkom pitanju'.<sup>82</sup>

*Facebook* je prvi uspostavio biblioteku oglasa. Iako je to doprinijelo ukupnoj transparentnosti političkog oglašavanja, mjere se primjenjuju neujednačeno u različitim zemljama. Nadalje, preuzimanje podataka s *Facebook*ova sučelja nekim je korisnicima komplicirano. Razne biblioteke prikupljaju podatke grupirane u različite 'cjeline', npr., u različitim vremenskim razdobljima, što često ne odgovara vremenskim okvirima za podnošenje izvješća o financiranju kampanje, dok se u mnogim slučajevima plaćeni iznosi navode u širokim 'rasponima' (npr., 500 – 4.999 EUR), što ne omogućava realne procjene ukupnih troškova. *Google* je također pokrenuo globalnu biblioteku oglasa za svoje platforme, ali je uvođenje mjera transparentnosti na sličan način neujednačeno. Nadalje, ova kompanija nije uspostavila jednaku razinu transparentnosti za oglase treće strane ili one o 'političkom pitanju', čime je dodatno ograničila učinkovitost ovih mjera. Pozitivno u pogledu (mikro)ciljanja je da je *Google* uveo mjere kojima nekomercijalnim oglašivačima može ograničiti mogućnost dobivanja podataka o specifičnim kategorijama korisnika i oglašivačima onemogućuje postavljanje lažnih tvrdnji koje je moguće provjeriti. *Google*ova biblioteka oglasa uključuje zabranjene oglase, čime se pozitivno povećava transparentnost. Godine 2019, *Twitter* je odlučio da više neće dozvoljavati političko oglašavanje na svojoj platformi.

### iii. Nastojanja međunarodne zajednice

Iako je reguliranje izbornih kampanja nadležnost pojedinačnih država članica OEES-a, međunarodni akteri prepoznali su značaj transparentnosti u političkom oglašavanju i u određenim aspektima također preuzeli inicijativu u rješavanju nekih od ranije spomenutih izazova. Kako je to razrađeno u prethodnom poglavlju, većina inicijativa međuvladinih organizacija koje se bave pitanjima glede rješavanja problema manipulativnog sadržaja i zaštite podataka uključuje i mjere za povećanje transparentnosti financiranja stranaka i izbora.

**EU** prednjači u međunarodnim nastojanjima u rješavanju izazova političkog oglašavanja i oglašavanja tijekom kampanje na internetu. Paket zakona EU-a o digitalnim

<sup>82</sup> Izborni promatrači, akademska zajednica i drugi akteri izrazili su kritiku na račun učinkovitosti *big-tech* kompanija u provedbi mjera transparentnosti, u vezi s nedostatkom standardiziranih podataka i ispravnog označavanja oglasa i sponzora, ograničenih funkcija pretraživanja i sučelja za biblioteke oglasa, kao i u odnosu na nekonzistentna i nekompatibilna razdoblja u kojima se podaci objavljuju u odnosu na razdoblja izborne kampanje u kojima se od kandidata često traži otkrivanje njihove financijske aktivnosti.

uslugama i Europski akcijski plan za demokraciju usmjereni su, između ostalog, na vidove političkog oglašavanja na internetu.<sup>83</sup> Ovaj paket mjera za osiguravanje slobodnih i pravednih izbora za Europski parlament sadrži preporuke državama članicama i političkim strankama za osiguravanje veće transparentnosti političke komunikacije. **Vijeće Europe** uspostavilo je okvir za raspravu o političkom oglašavanju u pogledu temeljnih prava, prepoznavši neraskidivu vezu između političkog oglašavanja i slobode izražavanja. ECtHR je usvojio široko tumačenje ECHR-a o političkom oglašavanju, koje uključuje plaćene oglase o pitanjima od javnog interesa, uključujući one koje promovira civilno društvo i skupine koje sudjeluju u kampanji. Sud smatra da se, u skladu s ECHR-om, objavljivanje informacija „kojima se želi utjecati na birače“ mora tretirati kao ostvarivanje slobode izražavanja, bez obzira je li ono plaćeno ili ne.<sup>84</sup>

#### *iv. Inicijative civilnog društva*

U mnogim državama članicama OESS-a, organizacije civilnog društva sve su aktivnije u zagovaranju uvođenja pravila i veće transparentnosti političkog oglašavanja na internetu, uključujući i oglašavanje u razdobljima kampanje. Budući da građanske skupine promatrača vrše dugoročne aktivnosti i upućenije su u specifične kontekste pojedinih zemalja, one su osobito važne u pružanju kontekstualnih informacija, ukazivanju na kampanje koje vode treće strane i kampanje o ‘političkom pitanju’, te u bilježenju slučajeva (mikro) ciljanja birača. Osim zagovaranja, inicijative civilnog društva sve se više angažiraju u praćenju političkog oglašavanja na društvenim mrežama, te posebice dobro mogu procijeniti udovoljava li se zahtjevima u pogledu izvještavanja i mjera nadzora na ispravan način, i jesu li oni općenito učinkoviti. Međunarodno umrežavanje nacionalnih organizacija civilnog društva služi i povećanju kapaciteta određenih skupina i pomoglo je u postizanju maksimalnih rezultata njihova rada koji često raspolaže ograničenim sredstvima.

### **3.3 ZAŠTITA PRIVATNOSTI PODATAKA**

Sve donedavno, pravila koja se tiču privatnih podataka nisu bila u središtu interesa međunarodnih promatrača, a tradicionalno su vidovi zaštite osobnih podataka i privatnosti podataka na izborima uglavnom razmatrani

<sup>83</sup> Vidi EU-ov [Paket zakona o digitalnim uslugama](#) i [Europski akcijski plan za demokraciju](#).

<sup>84</sup> Neki smatraju da je ECtHR donio različite presude u dva slučaja koja se tiču zabrane političkog oglašavanja na radiju i televiziji, u kojima se naglašava ograničena izvjesnost u pogledu razmjernosti ograničenja slobode govora u političkom oglašavanju koja se može uspostaviti, i naglašava suštinska uloga specifičnog konteksta svake zemlje. Presude također ukazuju na to da, iako prema ECHR-u slobodni govor ima prednost, u određenim okolnostima Sud može prihvatiti da su neka ograničenja u skladu s ciljem zaštite slobode izražavanja. Vidi ECtHR-ove slučajeve [TV Vest i Stranka umirovljenika Rogalanda protiv Norveške](#) iz 2009. i [Animal Defenders International protiv Ujedinjenog Kraljevstva](#) iz 2013.

u kontekstu registracije birača.<sup>85</sup> Međutim, s pojavom društvenih mreža, zaštita privatnih podataka birača postala je posebno relevantna. Zaštita prava na privatnost podataka ugrađena je u mnoge regionalne instrumente, uključujući OESS-ov Kopenhaški dokument.<sup>86</sup> U većini država članica OESS-a, kandidati imaju pravo pristupiti biračkom popisu kako bi potvrdili njegovu točnost, ažurnost i potpunost, dok se u nekim državama popisi birača koriste kako za vođenje kampanje, tako i za kreiranje izbornih strategija. Ipak, korištenje i eksploatacija podataka birača u svrhu vođenja kampanja i dalje je kontroverzna tema.

U skladu s međunarodnim standardima, uvjeti pod kojima se podaci o biraču mogu dobiti i svrha njihova korištenja trebaju se formulirati u zakonu i dalje regulirati podzakonskim aktima. Nepostojanje jasne regulative i procedura za postupanje s podacima birače može potencijalno izložiti neželjenoj komunikaciji, bilo u obliku slobodnog vođenja kampanje ili plaćenog političkog oglašavanja. Zloupotreba podataka o biraču može negativno utjecati na integritet procesa, davanjem informacija kandidatima o naklonosti birača te davanjem neopravdane prednosti nekim kandidatima. U ekstremnijim slučajevima, takve situacije mogu birače učiniti ranjivima na pritisak, zastrašivanje ili manipulaciju.

Uključivanjem u društvene mreže, najčešće rutinskim prihvaćanjem uvjeta korištenja koje one postavljaju, birači iznose i stavljaju na raspolaganje raznim privatnim kompanijama, kao što su big-tech kompanije, brokери podacima ili politički i državni akteri, širok raspon svojih osobnih podataka koji se koriste u razne poslovne i političke svrhe. Kao takvi, osobni podaci sve više postaju roba i koriste se za političke i izborne kampanje. S obzirom na rizike koje to povlači, prikupljanje, pohranjivanje, obrada i korištenje podataka trebaju biti predmet strogih propisa i nadzora. Općenito gledano, ključni standardi za zaštitu osobnih podataka zahtijevaju zakonitost, transparentnost, pravičnost, ograničavanje svrhe korištenja podataka, svodenje podataka na minimum, točnost, ograničenja u pogledu pohranjivanja, adekvatna sigurnosna jamstva i odgovornost onih kojima je odobren pristup podacima birača.

Osobni podaci u kontekstu izbornih kampanja koriste se i za takozvano **'profiliranje' i za ciljane kampanje i oglašavanje**. 'Profiliranje' i ciljano oglašavanje ne moraju nužno predstavljati problem, ako su birači svjesni da su predmetom posebice 'skrojjenih' oglasa, ali problem se javlja kada se takvi oglasi koriste za manipulaciju birača, kao što je izdvajanje određenih kategorija birača za vođenje političke kampanje. Primjerice, neodlučnim biračima može se obraćati putem 'skrojjenih' političkih poruka

85 Osobni podaci često se definiraju kao informacije koje se odnose na identificiranog pojedinca ili na onog koji se ne može identificirati.

86 OESS-ov Kopenhaški dokument iz 1990. od država zahtijeva osiguravanje pristupa informacijama i zaštitu privatnosti.

koje ciljaju njihova osobna stajališta ili im može biti odbijen pristup određenim informacijama, robama ili uslugama.

Mnoge države članice OESS-a uvele su, ili sve više uvode, sustave zaštite privatnosti podataka, primjenjive u kontekstu vođenja izborne kampanje, uključujući i one koje se tiču kandidata i trećih strana. Svrha tih odredbi je smisljena zaštita privatnosti birača propisima koji jasno reguliraju tko i pod kojim uvjetima može pristupiti podacima birača. Nadalje, političke stranke i kandidati trebaju imati vlastita pravila kojima osiguravaju tretiranje privatnih podataka u skladu s međunarodnim standardima. Regulatori trebaju biti neovisni i imati dovoljno resursa za obavljanje svojih zadataka, dok istodobno trebaju imati kapacitete i dobiti ovlasti za provedbu/sankcioniranje kako bi mogli učinkovito ispuniti svoju ulogu.<sup>87</sup>

Dok su *big-tech* tvrtke dobro pozicionirane za prikupljanje mnoštva osjetljivih podataka o svojim korisnicima, uveliko je prepoznato da je potrebno strogim pravilima definirati koju vrstu informacija one mogu prikupljati i kako njima trebaju baratati. Važno je da sami korisnici budu informirani o tome koji podaci su sabrani i tko im može pristupiti. Oni uvijek trebaju imati pravo dati ili povući suglasnost kada se radi o prikupljanju, pohranjivanju i obradi njihovih podataka. Na isti način, pristup podacima u legitimne svrhe na temelju uvjeta usklađenih s međunarodnim standardima treba biti jednak za sve kandidate.

Jedna od prvih međunarodnih inicijativa, kao odgovor na pojavu informacijskih tehnologija i potrebu za zaštitom privatnih podataka je **Konvencija Vijeća Europe za zaštitu osoba u pogledu automatske obrade osobnih podataka (Konvencija 108)**.<sup>88</sup> Konvencija 108 primjenjuje se na svaku obradu podataka koju vrše privatni i javni sektor i štiti pojedince od zlouporabe koja može pratiti obradu osobnih podataka, uključujući prekogranični protok podataka. Također, za neke dijelove OESS-ove regije, relevantne su inicijative EU-a koje predstavljaju dosad najdetaljnije i najsveobuhvatnije propise i zaštitu privatnih podataka. Relevantne inicijative EU-a uključuju **okvir Opće uredbe o zaštiti podataka (GDPR), Europski odbor za zaštitu podataka, i dobrovoljni Kodeks dobre prakse EU-a u suzbijanju dezinformacija**. GDPR je uspostavio stroga pravila na temelju individualne suglasnosti za prikupljanje i obradu osobnih podataka; također je postavio ograničenja na korištenje (mikro) ciljanja. Taj dokument navodi i neke od razloga za zabrinutost glede internetskog (mikro)ciljanja, uključujući napomenu da ono otvara mogućnosti za komunikaciju na

87 Najčešće, zakoni o zaštiti podataka osiguravaju biračima pravo na informiranost, pravo pristupa, pravo ispravke, pravo brisanja, pravo na ograničenje obrade i pravo na upućivanje prigovora.

88 **Konvencija 108 Vijeća Europe** iz 1981. jedini je obvezujući međunarodni instrument o zaštiti podataka. Vidi također **web-stranicu** Vijeća Europe posvećenu zaštiti podataka. **Modernizirana Konvencija 108** iz 2018. (poznata i kao Konvencija 108+) ponovo je potvrdila načela ugrađena u prvobitnu Konvenciju 108 te uvela dodatna jamstva zaštite podataka “**koja se trebaju primjenjivati u novim prilikama internetskog svijeta**“.

„netransparentne načine“ i da može uključivati obradu osobnih podataka koja se vrši „nezakonito u kontekstu izbora“.<sup>89</sup> Neke organizacije civilnog društva također se bave aspektima korištenja osobnih podataka u svrhu izbora i kampanja. Neke od tih inicijativa imaju globalni doseg i utjecale su na razne vlade i međunarodne organizacije u usvajanju zakona i propisa o zaštiti podataka, uključujući i njihovu zaštitu u kontekstu izbora.<sup>90</sup>

---

89 Vidi EU-ove Opće uredbe o zaštiti podataka (GDPR), Europski odbor za zaštitu podataka, *Kodeks dobre prakse u suzbijanju dezinformacija iz 2016.* i *Priručnik o europskom pravu o zaštiti podataka EU Agencije za temeljna prava iz 2018.*

90 Vidi Privacy International, *Tehnology, data and elections: A ‘checklist’ on the election cycle iz 2019.*



## 4.

# ODIHR-ov PRISTUP PROMATRANJU I PROCJENI VOĐENJA IZBORNE KAMPANJE NA DRUŠTVENIM MREŽAMA

Ovaj dio Smjernica obrađuje vezu između ključnih elemenata vođenja kampanje na društvenim mrežama i opće izborne kampanje i ODIHR-ova pristupa promatranju i procjeni tih aspekata.



ODIHR promatra vođenje kampanje na društvenim mrežama na način sličan promatranju kampanje općenito. ODIHR-ovi promatrači bave se pravnim okvirom za vođenje kampanje općenito i specifično na društvenim mrežama, internetskim aktivnostima izbornih kandidata i angažmanom drugih relevantnih aktera, te financijskim i oglašivačkim aspektima izborne kampanje. Zbog ograničenih resursa i relativno kratkih razdoblja za promatranje, ODIHR-ovi promatrači procjenjuju samo zakonski i institucionalni okvir u vezi s pitanjima zaštite privatnosti podataka. ODIHR-ovi promatrači nisu u poziciji u potpunosti pratiti, procjenjivati ili brojčano utvrđivati razinu aktivnosti u kampanji i angažman kandidata na društvenim mrežama niti točnost prijavljenih sredstava koja se koriste za oglašavanje na društvenim mrežama. Iako se aktivnosti financiranja kampanje i aspekti u vezi sa zaštitom podataka ne poklapaju uvijek s razdobljem aktivnosti promatranja, ODIHR-ovi promatrači ipak mogu prikupiti dovoljno informacija na temelju neposrednog promatranja i sastanaka sa sugovornicima kako bi došli do utemeljene procjene.

#### **4.1 MISIJA PROCJENE POTREBA**

ODIHR organizira misije procjene potreba (NAM) kako bi se procijenile potrebe aktivnosti promatranja izbora u pojedinoj državi članici OESS-a. Cilj NAM-a je dobiti uvid u povjerenje izbornih aktera u izborni proces, stanje priprema za izbore, prilike glede pravnog okvira i planova kandidata za vođenje kampanje, u smislu strategija i tema kampanje. U ovom kontekstu, od temeljnog je značaja NAM-ovo prikazivanje regulatornog okvira za vođenje kampanje na društvenim mrežama te razumijevanje korištenja društvenih mreža u političke svrhe i namjera kandidata njihova korištenja za vođenje kampanje. Na temelju procjene ovih aspekata, NAM treba preporučiti prikladan sastav osnovnog tima koji će odražavati potrebe države članice i aktivnosti promatranja. U kontekstima gdje kampanja zavrjeđuje posebnu pozornost, NAM može preporučiti slanje dva politička analitičara.

#### **4.2 PROMATRAČKA MISIJA**

U kontekstu ODIHR-ovih aktivnosti u vezi s izborima, politički analitičar ima ukupnu odgovornost za procjenu izborne kampanje, uključujući i onu koja se vodi na društvenim mrežama. Međutim, različiti članovi osnovnog tima imaju specifične uloge u procjeni različitih aspekata izborne kampanje, a prilikom vršenja te procjene politički analitičar treba surađivati s analitičarima medija, pravnog okvira ili analitičarem financiranja kampanje te s koordinatorom dugoročno raspoređenih promatrača. Uloga političkog analitičara u procjeni kampanje na društvenim mrežama detaljnije je objašnjena u sljedećem poglavlju ovih Smjernica.

Dok društvene mreže treba tretirati kao jedinstvenu pojavu, drugačiju od internetskih medija, ovi potonji očito su bliski tradicionalnim medijima i podložni sličnim standardima, pa često i regulatornim zahtjevima. Zbog toga što internetski mediji i dalje dijele mnoge ključne karakteristike s tradicionalnim medijima, procjenu njihove uloge u izborima najbolje je prepustiti medijskim analitičarima koji rade primjenjujući svoje dobro ustanovljene, a opet 'žive' metodologije kvalitativnog i kvantitativnog promatranja i analize. Društvene mreže, s druge strane, miješaju različite tipove sadržaja, uključujući organske 'postove' i oglašavanje, difuznije su, i prikladnije za analizu od strane političkih analitičara dobro osposobljenih za procjenu strategija koje izborni kandidati slijede izvan interneta i na internetu, i sposobnih bolje razumjeti aktivnosti drugih aktera na tim platformama, uključujući i one čija je neutralnost od najvećeg značaja za osiguravanje poštivanja jednakosti u izornoj utrci. Istodobno, s obzirom na često mješovitu prirodu kampanja na internetu s jedne strane, i ulogu tradicionalnih ili *online* medija i fenomena 'ponovnog postavljanja' medijskog sadržaja na društvene mreže s druge strane, politički i medijski analitičari moraju raditi zajedno kako bi postigli najbolje rezultate.

Politički analitičar blisko će surađivati s nekoliko drugih članova osnovnog tima s ciljem praćenja i procjene vođenja kampanje na društvenim mrežama. Budući da je istinski demokratska kampanja ona u kojoj se kandidati natječu u jednakim uvjetima i ispunjavaju postojeće zahtjeve za transparentnošću u pogledu prihoda i rashoda kampanje, važno je da aktivnosti vođenja kampanje na internetu, uključujući i one na društvenim mrežama, budu propisno provjerene u pogledu učinkovitog sustava podnošenja izvješća i nadzora. S obzirom na ponekad nejasnu granicu između plaćenog materijala i 'sistematične' potpore kandidatima putem tehnika umjetnog pojačavanja ili ručnog 'ponovnog postavljanja' sadržaja na društvene mreže, utvrđivanje jasne podjele između 'oglašavanja' i pružanja (informacija) 'sadržaja' može predstavljati izazov. Na sličan način, vođenje kampanje 'treće strane' i/ili o 'političkom pitanju' naročito prevladava na društvenim mrežama. Kad misije uključuju posebnog analitičara financiranja kampanje, važna je njegova bliska suradnja s političkim analitičarem na aspektima koji se tiču financiranja kampanja na internetu.

Na kraju, kako bi se rješavali aspekti privatnosti i zaštite podataka u kampanji vođenoj na društvenim mrežama, politički analitičar također mora usko surađivati s pravnim i izbornim analitičarima u osnovnom timu. Oni će zajedno utvrditi jesu li uvedena pravila koja bi trebala pomoći u zaštiti privatnosti birača, ako jesu, koja su to pravila. Osim procjene ispunjava li pravni okvir za baratanje privatnim podacima međunarodne standarde, članovi tima trebaju zajednički procijeniti učinkovitost institucionalnog nadzora s ciljem zaštite privatnih podataka, što je predmet razmatranja u kasnijem dijelu u ovih Smjernica.

### 4.3 IZRADA PREPORUKA

ODIHR-ovi promatrači mogu dati preporuke za različite aspekte izborne kampanje, uključujući i one za vođenje kampanje na društvenim mrežama. Ove se preporuke mogu baviti pravnim okvirom ili njegovom primjenom, provođenjem kampanje, internetskom aktivnošću i ponašanjem kandidata i drugih aktera u kampanji, uključujući plaćenu kampanju, institucionalni nadzor i odgovore na kršenja vođenja kampanje i angažman drugih aktera, npr. treće strane i big-tech kompanija.

S obzirom na relativno novo i dinamično područje koje se stalno mijenja, kao i na kompleksnost aktera uključenih u ovaj tip vođenja kampanje, prilikom davanja preporuka ODIHR-ovi promatrači trebaju imati pažljiv i izbalansiran pristup, uzimajući u obzir sve relevantne aspekte i aktere. U svim slučajevima, te preporuke trebaju biti potkrijepljene konkretnim nalazima, detaljno opisanima u izvješću, te referencama na preuzete obveze, međunarodne obveze, standarde i dobru praksu.

ODIHR-ove preporuke u vezi s kampanjama imaju za cilj državama članicama pomoći u njihovim nastojanjima osiguravanja slobodnog i pravičnog okruženja za kampanju s jednakim uvjetima za provođenje kampanje za sve kandidate. Iako je teško predvidjeti specifična pitanja koja mogu iskrsnuti tijekom promatranja i navesti konkretne primjere, te zbog činjenice da se promatranje izbora u ovom području i dalje razvija, sljedeće sugestije služe kao polazišna točka:

- Poštivanje temeljnih sloboda, uključujući slobodu izražavanja na internetu i činjenicu da je potencijalna ograničenja bilo koje temeljne slobode moguće nametnuti samo u skladu s relevantnim međunarodnim dokumentima;
- Promocija univerzalnog pristupa internetu i mrežna neutralnost;
- Provedba antidiskriminacijskog načela u svim aspektima kampanje na društvenim mrežama;
- Provedba načela transparentnosti, posebice glede oglašavanja na društvenim mrežama i moderiranja sadržaja od strane big-tech kompanija;
- Osiguravanje okruženja za kampanju u kojem će izborni kandidati imati jednake prilike u vođenju kampanje;
- Uvođenje učinkovitih mjera promocije i zaštite različitih podzastupljenih skupina u političkom životu i na izborima;
- Kreiranje sveobuhvatnog i učinkovitog okvira za rješavanje izazova koje predstavlja širenje informacija manipulativnog sadržaja;

- Promocija informiranja javnosti i kampanja podizanja svijesti radi jačanja povjerenja birača u izborni proces;
- Dizajniranje robusnog regulatornog okvira za oglašavanje i zaštitu privatnih podataka na društvenim mrežama;
- Jačanje institucionalnog okvira i kapaciteta za nadzor financiranja kampanje i zaštitu podataka;
- Pružanje pravodobnog i učinkovitog pravnog lijeka i sankcija koje suzbijaju kršenja glede kampanje na društvenim mrežama.<sup>91</sup>

Kao što je slučaj s davanjem preporuka o drugim aspektima izbornog procesa, ODIHR-ovi promatrači moraju dati preporuke za vođenje izborne kampanje na društvenim mrežama koje trebaju biti točne, precizne i provedive, te ciljane. To znači da se preporuke odnose na glavne nedostatke kampanje i teže ispraviti uzroke koji stoje iza njih (precizne); da su specifične u pogledu krajnjeg rezultata koji je potrebno postići, kao i mogućih sredstava za postizanje tog rezultata (konkretne i provedive); te da jasno naznačuju kojem su akteru upućene (ciljane).

---

91 Zajednička deklaracija UN-a, OESS-a i OAS-a iz 2020. o [Slobodi izražavanja i izborima u digitalnom dobu](#) daje skup preporuka državnim i nedržavnim akterima o različitim aspektima općih načela za vođenje kampanje na internetu koje analitičari mogu koristiti u procesu izrade preporuka. Važno je istaknuti da se taj dokument treba koristiti kao referenca i svaka ODIHR-ova preporuka treba biti specifična za određenu državu članicu i za određene izbore.





## 5.

# ULOGA POLITIČKOG ANALITIČARA U PROMATRANJU I PROCJENI VOĐENJA IZBORNE KAMPANJE NA DRUŠTVENIM MREŽAMA

Ovaj dio izbornim promatračima daje praktične smjernice o tome kako procijeniti i pratiti kampanje na društvenim mrežama i na koje aspekte promatranja se usredotočiti. Iznimno je važno napomenuti da je ova tema relativno nova te da se i dalje razvija, što može promijeniti pristupe procjeni.

Kao što je ranije navedeno, politički analitičar je član osnovnog tima čija je odgovornost procjena vođenja izborne kampanje, uključujući i onu na društvenim mrežama. Kao i u drugim aspektima izbornog procesa, procjena kampanje na društvenim mrežama treba se vršiti u odnosu na međunarodne obveze, stajališta, standarde i načela, kao i na domaće zakonodavstvo, i treba se temeljiti na analizi pravnog okvira, sastancima sa sugovornicima i izvješćima dugoročno raspoređenih promatrača (LTO), kao i na zaključcima izvedenim iz neposrednog promatranja. Takav pristup omogućava precizniju izradu nalaza. Širok krug sugovornika koje politički analitičar obično susreće tijekom svoje misije treba uključivati nove aktere, kao što su organizacije koje prate društvene mreže i predstavnici društvenih platformi.<sup>92</sup> Iako su važnost i razina aktivnosti kampanje na internetu u porastu, mnogi politički akteri u cijeloj OESS-ovoj regiji društvene mreže tretiraju kao dodatni prostor za dopiranje do javnosti, umjesto kao zamjenu za tradicionalno vođenje kampanje. Stoga politički analitičari trebaju usvojiti sveobuhvatniji pristup promatranju i procjeni izborne kampanje u cjelini.

Jedan od glavnih izazova s kojima se politički analitičari suočavaju u ovom području je golem broj internetskih računa, profila, stranica i objava aktera, kao i određivanje onih koje je potrebno promatrati. Nadalje, svaki akter može kreirati brojne anonimne, automatizirane i lažne račune primjenjujući mnoštvo strategija za dopiranje do birača. Pojedinci ili organizacije mogu voditi kampanju u ime ili protiv određenog kandidata, primjerice kupovanjem sponzoriranog sadržaja, pojačavanjem poruka kampanje i korištenjem 'botova' u svrhu širenju njihova dosega. Prilikom provođenja procjene, politički analitičar mora imati na umu da se akteri bez formalnih veza sa službenim kampanjama kandidata, kao što su treće strane i influenseri, također mogu aktivirati. Kompleksnost rada s velikom količinom podataka dodatno usložnjavaju brzina kojom se objave pojavljuju i teškoće u utvrđivanju njihove istinitosti. Na kraju, provođenje pravila može predstavljati poseban izazov i biti teško procijeniti uslijed ekstrateritorijalne prirode interneta.

**Transparentno promatranje:** ODIHR održava visok stupanj transparentnosti u misijama glede izbora te na samom početku javnosti treba najaviti da prati internetske aktivnosti raznih aktera u izborima. Uvodna konferencija za medije misije dobra je prilika za tu najavu.

<sup>92</sup> Politički analitičar morat će blisko surađivati s pravnim analitičarem kako bi učinkovito procijenio pitanja koja se izravno tiču pravnog okvira i onu vezi sa širom primjenom temeljnih sloboda i ljudskih prava, on ili ona također trebaju usko surađivati s medijskim analitičarem na procjeni kampanje na društvenim mrežama, naročito prilikom izbora uzorka za promatranje i u vezi s pitanjima glede slobode izražavanja.

## 5.1 PROCJENA PRAVNOG OKVIRA

Kao prvi zadatak, politički analitičar trebat će analizirati i procijeniti pravni okvir koji se odnosi na:

1. odredbe glede kampanje na internetu i propisa o sadržaju;
2. odredbe glede političkog oglašavanja i oglašavanja tijekom kampanje; i
3. zajedno s pravnim analitičarem, uređenje zaštite privatnosti i podataka relevantno za vođenje kampanje na društvenim mrežama.

### a. Sadržaj na internetu

Sveobuhvatna procjena vođenja kampanje na internetu uključuje analizu ukupnog pravnog okvira u vezi s građanskim i političkim pravima koja su preduvjet za pošteno natjecanje. U skladu s ODIHR-ovom metodologijom promatranja izbora, pravom na slobodu izražavanja i njegovom primjenom obično se bavi procjena ukupnog pravnog okvira i propisa u vezi s medijskom slobodom. Prema tome, politički analitičar treba blisko surađivati s pravnim i medijskim analitičarima prilikom analize usklađenosti postojećeg pravnog okvira s međunarodnim standardima i osiguravanja pristupa temeljnim slobodama na internetu. Politički analitičar također treba utvrditi pruža li pravni okvir neometan pristup društvenim mrežama i sadrži li dovoljna jamstva za internetsko okruženje slobodno od nasilja, maltretiranja i zastrašivanja, kako birača tako i kandidata.<sup>93</sup>

Politički analitičar treba ustanoviti jesu li opći propisi o kampanji prošireni na kampanju na internetu, ili primjenjuju li se na nju specifični propisi. Nadalje, politički analitičar treba procijeniti omogućavaju li propisi kandidatima vođenje demokratske i kompetitivne izborne kampanje. Kako bi to postigao, politički analitičar treba provjeriti postoje li odredbe koje osiguravaju jednake uvjete i tretman izbornih kandidata i provode li se takve odredbe. Politički analitičar također treba procijeniti postoje li u zakonu ili praksi bilo kakva neopravdana ograničenja mogućnosti kandidata za slobodno vođenje kampanje. Jednako tako, treba procijeniti odredbe o zlouporabi administrativnih resursa na internetu.

---

93 Uz Opći i izborni pravni okvir koji najčešće regulira vođenje izborne kampanje, specifično za vođenje kampanje na internetu, pravni i politički analitičari trebaju razmotriti postoje li zakoni o borbi protiv terorizma, kibernetičkog kriminala ili borbi protiv dezinformacija i lažnih vijesti, kao i neki specifični propisi u vezi s blokiranjem i filtriranjem internetskog sadržaja, uključujući režime odgovornosti posrednika.



Politički analitičar treba analizirati zakone i propise države u pogledu usklađenosti s međunarodnim obvezama, standardima i OESS-ovim stajalištima u vezi s distribucijom štetnog sadržaja i govora koji potiče na mržnju i nasilje, kao i drugih tipova negativne retorike, manipulativnog sadržaja i dezinformacija. Politički analitičar treba procijeniti ima li što od toga potencijal utjecati na sposobnost birača za donošenje utemeljene odluke i jesu li država i/ili neki drugi akteri poduzeli odgovarajuće radnje kako bi riješili problem manipulativnog sadržaja u skladu s međunarodnim obvezama, standardima i načelima, te s OESS-ovim stajalištima.

#### Usmjerena pitanja:

- ✓ Je li postojeći pravni okvir u skladu s međunarodnim standardima i osigurava li pristup temeljnim slobodama, uključujući slobodu izražavanja?
- ✓ Postoje li specifični zakoni ili propisi kojima se regulira vođenje izborne kampanje na internetu?
- ✓ Osiguravaju li zakonske odredbe raznolikost, pluralitet i konkurentnost kampanje?
- ✓ Uživaju li svi kandidati u izborima jednake uvjete u svom pristupu i prilikom korištenja društvenih mreža ?
- ✓ Suočava li se koji od kandidata s neopravdanim ograničenjima ili preprekama u pogledu sadržaja njihovih platformi ili poruka u kampanji?
- ✓ Jesu li primijećeni slučajevi nasilja, maltretiranja ili zastrašivanja na internetu protiv specifične skupine ili kandidata?
- ✓ Jesu li žene ili pripadnici nacionalnih manjina među kandidatima i biračima u nepovoljnijem položaju kada se radi o ostvarivanju prava na temeljne slobode?
- ✓ Nudi li postojeći pravni okvir mjere protiv opasnog ili štetnog govora, uključujući poticanje na mržnju?
- ✓ Smatraju li se društvene mreže odgovornima za sadržaj objavljen na njihovim platformama?
- ✓ Jesu li kriteriji za uklanjanje jasni, konzistentni i utvrđeni zakonom? Koje sankcije postoje za nepoštivanje zakona? Jesu li na raspolaganju bilo kakvi pravni lijekovi?
- ✓ Ima li bilo kakvih pravnih odredbi u pogledu šutnje tijekom kampanja na internetu?
- ✓ Ima li bilo kakvih propisa u vezi s objavljivanjem anketa javnog mnijenja/anketa o izlaznosti na internetu?

#### b. Političko oglašavanje i oglašavanje tijekom kampanje

Politički analitičar, u suradnji s pravnim analitičarem (ili analitičarem financiranja kampanje, ako je angažiran), treba utvrditi je li političko oglašavanje i oglašavanje tijekom kampanje na društvenim mrežama regulirano i jesu li odredbe o financiranju kampanja, kao što su limiti rashoda, zahtjevi za podnošenje izvješća, mehanizmi nadzora i sankcije primjenjivi na internetu. Analitičari moraju utvrditi pružaju li zahtjevi za podnošenje

izvješća i drugi propisi uistinu dovoljno podataka kako bi birači bili bolje informirani o troškovima kandidata za kampanju na društvenim mrežama, prije izlaska na glasovanje. Nepostojanje propisa i mehanizama provedbe za političko oglašavanje na društvenim mrežama umanjuje ukupnu transparentnost političkog financiranja i financiranja kampanje.

Regulatorna nastojanja za povećanje transparentnosti političkog oglašavanja na internetu često uključuju zahtjeve za označavanjem svih materijala kampanje, kao i propise o objavljivanju i podnošenju izvješća o troškovima, te o zabrani donacija javnih tijela i stranaca, među ostalim ograničenjima. Politički analitičar treba procijeniti i pravila i njihovu jednoobraznu provedbu. Politički analitičar također treba pokušati provjeriti mjere transparentnosti koje su platforme društvenih mreža uspostavile u pojedinim državama članicama OESS-a, i razinu do koje te mjere doprinose ukupnoj robusnosti financijskog okvira kampanje. Važno je upamtiti da svako ograničenje primjenjivo na vođenje kampanje mora biti potrebno, razmjerno i provedeno u skladu sa zakonom, što treba uključivati i precizne definicije prekršaja. Analitičari trebaju utvrditi i regulira li zakon kampanju treće strane i onu o 'političkom pitanju'.

#### **Usmjerena pitanja:**

- ✓ Postoji li regulatorni okvir za plaćeno političko oglašavanje na internetu?
- ✓ Pruža li taj pravni okvir dovoljno transparentnosti u oglašavanju na internetu?
- ✓ Pruža li pravni okvir adekvatna jamstva i zahtijeva li dovoljnu transparentnost oglašavanja tijekom kampanje na društvenim mrežama?
- ✓ Traži li se od kandidata objavljivanje informacija o troškovima i jesu li izvješća o financiranju kampanje dovoljno detaljna da uključuju troškove oglašavanja na internetu?
- ✓ Reguliraju li zakoni kampanje koje na internetu vodi treća strana ili vođenje kampanje o 'političkom pitanju'? Ako je tako, kako se ti zakoni provode?
- ✓ Postoje li bilo kakvi propisi koji zabranjuju zlouporabu administrativnih sredstava na internetu?
- ✓ Regulira li pravni okvir u dovoljnoj mjeri praksu kampanje koju vodi treća strana na internetu?

### **c. Zaštita privatnosti podataka**

Politički analitičar, zajedno s pravnim i izbornim analitičarima, treba procijeniti je li pravo na privatnost na internetu i u kontekstu tradicionalnog vođenja kampanje zakonom zaštićeno, uključujući i aspekte registracije birača i upravljanje biračima. Daljnju provjeru treba izvršiti u pogledu međunarodnih obveza koje od država zahtijevaju osiguravanje poštovanja privatnih pojedinaca i zakonito korištenje osobnih podataka, samo u

odobrene svrhe, te jesu li dotični pojedinci eksplicitno dali svoju suglasnost i mogu li je povući u bilo kojem trenutku. Politički analitičar također tijekom sastanaka s političkim strankama i kandidatima treba provjeriti postoje li uspostavljene politike koje bi osigurale baratanje privatnim podacima na načine koji su usklađeni s međunarodnim standardima. Konačno, tamo gdje su podaci o biračima dostupni, politički analitičar treba procijeniti kako su ih razni akteri pribavili, jesu li birači dali suglasnost za njihovo korištenje, te mogu li političke stranke, kandidati i treće strane pristupiti informacijama pod jednakim uvjetima.

Zakoni trebaju regulirati pribavljanje, pohranjivanje, obradu i korištenje podataka i osigurati učinkovit nadzor koji provodi nadležno i neovisno tijelo. Procjena koju radi misija treba uključivati razmatranje o tome postoje li specifični propisi o zaštiti podataka o biračima, kao i koje su ovlasti nadležnog nadzornog tijela (što je obrađeno kasnije u ovim Smjernicama). Podaci se ne mogu dijeliti ni s kim tko nije ovlašten za njihovo dobivanje, pohranu, obradu ili korištenje. Međunarodni standardi propisuju objavljivanje birača o opsegu njihovih podataka kojima se može pristupiti i koje mogu koristiti državni ili privatni akteri. U svjetlu sve većeg porasta (mikro) ciljanja birača na internetu, dolazi do sve većeg konsenzusa da birači ne samo trebaju biti u stanju identificirati političke oglase putem označavanja ili stavljanja otiska na podatke, već trebaju biti obaviješteni i kada i zašto ih se cilja.

#### Usmjerena pitanja:

- ✓ Je li uspostavljen sustav zaštite podataka?
- ✓ Štite li zakoni adekvatno osobne podatke birača?
- ✓ Pružaju li zakoni jasne propise po kojima izborni kandidati mogu koristiti podatke korisnika društvenih mreža?
- ✓ Pružaju li zakoni učinkovite pravne lijekove za zlouporabu privatnih podataka birača?
- ✓ Je li praksa ciljanja (birača) regulirana zakonom i primjenjuju li se ta pravila u praksi?
- ✓ Je li sustav zaštite privatnosti i podataka primjenjiv u kontekstu vođenja izborne kampanje?
- ✓ Obuhvaća li to kandidate i treće strane?
- ✓ Imaju li političke stranke i kandidati uspostavljene politike za osiguravanje poštivanja zaštite privatnosti i podataka?
- ✓ Imaju li kvalificirani akteri pravo pristupiti podacima birača pod jednakim uvjetima?

## 5.2 PROMATRANJE I PROCJENA AKTIVNOSTI TIJEKOM KAMPANJE

Uz analizu pravnog okvira, politički analitičar treba procijeniti aktivnosti i ponašanje kandidata i drugih aktera na društvenim mrežama tijekom razdoblja kampanje. U prvom koraku, treba mapirati društvene mreže relevantne za izborni proces, izabrati ograničeni broj korisničkih računa i uspostaviti opseg i svrhe njihova angažmana u kampanji. Izabrane račune treba pratiti kako bi se procijenila uloga koju igraju sudionici u izborima, drugi relevantni politički akteri poput javnih institucija ili dužnosnika, kao i treće strane, uključujući najistaknutije ‘influensere’. Politički analitičar treba moći povući paralele između provođenja kampanje na terenu i kampanje na društvenim mrežama, bilježeći sličnosti, ali i precizirajući bilo kakve vidljive razlike.

Prilikom provođenja procjene i promatranja vođenja kampanje na društvenim mrežama, politički analitičar imat će potporu barem jednog domaćeg pomoćnika kojem će biti dodijeljene konkretne odgovornosti i zadaci. Kao i u slučaju domaćeg pomoćnika koji pruža potporu političkom analitičaru u promatranju tradicionalnog vođenja kampanje, važno je upamtiti da se oni, kao domaći službenici, i samim time kao neposredni akteri u izborima, mogu suočiti s izazovima očuvanja pune neutralnosti ili percepcije o njima kao neutralnima, pogotovo kada su suočeni s političkim pitanjima koja izazivaju podjele. Od svih članova misije traži se pridržavanje Kodeksa ponašanja, ali zbog izloženosti političkim akterima, politički analitičar i njegovi pomoćnici trebaju posvetiti posebnu pozornost očuvanju nepristranosti i integriteta promatračke aktivnosti, zbog njihove izloženosti političkim i izbornim akterima.

U promatranju i procjeni vođenja kampanje na internetu politički analitičar treba razmotriti sljedeće aspekte:

- ♦ **Metode i strategije:** Politički analitičar morat će utvrditi koje platforme, metode i aktivnosti koriste sudionici u izborima u vođenju kampanje na internetu. Prilikom promatranja, on ili ona trebaju razmotriti jesu li aktivnosti generirane od strane korisnika ili reproducirane, primjerice, dijeljenjem sadržaja ili poveznica na članke u medijima, jesu li usredotočene na mobilizaciju birača ili ih mogu obeshrabriti u sudjelovanju na izborima, kao i koji se tip materijala dijeli (tekstovi, slike, videomaterijali ili njihova kombinacija). Nadalje, promatranje treba uključivati aspekte poput toga dopiru li informacije do specifičnih skupina birača, kao što su mladi i oni koji glasuju prvi put, žene, nacionalne manjine, osobe s invaliditetom, i, ako je moguće, treba utvrditi vode li kandidati kampanju individualiziranog stila ili slijede pristup svoje stranke i prenose glavne poruke kampanje svoje stranke.

- ♦ **Ključne teme kampanje:** Politički analitičar također treba utvrditi i pratiti o kojim temama se raspravlja na društvenim mrežama i do koje mjere one odražavaju teme prisutne u medijima i na skupovima tijekom kampanje. Važno je utvrditi pruža li kampanja na internetu biračima dovoljno bitnog sadržaja kako bi odabrali na temelju pune informiranosti, i ustanoviti ima li možda nekih aspekata od šireg javnog interesa ili interesa glede izbora koji se spominju ili ne spominju na internetu ili razmatraju u debatama na internetu, ali ih nema u okviru tradicionalnog vođenja kampanje. Politički analitičar treba utvrditi koje su najvažnije teme i procijeniti koliko je god moguće za koje se teme i objave čini da imaju najveći odjek.<sup>94</sup>
- ♦ **Ton i retorika:** Kao i kod tradicionalne kampanje, politički analitičar treba procijeniti ukupni ton, te stil i tip retorike koju koriste izborni akteri na društvenim mrežama. Slučajevi poticanja na nasilje ili neprijateljstvo, zapaljiva retorika, opasan i štetan govor, kao i korištenje manipulativnog sadržaja trebaju se zabilježiti, uključujući i sadrže li komentare o tehničkim ili političkim aspektima izbornog procesa ili diskreditiraju druge kandidate. Također treba procijeniti razlikuju li se ton i jezik koji se koriste na internetu od onih koji se čuju na skupovima tijekom kampanje ili prilikom drugih pojavljivanja u javnosti.
- ♦ **Plaćena kampanja:** Politički analitičar treba procijeniti korištenje plaćenih oglasa od strane kandidata ili drugih aktera, uključujući one koji idu u prilog i one koji su protiv određenog kandidata. Nakon uvođenja politika transparentnosti uspostavljenih u nekim zemljama od strane *big-tech* kompanija, financijske aktivnosti političkih stranaka, kandidata i drugih aktera u izborima uključene su u takozvane biblioteke oglasa ili je plaćeni sadržaj označen kao takav. Politički analitičar treba utvrditi jesu li oni dovoljno transparentni kako bi gledateljima omogućili identificiranje njihovih sponzora. Promatranje i procjena plaćenog sadržaja i aktivnosti obrađeni su u nastavku.

Odabir 'što' i 'koga' pratiti na društvenim mrežama treba se temeljiti na sredstvima koja su političkom analitičaru na raspolaganju. Ograničeno vrijeme i broj angažiranih suradnika na raspolaganju tijekom misije s jedne strane, i obilje materijala na raspolaganju na internetu s druge strane, znače da analitičar svoje napore treba usredotočiti na savladivu količinu uzoraka. Svaka analiza i procjena treba slijediti temeljna načela ODIHR-ove metodologije promatranja izbora i osloniti se na sistematičan, konzistentan i pouzdan pristup na temelju neposrednog promatranja. Fokus

94 Kao što je gore navedeno, zbog decentralizirane prirode društvenih mreža i sadržaja koji generiraju korisnici, što omogućava biračima da zajedno oblikuju agendu u domeni interneta, u nekim slučajevima opseg tema o kojima se raspravlja na internetu širi je od onih koje su prezentirane u tradicionalnim medijima, koje su predmet uređivačkih politika i strožeg reguliranja. Politički i medijski analitičari trebaju zajednički utvrditi jesu li neke teme od javnog interesa cenzurirane iz političkog diskursa, te identificirati razloge za to, i ovisno o kontekstu, uključiti to u izvješću misije u dijelovima koji se odnose na okruženje kampanje i medije.

političkog analitičara treba biti na strogo definiranom razdoblju, često od trenutka kada može započeti promatranje vođenja kampanje na internetu i tijekom njezina trajanja ili tijekom razdoblja općih izbora, kao i na jasno definirani uzorak. Umjesto analiziranja pojedinačnih objava ili davanja kvantitativnih izvješća, važno je obuhvatiti glavne trendove na raznim platformama i sačiniti kvalitativnu procjenu koja odražava strategije vođenja kampanje, ton, jezik i teme, te procijeniti poštivanje i provedbu propisa o kampanji, kao i zabilježiti bilo kakva potencijalna kršenja propisa, uključujući zlouporabu administrativnih sredstava.

## a. Izbor platformi

Politički analitičar treba identificirati koje se društvene mreže najviše koriste tijekom izbornog procesa.<sup>95</sup> Odluka koje platforme pratiti treba biti specifična za kontekst i treba uzeti u obzir druga izvješća relevantnih međunarodnih ili domaćih organizacija, sastanke sa sugovornicima, a ne isključivo broj korisnika ili pratitelja i doseg internetskih računa. Izbor platformi također treba odraziti obuhvat, što uključuje prosječnu starost korisnika, jezik i etničku raznolikost. U većini država članica OESS-a, *Facebook* i *YouTube* su najuobičajenije društvene mreže koje se koriste za političku komunikaciju i oglašavanje tijekom kampanje, dok *Twitter* općenito koriste političari i kreatori javnog mnijenja u oblikovanju političkog narativa. *Instagram* se često koristi za prenošenje poruka kampanje, čak i fotografija i kratkih dijelova govora, ali i za dnevne objave i pisane narative. Ovisno o zemlji ili regiji, politički analitičar će možda ustvrditi da su druge društvene mreže relevantnije, kao što su *VKontakte* i *Odnoklasniki*.

### Usmjerena pitanja:

- ✓ Koje platforme najviše koriste birači, izborni kandidati i drugi politički akteri i zainteresirani sudionici u izborima?
- ✓ Koje su platforme najpopularnije za politički sadržaj i vijesti?
- ✓ Kako politički akteri koriste različite platforme tijekom kampanje?
- ✓ Postoje li platforme poznate po korištenju dezinformacija?
- ✓ Postoje li platforme na kojima je manje ili više vjerojatno da će biti aktivne (ili isključene) specifične skupine birača, poput nacionalnih ili jezičnih manjina, mladih birača itd.?

<sup>95</sup> Postoji nekoliko izvora analitičkih i metričkih podataka o prometu na internetu koji mogu biti od pomoći političkom analitičaru pri izboru platformi koje treba pratiti u konkretnoj zemlji. Neki od njih su: [www.similarweb.com](http://www.similarweb.com); [www.alexa.com](http://www.alexa.com); [www.statista.com](http://www.statista.com).

## **b. Izbor računa**

Nakon izbora platformi, politički analitičar morat će odlučiti o opsegu računa koji će se pratiti. S tim ciljem, treba sačiniti listu računa korisnika, relevantnih stranaka, kandidata, 'influensera' i državnih institucija na temelju nekoliko različitih platformi. Budući da se popularni akteri u digitalnoj domeni mogu brzo mijenjati, važno je zadržati određeni stupanj fleksibilnosti i uključiti nove račune koji se istaknu tijekom kampanje. Kao i kod procesa izbora platformi, uzorak računa treba biti što je moguće reprezentativniji i treba odražavati političku, socioekonomsku, regionalnu, etničku i jezičnu raznolikost zemlje. Izbor treba imati za cilj otkriti opće trendove koji karakteriziraju okruženje kampanje na internetu i pružiti solidnu osnovu za procjenu.

Ako u određenom kontekstu postoji tek ograničena aktivnost na internetu i ako to sredstva misije dozvoljavaju, kako bi se proširila saznanja, može biti korisno da se za parlamentarne i lokalne izbore identificiraju ključni kandidati i politički akteri na lokalnoj i regionalnoj razini, mimo najistaknutijih na državnoj razini, i da se njihovi računi uključe u promatranje. Može biti korisno procijeniti koje alate kampanje oni koriste i ispitati jesu li njihove strategije i poruke slične onima na državnoj razini ili pokazuju jedinstvene trendove. LTO-i mogu biti naročito korisni u identificiranju tih regionalnih aktera. Međutim, važno je upamtiti da, iako LTO-i mogu rasvijetliti određena regionalna zbivanja na društvenim mrežama, prikupljanje podataka i procjenu treba kompletirati politički analitičar.

Kako bi zadržao konzistentnost s ključnim načelima ODIHR-ove metodologije promatranja izbora, uključujući istinitost nalaza, politički analitičar treba uključiti u uzorak i ispravno označiti samo autentične račune korisnika. Može postojati više računa na društvenoj mreži koje koriste ista ili slična imena različitih aktera u izborima – ako je njihova autentičnost sporna, ne smije se jednostavno pretpostaviti da oni pripadaju navedenim akterima. Ako postoje 'lažni' računi koji privlače značajnu pozornost javnosti, oni se mogu uključiti u analizu i procijeniti zasebno, posebice kad se radi o širenju štetnog ili manipulativnog sadržaja. Načela Kodeksa ponašanja za ODIHR-ove promatrače trebaju se poštovati i potrebno je zadržati neovisnost u svakom trenutku prilikom promatranja društvenih mreža. Kada se prate računi političara, stranaka i drugih aktera, članovi misije moraju se suzdržati od dijeljenja, komentiranja ili bilo koje druge aktivnosti koja može kompromitirati integritet aktivnosti u vezi s izborima.

## *i. Izborni kandidati*

Uz biračko tijelo, kandidati i političke stranke ključni su sudionici u izborom natjecanju. Politički analitičar, naravno treba pratiti njihove profile i račune. Kod parlamentarnih ili lokalnih izbora, tamo gdje nije moguće pratiti sve kandidate, kako bi se sačuvala nepristranost i objektivnost, odabrani

računi trebaju ponuditi reprezentativan uzorak kandidata u cijelom političkom spektru, uključujući one koji podržavaju vladu, opoziciju, kandidate koje su imenovale formacije zastupljene u parlamentu, i one bez mjesta u parlamentu, kao i stranke ili kandidati koji predstavljaju različite nacionalne ili vjerske manjine. Također je važno pratiti račune koji pripadaju onima koji zastupaju kandidatkinje, osobe s invaliditetom i druge ranjive skupine. U slučaju da je broj kandidata veliki, politički analitičar treba sastaviti užu listu i donijeti odluku praćenja kandidata koji su osobito vidljivi.<sup>96</sup> Međutim, takva prethodna selekcija treba biti razmjerna i ne treba se vršiti na štetu kandidata koji predstavljaju male političke stranke ili manjinske skupine.

### *ii. Državne institucije i drugi politički akteri*

Pored neposrednih sudionika u izborima, politički analitičar treba razmotriti praćenje aktivnosti na internetu drugih političkih aktera, uključujući stranke koje nisu predložile nijednog kandidata ili državne, lokalne ili druge javne institucije relevantne za izborni proces i kampanju. Izbor treba biti na sličan način specifičan za kontekst i može uključivati račune tijela za upravljanje izborima (EMB), vlade, premijera ili predsjednika. Nadalje, neki ministri, pravosudna tijela ili ured pravobranitelja također mogu biti obuhvaćeni promatranjem. Politički analitičar treba ispitati koristi li koji od ovih aktera društvene mreže u svrhu kampanje. Osobito je važno pratiti zloupotrebljavaju li se sredstva namijenjena upravljanju kampanjom za vođenje kampanje na internetu ili, alternativno, procijeniti može li sadržaj koji uključuje stranice tih institucija implicitno davati neopravdanu prednost nekim kandidatima. Stoga je važno, u mjeri u kojoj je to moguće, pratiti i aktivnosti na internetu visokorangiranih lokalnih ili regionalnih javnih dužnosnika, uključujući guvernera i gradonačelnike, i, ako je imaju, steći dobro razumijevanje njihove uloge u kampanji.

### *iii. Ostali akteri*

Kako bi se stekao sveobuhvatni pregled kampanje na internetu, važno je da politički analitičar razmotri praćenje šireg spektra sudionika u izborima. To ne treba podrazumijevati utvrđeni, prethodno definirani skup aktera, već politički analitičar treba zadržati izvjestan stupanj fleksibilnosti. Svaki odabir će ovisiti o kontekstu specifičnom za pojedinu zemlju – akteri mogu uključivati organizacije civilnog društva, aktiviste i ‘influensere’, kao i bilo koje treće strane koje su angažirane u kampanji. Ukupno gledano, politički analitičar treba nastojati utvrditi kontekst i motive za angažman trećih

<sup>96</sup> Tijekom parlamentarnih ili lokalnih izbora, izbor korisničkih računa može biti posebno izazovan zadatak s obzirom na broj kandidata. U nekim slučajevima, politički analitičar može ograničiti praćenje na korisničke račune vodećih stranaka koje su nominirale kandidate, i njihovih lidera, kao i kandidata koji su osobito aktivni na internetu.



strana i, ako je moguće, ustanoviti jesu li njihove aktivnosti, ili trebaju biti, podložne propisima o financiranju kampanje. U ovom kontekstu, promatra- nje može obuhvatiti kreatore javnog mnijenja, novinare, pripadnike aka- demske zajednice, vjerska tijela ili njihove visokorangirane predstavnike, sindikate, kao i organizacije koje predstavljaju mlade, rodne ili nacionalne manjine.

Sveobuhvatna lista aktera i računa može se utvrditi uz potporu domaćih pomoć- nika, koji bi trebali dobro razumjeti političko i izbornu okruženje. Izbor se također može sačiniti uz konzultacije s medijskim analitičarom. Proces također može koristiti informacije prikupljene tijekom sastanaka sa sugovornicima i rasprava s medijskim ili političkim stručnjacima. Kada se kontekstualiziraju i tumače prikupljeni podaci, tako- đer se savjetuje sastajanje političkog analitičara s organizacijama civilnog društva, domaćim skupinama za monitoring i lokalnim organizacijama koje se bave društve- nim mrežama.

### **c. Prikupljanje informacija**

Informacije s javnih objava nađenih na odabranim računima trebaju biti sis- tematično prikupljene i metodološki organizirane. U ovu svrhu, politički ana- litičar treba razviti bazu podataka u kojoj čuva evidenciju različitih eleme- nata svojih promatranja. Vremenski okvir za promatranje treba uključivati razdoblje kampanje, često od trenutka kada politički analitičar može započeti promatranje vođenja kampanje na internetu, do i tijekom trajanja kampanje ili općeg izbornog razdoblja, ili nakon što su kandidati nominirani.

Na temelju podataka prikupljenih s društvenih mreža, politički analitičar treba moći utvrditi sličnosti između internetskih i tradicionalnih oblika vođenja kampanje te ukazati na bilo kakve značajne razlike. Baza podataka političkom analitičaru također treba pružiti dovoljno informacija za donoše- nje zaključaka o metodama i strategijama korištenim u vođenju kampanje na društvenim mrežama, uključujući prirodu sadržaja (slobodan ‘organski’ ili plaćeni, onaj koji generiraju i dijele korisnici, za ili protiv sudjelovanja birača itd.) i tip (tekst, slike, videomaterijal ili njihova kombinacija). Nadalje, analiza treba uključivati aspekte glede uključenosti specifičnih skupina birača, kao što su mladi, birači koji glasuju prvi put, žene ili nacionalne manjine. Ako to opseg i vremenski okvir misije dozvoljavaju, moglo bi biti korisno procijeniti jesu li se strategije kampanje promijenile tijekom same kampanje, na primjer, poslije nekog značajnog događaja.

Kako bi se dobro razumjele strategije dopiranja do javnosti, politički analiti- čar treba obratiti pozornost na obujam i razinu aktivnosti, što može uključiti broj objava, plaćenih oglasa, komentara i reakcija korisnika. Iako se ne oče- kuje rigorozno nabranje tih detalja, već politički analitičar treba nastojati

postići kvalitativnu procjenu, neki se osnovni brojevi trendovi mogu ustanoviti. To može uključiti okvirno navođenje učestalosti objava kandidata u izborima i reakcije i komentare osoba koje ih prate. Aktivnosti drugih političkih aktera, državnih ili javnih institucija, ali i trećih strana, mogu se analizirati kvantitativno. Incidente koji se odnose na zluporabu administrativnih sredstava, 'govor mržnje', negativnu retoriku ili drugi manipulativni sadržaj treba zasebno analizirati, i to od slučaja do slučaja, te potkrijepiti detaljnijim opisima.<sup>97</sup>

Ako vrijeme i drugi resursi dozvole, politički analitičar mogao bi ići korak dalje od navedenog pristupa koji se odnose na i provoditi pretrage po ključnim riječima, uključujući pojmove za koje se smatra ili očekuje da će biti važne teme u kampanji. Kako bi se to olakšalo, politički analitičar mora identificirati relevantne fraze, slogane i hashtagove (npr. #referendum2018), koji se koriste, ili će se vjerojatno koristiti, za označavanje sadržaja povezanog s izborima ili kampanjom.

Kao što je ranije rečeno, politički analitičar treba posvetiti posebnu pozornost tretmanu i retorici koja se koristi o različitim podzastupljenim skupinama. Primjerice, kibernetičko nasilje protiv žena sve je prisutnije tijekom razdoblja kampanje.<sup>98</sup> To se može manifestirati kroz uznemiravanje, bullying, mobbing, postavljanje eksplicitnog vizualnog materijala, postavljanje i dijeljenje nasilnog sadržaja, prijetnje smrću i korištenje seksualnih ili uvredljivih komentara i ponižavajućih/izmijenjenih slika ili videa (*deepfake*). Zbog mogućnosti anonimnosti korisnika i decentralizirane prirode društvenih mreža, ovi nasilni čini mogu lako preći državne granice i postići učinke koje je teško rješavati ili ispraviti. Politički analitičari trebaju pažljivo pratiti prisustvo ovih pojava u kampanji, upućenih kandidatima, ali i ženama biračima i onima koje podržavaju kandidate, te procjenjivati njihov utjecaj na vođenje izborne kampanje kao i institucionalne i društvene odgovore na te negativne prakse.<sup>99</sup> Nadalje, politički analitičar može zabilježiti i prijaviti neke pozitivne mjere i inicijative koje poduzimaju države, političke stranke i izborni kandidati, civilno društvo ili društvene mreže, čiji je cilj bavljenje i rješavanje problema nasilja nad ženama na internetu. Uz kampanje podizanja svijesti radi

97 Promatranje incidenata na internetu, uključujući one koji se odnose na 'govor mržnje', poticanje na nasilje, ili drugi manipulativni sadržaji trebaju biti propisno evidentirani, ako je moguće sa snimcima, i arhivirani.

98 Vidi [Vodič za prevenciju nasilja nad ženama na izborima](#) koji su 2017. godine objavili UN Women i UNDP. Ovaj Vodič navodi da je „nasilje nad ženama u političkom životu, uključujući tijekom i mimo razdoblja izbora, bilo koji akt, ili prijetnja, rodno zasnovanim nasiljem koje rezultira fizičkom, seksualnom, psihološkom štetom ili patnjom žena, koje ih sprječava u ostvarivanju svojih političkih prava, bilo u javnom ili privatnom sektoru, uključujući pravo na glasovanje i preuzimanje javne dužnosti, tajno glasovanje, i slobodno vođenje kampanje, udruživanje i okupljanje i uživanje sloboda mišljenja i izražavanja. Takvo nasilje može počinuti član obitelji, član zajednice i/ili država.”

99 Vidi OESS-u [Odluku Ministarskog vijeća o prevenciji i borbi protiv nasilja nad ženama br. 4/18](#) koja poziva države članice na „ohrabrivanje svih relevantnih aktera [...] u doprinosu sprječavanju i borbi protiv svih oblika nasilja nad ženama, što uključuje žene koje se bave profesionalnim aktivnostima, pri čemu su izložene javnosti i/ili interesu društva“. Vidi također [Preporuku Odbora ministara \(2019\)1 o prevenciji i borbi protiv seksizma](#) Vijeća Europe

spriječavanja nasilja nad ženama, što se uglavnom provodi u suradnji s civilnim društvom i međunarodnim organizacijama, neke od inicijativa koje poduzimaju društvene mreže su: primjena takozvanih 'standarda zajednice' koji se odnose na zaštitu žena, uvođenje dodatnih mehanizama zaštite privatnosti i sigurnosti, kao i razvoj automatizirane tehnologije za otkrivanje i uklanjanje sadržaja koji uključuje ovu vrstu nasilja.

### 5.3 PROMATRANJE I PROCJENA POLITIČKOG OGLAŠAVANJA I OGLAŠAVANJA TIJEKOM KAMPANJE

Nekoliko aspekata oglašavanja tijekom kampanje na društvenim mrežama zaslužuje posebnu pozornost, npr.:

1. Poštivanje načela transparentnosti, uključujući količinu javno dostupnih podataka o oglašavanju izbornih kandidata, političkih stranaka i *big-tech* kompanija na društvenim mrežama;
2. Obveza podnošenja izvješća kandidata ili drugih aktera o njihovim oglašivačkim aktivnostima na internetu; i
3. Uključenost raznih aktera u kampanju, uključujući treće strane, koji ne tvrde da su povezani s kandidatima.

#### a. Transparentnost oglašavanja

Nakon procjene pravnog okvira, politički analitičar ili analitičar financiranja kampanje, ako je angažiran, treba procijeniti provedbu odredbi koje u praksi povećavaju transparentnost izbornih kampanja na društvenim mrežama. Naime, potrebno je utvrditi je li sadržaj kampanje jasno označen kako bi ukazao na to tko promovira oglas i jesu li informacije u vezi s prihodom *big-tech* kompanija stečenim u političkim i izbornim kampanjama javno dostupne. Nadalje, glede jednakih uvjeta, politički analitičar treba procijeniti imaju li izborni kandidati jednak pristup kampanji na društvenim mrežama na nediskriminatornoj osnovi i s jednakim prilikama vođenja kampanje (primjerice, postoje li razlike u cijenama oglasa).<sup>100</sup>

Suočene sa sve većom zabrinutošću zbog zlonamjernog korištenja društvenih mreža u izbornim kampanjama, *big-tech* tvrtke počele su uvoditi mjere za veću transparentnost političkog oglašavanja. Te mjere uključuju

<sup>100</sup> U skladu s međunarodnim standardima i stajalištima, kako bi imali jednake mogućnosti za vođenje kampanje, kandidati trebaju dobiti jednake cijene za korištenje tradicionalnih oblika vođenja kampanje, kao što su veliki panoji, poster i displeji drugog tiskanog materijala i kada vode kampanju na radiju i televiziji. Međutim, za vođenje kampanje na internetu, većina *big-tech* kompanija koristi aukcije za oglašavanje ili sustav ponuda, što često rezultira različitim cijenama za kandidate.

ograničenja na to tko može postaviti političke oglase, podvrgavanje oglašivača strožim procedurama verifikacije i javno obznajivanje njihovog identiteta. Najvidljivije je to što su neke *big-tech* kompanije počele označavati plaćene političke oglase i omogućavati lakšu dostupnost na internetu zbirnih informacija o njima. U nekim državama članicama OESS-a, biblioteke oglasa na platformama postale su sve važniji resurs za zainteresirane aktere, kao što su medijski izborni promatrači i civilno društvo. Važno je napomenuti da politički analitičari trebaju nastojati utvrditi jesu li platforme osigurale propisno odvajanje političkih oglasa od drugih oblika sponzoriranog političkog i za izbore vezanog sadržaja.

Kako bi potkrijepio svoju ukupnu procjenu, politički analitičar može koristiti alate za objedinjavanje podataka koje pružaju platforme, kao što su biblioteke oglasa, kako bi identificirao koje su političke stranke ili kandidati najaktivniji, uživaju najviše pozornosti ili su potrošili najveći iznos novca na društvene mreže. Biblioteke oglasa mogu također pomoći političkom analitičaru u boljem određivanju tona kampanje, i pronalasku elemenata negativne kampanje ili aspekata za koje se smatra da krše zakone ili međunarodne standarde, uključujući poticanje i štetni govor. Politički analitičar treba imati za cilj utvrditi da li količina informacija koje se nalaze u bibliotekama oglasa odgovara količini koju su kandidati prijavili nadzornom organu. Neki od raspoloživih alata razrađeni su u nastavku.

Zbog velike količine plaćenog sadržaja na internetu i tehnika (mikro)ciljanja koje koriste *big-tech* kompanije i drugi subjekti, politički analitičar možda neće biti u poziciji pratiti i procjenjivati sve oglase koje produciraju izborni kandidati ili treće strane. Nadalje, ono što različite platforme uključuju u svoje biblioteke oglasa razlikuje se od jedne do druge države članice OESS-a. Primjerice, u nekim se zemljama navode samo oglasi koje postave registriрани kandidati, dok su u drugima također uključeni oglasi treće strane ili o 'političkom pitanju'. Mnoge platforme prikupljaju i stavljaju na raspolaganje neke podatke o (mikro)ciljanju birača ili 'boostingu' (pojačavanju) sadržaja, što može biti nalik oglašavanju.

#### Usmjerena pitanja:

- ✓ Je li političko oglašavanje i oglašavanje tijekom kampanje jasno označeno?
- ✓ Imaju li izborni kandidati jednake prilike za vođenje kampanje, odnosno jesu li cijene za oglašavanje jednake za sve кандидате?
- ✓ Jesu li cijene dostupne javnosti?
- ✓ Postoje li bilo kakve tehnike (mikro)ciljanja koje koriste *big-tech* kompanije, izborni kandidati i drugi akteri i jesu li birači o tome obaviješteni?
- ✓ Koliko su učinkovita nastojanja *big-tech* kompanija u rješavanju pitanja zlorabe u području političkog oglašavanja i/ili oglašavanja tijekom kampanje na društvenim mrežama?

- ✓ Pomažu li alati za povećavanje transparentnosti koje su kreirale *big-tech* kompanije u povećanju ukupne transparentnosti političkog financiranja i financiranja kampanje?

## b. Zahtjevi u pogledu izvještavanja

Izvještavanje i objavljivanje financija kampanje važne mjere su za osiguranje odgovornosti i transparentnosti, što uključuje i društvene mreže.<sup>101</sup> U većini država članica OESS-a, izborni kandidati obvezni su otkriti svoje troškove za kampanju. Važno je, između ostalog, da i stranke i kandidati odgovaraju za svoje oglašavanje na društvenim mrežama. To znači da njihova izvješća o financiranju kampanje trebaju biti dovoljno detaljna i odraziti troškove vođenja kampanje na internetu. Misija treba procijeniti odgovaraju li brojke u tim izvješćima približnom broju, učestalosti i geografskom doseg u oglasa tijekom kampanje, onako kako su oni praćeni tijekom misije i kako su ih prijavili kandidati i treće strane u biblioteke društvenih mreža, ako su one na raspolaganju. Misija također treba procijeniti odražavaju li troškovi izvješća o financiranju kampanje kandidata transparentno i utvrditi koliko su ta izvješća detaljna i pravodobna.

Politički analitičar treba pažljivo procijeniti ravnotežu između javnog objavljivanja i zaštite osobnih podataka. Općenito gledano, informacije koje se moraju obznaniti trebaju javnosti omogućiti identificiranje donatora, iznos priloga te kada je prilog dan. Financijska izvješća izbornih kandidata trebaju uključiti priloge u naravi za vođenje kampanje na internetu; politički analitičar treba procijeniti kako se takve donacije vrednuju i primjenjuju li se standardi transparentnosti jednako na sve kandidate.

### Usmjerena pitanja:

- ✓ Zahtijeva li se od izbornih kandidata i trećih strana uključenih u kampanju podnošenje izvješća o aktivnostima vođenja kampanje na internetu?
- ✓ Objavljuju li se ova izvješća pravodobno?
- ✓ Jesu li zakonske odredbe provedene na konzistentan i djelotvoran način?
- ✓ Jesu li *big-tech* kompanije primijenile neke mjere povećane transparentnosti, kao što je kreiranje biblioteka oglasa?
- ✓ Ispunjavaju li platforme društvenih mreža svoje obveze izvještavanja?

<sup>101</sup> U ODIHR-ovu [Handbook for the Observation of Campaign Finance](#) zapaža se da su izvješća o financiranju kampanje ključni instrument politika kojima se osigurava sistematično i sveobuhvatno poštivanje zakona o financiranju kampanje od strane izbornih natjecatelja. Takvi zakoni općenito propisuju koje informacije političke stranke i kandidati moraju dostaviti o svojoj kampanji, priložima i troškovima, te kada i kako ta izvješća moraju biti dostavljena. Ove informacije pomažu nadzornom tijelu u procjeni jesu li stranke i kandidati poštivali zakon.

- ✓ Koja se vrsta podataka i informacija o oglašavanju kampanje i političkom oglašavanju u razdoblju kampanje može izvući s platformi?
- ✓ Podudaraju li se iznosi koje su nadzornim tijelima prijavili kandidati i treće strane koje su uključene u kampanju s onima koji se objave na platformama društvenih mreža?

### c. Kampanja koju vodi treća strana

Procjena uključenosti treće strane i oglašavanja o 'političkom pitanju' na društvenim mrežama može predstavljati izazov. Kao i u tradicionalnim oblicima vođenja kampanje, izborna agitiranje nije u isključivoj nadležnosti političkih stranaka i kandidata. Skupine i pojedinci mogu aktivno promovirati kandidate izravno ili profiliranjem pitanja koja imaju dobar odjek među biračima i mogu se povezati s konkretnim političkim opcijama ili kandidatima.

Oglašavanje treće strane i ono o 'političkom pitanju' mogu biti pozitivne karakteristike vođenja izborne kampanje, jer ukazuju na širi društveni angažman u politici i izborima. Interesne skupine i organizacije civilnog društva mogu mobilizirati veću aktivnost, omogućavajući pluralističkiji i inkluzivniji proces. U nekim kontekstima, kandidati na izborima također mogu prenositi svoje poruke, ne samo one kojim zagovaraju sudjelovanje birača, već i one kojima pozivaju na bojkot izbora za koje smatraju da su nelegitimni.

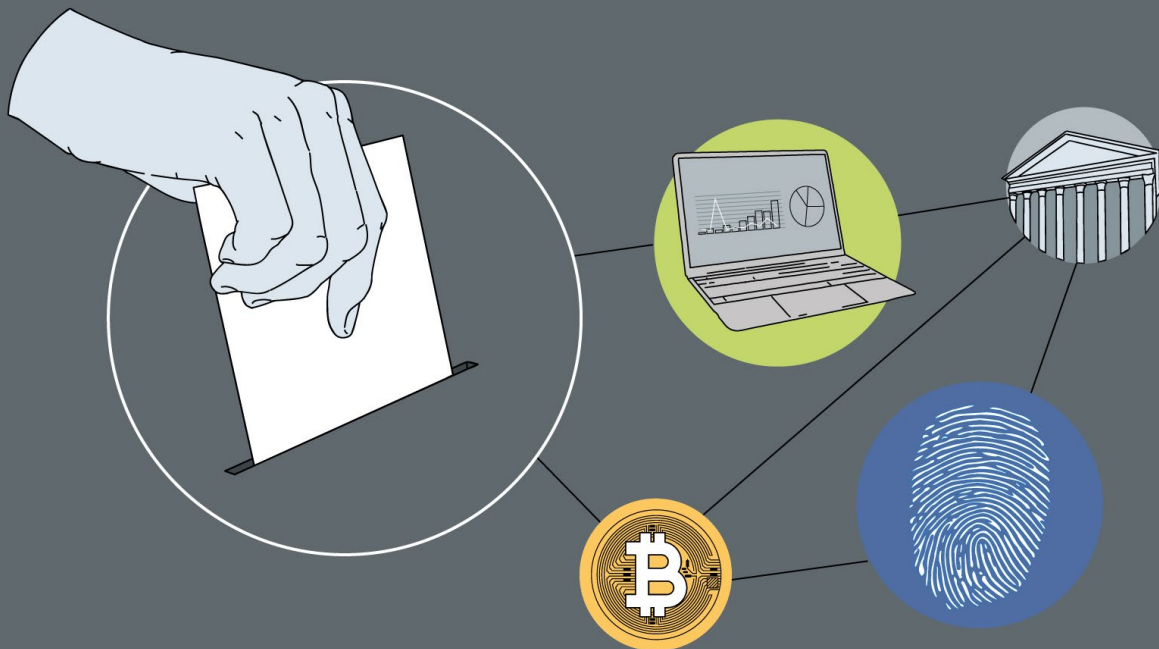
Negativna strana kampanja koju vodi treća strana u kontekstu interneta je što akteri mogu koristiti manje transparentne metode potpore kandidaturi ili pojačati poruke određenih kandidata. Kada nisu dovoljno regulirani, oglašivači treće strane ili oni o 'političkom pitanju' mogu omogućiti onima koji vode kampanju zaobilazanje limita troškova. Važno je da politički analitičar utvrdi jesu li kampanja koju vodi treća strana i ona o 'političkom pitanju' regulirane na analogan način onome koji se odnosi na registrirane kandidate: je li transparentnost definirana u zakonu i osigurana u praksi, uključujući i transparentnost u pogledu obznanjivanja donatora i donacija, troškova i poštivanja njihovih ograničenja, kao i obveze izvještavanja, nadzora i mogućih sankcija.

Na kraju, politički analitičar treba nastojati identificirati bilo koje slučajeve skrivene kampanje koju vodi treća strana ili one o 'političkom pitanju', koje su često povezane s negativnom kampanjom i informacijama manipulativnog sadržaja (npr., o kandidatima) ili općenitije, pokušajima da se

delegitimizira sâm proces. To može biti posebice opasno kada je, umjesto jasne oznake, sadržaj koji sponzorira treća strana sačinjen tako da izgleda organski te time može zaobići propise o financiranju kampanje. Iako to može predstavljati izazov, politički analitičar treba nastojati utvrditi i izvijestiti o tome koliko je ova vrsta ponašanja raširena na društvenim mrežama. Na kraju, politički analitičar treba razmotriti različite pojavne oblike agitiranja, uključujući potporu ključnih 'influensera', i procijeniti poduzimaju li tijela vlasti korake kojima će se osigurati da takvi slučajevi poštuju jednake uvjete za kandidate, i da za to snose odgovornost.

#### **Usmjerena pitanja:**

- ✓ Prevladava li na društvenim mrežama oglašavanje treće strane ?
- ✓ Imaju li bilo koji konkretni kandidati od toga koristi?
- ✓ Čine li platforme napore kako bi ograničile štetne aktivnosti u području oglašavanja treće strane?
- ✓ Jesu li te mjere učinkovite i konzistentne?
- ✓ Regulira li pravni okvir na zadovoljavajući način praksu vođenja kampanje treće strane na internetu, između ostalog u pogledu financiranja kampanje?
- ✓ Zahtjeva li se od trećih strana koje vode kampanju podnošenje izvješća nadzornim tijelima o svojim aktivnostima tijekom vođenja kampanje?
- ✓ Objavljuju li platforme društvenih mreža na transparentan i za korisnika pogodan način financijske priloge trećih strana?
- ✓ Je li sadržaj koji produciraju treće strane jasno označen?



## 6. NADZOR

Rasprave oko nadzora, učinkovitog pravnog lijeka i sankcija u području vođenja kampanje na društvenim mrežama oblikovale su se uz proces pojave propisa o političkom sadržaju i vođenju kampanje na internetu. Kako se propisi najčešće odnose na oglašavanje tijekom kampanje, financiranje kampanje, ankete javnog mnijenja i pravila o izbornoj šutnji, za nadzor su obično odgovorne iste one institucije koje imaju i regulatorne ovlasti u ovim područjima izvan interneta (npr., medijski regulator, EMB, ili bilo koja agencija zadužena za nadzor nad financiranjem kampanje). Politički analitičar treba ispitati način na koji pravni okvir definira ključne aspekte rada regulatora, uključujući njihove nadležnosti i kapacitete.



U nekim kontekstima, tijela odgovorna za reguliranje i nadzor nad tradicionalnim i internetskim medijima dobila su ovlasti nadzora društvenih mreža. Politički analitičar treba koordinirati s medijskim analitičarem prilikom sastajanja s ovim institucijama. Oni također trebaju procijeniti jesu li nadzorna tijela politički neovisna, i jesu li dovoljno odgovorna, donose li odluke na pravodoban i transparentan način, i mogu li se sudionici u kampanji žaliti, te uputiti prigovor i tražiti pravodobni pravni lijek na prigovor.

Što se tiče drugih tema, pogotovo manipulativnog sadržaja ili dezinformacija na društvenim mrežama, debata oko pravičnih mjera nadzora i sankcija i dalje je kontroverzna, s obzirom da postavlja važna načela koja su međusobno suprotstavljena, i time zaoštrava tenzije između prava birača na biranje na temelju pune informiranosti (slobodno od manipulacije bilo koje vrste) s jedne strane, i slobode izražavanja političara, oglašivača i drugih aktera na internetu, s druge.

Važno je naglasiti da, iako je formalna ovlast za nadzor neizbježno na regulatoru ili konkretnom nadzornom tijelu, domaći akteri, uključujući organizacije civilnog društva i medije, igraju važnu ulogu pozivajući na odgovornost izborne kandidate i druge aktere. Izjave civilnog društva i građana promatrača te medijska izvješća u nekim kontekstima mogu imati ključan utjecaj na javnu percepciju integriteta izbora. Tamo gdje imaju potrebne alate i resurse, ti akteri mogu pružiti precizne procjene ključnih aspekata vođenja kampanje na internetu, kao i u vezi s poštivanjem propisa o financiranju kampanje.

## 6.1 NADZOR NAD SADRŽAJEM

U samom središtu rasprave o reguliranju sadržaja stoji pitanje koje je već identificirano na početku, odnosno, treba li društvene mreže tretirati kao i bilo koje druge (tradicionalne) medije i trebaju li one biti odgovorne za ono što postavljaju na svoje platforme, ili ih treba shvatiti kao puke prenosiocice informacija koje generiraju korisnici, pri čemu oni snose konačnu odgovornost.<sup>102</sup> Dvojba koja iz toga proizlazi tiče se rasprave o tome trebaju li države regulirati i nadzirati sadržaj, što bi ih potencijalno moglo dovesti do toga da ograničavaju govor na internetu, ili je li sloboda izražavanja apsolutna te stoga platformama treba prepustiti da se samoreguliraju i, u konačnici, pridržavaju viših standarda ponašanja bez interveniranja vlasti.

<sup>102</sup> Važno je zapaziti da čak i u ovom drugom slučaju, algoritmi društvenih mreža određuju prioritet sadržaja, tj. u konačnici sudjeluju barem u suodlučivanju o tome tko što vidi i kada.

Prepoznavši širinu i dubinu odgovornosti koja dolazi sa samoreguliranjem, neke od big-tech kompanija uvele su interne inicijative za provođenje nadzora.<sup>103</sup> Nastojanja reguliranja ukupnog funkcioniranja društvenih mreža, u nekim državama članicama OESS-a prate nastojanja reguliranja i sadržaja na internetu, čime se povećava učinkovitost nadzora.<sup>104</sup>

Dok se nadzor može relativno lako uspostaviti u područjima gdje su ograničenja na prava i slobode jasno definirana u međunarodnom pravu i gdje se nedvosmisleno odražavaju i u domaćem zakonodavstvu (na primjer u pogledu poticanja na nasilje ili zaštite maloljetnika ili drugih specifičnih grupa građana i birača), drugi manje jasno definirani aspekti, kao što su blaženje, kleveta i razni tipovi manipulativnog sadržaja, predstavljaju ozbiljniji izazov. Reguliranje ovih aspekata ne samo da nije potpuno podržano međunarodnim instrumentima, već je često suprotno ljudskim pravima i temeljnim slobodama, kao što je pravo na slobodu izražavanja i pravo na dijeljenje i primanje informacija.

Ukazujući na nepostojanje učinkovite samoregulacije od strane društvenih mreža, neke vlade nastoje ograničiti širenje ‘lažnih vijesti’ tako što platforme drže odgovornima za sadržaj, što uključuje i novčane kazne. Neke države članice OESS-a također su počele uspostavljati agencije čiji je zadatak praćenje protoka informacija na internetu, s ciljem identificiranja različitih tipova manipulativnog sadržaja i postavljanja zahtjeva platformama da takav sadržaj uklone. U odsustvu konkretnih međunarodnih standarda i slabih ili dvosmislenih domaćih zakona, tijelo za upravljanje izborima i druga tijela općenito se ustručavaju provjeravati sadržaj, u nekim slučajevima i na štetu načela transparentnosti, koje je u samom središtu borbe protiv zlonamjernih praksi u vezi s kampanjama.

---

103 Primjerice, 2020. godine, Facebook je uspostavio Nadzorni odbor, tijelo koje donosi odluke o moderiranju sadržaja na ovoj platformi – pogotovo one o žalbama za blokirani ili uklonjeni sadržaj. Godine 2021., Twitter je pokrenuo vlastiti „pristup koji provodi društvena zajednica kako bi se pomoglo u rješavanju obmanjujućih informacija“, koji je, međutim, dostupan samo na tržištu SAD-a.

104 U kontekstu EU-a, [Direktiva o audiovizualnim medijskim uslugama](#) usvojena je 2018. godine kako bi se uspostavio regulatorni okvir za audiovizualni sadržaj za tradicionalne TV emitere i servise na zahtjev (eng. *on-demand*), čime je doneseno važno rješenje za reguliranje sadržaja na platformama koje dijele videomaterijale. Neovisno o EU okviru, neke države članice OESS-a donijele su zakone i obvezale tijela odgovorna za nadzor nad tradicionalnim medijima da također nadziru i reguliraju sadržaj koji se dijeli na društvenim mrežama. Takve radnje, ako se primjenjuju svojevrijedno i selektivno na određene dijelove društva i bez vjerodostojne metodologije, mogu biti suprotne obvezi poštivanja temeljnih sloboda i međunarodnih obveza, standarda i stajališta demokratskih izbora.

Politički analitičar treba biti svjestan da u nekim državama članicama OESS-a nastojanja reguliranja sadržaja mogu zapravo biti vođena ciljem sprječavanja govora ili mogu voditi do gušenja govora. Nelegitimno cenzuriranje sadržaja može nenamjerno ograničavati slobodno izražavanje i imati učinak gušenja političkog diskursa općenito. Restriktivni propisi i kontrola govora na internetu u demokratskom društvu mogu postaviti opasan presedan i ohrabriti nedemokratske režime na širenje cenzure. Budući da se vode žestoke rasprave o reguliranju sadržaja i nadzoru nad njim, tako i tehnološki razvoj također napreduje brzim tempom. Raširenost manipulativnog sadržaja u kampanjama i njegovo sve veće širenje mogu biti osobito štetni za žene i kandidate koji predstavljaju razne manjinske ili ranjive skupine, te ističu nužnost savladavanja ovog fenomena. Politički analitičar treba bilježiti pokušaje reguliranja sadržaja i pažljivo ih odvagnuti u odnosu na načela kao što su sloboda izražavanja i formiranja mišljenja bez neopravdanog uplitanja.

## **6.2 NADZOR NAD POLITIČKIM OGLAŠAVANJEM I OGLAŠAVANJEM TIJEKOM KAMPANJE**

Nadzor nad oglašavanjem tijekom kampanje normalno je odgovornost institucije koja nadzire političko financiranje i financiranje kampanje izvan interneta, što mogu biti tijela za upravljanje izborima, sudstvo, državna revizorska institucija, regulator RTV operatera ili neko drugo specijalizirano tijelo, ili odbor, i kao takve te institucije trebaju imati iste ili slične nadležnosti u području vođenja kampanje na internetu. Važno je da politički analitičar procijeni je li ta institucija neovisna i obavlja li svoje zadatke na neutralan način, te posjeduje li stručno znanje, tehnički kapacitet i resurse potrebne za smisleno ispunjavanje svoje nadzorne uloge.

Nadalje, politički analitičar treba nastojati shvatiti prati li nadzorno tijelo učinkovito plaćene aktivnosti izbornih kandidata i drugih aktera i ima li ovlasti pokretanja istrage i nametanja sankcija za neprijavljene troškove i oglašivačku aktivnost. Nadzorna tijela trebaju uspostaviti i održavati redovite kontakte s predstavnicima društvenih mreža kako bi osigurali učinkovito praćenje i provedbu propisa i, ako je potrebno, nametnuli učinkovite i pravodobne sankcije.

Financijska izvješća u vezi s kampanjama koje podnose kandidati i drugi izborni akteri trebaju biti dovoljno detaljna i prezentirana na način pogodan biračima kako bi oni mogli jasno razumjeti troškove u vezi s aktivnostima kampanje, te kako bi bili objavljeni na pravodoban način. Dobra praksa je da se prijelazna izvješća dostavljaju tijekom izborne kampanje i prije dana izbora tako da birači mogu izabrati kandidate na temelju pune

informiranosti, a konačna izvješća nakon dana izbora u roku koji će biti dovoljan kako bi kandidati na izborima i drugi akteri završili financijske transakcije u vezi s kampanjom. Izvješća trebaju ostati na raspolaganju tijekom dužeg perioda nakon izbora i mogu biti objavljeni na web-stranici nadzornog tijela ili kandidata i drugih izbornih aktera, ili oboje, kao i na društvenim mrežama za troškove povezane s vođenjem kampanje na internetu.

Drugi propisi o kampanji koji mogu igrati ulogu u okruženju interneta uključuju odredbe u pogledu izborne šutnje na dan prije izbora. U nekim slučajevima, takve mjere uključuju zahtjeve da se oglasi uklone prije nego što počne glasovanje. Tijelo za upravljanje izborima često je zaduženo za nadzor, ali tu mogu biti angažirani i ostali akteri, uključujući općinska tijela vlasti. Politički analitičar treba utvrditi postoje li jasna pravila, identificirati koja tijela imaju ovlast za nadzor i procijeniti jesu li ona sposobna i voljna tu ovlast učinkovito provoditi.

Drugi propisi kampanje koji mogu igrati ulogu u online okruženju uključuju odredbe o izbornoj tišini dan prije i na dan izbora. U nekim slučajevima, takve mjere uključuju zahtjeve da se reklame uklone prije početka glasanja. Tijelo za provođenje izbora je često zaduženo za nadzor, ali mogu biti angažovani i drugi akteri, uključujući općinske vlasti. Politički analitičar treba utvrditi postoje li jasna pravila, identificirati koja tijela imaju nadzorne ovlasti i procijeniti jesu li ona u stanju i voljna učinkovito ih primjenjivati.

ODIHR-ov Priručnik za promatranje financiranja kampanja pruža najsveobuhvatnije smjernice za OESS-ove izborne promatrače za procjenjivanje oglašavanja tijekom kampanje, uključujući odgovornosti država članica za nadzor. U skladu s vlastitim obvezama i međunarodnom dobrom praksom, države trebaju osigurati neovisan nadzor i promatranje financiranja kampanje. Odgovornost treba dodijeliti neovisnom i profesionalnom regulatornom tijelu, koje ima mandat davanja smjernica izbornim akterima, provjeravanja izvješća o financiranju kampanje i istraživanje potencijalnih kršenja, te ovlast sankcioniranja s ciljem promicanja učinkovite provedbe zakona i osiguravanja odgovornosti svih aktera.

### **6.3 NADZOR NAD ZAŠTITOM PRIVATNOSTI PODATAKA**

U vođenju kampanje na internetu, količina raspoloživih osobnih podataka i metode koje se primjenjuju razlikuju se od tradicionalnih metoda oglašavanja i mogu imati veći utjecaj na temeljne slobode i prava birača. Kako je opisano u prethodnim poglavljima, međunarodni instrumenti pružaju jamstva za pribavljanje, pohranjivanje, obradu i korištenje podataka. Države su obvezne osigurati podatke od uništenja, slučajnog gubitka, krađe ili bilo

kojeg drugog oblika neovlaštenog pristupa, mijenjanja ili širenja.<sup>105</sup> Pravni okvir treba eksplicitno precizirati uvjete za dobivanje informacija o biračima i svrhe za koje se one traže. Također treba utvrditi mogu li podaci biti stavljeni na raspolaganje kandidatima na izborima u svrhe vođenja kampanje. Važno je da također treba identificirati i instituciju ovlaštenu za nadziranje odgovornost i navesti sankcije za zlouporabu privatnih podataka.

Iako je vjerojatno da će tijela za upravljanje izborima ili tijela za vođenje popisa stanovništva dobiti ovlasti za upravljanje i nadzor biračkih popisa, druge i specijaliziranije agencije često su odgovorne za nadzor nad poštivanjem postojećih zakona u području zaštite podataka. Kao i u slučaju provjeravanja rada medijskih regulatornih tijela (ako su ona nadležna za nadzor nad društvenim mrežama), kada se radi o korištenju podataka u kampanjama, politički analitičar će, u suradnji s medijskim analitičarem, i zajedno s izbornim ili pravnim analitičarem procijeniti zakone i rad institucija za zaštitu podataka, što uključuje njihovu neovisnost. Oni zajednički trebaju utvrditi donosi li dotično tijelo odluke na transparentan način i jesu li te odluke predmet sudske revizije. Također trebaju kontrolirati ovlasti tog tijela za provedbu, uključujući njegovu sposobnost upućivanja predmeta drugim institucijama na istragu ili neposrednog novčanog kažnjavanja prekršitelja.

Svi izborni akteri i kompanije za brokering privatnih podataka trebaju biti predmet neovisnog nadzora. Taj nadzor često uključuje poštivanje režima zaštite podataka i razinu transparentnosti do koje stranke, kandidati i druge kompanije koriste privatne podatke. U tu svrhu, dobra je praksa da:

- nadzorna tijela prate pružaju li svi kontrolori i obrađivači podataka javnosti jasne informacije o tome kako se njihovi podaci koriste i kako će biti korišteni;
- jesu li birači obaviješteni kada se vrši indiskretno profiliranje, kao što je kombiniranje informacija o njima iz različitih izvora kako bi se saznalo više o njihovim biračkim naklonostima;
- da pokažu odgovornost prema javnosti, pokazivanjem kako stranke ispunjavaju svoje obveze i štite prava birača;
- ispunjavaju li svi obrađivači podataka, uključujući treće strane, ključne zahtjeve u pogledu transparentnosti, sigurnosti i odgovornosti za zaštitu podataka;

---

105 Vidi [Konvenciju za zaštitu pojedinaca u pogledu automatizirane obrade osobnih podataka Vijeća Europe](#) (Konvencija 108) iz 1981, posebno članke 3, 5 i 7. Vidi također [Dodatni protokol Konvencije za zaštitu pojedinaca u pogledu automatizirane obrade osobnih podataka, o nadzornim tijelima i prekograničnom protoku podataka iz 2001.](#)

- da analiziraju njihove zakonite osnove za različite tipove obrade osobnih podataka koji se primjenjuju kako bi se osiguralo korištenje najprimjerenije osnove.

#### **Usmjerena pitanja:**

- ✓ Postoji li režim privatnosti i zaštite podataka?
- ✓ Je li to primjenjivo i provodi li se u kontekstu izbora, pogotovo kada se tiče vođenja kampanje od strane kandidata i trećih strana?
- ✓ Koja državna tijela imaju nadzor i ovlast za reguliranje/sankcioniranje u području zaštite podataka?
- ✓ Smatraju li se ona u svom djelovanju politički neovisnima i neutralnima?
- ✓ Ima li tijelo za zaštitu privatnosti i podataka kapacitete, resurse i volju ispuniti svoju ulogu u praksi?
- ✓ Ima li tijelo za zaštitu privatnosti i podataka potrebne ovlasti za provedbu kako bi bilo učinkovito, uključujući ovlast novčanog kažnjavanja?
- ✓ Je li odlučivanje tijela za zaštitu privatnosti i podataka transparentno i je li predmet sudske revizije?
- ✓ Imaju li političke stranke i/ili kandidati uspostavljene politike kako bi osigurali baratanje osobnim podacima u skladu sa zakonom i/ili međunarodnim standardima?
- ✓ Mogu li svi akteri pristupiti podacima pod jednakim uvjetima?
- ✓ Postoje li bilo koji kandidati koji (mikro)ciljaju birače tijekom kampanje?
- ✓ Je li (mikro)ciljanje regulirano zakonom?
- ✓ Kako akteri dobivaju podatke o biračima, i daju li birači suglasnost za njihovo korištenje?
- ✓ Mogu li oni povući svoju suglasnost?





## 7.

# IZAZOVI I PRILIKE ZA KVANTITATIVNU PROCJENU

### 7.1 METODOLOŠKA OGRANIČENJA

Mada je metodologija za procjenu vođenja kampanje na društvenim mrežama u začetku i nastavit će se razvijati s budućim tehnološkim razvojem, ODIHR-ove izborne misije već nekoliko godina u različitoj mjeri prate internetske kampanje raznih aktera. Važno je odmah zapaziti da ne postoji jedan univerzalan ili jedinstveni pristup i da postoje različite metodologije koje se provode u jednom broju promatračkih organizacija u procjeni vođenja kampanje na društvenim mrežama, od kojih neke svoje zaključke temelje na opsežnijem kvantitativnom i statističkom mjerenju. Međutim, zadatak izvođenja zaključaka utemeljenih na kvantitativnoj analizi još uvijek je nedefiniran i sa sobom nosi određene izazove i ograničenja koje vrijedi spomenuti. Izbor uzorka i metodološka osnova za kvantitativnu procjenu



vođenja kampanje na društvenim mrežama opterećeni su kompleksnošću koja se u nekim okolnostima može opirati sistematičnim nastojanjima praćenja izbornih aktivnosti ograničenih vremenom i drugim ograničenjima u pogledu sredstava.

Prvi skup izazova odnosi se na opseg ili na veoma veliki broj različitih platformi, profila i objava koji čine korpus materijala za analizu. *Izbor platformi* mora uzeti u obzir njihovu popularnost među različitim demografskim skupinama, kako bi se obuhvatio najširi mogući presjek – čak i ako su, ukupno gledano, korisnici vjerojatno mlađi birači, pri čemu je moguća pristranost u odabiru. Drugi problem odnosi se na identificiranje reprezentativnih *uzoraka profila* za monitoring. Taj izbor usložnjava činjenica da njihova popularnost može biti privremena, te tako profili koji su danas u trendu i privlače mnogo pozornosti mogu vrlo brzo postati irelevantni. Drugi izazov je *anonimnost i točnost računa* pošto je često teže utvrditi pripada li profil određenoj osobi ili je kompjuterski generiran. Na kraju, *obujam objava* koje se generiraju na društvenim mrežama može biti beskonačan. Brzina kojom se nove objave pojavljuju, šire i zamjenjuju sljedećom stavkom koja postaje trend može biti iznimno velika i praktično je nemoguće zabilježiti ih bez odgovarajućeg softvera.<sup>106</sup>

Rad s velikom količinom materijala zahtijeva korištenje digitalnih alata i sofisticiranih metoda odabira uzoraka koje je moguće procesuirati. Međutim, ova vrsta uzorkovanja krije metodološke rizike, kao što su inherentne pristranosti digitalnih alata i problem vanjske valjanosti ili generalizacije rezultata. S obzirom na heterogenost informacija koje su na raspolaganju na internetu, sve je teže izvući zaključke i donijeti procjene samo na temelju veoma zbirnih podataka i mjerenja ‘angažmana’, koji može biti teško tumačiti i čija veličina može dovesti u zabludu. Nadalje, uzorkovanje ne smanjuje nužno podatke na savladive količine bez potrebe da se posegne za automatiziranim alatima za njihovo prikupljanje i obradu, što vodi do drugih problema kao što je automatizirano isključivanje relevantnog sadržaja.

Drugi skup izazova je tehničke prirode. Dok osnovna kvantitativna analiza ručno odabranih uzoraka može biti izvodiva i može biti uključena u procjenu, obuhvaćanje šireg područja zahtijeva korištenje vanjskih digitalnih alata za prikupljanje i analizu podataka s raznih platformi. Budući da točnost prikupljenih podataka s istih platformi korištenjem različitih alata često varira, konzistentnost analize i kvalitete nalaza možda neće biti

---

106 Objave redovito nestaju, bilo na temelju politike arhiviranja same platforme ili zato što su uklonjeni, primjerice, na temelju toga da krše standarde zajednice. Nadalje, ne mora uvijek biti moguće utvrditi jesu li objave organske ili kompjuterski generirane.

jednoobrazni.<sup>107</sup> Alati će se možda morati podešavati (eng. *tweaked*) kako bi se uklopili u realno stanje u datom mjestu, te se moraju uzeti u obzir i metode i stil političke komunikacije koja je popularna u određenom kontekstu. Na kraju, mnoge aplikacije upravljaju tekstualnim podacima, ali mogu biti manje od pomoći s drugim tipovima sadržaja, kao što su videosnimci i slike, čije bi propuštanje moglo narušiti reprezentativnost rezultata.

Osim opsega i tehničkih pitanja, drugi tip izazova za kvantificiranje nalaza i analizu vođenja kampanje na internetu je urođena kompleksnost društvenih mreža. Za razliku od praćenja tradicionalnih medija, gdje se uspostavljaju relativne mjere, kao što su udio i ton izvještavanja, kvantitativna analiza društvenih mreža nudi mnogo širi opseg mjerenja, uključujući učestalost postavljanja objava, pitanja koja su u trendu (eng. *rending issues*), analizu mreža, neautentične račune, broj plaćenih oglasa, doseg angažmana javnosti i mnogo više. Kad se koriste zajedno s kvantitativnom procjenom, ovi podaci rasvjetljavaju različite trendove, uključujući pitanja koja se odnose na zlonamjerno korištenje društvenih mreža, kao što su 'govor mržnje', poticanje, dezinformacije, zlouporaba administrativnih resursa, kompjuterski generirana propaganda, pojačavanje neautentičnog ili manipulativnog sadržaja ili skriveno (mikro)ciljanje. Međutim, bez jasnih referentnih točaka, kao što je približna rasprostranjenost konkretnog fenomena kao dio ukupnih nalaza, ovi nalazi političkom analitičaru neće nužno omogućiti pouzdano utvrđivanje njihova stvarnog značaja u datoj izornoj kampanji.

Konačno, i dalje se rade istraživanja utjecaja društvenih mreža na kreiranje mišljenja i ponašanje birača, pri čemu izazov predstavljaju suprotni nalazi. Ukupan značaj, utjecaj i cirkulaciju serije zlonamjernih objava ili trendovskih priča, uključujući one koje također mogu koristiti tradicionalni mediji, teško je mjeriti. Transparentnost, ili razotkrivanje načina na koji se manipulira činjeničnim informacijama ili na koji su birači predmetom mikro(ciljanja) zaslužuje pozornost i procjenu misije o pozadini i potencijalnim učincima tih radnji, ali kvantitativna analiza neće nužno značiti dodanu vrijednost nalaza koji su već dobiveni na temelju kontekstualnog promatranja i procjene utemeljene na kvalitativnim metodama.

Općenito, politički analitičar treba pristupiti zadatku kvantitativnog mjerenja iz kritičke perspektive i s jasnom sviješću o tome što se može postići s ograničenim resursima i vremenom koji su mu na raspolaganju. Politički analitičar također treba imati na umu očekivanja koja otvara kvantitativna analiza. Iako nabiranje može biti vrijedno, ono u konačnici ne smije biti primarna osnova za procjenu. Različiti aspekti koji se pojavljuju u kampanjama na internetu – uključujući oblike manipuliranja informacijama ili

107 Optimalno korištenje ovih instrumenata također zahtijeva dublje poznavanje lokalnog konteksta kako bi se omogućilo prikupljanje i analiza informacija o važnim, ali nekada manje vidljivim fenomenima, kao što je poslovična šifrirana (eng. 'dog whistle') komunikacija između političara i njihovih birača, što vanjskim promatračima možda neće biti lako razumljivo

‘govor mržnje’– i dalje su opterećeni nedostacima u pogledu definicije, koja može poremetiti nalaze i učiniti ih neusporedivima, te često nepouzdanima. I dok se stalno razvijaju novi alati s ciljem poboljšanja mjerenja, tehnologije i modusi digitalne komunikacije također ubrzano napreduju. Stoga kvantitativni pristupi ponekad mogu zaostajati za tehnološkim razvojem i biti manje korisni za rasvjetljavanje novih oblika manipulacija, što ugrožava vjerodostojnost ukupne procjene.

## 7.2 PODACI IZ VANJSKIH IZVORA

Okosnica ODIHR-ove metodologije neposredno je promatranje, u kombinaciji s informacijama dobivenima od sugovornika i drugim podacima identificiranim tijekom promatranja. Politički analitičari često nailaze na informacije i analize drugih promatračkih skupina. Te dodatne informacije i analize mogu biti dragocjene za općenitija saznanja misije o određenoj temi. Iako vanjski izvori mogu služiti kao koristan kontekst, najvažnije je da se nikada ne smiju koristiti kao jedina osnova nalaza i izvješća izbornih misija. Poštujući opće zahtjeve u pogledu neovisnosti i neutralnosti, politički analitičar treba navoditi samo informacije ili zaključke do kojih su došle druge ugledne organizacije. Naravno, to važi za sve aspekte promatranja, što uključuje i područja u kojima su kapaciteti misije ograničeni.

S razvojem digitalnih tehnologija i njihovim sve većim korištenjem u izbornim kampanjama, sve je veći broj aktera koji prikupljaju i analiziraju podatke u vezi s ulogom ulogu društvenih mreža u političkoj komunikaciji. Tu se svrstavaju profitne tvrtke, poput big-tech tvrtki i kompanija s brokering podacima, istraživački centri i neprofitni akteri, kao što su organizacije civilnog društva, od kojih neki mogu biti povezani s građanskim promatračkim skupinama. Politički analitičar treba biti upoznat s vodećim subjektima i, kad god je moguće tijekom izborne aktivnosti, sastajati se s odabranim akterima kako bi svoje nalaze stavio u kontekst, razjasnio metodologije i prikupio dodatne detalje.

Politički analitičari veliku pozornost trebaju posvetiti komercijalnim i neprofitnim inicijativama koje proizvode analitičke alate za sistematično automatsko učitavanje podataka (‘scraping’) s platformi društvenih mreža. Neki od tih proizvoda uključuju već gotove instrumente koji, ako se koriste na ispravan način, mogu potkrijepiti nalaze i pomoći političkom analitičaru temeljitije razumjeti ulogu društvenih mreža u izornoj kampanji. Također, postoje organizacije koje se bave provjerom činjenica i koje su specijalizirane za otkrivanje, razotkrivanje i ispravljanje neistina na internetu, a one su posebno aktivne tijekom izbornih razdoblja. Na kraju, platforme društvenih mreža same mogu biti važni sugovornici jer često javno objavljuju podatke koji nekada mogu obogatiti promatračka i analitička nastojanja misije.

Specifična priroda i kompleksnost društvenih mreža, u kombinaciji s ograničenim vremenom i resursima koje misija ima na raspolaganju, može promatračima koji analiziraju vođenje kampanje na internetu nametnuti potrebu korištenja podataka iz vanjskih izvora u većoj mjeri nego što je to normalno slučaj u kontekstu međunarodnih promatranja ili procjene izbora. Politički analitičar mora biti posebice oprezan pri utvrđivanju neutralnosti, autentičnosti i vjerodostojnosti tih informacija i treba uvijek nastojati verificirati podatke, bilo da su generirani manualno ili automatski uz pomoć eksternih alata. Politički analitičar mora uvijek kombinirati nalaze; ponekad može biti uputno ne navoditi izravno vanjske zaključke, osim u slučajevima gdje oni predstavljaju važnu komponentu općenitijeg konteksta. Važno je ukazati na to da se vanjske procjene i analize često provode na temelju nalaza akumuliranih u određenom razdoblju koji se ne podudara s vremenskim okvirom izborne promatračke misije ili razdobljem izborne kampanje. Dok može biti od manjeg značaja za razumijevanje opće političke pozadine i konteksta, korištenje takvih nalaza, koji se konkretno odnose na izbornu kampanju, može biti limitirano i treba uključivati oprez.

#### **a. Alati za praćenje društvenih mreža (Web listening) i automatsko učitavanje podataka (Data Scraping)**

Alati za ‘web listening’ ili data scraping mogu, općenito govoreći, pružiti dobar uvid u opće trendove u datom političkom kontekstu i okruženju kampanje. Ako politički analitičari posjeduju potrebne vještine, mogu te alatke koristiti kao potporu ukupnoj procjeni kampanje. Kad to čine, trebaju obaviti manualne pretrage i kodirati podatke kako bi utvrdili osnovne kvantitativne nalaze i na temelju tih elemenata izvukli vlastite zaključke.

Postoji nekoliko načina za pribavljanje podataka s društvenih mreža. Najuočljivija metoda je korištenje vlastitih aplikacija za programiranje sučelja (Application Programming Interfaces - skraćeno APIs) samih platformi.<sup>108</sup> Drugi način je korištenje posebno dizajniranih ili gotovih alata za ‘data scraping’. Danas na raspolaganju ima mnogo instrumenata, uključujući najosnovnije s ograničenim mogućnostima, i kompleksnije instrumente; besplatne programe i one koji funkcioniraju na temelju plaćanja pretplate; kao i one koji su razvijeni za rad s više platformi, kao i druge koji su specijalizirani za jednu aplikaciju.<sup>109</sup> Iako su mnogi od ovih alata prvobitno dizajnirani u komercijalne svrhe, neki se mogu prilagoditi procesu za obradu političkog sadržaja i onog glede kampanje. To se brzo mijenja, pri čemu mnogi

108 Sredstva kojima se podaci s jednog web-alata ili aplikacije mogu razmijeniti s drugom ili dobiti od nje.

109 Korisnici ovih Smjernica trebaju voditi računa o brzom razvoju u ovom krajnje dinamičnom području, budući da neki od alata mogu u kratkom vremenu postati suvišni i zastarjeli, a mogu se pojaviti novi. U vrijeme pisanja ovih Smjernica, neki od raspoloživih alata su: *CrowdTangle*, *BuzzSumo*, *TalkWalker*, *NapoleonCat*, *Social Bakers*, *Brandwatch*, *Twitonomy*, *SentiOne*, *Factalyzer*, *Versus*, *Google Trends Facebook Ad Library*, *BotOrNot*.

instrumenti brzo zastarijevaju, a redovito se kreiraju novi koji dolaze na njihovo mjesto.

Dok se mnogi alati mogu koristiti za pribavljanje podataka s različitih društvenih mreža, trenutno nema jedinstvenog instrumenta koji može učitati podatke sa svih mreža. Nekoliko programa također se može koristiti na platformama poput *Vkontakte*, *Odnoklassniki* i na servisima za razmjenu izravnih poruka (eng. instant messaging services, skraćeno IMS) kao što su *WeChat* i *SnapChat*; međutim, razina dozvoljenog pristupa tim servisima varira. Zbog enkripcije, podaci se ne mogu dobiti sa servisa za razmjenu poruka kao što su *WhatsApp*, *Telegram*, *Signal* ili *Viber* – štoviše, pošto je komunikacija u zatvorenim skupinama u krajnjoj instanci privatna, opće je pravilo da politički analitičar ne smije ni u kakvim okolnostima pribavljati te podatke.

Općenito gledano, s ciljem mjerenja tona političke debate na društvenim mrežama, savjetuje se, i često je potrebna, manualna verifikacija.<sup>110</sup> Kad se koriste neki od navedenih instrumenata, važno je imati na umu da građanska i politička kultura, različiti tipovi diskursa i korištenje žargona specifičnog za kontekst mogu utjecati na rezultate. Politički analitičari stoga trebaju biti oprezni prilikom biranja ključnih riječi za pretrage, što uključuje različite 'hashtagove'.

## **b. Pristup podacima *big-tech* kompanija**

*Big-tech* kompanije počele su sve više prepoznavati svoju ključnu ulogu u zaštiti integriteta izbora. Njihov angažman je, ukupno gledano, bio neujednačen na različitim platformama i unutar jedne platforme u različitim zemljama. Kada se radi o tehničkim mogućnostima koje koriste istraživači ili promatrači za nalaženje metapodataka, *big-tech* kompanije su s vremenom suzile takve mogućnosti, ali su kreirale neke alate za prikupljanje podataka. Slijede neka od nastojanja i alati koje su uvele najveće društvene mreže u OESS-ovoj regiji s ciljem povećanja transparentnosti svojih platformi:

- ♦ *Facebook* je i dalje glavna platforma za vođenje kampanje u mnogim državama članicama OESS-a. Zabrinuta zbog potencijalne zlorabe podataka, ova je kompanija 2018. godine ograničila pristup svom API-ju tako da više nije moguće dobiti informacije na način kojim bi se ispoštovao sporazum s korisnikom. Korisnici za to moraju podnijeti zahtjev *Facebooku* dobrano unaprijed i bez zajamčenog uspjeha. Dok mnogi podnositelji zahtjeva dobivaju suglasnost putem *CrowdTangle*, drugima se

<sup>110</sup> U radu s naprednim alatima, politički analitičar treba, kao opću praksu, nastojati odabrati uzorke podataka s ciljem utvrđivanja je li sustav ispravno identificirao određeni fenomen i uspoređivanja bilo kakvih novih trendova s kvalitativno generiranim nalazima.

nudi ograničeniji pristup putem API-ja. Unatoč ovim poteškoćama, *Facebook* u ovom trenutku daje besplatan pristup svojim podacima, što što više ne zahtijeva vještine programiranja. Kompanija također teži povećati transparentnost putem biblioteke oglasa i objavljivanjem izvješća o transparentnosti, koji sada uključuju kvartalna izvješća o provedbi standarda zajednice i detaljno opisuju radnje poduzete radi sprječavanja sadržaja koji krši politike koje se odnose na korisnike, uključujući i na *Instagramu*.

- ♦ Raspoloživost podataka na *Googlu* također je, ukupno gledano, neujednačena i s vremenom se mijenja. Ranije je pristup *YouTubeovom* API-ju bio relativno jednostavan, ali korisnici su morali posjedovati određenu razinu vještine programiranja. Ta je kompanija ponudila dokumentaciju i resurse za korištenje svog servisa, uključujući kodove na različitim programskim jezicima za pristup API-ju. To je sada teže dobiti, pri čemu podnositelji zahtjeva moraju osobno uputiti zahtjev u kojem se po pravilu moraju pozvati na domaće zakone koji eksplicitno obvezuju tvrtke na omogućavanje pristupa. *Google* od 2010. objavljuje redovita izvješća o transparentnosti, koja su s vremenom postala sve detaljnija i sada obuhvaćaju sve njegove platforme.
- ♦ *Twitter* se općenito doživljava kao najtransparentnija platforma, dostupna za istraživanje akademskoj zajednici. Njegov API je besplatno dostupan istraživačima, a podaci su raspoloživi na svim tržištima ove kompanije. *Twitter* samoinicijativno objavljuje informacije o uklanjanju lažnih računa, u nekim slučajevima najavljujući njihovo ukidanje.

Ukupno gledano, izvještavanje samih *big-tech* kompanija ne poklapa se s konkretnim izbornim ciklusima i nekompatibilno je s potrebama ODIHR-ovih aktivnosti promatranja ili procjene izbora. Neujednačena razina pristupa podacima u različitim zemljama OESS-a usložnjava analizu podataka, a to je posebno problematično u kratkom razdoblju uoči izbora kada je pouzdanost podataka najvažnija. Praksa je pokazala da su platforme otvorenije sa svojim podacima tamo gdje postoje odgovarajući zakoni koji nalažu obvezan pristup. Nadalje, različite platforme nude jasno određene 'vremenske blokove' povijesnih podataka i, dok neke dozvoljavaju automatsko učitavanje podataka godinama unatrag, druge su u tome ograničenije.<sup>111</sup> Na kraju, jedan od ključnih razvoja u političkoj komunikaciji je odmak od javnih rasprava na društvenim mrežama u smjeru razgovora u zatvorenim

---

111 Primjerice, postovi na *Twitteru* nestaju nakon malo više od tjedan dana, te je stoga potrebno redovito i pravodobno bilježenje informacija. Nadalje, tvrtke vlasnici društvenih mreža često uklanjaju problematične postove, što izaziva dvostruki problem: uklonjeni post ne može se ni adekvatno analizirati, niti se njegovi učinci mogu istražiti kad je njegovo prisustvo na internetu bili posebno kratko.

mrežama ili na aplikacijama s izravnim porukama, što je u ovom trenutku izvan dosega izbornih promatrača.<sup>112</sup>

I kvantiteta podataka i neujednačena razina pristupa podacima dovode do ograničenja u smislu dosljednog visokokvalitetnog izvještavanja koje je relevantno za promatranje i procjenu. Ovi izazovi naglašavaju značaj velike pozornosti koja se mora posvetiti onome što je moguće postići u kontekstu i s resursima misije. Procjena kampanje na društvenim mrežama koju vrši politički analitičar mora jasno navesti na koju se platformu i račune odnosi. Ako se koriste u procjeni, treba uključiti informacije o tome kako su podaci pribavljeni i koje su metode primijenjene u njihovoj analizi. Nalazi moraju biti verificirani manualnom provjerom odabranih uzoraka automatski generiranog materijala. Također je dobra praksa pratiti saznanja i nalaze drugih vjerodostojnih organizacija, uz veliki oprez i preciznost, kako bi se osigurala usklađenost općih dojmova, razumijevanje uzroka za to, te u slučaju kad nisu, razmatranje mogućih objašnjenja za to.

### c. Provjeritelji činjenica

Širenje informacija manipulativnog sadržaja koje prati rast društvenih mreža, dovelo je i do organiziranih napora identificiranja, razotkrivanja i ispravljanja neistinitosti koje su u trendu na internetu. Širenje takozvanih ‘lažnih vijesti’ na internetu potaknulo je razvoj novih tehnika rješavanja ovog problema. Često u suradnji s medijima i *big-tech* kompanijama, pojavilo se na desetke organizacija poznatih kao provjeritelji činjenica s ciljem oponašanja onoga što je dugo vremena bilo povezano s tradicionalnom medijskom praksom interne ispravke činjeničnih grešaka *ante hoc*. U kontekstu društvenih mreža, ono se sada često provodi korištenjem softvera za rudarenje podataka, i *post hoc*, tj. nakon što su lažne vijesti već dospjele u javnu domenu.

Organizacije za provjeru činjenica nastoje utvrditi točnost i ispraviti objavljenu informaciju, uključujući novinska izvješća i izjave političara. To su često građanske ili medijske inicijative, ali i društveni influenseri, te mogu biti povezani s tradicionalnim medijskim kućama. U suradnji s *big-tech* tvrtkama, ‘tagovi’ provjeritelja činjenica počeli su se pojavljivati na nekim platformama s ciljem označavanja verificiranog sadržaja i pomaganju u

---

112 Zatvorene skupine predstavljaju značajan i trenutačno nesavladiv izazov za međunarodne promatrače izbora. Zbog toga što nisu u javnoj domeni, promatrači im ne mogu pristupiti, osim ako ne postanu članovi skupine, što oni nikada ne bi trebali raditi zbog očuvanja vlastite neutralnosti. Nadalje, nazočnost promatrača unutar neke skupine mogla bi utjecati na ponašanje njezinih članova. Budući da je transparentnost od najvećeg značaja, politički analitičar ne smije ni pod kojim okolnostima postati član skupine pod aliasom ili preko drugog pojedinca ili skupine.

postizanju veće istinitosti tvrdnji koje se objavljuju na internetu.<sup>113</sup> Mnoge skupine provjeritelja činjenica djeluju transnacionalno i koriste redovite međusobne razmjene.<sup>114</sup> Potpora koja se pruža mrežama za provjeru činjenica uspostavljenih iz zabrinutosti zbog širenja lažnih vijesti u izborne svrhe pomogla je njihovu brzom rastu.<sup>115</sup>

Politički analitičar nije u poziciji da presuđuje o točnosti tvrdnji ili da utvrđuje kvalitetu inicijativa za provjeru činjenica, ali bi se mogao upoznati sa situacijom i uzeti u obzir prisustvo i aktivnosti vodećih organizacija za provjeru činjenica. Ako to vrijeme dozvoli, politički analitičar bi se mogao udružiti s medijskim analitičarem i sastati s istaknutijim skupinama kako bi utvrdili da li se provjeritelji činjenica suočavaju s bilo kakvim preprekama u svom radu te dodatno procijenili kvalitetu njihovih odnosa s drugim akterima, uključujući izborne kandidate, tradicionalne medije i tijelo za upravljanje izborima. Oni bi također mogli utvrditi postojanje veze između skupina za provjeru činjenica i *big-tech* kompanija, uključujući provjeru do koje mjere kompanije odgovaraju na izvješća na koja upozore provjeritelji činjenica.

#### Usmjerena pitanja:

- ✓ Postoje li domaće organizacije koje prate društvene mreže tijekom izbora?
- ✓ Koji su njihovi ciljevi i opći zaključci?
- ✓ Koji su ključni nalazi ili teme koje se pojavljuju na temelju njihovih zapažanja s bilo koje prethodne ili aktualne kampanje na društvenim mrežama?
- ✓ Postoje li ugledne nacionalne inicijative koje prate vođenje kampanje na društvenim mrežama i pritom koriste automatizirane alate, i koji su njihovi nalazi?
- ✓ Koliko su lako dostupni podaci *big-tech* kompanija u državama članicama OESS-a?
- ✓ Izvještavaju li domaće organizacije za monitoring o bilo kojim pitanjima glede raspoloživosti podataka ili njihove dosljednosti?
- ✓ Jesu li skupine za provjeru činjenica nazočne i angažirane u razotkrivanju lažnih vijesti tijekom kampanje?
- ✓ Jesu li one istinski politički neovisne u odnosu na stranke? Postoji li zabrinutost u pogledu kvalitete njihova rada?

113 *Facebook* se, primjerice, udružio s nekoliko organizacija u provjeravanju činjenica i označavanju sadržaja, dok *Google* tvrdi da je podeseo svoje algoritme kako bi prioritet dao činjenično provjerenim sadržajima. *Twitter* je razvio alatke kako bi pomogao korisnicima označiti zastavicom sadržaj čiji je cilj odvratanje birača od izlaska na izbore, koje ova kompanija uklanja sa svoje platforme kada su izvješća o njima potkrijepljena dokazima. *Facebook* navodi da je ovo partnerstvo smanjilo prisustvo lažnih vijesti za nekih 80 posto.

114 Jedan od predvodnika međunarodnih nastojanja na polju umrežavanja je Međunarodna mreža za provjeru činjenica (IFCN), čiji je cilj poticanje razvoja zajedničkih metoda rada i institucionalizacija razmjene najboljih praksi. Neke od mreža uživaju potporu međunarodnih aktera, uključujući organizacije kao što je EU, koja je također pomogla uspostaviti neovisne europske mreže provjeritelja činjenica.

115 Broj inicijativa za provjeru činjenica eksponencijalno raste posljednjih godina. Uz pojavu iskrenih pokušaja da se riješi problem 'neistina', došlo je i do porasta broja lažnih provjeritelja činjenica koji nastoje potvrditi lažne informacije koje se šire na internetu.



- ✓ Postoji li bilo kakav odnos između provjeritelja činjenica i države ili tijela za upravljanje izborima?
- ✓ Suraduju li platforme s lokalnim provjeriteljima činjenica?
- ✓ Koliko su one spremne odgovoriti na njihova izvješća?
- ✓ Postoji li suradnja između organizacija za provjeru činjenica i ključnih medija?
- ✓ Pružaju li društvene mreže korisnicima tehnološka rješenja za otkrivanje manipulativnih ili štetnih sadržaja (npr., označavanje zastavicama)?

# Aneks 1:

## RELEVANTNI MEĐUNARODNI DOKUMENTI

### **OESS**

#### **OESS-ov Kopenhaški dokument 1990.**

**Stavak (5.1):** slobodni izbori koji će se održavati u razumnim intervalima, tajnim glasovanjem ili ekvivalentnim procedurama slobodnog glasovanja pod uvjetima koji u praksi osiguravaju slobodno izražavanje mišljenja birača prilikom izbora njihovih predstavnika;

**Stavak (7.5):** poštivanje prava građana na natjecanje za političku ili javnu dužnost, pojedinačno ili kao predstavnici političkih stranaka ili organizacija, bez diskriminacije;

**Stavak (7.6):** poštivanje prava pojedinaca i skupina na osnivanje, potpuno slobodno, svoje političke stranke ili druge političke organizacije i pružanje takvim političkim strankama i organizacijama potrebnih pravnih jamstava kako bi im se omogućilo međusobno natjecanje na temelju jednakog tretmana pred zakonom i od strane vlasti;

**Stavak (7.7):** osiguravanje da zakon i javna politika djeluju tako da omogućuju vođenje političke kampanje u pravednoj i slobodnoj atmosferi u kojoj ni administrativne radnje, ni nasilje niti zastrašivanje ne onemogućavaju strankama i kandidatima slobodno iznošenje svojih gledišta i kvalifikacija, niti sprječavaju birače u informiranju i raspravljaju o njima ili glasovanju oslobođeni straha od odmazde;

**Stavak (9.1):** svatko ima pravo na slobodu izražavanja, što uključuje i pravo na komunikaciju. Ovo pravo će uključivati slobodu mišljenja i dobivanja i davanja informacija i ideja bez uplitanja javnih vlasti i bez obzira na granice. Ostvarivanje ovog prava može biti predmet jedino ograničenja koja su propisana zakonom i koja su u skladu s međunarodnim standardima. Posebno, nikakvo ograničenje neće biti nametnuto pristupu i korištenju sredstava reproduciranja dokumenata bilo koje vrste, međutim, uz poštivanje prava glede intelektualnog vlasništva, uključujući autorsko pravo;

**Stavak (9.2):** svatko ima pravo na mirno okupljanje i prosvjedovanje. Bilo koje ograničenje koje može biti nametnuto na ostvarenje ovih prava bit će propisano zakonom i u skladu s međunarodnim standardima;

**Stavak (9.3):** pravo udruživanja bit će zajamčeno. [...]

**Stavak (10.1):** poštivanje prava svih, pojedinačno ili udruženo s drugima, slobodnog traženja, dobivanja i iznošenja gledišta i informacija o ljudskim pravima i temeljnim slobodama, što uključuje pravo na širenje i objavljivanje takvih gledišta i informacija.

## **UJEDINJENI NARODI**

### **Međunarodni pakt o građanskim i političkim pravima (ICCPR)**

**Članak 9:** 1. Svatko ima pravo na slobodu i osobnu sigurnost. Nitko ne može biti samovoljno uhićen ili pritvoren. Nitko se ne može lišiti slobode osim iz razloga i u skladu sa zakonom predviđenim postupkom.

**Članak 17:** 1. Nitko ne može biti izložen proizvoljnom ili nezakonitom uplitanju u privatni život, obitelj, stan ili prepisku, niti protuzakonitim napadima na čast i ugled. 2. Svatko ima pravo na zakonsku zaštitu od takvog uplitanja ili napada.

**Članak 19:** 1. Nitko ne može biti uznemiravan zbog svojeg mišljenja. 2. Svatko ima pravo na slobodu izražavanja; to pravo obuhvaća slobodu traženja, dobivanja i širenja informacije i misli svake vrste, bez obzira na granice, bilo usmeno, pismeno, putem tiska ili u umjetničkoj formi, ili bilo kojim drugim sredstvom po svom izboru. 3. Ostvarivanje prava predviđenih u stavku 2. ovog članka nosi sa sobom posebne dužnosti i odgovornosti. Zbog toga ono može biti podložno određenim ograničenjima koja moraju biti utvrđena zakonom i biti neophodna: a) za poštivanje prava ili ugleda drugih osoba; b) za zaštitu državne sigurnosti ili javnog reda, ili javnog zdravlja ili morala.

**Članak 20:** 2. Svako pozivanje na nacionalnu, rasnu ili vjersku mržnju koje predstavlja poticanje na diskriminaciju, netrpeljivost ili nasilje treba biti zabranjeno zakonom.

**Članak 26:** Sve su osobe jednake pred zakonom i imaju pravo, bez ikakve diskriminacije, na jednaku zakonsku zaštitu. Zakon treba zabraniti svaku diskriminaciju i jamčiti svim osobama jednaku i djelotvornu zaštitu protiv diskriminacije bilo po osnovi rase, boje kože, spola, jezika, vjere, političkog i drugog mišljenja, nacionalnog i društvenog podrijetla, imovine, roda ili bilo kojeg drugog statusa.

## Odbor za ljudska prava – Opći komentar 16

**Stavak 10:** Prikupljanje i čuvanje osobnih informacija na računalima, u bankama podataka i drugim sredstvima, bilo od strane javnih vlasti ili privatnih pojedinaca ili tijela, mora se regulirati zakonom. Država mora poduzeti učinkovite mjere kojima će osigurati da informacije **koje se tiču** privatnog života osobe ne dospiju u ruke osoba koje nisu zakonom ovlaštene dobiti ih, obrađivati ili koristiti, te da se nikad ne koriste u svrhu koja nije u skladu s ovim Paktom. Kako bi ostvario najučinkovitiju zaštitu svog privatnog života, svaki pojedinac treba imati pravo ustanoviti, u razumljivom obliku, jesu li, i ako jesu, koji su osobni podaci pohranjeni u automatskim datotekama podataka, i u koju svrhu.

## Odbor za ljudska prava – Opći komentar 25

**Stavak 8:** Građani također sudjeluju u vođenju javnih poslova vršenjem utjecaja kroz javnu raspravu i dijalog sa svojim predstavnicima ili svojim kapacitetom organiziranja.

**Stavak 11:** Kampanje obrazovanja i registracije birača potrebne su kako bi se osiguralo učinkovito ostvarivanje prava informirane zajednice iz članka 25.

**Stavak 12:** Sloboda izražavanja, okupljanja i udruživanja temeljni su uvjet za učinkovito ostvarenje prava glasovanja i mora biti potpuno zaštićena. Trebaju se poduzeti pozitivne mjere za prevladavanje specifičnih teškoća, kao što su nepismenost, jezične barijere, siromaštvo, ili prepreke slobodi kretanja koje sprječavaju osobe s pravom glasa u učinkovitom ostvarivanju svojih prava. Informacije i materijali o glasovanju trebaju biti na raspolaganju na manjinskim jezicima.

**Stavak 19:** Biračima treba omogućiti neovisno formiranje mišljenja, slobodno od nasilja ili prijetnje nasiljem, prisile, navođenja ili manipulativnog uplitanja bilo koje vrste. Ozbiljna ograničenja na troškove kampanje moraju biti opravdana tamo gdje je to potrebno kako bi se osiguralo neugrožavanje slobodnog izbora birača ili neometanje demokratskih procesa neproporcionalnim troškovima u ime bilo kojeg kandidata ili stranke.

**Stavak 25:** Kako bi se osiguralo puno ostvarenje prava zaštićenih člankom 25, od ključnog je značaja slobodno prenošenje informacija i ideja o javnim i političkim pitanjima između građana, kandidata i izabranih predstavnika. To podrazumijeva slobodan tisak i druge medije sposobne komentirati pitanja od interesa javnosti bez cenzure ili ustezanja te informiranje javnog mnijenja o njima.

## Odbor za ljudska prava – Opći komentar 34

**Stavak 15:** Države potpisnice trebaju uzeti u obzir opseg u kojem je razvoj informacijskih i komunikacijskih tehnologija, kao što su internet i sustavi širenja **elektronskih** informacija putem mobilnih aparata znatno promijenio prakse komunikacije diljem svijeta. Sada je to globalna mreža za razmjenu ideja i mišljenja koja se ne oslanja nužno na tradicionalne posrednike masovnih medija. Države potpisnice trebaju poduzeti sve potrebne korake u jačanju neovisnosti tih novih medija i osiguravanju pojedincima pristupa njima.

**Stavak 19:** Kako bi pravo na pristup informacijama učinile učinkovitim, države potpisnice trebaju proaktivno staviti u javnu domenu vladine informacije od javnog interesa. Države **potpisnice** trebaju učiniti svaki napor u osiguravanju laganog, promptnog, učinkovitog i praktičnog pristupa takvim informacijama. Države potpisnice također trebaju usvojiti potrebne procedure, kojim se omogućuje ostvarenje pristupa informacijama, recimo putem zakona o slobodi informiranja.

**Stavak 41:** Važno je osigurati da se sustavi vladinih subvencija medijskim kućama i objavljivanje vladinih oglasa ne vrše na način da imaju učinak prepreke.

**Stavak 42:** Kažnjavanje medijskih kuća, nakladnika ili novinara samo zato što su kritični prema vladi ili političkom društvenom sustavu koji je vlada usvojila nikada se **ne mogu** smatrati potrebnim ograničenjem slobode izražavanja.

**Stavak 43:** Bilo koja ograničenja na funkcioniranje web-stranica, blogova ili bilo kojih sustava širenja informacija temeljenih na internetu, elektroničkih ili drugih, uključujući sustave potpore takvim komunikacijama kao što su internetski pružatelji usluga ili pretraživači, dopuštena su samo do mjere do koje su u skladu sa stavkom 3. Dopustiva ograničenja općenito trebaju biti vezana uz konkretan kontekst; generičke zabrane rada određenih web-stranica i sustava nisu kompatibilne sa stavkom 3. Također nije u skladu sa stavkom 3. zabranjivati nekoj web stranici ili sustavu širenja informacija objavljivanje materijala samo na temelju toga što bi mogao biti kritičan prema vladi ili političkom društvenom uređenju koji je vlada usvojila.

### Međunarodna konvencija o ukidanju svih oblika rasne diskriminacije (ICERD)

### Konvencija o pravima osoba s invaliditetom (CRPD)

### Konvencija UN-a protiv korupcije (UNCAC)

## **DRUGI REGIONALNI INSTRUMENTI**

**Europska konvencija o zaštiti ljudskih prava i temeljnih sloboda**

**Konvencija Zajednice neovisnih država o ljudskim pravima i temeljnim slobodama**

**Američka konvencija o ljudskim pravima**

**Standardi za slobodan, otvoren i inkluzivan internet, Interamerička komisija za ljudska prava**

**Ugovor o Europskoj uniji**

**Konvencija Vijeća Europe za zaštitu pojedinaca u pogledu automatske obrade osobnih podataka**

**Opća uredba Europske unije o zaštiti podataka**

## **ZAJEDNIČKE DEKLARACIJE, VODEĆA NAČELA I IZVJEŠĆA**

**Zajedničke deklaracije posebnog izvjestitelja UN-a o slobodi mišljenja i izražavanja, OEES-ova predstavnika za slobodu medija, OAS-ova posebnog izvjestitelja o slobodi izražavanja i posebnog izvjestitelja o slobodi izražavanja i pristupu informacijama Afričke komisije za ljudska prava i prava naroda o:**

- Slobodi izražavanja i internetu, 2011.
- Slobodi izražavanja i borbi protiv nasilnog ekstremizma, 2016.
- Slobodi izražavanja i „lažnim vijestima“, dezinformacijama i propagandi, 2017.
- Medijskoj neovisnosti i raznolikosti u digitalnoj eri, 2018.
- Izazovima za slobodu izražavanja u sljedećem desetljeću, 2019.
- Slobodi izražavanja i izborima u digitalnoj eri, 2020.

**UN-ove Smjernice o poslovnom sektoru i ljudskim pravima (HR/PUB/11/04), 2011.**

**Izvešće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja UN-ovog Vijeća za ljudska prava (A/HRC/17/27), 2011**  
*(O ključnim trendovima i izazovima za pravo svih pojedinaca na traženje, dobivanje i prenošenje svih vrsta informacija i ideja putem interneta)*

**Izvešće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja UN-ovog Vijeća za ljudska prava (A/HRC/26/30), 2014**  
*(O pravu na slobodu izražavanja u kontekstima izbora)*

**Izvešće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja UN-ovog Vijeća za ljudska prava (A/HRC/35/22), 2017**  
*(O ulozi pružatelja digitalnog pristupa)*

**Izvešće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja UN-ovog Vijeća za ljudska prava (A/HRC/38/35), 2018**  
*(O reguliranju sadržaja na internetu)*

**Izvešće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja UN-ove Opće skupštine (A/74/486), 2019**  
*(O govoru mržnje)*<sup>116</sup>

**Izvešće UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja (A/HRC/47/25), 2021**  
*(O dezinformaciji i slobodi mišljenja i izražavanja)*

---

<sup>116</sup> Sva UN-ova izvješća UN-ova posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja dostupna su na sljedećoj poveznici: <https://www.ohchr.org/en/issues/freedomofopinion/pages/annual.aspx>

# Aneks 2:

## GLOSAR RELEVANTNIH TERMINA

**Algoritam** – fiksirana serija koraka koje obavlja računalo kako bi riješilo neki problem ili dovršilo zadatak.

**Application programming interface (API)** – sredstvo pomoću kojeg se podaci s jednog web-alata ili aplikacije mogu razmijeniti s drugom ili od nje primiti.

**Umjetna inteligencija (AI)** – kompjuterski programi ‘obučeni’ za rješavanje problema i programi koji ‘uče’ iz podataka koje su oni analizirali, prilagođavajući metode i odgovore na način da podiže točnost do najviše moguće mjere. (Vidi *Machine Learning*)

**Automatizacija** – proces dizajniranja ‘stroja’ za dovršavanje zadatka uz malo ili nimalo čovjekova usmjeravanja.

**Big-data** – veliki skupovi nestrukturiranih ili strukturiranih podataka.

**Big-tech kompanije** – privatni subjekti koji pružaju usluge informacijsko-komunikacijske tehnologije i vlasnici su platformi društvenih mreža.

**Botovi** – računari na društvenim mrežama kojima u potpunosti upravljaju kompjuterski programi i koji su dizajnirani za generiranje objava i/ili djelovanje na sadržaj određene platforme.

**Botnet** – zbirka ili mreža botova koji koordinirano djeluju.

**Crowdsourcing** – prikupljanje ideja ili sadržaja koje postavi skupina ljudi, tipično na internetu.

**Računalna propaganda** – korištenje algoritama, automatizacije i čovjekova djelovanja s ciljem svjesnog distribuiranja obmanjujućih informacija i drugih tipova manipulativnog sadržaja putem društvenih mreža.

**Koordinirano neautentično ponašanje (CIB)** – skupine računara koje djeluju zajedno kako bi obmanule druge o tome tko su ili što rade u internetskom okruženju.

**Cyborg** – odnosi se na čovjeka koji djeluje uz pomoć bota ili bota koji djeluje uz pomoć čovjeka.



**Rudarenje podataka** – proces praćenja velikih količina podataka kombiniranjem alata i statistike i umjetne inteligencije s ciljem prepoznavanja korisnih obrazaca.

**Dark ads** – oglasi koji su vidljivi samo onom tko ih objavi i njegovoj ciljanoj publici.

**Dashboard** – interface koji često daje prepoznatljive grafičke pregledne ključnih pokazatelja performansi relevantnih za određeni cilj. On vizualno prati, analizira i pokazuje ključne pokazatelje, metričke podatke i ključne točke podataka s ciljem praćenja specifičnih procesa.

**Debunking** – proces pokazivanja da je jedna stavka (tekst, slika ili video) manje relevantna, manje točna ili manje istinita nego što se prikazuje.

**Deep fakes** – širenje izmišljenih sadržaja na društvenim mrežama proizvedenih uz korištenje umjetne inteligencije i sintezom različitih elemenata postojećih video ili audiodatoteka, u kojima se, primjerice, pojedinac pojavljuje kako govori riječi ili obavlja radnje koje nisu utemeljene u stvarnosti.

**Dezinformacija** – lažna informacija koja je namjerno kreirana ili proširena s očiglednom svrhom izazivanja štete.

**Doxing** – čin objavlivanja privatne informacije ili one koja osobu identifikira na internetu bez njegove ili njezine privole. Ove informacije mogu sadržavati puna imena, adrese, telefonske brojeve, fotografije i više.

**Echo-chamber** – virtualni prostor, kontekst ili situacija gdje se određene ideje, uvjerenja ili podaci pojačavaju ponavljanjem zatvorene skupine računara koja ne dozvoljava slobodni unos alternativnih ili suprotstavljenih ideja i koncepata.

**Enkripcija** – proces kodiranja podataka tako da ih mogu tumačiti samo namjeravani primatelji.

**Stopa angažmana** – mjerni podaci koji se koriste za opisivanje količine interakcija na internetu – ‘lajkovi’, ‘dijeljenja’, ‘komentari’ – koje dobije neki dio sadržaja.

**Facebook reach** – broj pojedinačnih korisnika koji su vidjeli sadržaj na stranici Facebooka. Facebook pruža dva različita tipa mjerenja dosega: 1) ukupni doseg: broj pojedinačnih korisnika koji su vidjeli neki sadržaj povezan sa stranicom Facebooka tijekom posljednjih sedam dana; 2) naknadni doseg: broj pojedinačnih korisnika koji su vidjeli određeni post na Facebooku u svom ‘News Feedu’. Ove dvije kategorije mogu se podijeliti na: 1) Organiski doseg: broj pojedinačnih korisnika koji su besplatno vidjeli sadržaj; i 2) Plaćeni doseg: broj pojedinačnih korisnika koji su vidjeli sadržaj zato što je

njegova vidljivost dodatno plaćena, bilo pojačavanjem (boosting) ili kupovinom oglasa.

**Fact-checking** – proces utvrđivanja istinitosti i točnosti službenih, objavljenih informacija, npr. izjava političara i vijesti.

**Lažni pratitelji** – anonimni ili lažni računi na društvenim mrežama koji su kreirani s ciljem prikazivanja lažnog dojma popularnosti drugog računa.

**Filter bubble** – proces kojim web-stranice i društvene platforme koriste algoritme za selektivno pretpostavljanje koje informacije neki korisnik želi vidjeti i potom tom korisniku daju informacije na temelju te pretpostavke. Ove pretpostavke web-stranice temelje na informacijama u vezi s korisnikom, kao što je ranije ponašanje u pogledu klikova, povijesti pregleda, povijesti pretraživanja i lokacija.

**Geociljanje** – element koja korisnicima dozvoljava dijeljenje svojeg sadržaja s geografski definiranom publikom. Umjesto slanja generičke poruke da je vidi cijeli svijet, poruke i jezik nekog sadržaja podešeni su tako da budu zanimljivi osobama u određenim gradovima, zemljama i regijama.

**Hashtag** – riječ ili fraza ispred koje stoje ljestve “#” (npr. #izbori) kao način obilježavanja poruka ili kategoriziranja informacija te time olakšavanja pretraživanja za korisnike.

**Informacijski nered** – konceptualni okvir za provjeru obmanjujućih ili manipulativnih tipova sadržaja, kao što su propaganda, laži, teorije zavjere, glasine, prijevare, krajnje pristrani sadržaj, neistine ili manipulirani mediji. Čine ga tri različita tipa: mis-, dez- i mal-informacija.

**Influenser** – korisnik društvene mreže sa značajnim brojem pratitelja koji može promovirati neki trend, temu, kompaniju ili proizvod.

**Instant messages (IM)** – oblik izravnih i u realnom vremenu ostvarenih tekstualnih, glasovnih ili videokomunikacija između dvoje ili više ljudi.

**Manufactured amplification** – doseg ili širenje informacija pojačano korištenjem umjetnih sredstava, što može uključivati čovjekovu ili automatiziranu manipulaciju rezultatima pretraživača i listama trendova, te promociju određenih poveznica ili hashtagova na društvenim mrežama.

**Machine learning** – tip umjetne inteligencije u kojem kompjuteri koriste velike količine podataka za učenje zadataka koje obavljaju na temelju iskustva i ranijih operacija, umjesto da ih je potrebno programirati za to.

**Meme** – fotografije s natpisom koje se šire internetom.

**(Mikro)ciljanje** – tehnika koja koristi podatke o ljudima – demografske, o tome što vole, s kim su povezani, što su kupili, itd. – s ciljem dijeljenja na manje skupine radi promocije sadržaja.

**Mrežna neutralnost** – ideja, načelo ili zahtjev da pružatelji usluge interneta trebaju ili moraju tretirati sve podatke na internetu kao iste, bez obzira na njihovu vrstu, izvor ili odredište.

**Organski sadržaj** – slobodan ili nesponzorirani sadržaj na računima ljudi, sadržaji producirani na društvenim mrežama bez plaćene promocije.

**Organski doseg** – broj pojedinačnih korisnika koji gledaju sadržaj bez plaćene promocije.

**Plaćeni doseg** – broj korisnika koji pogledaju objavljeni plaćeni sadržaj. Plaćeni doseg se općenito širi na mnogo većoj mreži nego organski doseg – poruke potencijalno mogu pročitati ljudi izvan konkretne liste kontakata. Doseg – mjerni podaci kojima se utvrđuje maksimalna potencijalna publika za bilo koju poruku određena računanjem broja pratitelja, podjela objava i dojmova.

**Stopa odgovara** – mjerni podaci za angažman kojim se procjenjuje razina interakcije računa s njihovom publikom na društvenoj mreži, izračunat kao rezultat odnosa između spominjanja na koje je korisnik odgovorio u određenom razdoblju i ukupnog broja spominjanja koje je osoba dobila.

**Scraping** – proces automatskog učitavanja podataka s neke web-stranice ili društvene platforme.

**Tema u trendu** – najviše diskutirane teme i hashtagovi na društvenoj mreži.

**Trolovanje** – čin namjernog postavljanja uvredljivog ili zapaljivog sadržaja internetskoj zajednici s namjerom provociranja čitatelja ili ometanja razgovora.

**Farma trolova** – skupina pojedinaca koji se bave koordiniranim *trolanjem* ili promocijom narativa poput botova.

**Sadržaj koji generira korisnik (UGC)** – tekst, snimak glasa, videomaterijali, fotografije, citati itd., koje kreiraju pojedinac ili skupina korisnika društvene mreže.

**Stopa odgovora (eng. response rate)** - metrika angažiranja koja procjenjuje razinu interakcije naloga s njihovom publikom, izračunata kao rezultat odnosa između spominjanja na koje je korisnik odgovorio u datom razdoblju periodu i ukupnog broja spominjanja koje je primio.

**Povlačenje ili „struganje” podataka (eng. scraping)** - proces izdvajanja analitičkih podataka sa web-stranice ili društvene platforme.

**Tema u trendu (eng. trending topic)** - teme o kojima se najviše raspravlja i koriste heštegovi na društvenoj mreži.

**Trolovanje (eng. trolling)** - čin namjernog postavljanja uvrjedljivog ili zapaljivog sadržaja u online zajednicu s namjerom da se provociraju čitatelji ili ometaju razgovori.

**Farma trolova (eng. troll farm)** - skupina pojedinaca koji se na koordiniran način bave trolovanjem ili promocijom narativa nalik na botove.

**Korisnički generirani sadržaj (eng. User-Generated Content (UGC))** - tekst, glasovni snimak, videosnimci, fotografije, citati itd. koje kreiraju pojedinci ili skupina korisnika društvenih mreža.

Društvene mreže na internetu povele su izborne kampanje u novo doba komunikacija, u kojem birači imaju raširene kanale za izražavanje svojih mišljenja. Iako društvene mreže pružaju prostor biračima za pojačavanje neposrednog sudjelovanja u kampanjama i omogućavaju kandidatima bolje mobiliziranje potpore, korištenje društvenih mreža, pogotovo tijekom izbornih kampanja, nosi sa sobom široki spektar izazova. Neki od njih predstavljaju prijetnje ostvarenju i zaštiti ljudskih prava i temeljnih sloboda, kao i po ukupni integritet izbornog procesa.

Cilj ovih Smjernica je pružiti okvir, prvenstveno ODIHR-ovim izbornim promatračima kako bi na odgovarajući način procijenili utjecaj ključnih aspekata vođenja kampanje na internetu na integritet izbornog procesa i demokratsko vođenje izbornih kampanja. Ti aspekti uključuju aktivnosti kandidata na internetu, širenje određenih tipova sadržaja važnih za izborni proces, političko oglašavanje i oglašavanje tijekom kampanje, i zaštitu privatnih podataka.

