BORBA PROTIV DEZINFORMACIJA U CRNOJ GORI

kroz unapređenje zaštite podataka o ličnosti – pravni nedostaci i prilike

LISTA SKRAĆENICA

AEM – Agencija za elektronske medije

AMU – Agencija za audiovizuelne medijske usluge

AZLP – Agencija za zaštitu ličnih podataka

AVMS – Audiovisual Media Services Directive, Direktiva o audiovizuelnim medijskim uslugama Evropske unije

CIRT – Computer Security Incident Response Team, nacionalni tim za reagovanje na računarske incidente

DMA – Digital Markets Act, Zakon o digitalnim tržištima Evropske unije

DSA – Digital Services Act, Zakon o digitalnim uslugama Evropske unije

DPIA – Data Protection Impact Assessment, procjena uticaja na zaštitu podataka o ličnosti

GDPR – General Data Protection Regulation, Opšta uredba EU o zaštiti podataka o ličnosti

LED – Law Enforcement Directive, Direktiva o zaštiti podataka u oblasti krivičnog gonjenja

NIS 2 – Network and Information Security Directive 2, druga direktiva EU o mrežnoj i informatičkoj bezbjednosti

ZIB – Zakon o informacionoj bezbjednosti

ZZPL – Zakon o zaštiti podataka o ličnosti

SADRŽAJ:

Osnovni pojmovi

Podatak o ličnosti - Svaka informacija kojom se neposredno ili posredno može identifikovati fizičko lice. Na primjer - ime, e-mail, IP adresa, lokacija, genetski ili biometrijski zapis (GDPR, čl. 4(1)).

Posebne vrste podataka - Podaci koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska uvjerenja, članstvo u sindikatu, kao i genetski, biometrijski i zdravstveni podaci. Obrada ovih podataka je načelno zabranjena, osim ako postoji jedna od izričito navedenih izuzetnih osnova (GDPR, čl. 9).

Obrada - Svaka radnja nad podacima o ličnosti – prikupljanje, evidentiranje, organizovanje, čuvanje, mijenjanje, objavljivanje, brisanje itd, bilo automatskim ili ručnim sredstvima (GDPR, čl. 4(2)).

Rukovalac - Fizičko ili pravno lice koje određuje svrhe i sredstva obrade podataka (GDPR, čl. 4(7)).

Obrađivač – Fizičko ili pravno lice koji vrši radnje obrade u ime rukovaoca (GDPR, čl. 4(8)). Profilisanje - Svaka automatizovana obrada podataka radi procjene ličnih aspekata osobe (npr. politički stavovi, interesovanja), posebno za analizu ili predviđanje njenog ponašanja (GDPR, čl. 4(4)).

Automatska obrada (automatizovano donošenje odluka) - Potpuno automatizovan proces koji proizvodi pravne ili slične značajne efekte po lice; licu pripada pravo da zatraži ljudsku intervenciju (GDPR, čl. 22).

Algoritam - Skup programskih pravila/instrukcija koje kompjuter izvršava da bi obradio podatke.

Sistem preporuka - Specifična vrsta algoritamskog modela koji rangira ili sugeriše sadržaj, proizvode ili oglase pojedincu na osnovu prikupljenih ili izvedenih podataka. Ukoliko se odlučivanje zasniva na profilisanju ili automatskoj obradi, potpada pod obaveze iz čl. 22 GDPR-a; vrlo velike platforme dodatno podliježu obavezama transparentnosti prema DSA-u.

Podaci o ličnosti kao sredstvo za širenje dezinformacija

Iako je pravo na privatnost prepoznatno najznačajnijim međunarodnim instrumentima za zaštitu ljudskih prava (poput Univerzalne deklaracije o ljudskim pravima, Međunarodnog pakta o građanskim i političkim pravima, te Evropske konvencije o ljudskim pravima), razvoj i široka primjena tehnologije posljednje dvije decenije donose potpuno novu dimenziju, ali i izazove u zaštiti ovog prava. Prije svega, zaštita podataka o ličnosti, kao jedan od elemenata prava na privatnost, dobija sve više na značaju, imajući u vidu da su savremeni poslovni modeli zasnovani na prikupljanju i analizi velikog obima podataka. Takođe, podaci su osnova i razvoja vještačke inteligencije, tehnologije koja ubrzano mijenja način na koji se edukujemo, informišemo, kreiramo nove sadržaje, itd.

Medijski ekosistem u tom smislu nije izuzetak. Online portali, ali i društvene mreže kao prostori na kojima mediji, i drugi akteri, plasiraju svoje sadržaje, svoje poslovne modele zasnivaju na praćenju ponašanja i profilisanju korisnika, kako bi njihovim preferencama prilagođavali i nudili određene sadržaje ili usluge.

Uticaj ovakvih praksi na ljudska prava, poput slobode izražavanja, prava na privatnost, zaštite od diskriminacije..., tema je tek posljednjih nekoliko godina. Tome je značajno doprinio **slučaj "Kembridž Analitika"**[1], još uvijek najpoznatiji primjer uticaja zloupotrebe ličnih podataka građana za podsticanje širenja dezinfomacija i političke manipulacije. Naime, Kembridž Analitika (eng. Cambridge Analytica), britanska kompanija koja se bavila političkim konsaltingom, nezakonito (bez saglasnosti korisnika) je prikupljala lične podatke na desetine miliona korisnika Facebook-a kako bi se kreirali njihovi psihološki profili i posljedično uticalo na političke odluke i izbore građana. Ovaj uticaj posebno je registrovan u kampanji za predsjedničke izbore u Sjedinjenim Američkim Državama 2016[2], kao i kampanji za Brexit referendum u Velikoj Britaniji,[3] što je izazvalo i reakcije nadležnih organa. Naime, Facebook je kažnjen sa 5 milijardi USD zbog nezakonitog ustupanja podataka korisnika, Mark Zuckerberg svjedočio je pred američkim Kongresom i Evropskim parlamentom, a kompanija Kembridž Analitika (bar u formatu u kome je funkcionisala u vrijeme skandala) zatvorena je 2018.

Pored toga, slučaj Kembridž Analitike podstakao je debate o mikrotargetiranju i političkom oglašavanju, posebno imajući u vidu standarde zaštite podataka o ličnosti, poput onih propisanih **Opštom uredbom o zaštiti podataka EU** (General Data Protection Regulation/ GDPR).[4] Uz to, ovaj slučaj uticao je i na dalji razvoj regulative, prije svega u Evropskoj uniji, koja je 2022. godine usvojila **Akt o digitalnim uslugama** (Digital Services Act/DSA)[5] i **Akt o digitalnim tržištima** (Digital Markets Act/DMA).[6] Kako je primjena ovih regulativa počela tek prošle godine, njihovi efekti i uticaj na prakse prikupljanja informacija o korisnicima biće poznati tek u godinama pred nama.

[1] Vidjeti više na: Cambridge Analytica's black box - Margaret Hu, 2020
[2] CASE STUDY 1: Cambridge Analytica and the 2016 U.S. presidential election Cambridge Analytica and the 2016 U.S. presidential election from Power Dynamics in an Era of Big Data on JSTOR
[3] Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower – POLITICO
[4] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[5] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
[6] REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

Regulatorne intervencije, ali i izvještaji međunarodnih organizacija,[7] sve jasnije ukazuju na vezu između sistema za upravljanje informacijama (kako na nivou država, tako i na nivou korporativnih subjekata) i stanja ljudskih prava i sloboda u jednom društvu. Ključni izazov u slučaju poremećaja u sistemu informisanja (tzv. Information disorders) zapravo jeste zaštita ljudskih prava i sloboda, pa se dezinformacije brže i lakše šire tamo gdje su ljudska prava ograničena, gdje sistem javnog informisanja nije stabilan i kvalitetan, i gdje ne postoji dovoljna raznolikost i nezavisnost medija.[8] Zbog toga, **ljudska prava, a prije svega međunarodni instrumenti i mehanizmi za njihovu zaštitu, predstavljaju jedan od ključnih elemenata borbe protiv dezinformacija.**

Uopšteno govoreći, zaštita od dezinformacija i pravo na zaštitu podataka o ličnosti u digitalnom okruženju u neraskidivoj su vezi, prije svega kroz:

- **Upotrebu podataka o ličnosti za širenje dezinformacija.** Kampanje dezinformacija često se oslanjaju na lične podatke kako bi bile djelotvornije. Na primjer, lični podaci (poput starosti, lokacije, interesa, političkih uvjerenja) se koriste za kreiranje ciljanih dezinformacija, kao što su lažne vijesti prilagođene određenoj grupi (tzv. **mikrotargetiranje**). Podaci prikupljeni sa društvenih mreža ili drugog online ponašanja mogu se koristiti za manipulisanje emocijama ili učvršćivanje predrasuda, čineći ljude podložnijim lažnim informacijama (tzv. **psihološko profilisanje**);

- **Povrede bezbjednosti podataka o ličnosti, poput curenja ili krađe podataka.** U ovakvim slučajevima, podaci se mogu koristiti za lažno predstavljanje pojedinaca na mreži, stvarajući lažne ličnosti koje šire dezinformacije. Mogu se takođe koristiti za pravljenje deepfake ili drugih neistinitih sadržaja koristeći stvarna imena i slike, obmanjujući druge i narušavajući reputaciju pojedinaca.

- **Manipulacije i odsustvo saglasnosti lica.** Kampanje dezinformacija često koriste lične podatke bez odgovarajućeg pristanka, kršeći pravila i načela zaštite podataka kao što su: transparentnost (lica na koja se podaci odnose treba da znaju kako se njihovi podaci koriste); ograničenje svrhe (podaci treba da se koriste samo za legitimne, jasno određene svrhe); minimizacija (mogu se koristiti samo podaci neophodni za određenu svrhu).

Kao što je pomenuto, zloupotreba podataka o ličnosti u svrhe širenja dezinformacija nema uticaj samo na pravo na privatnost korisnika, već i na širi spektar ljudskih prava i sloboda. Algoritmi, prikupljanje podataka velikog obima i ciljano oglašavanje tj. plasiranje prilagođenih sadržaja na društvenim mrežama,[9] nerijetko korisnike navode na "ekstremne" sadržaje i teorije zavere, posljedično ograničavajući i pravo na slobodu misli i slobodu izražavanja. Ukoliko se prikupljaju osjetljivi podaci, poput podataka o etničkom porijeklu, političkom uvjerenju ili seksualnoj orijentaciji, posljedice mogu biti još ozbiljnije – od diskriminacije (na primjer, LGBT+ osobama se ne omogućava pristup nekim uslugama ili proizvodima), do direktnog ugrožavanja fizičke bezbjednosti (na primjer, u odnosu na političke oponente, posebno u zemljama sa istorijom političkog nasilja).[10] Međutim, ono što je zajedničko svim ovim povredama jeste da imaju za osnov isti alat, tj. da se zasnivaju na zloupotrebama podataka o ličnosti građana.

[7] Vidjeti, na primjer, Disinformation and freedom of opinion and expression Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan: The UN Report on Disinformation: a role for privacy | Privacy International, Uncovering the Hidden Data Ecosystem | Privacy International

[8] Ibid. str. 2

[9] Why we're concerned about profiling and micro-targeting in elections. | Privacy International

[10] https://privacyinternational.org/news-analysis/4515/un-report-disinformation-role-privacy

Zbog svega navedenog, u izvještaju Specijalne izvjestiteljke Ujedinjenih nacija za promociju i zaštitu slobode misli i izražavanja, između ostalog se navodi da je zaštita podataka ključna za reorijentaciju poslovnog modela digitalne ekonomije koji podstiče poremećaje u sistemu informisanja i povezane zloupotrebe ljudskih prava. Takođe se preporučuje državama da usvoje snažne zakone o zaštiti podataka i ažuriraju izborne i druge relevantne zakone kako bi ograničile sveprisutno praćenje i ciljanje pojedinaca i njihovih aktivnosti na mreži.[11]

[11] Disinformation and freedom of opinion and expression Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, str. 18.

Zaštita podataka o ličnosti i dezinformacije na Zapadnom Balkanu

U kontekstu Crne Gore, ali i Zapadnog Balkana, gdje se izborni, referendumski i drugi društveno-politički ciklusi smjenjuju gotovo svake druge godine, lični podaci i digitalna infrastruktura postaju ključni alati za oblikovanje javnog mnjenja. Dezinformacije se više ne oslanjaju samo na sugestivni sadržaj, one direktno targetiraju građane kroz dva komplementarna mehanizma. Prvi je ciljana obrada podataka o ličnosti, kojom se građani profilišu prema političkim stavovima, medicinskim uvjerenjima, potrošačkim i finansijskim navikama ili etničkoj pripadnosti. Potom se svakoj ciljnoj grupi plasira prilagođena poruka koja manipuliše percepcijom i ponašanjem javnosti sa ciljem obezbjeđivanja političke, ekonomske ili društvene prednosti onoga ko je plasira. Kvalitet i količina prikupljenih ličnih podataka direktno određuju koliko će poruka biti uvjerljiva i koliko će duboko doprijeti do određene društvene grupe. Drugi mehanizam počiva na informacionoj bezbjednosti - kada su portali, državne baze podataka ili platforme nedovoljno zaštićeni, povećava se i ranjivost za kompromitovanje naloga i curenje podataka, čime se posljedično olakšava brza i široka distribucija manipulativnog sadržaja.

Zapadni Balkan zaostaje za Evropskom unijom i u normativnoj harmonizaciji i u kapacitetima za sprovođenje propisa u oblasti upravljanja informacijama. Nadzorna tijela su finansijski ograničena i podložna političkim uticajima, a kaznene odredbe daleko blaže od evropskih standarda. Istovremeno, globalne onlajn platforme resurse usmjeravaju na tržišta gdje su sankcije visoke i nadzor agilan, ostavljajući region kao „meku zonu" za testiranje dezinformacionih taktika. Ako zaštita podataka o ličnosti ostane parcijalno uređena, a informaciona bezbjednost ne ojača, posljedice prevazilaze povredu privatnosti - podstiče se društvena polarizacija, dodatno urušava povjerenje u institucije, stvaraju se ekonomski gubici kroz finansijske prevare i odvraćanje stranih investicija, a javno zdravlje se izlaže riziku širenjem netačnih medicinskih informacija. Stoga su sveobuhvatno uređena pravila o obradi podataka i čvrsti standardi informacione otpornosti nužan preduslov za efikasno suzbijanje dezinformacija i očuvanje demokratskog i društvenog poretka.

Imajući u vidu navedeno, u tekstu koji slijedi dat je **pregled propisa** relevantnih za ovu oblast u Crnoj Gori, sa ciljem ocjene njihove adekvatnosti za zaštitu građana od širenja dezinformacija zasnovanih na (zlo)upotrebi ličnih podataka.

Zaštita podataka o ličnosti i dezinformacije u Crnoj Gori

Preduslov za efikasnu borbu protiv dezinformacija predstavlja sveobuhvatan regulatorni i institucionalni okvir za upravljanje informacijama. On podrazumijeva elemente zaštite podataka o ličnosti, informacione bezbjednosti, ali i zaštite i efikasne (civilne) kontrole nad sistemom tajnosti podataka. U kontekstu kampanja dezinformacija zasnovanih na profilisanju, svakako najveći je značaj propisa u oblasti zaštite podataka o ličnosti, gdje Crna Gora i dalje kaska za Evropskom unijom, ali i većinom zemalja Zapadnog Balkana (poput Sjeverne Makedonije, Srbije, a od skoro i Albanije i Bosne i Hercegovine), u uspostavljanju savremenih standarda i pravila zaštite prava građana.

Kakvu zaštitu pruža važeći Zakon?

Zakon o zaštiti podataka o ličnosti[12] (u daljem tekstu: Zakon, ZZPL) donijet je 2008. godine, uz parcijalne izmene 2009, 2012. i 2017. godine. Iako je prilikom donošenja bio gotovo doslovna transpozicija tada važeće Direktive 95/46/EC[13], danas zaostaje za standardima koje postavlja Opšta uredba EU o zaštiti podataka o ličnosti (u daljem tekstu: GDPR)[14].

Prema važećem Zakonu o zaštiti podataka o ličnosti, **podatak o ličnosti** je svaka informacija koja se odnosi na određeno ili odredivo fizičko lice – od imena i broja pasoša, do IP adrese, fotografije ili zapisa o zdravstvenom stanju. **Obrada podataka o ličnosti** obuhvata svaku radnju koja se nad tim podacima vrši, automatski ili ne – prikupljanje, evidentiranje, organizovanje, čuvanje, mijenjanje, korišćenje, prosljeđivanje, objavljivanje, blokiranje, brisanje ili uništavanje. **Automatska obrada radi profilisanja** označava svaku automatizovanu radnju kojom se podaci koriste da bi se procijenile lične osobine pojedinca, posebno radi analize ili predviđanja njegovog ponašanja, političkih stavova ili ekonomskih navika. Ovi pojmovi čine zajedničku osnovu za razumijevanje daljih odredbi zakona i ključne su za ocjenu uloge podataka u kampanjama dezinformacija.

U nastavku su izdvojene odredbe koje imaju neposredan značaj za sprečavanje dezinformacija, uz kratku ocjenu njihove efikasnosti.

[12] "Službeni list Crne Gore", br. 079/08 od 23.12.2008, 070/09 od 21.10.2009, 044/12 od 09.08.2012, 022/17 od 03.04.2017, dostupan na linku u nastavku: Zakon o zaštiti podataka o ličnosti

[13] Pun naziv: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, dostupna na linku u nastavku: Directive - 95/46 - EN - Data Protection Directive - EUR-Lex

[14] Dostupna na linku u nastavku: Regulation - 2016/679 - EN - gdpr - EUR-Lex

1. Načela obrade – Zakon prepoznaje zakonitost, poštenje, ograničenje svrhe i minimizaciju podataka.[15] Ta načela su nužna osnova za svaku kasniju kontrolu, ali bez snažnih mehanizama sprovođenja ostaju deklarativna, jer rukovaoci nijesu obavezni da dokažu usklađenost, niti se propisuje procjena uticaja kada se građani profilišu u političke ili komercijalne svrhe.

2. Zabrana neovlašćenog marketinga – Obrada podataka za direktni marketing dozvoljena je samo uz mogućnost prigovora, a za posebne kategorije ličnih podataka zahtijeva se izričita saglasnost.[16] Odredba nominalno pokriva političko oglašavanje, ali ne razlikuje standardno od kompleksnog algoritamskog targetiranja, niti propisuje javnu transparentnost oglasnih kampanja.

3. Prava lica – Građani mogu zatražiti pristup, ispravku ili brisanje sopstvenih podataka u roku od 15 dana.[17] Ipak, u praksi dokazivanje zloupotrebe može biti otežano, jer rukovaoci nijesu obavezni da objasne logiku profilisanja.

4. Ovlašćenja Agencije[18] – Nadzorni organ može da zabrani obradu, naredi brisanje podataka i pokrene prekršajni postupak.[19] Međutim, maksimalna kazna iznosi 20 000 EUR za pravna lica i 2 000 EUR za odgovorno lice[20], što je simbolično u poređenju s profitom koji donosi masovno mikrotargetiranje ili trgovina podacima.

5. Međunarodni transferi – Izvoz podataka dozvoljen je ako država koja prima podatke nudi „odgovarajući nivo zaštite“ ili uz pojedinačnu saglasnost Agencije.[21] U odsustvu jasnih kriterijuma i proaktivnih provjera, baze ličnih podataka mogu završiti u jurisdikcijama u kojima su dezinformacije uobičajena praksa.

6. Specijalni režimi nadzora – Video nadzor, biometrija i identifikacione kartice detaljno su uređeni[22]. Ipak, zakon ne poznaje obavezu prijave povreda podataka, niti se bavi informacionom bezbjednošću servisa koji te podatke čuvaju, ostavljajući digitalne baze ranjivim za eksterne upade i curenja podataka.

GDPR dozvoljava državama članicama da, radi usklađivanja prava na privatnost sa slobodom izražavanja i prava javnosti da bude informisana, predvide posebna odstupanja kada se lični podaci obrađuju isključivo u novinarske svrhe (ili za akademske, umjetničke i književne potrebe). Radi se o tzv. **novinarskom izuzetku** od primjene pravila zaštite podataka o ličnosti, a u praksi to znači da nacionalni zakon može, za taj ograničeni kontekst, ublažiti ili suspendovati pojedine obaveze rukovaoca. Cilj izuzetka nije da medijima omogući bezuslovnu obradu, već da spriječi da striktna primjena svakog pojedinačnog prava onemogući izvještavanje o pitanjima od javnog interesa. Istovremeno, i u tom režimu važe osnovna načela (zakonitost, minimizacija i poštenje obrade), te novinar mora biti u mogućnosti da dokaže da su objavljeni podaci nužni, tačni i proporcionalni svrsi informisanja. U Crnoj Gori trenutno ne postoji sistemski novinarski izuzetak. ZZPL sadrži samo opštu klauzulu da primjena zakona ne smije ugroziti slobodu izražavanja, ali ne definiše konkretne derogativne norme.

[15] Član 2.
[16] Član 15.
[17] Članovi 43 i 44.
[18] Agencija za zaštitu ličnih podataka i slobodan pristup informacijama. Sajt Agencije: Agencija za zaštitu ličnih podataka i slobodan pristup informacijama
[19] Članovi 65 – 71.
[20] Član 74.
[21] Članovi 41 i 42.
[22] Članovi 31-40.

Iako pružaju osnovnu zaštitu, zakonska rješenja su nedjelotvorna u eri dezinformacija. Osnovna nedostaci su nepostojanje obavezne izrade procjene uticaja na zaštitu podataka o ličnosti (DPIA[23]) za obrade koje nose visok rizik, pa političke stranke i marketinške agencije mogu profilisati birače bez prethodne regulatorne provjere. Takođe, profilisanje i automatizovano odlučivanje obrađuju se tek marginalno, bez prava lica na ljudsku intervenciju. Kaznene odredbe su previše blage da bi odvratile velike kompanije od kršenja zakona.

Dakle, važeći zakon obezbjeđuje osnovnu formalnu zaštitu privatnosti, ali nedostaju mu preventivni i odvraćajući mehanizmi potrebni za savremeno digitalno okruženje. Upravo te praznine omogućuju da se lični podaci građana Crne Gore i regiona pretvore u pogonsko gorivo kampanja koje narušavaju povjerenje u institucije, polarizuju društvo i proizvode ekonomske gubitke i rizike po javno zdravlje.

[23] Data Protection Impact Assessment

Da li Nacrt novog zakona najavljuje bolja rješenja?

Usklađivanje propisa o zaštiti podataka sa pravom Evropske unije dio je pregovora u okviru Poglavlja 10 – Informaciono društvo i mediji, koje Crna Gora vodi još od 2014. godine.[24] U decembru 2024. zemlja je privremeno zatvorila ovo poglavlje, pri čemu je EU u Zajedničkoj poziciji[25] ocijenila da su izmene Zakona o zaštiti podataka „u potpunosti usklađene sa relevantnim acquis-om i međunarodnim standardima privatnosti" te pozdravila rad Crne Gore na „novom tehnološkom rješenju za otvaranje podataka u posjedu organa, u skladu sa svim tehničkim specifikacijama i EU standardima". Iako je rad na ovom dokumentu počeo još 2019. godine, Ministarstvo unutrašnjih poslova objavilo je Nacrt Zakona o zaštiti podataka o ličnosti[26] u martu 2024, ali nacrt još uvijek nije ušao u skupštinsku proceduru. Aktuelni Akcioni plan za poglavlje 23[27] kao rok za realizaciju navodi treći kvartal 2025. godine, a kao indikator rezultata označava usvajanje predloga dva propisa – Zakona o zaštiti podataka o ličnosti, kojim će se država uskladiti sa odredbama GDPR-a, i Zakona o zaštiti podataka o ličnosti koji sprovode Uprava policije, državno tužilaštvo i drugi organi za sprovođenje istraga, otkrivanja ili gonjenja učinilaca krivičnih djela ili izvršavanje krivičnih sankcija, koji će predstavljati transpoziciju Direktive o zaštiti podataka u oblasti krivičnog gonjenja (LED Direktive)[28]. U nastavku su nabrojana rješenja iz Nacrta Zakona o zaštiti podataka o ličnosti koja bi potencijalno uticala na suzbijanje dezinformacija.

1. **Eksteritorijalna primena** – Nacrt propisuje da se zakon primjenjuje ne samo na rukovaoce i obrađivače sa sjedištem u Crnoj Gori, već i na one koji su fizički izvan zemlje kada ispunjavaju dva uslova – nude robu ili usluge licima u Crnoj Gori, prate ponašanje lica na teritoriji Crne Gore.[29]

2. **Obavezna procjena uticaja na zaštitu podataka o ličnosti** – Za obrade koje uključuju sistematsko i obimno profilisanje, posebne kategorije podataka ili masovni video nadzor, rukovalac mora prije početka da sprovede DPIA.[30]

3. **Prijava povrede podataka u roku od 72 časa** – Rukovalac je dužan da Agenciju obavijesti najkasnije 72 sata po saznanju o incidentu[31], a da o visokorizičnoj povredi bez odlaganja informiše i pogođena lica.[32]

4. **Tehnička i organizaciona bezbjednost** – Usklađuje se minimum mjera (pseudonimizacija, enkripcija, redovno testiranje) koje rukovaoci moraju da primjenjuju. [33]

[24] Više o ovome dostupno na linku u nastavku: Chapter 10 – Information society and media | EUME
[25] European Union Common Position, chapter 10, December 13, 2024, tekst dostupan na linku u nastavku: https://data.consilium.europa.eu/doc/document/AD-27-2024-INIT/en/pdf
[26] Tekst nacrta dostupan je na linku u nastavku: Nacrt zakona o zaštiti podataka o ličnosti
[27] Dostupan na linku u nastavku: c21079de-5f68-4979-b16a-5420d7382b8d
[28] Pun naziv - Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, tekst dostupan na linku u nastavku: Directive - 2016/680 - EN - Law Enforcement Directive; LED - EUR-Lex
[29] Član 3.
[30] Članovi 62 i 63.
[31] Član 60.
[32] Član 61.
[33] Član 58.

Za razliku od GDPR-a, nacrt zadržava prekršajne kazne do 20 000 EUR za pravna lica i 2 000 EUR za odgovorno lice.[34] Ovi iznosi su i dalje daleko od nivoa koji bi odvratio velike platforme, data brokere ili političke aktere od nelegalnog mikrotargetiranja.

Šta najavljena rješenja znače za oblast dezinformacija? DPIA uvodi obavezu da se rizične kampanje procijene prije lansiranja. Time se bar formalno zatvara prostor za tajno profilisanje birača ili potrošača radi širenja lažnih narativa, ali u praksi bi to i dalje najviše zavisilo od rada Agencije. Takođe, mehanizam prijave povreda podataka u 72 časa stvara vezu između zaštite podataka i informacione bezbjednosti - čim baze „iscure“, Agencija dobija signal da se mogu očekivati zloupotrebe u dezinformacionim kampanjama. Ipak, niski kazneni rasponi znače da se ekonomska računica aktera dezinformacija ne mijenja – trošak potencijalno izrečene kazne se i dalje isplati u poređenju sa profitom ili političkom dobiti.

Iako u velikom dijelu usklađen sa GDPR-om, nacrt ne priža i garancije o političkom oglašavanju propisane Uredbom 2024/900 o transparentnosti političkih oglasa[35], čime „tamni oglasi“ ostaju neregulisani. Takođe, ukoliko nove nadležnosti Agencije ne budu propraćene i dodatnim budžetom, obukama kadrova, kao i formalnom saradnjom sa CIRT-om, Agencijom za sajber bezbednost i regulatorima iz oblasti medija i komunikacija, mogućnost njihove primjene ostaje upitna. Efikasnost ove reforme će se mjeriti i brzinom usvajanja podzakonskih akata, usaglašavanja sektorskih propisa i stvarnim ulaganjem u kapacitete Agencije, a ne samo finalnim tekstom budućeg novog zakona.

[34] Član 100.
[35] Pun naziv - Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, tekst dostupan na linku u nastavku: Regulation - EU - 2024/900 - EN - EUR-Lex

Informaciona bezbjednost – da li su nova rješenja otpornija na dezinformacije?

Zakon o informacionoj bezbjednosti[36] (u daljem tekstu: ZIB) usvojen je u novembru 2024. godine, a stupio na snagu 5. decembra 2024. godine. Time je stavljen van snage raniji Zakon iz 2010. godine, donijet prije prve verzije evropske NIS-direktive[37], pa novi zakon predstavlja prvi pokušaj Crne Gore da svoj režim sajber bezbednosti uskladi sa Direktivom (EU) 2022/2555 (NIS 2).[38]

Novi Zakon je u velikoj mjeri usaglašen sa NIS2 direktivom. U nastavku se nalazi nekoliko rješenja bitnih za oblast dezinformacija:

1. **Klasifikacija „ključnih" i „važnih" subjekata** - Među ključne subjekte svrstani su pružaoci usluga za razmjenu internet saobraćaja, pružaoci usluga računarstva u oblaku, pružaoci usluga data centara, pružaoci mreža za isporuku saobraćaja, pružaoci usluga informaciono-komunikacionih tehnologija, javna uprava i drugi relevantni akteri.[39] Time se infrastruktura koja najčešće služi kao kanal za širenje dezinformacija obavezuje na najstrože mjere zaštite.

2. **Politika upravljanja rizicima i lanac snabdijevanja** - Analiza rizika i politika bezbjednosti onemogućuju da se propusti u trećoj strani opravdavaju kao „viša sila"[40]. Za masovne kampanje manipulacije to znači manju mogućnost zloupotrebe media hostinga i distribu¬cionih mreža.

3. **Trostepeno prijavljivanje incidenata** - Prvo obavještenje CIRT-u i Agenciji za sajber bezbednost najkasnije 24 h.[41] Rani signal o krađi naloga, DDoS-u ili curenju baze omogućava da se proaktivno spriječi masovan rast dezinformacija.

4. **Obavezna ISO/IEC 27001 sertifikacija** - Ključni subjekti moraju uskladiti sisteme sa međunarodnim standardom, čime se smanjuje površina napada za sofisticirane aktere dezinformacija.[42]

[36] Službeni list CG", br. 113/2024, tekst dostupan na linku u nastavku: Zakon o informacionoj bezbjednosti
[37] Pun naziv - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, tekst dostupan na linku u nastavku: Directive - 2016/1148 - EN - EUR-Lex
[38] Pun naziv - Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), tekst dostupan na linku u nastavku: Directive - 2022/2555 - EN - EUR-Lex
[39] Član 19.
[40] Član 16.
[41] Član 30.
[42] Član 18., stav 4.

Zakon odstupa od NIS2 direktive u dva ključna aspekta. Prvi se odnosi na kaznene raspone, koji su u Crnoj Gori na simboličnom nivou u odnosu na one propisane u EU. Potom, odgovornost uprave koju upostavlja Zakon je sužena. NIS2 eksplicitno nalaže da članovi upravnih odbora snose ličnu odgovornost - moraju formalno odobriti politiku informacione bezbjednosti, a u slučaju grubog propusta država može da ih suspenduje ili trajno diskvalifikuje iz obavljanja funkcije. U ZIB-u ta obaveza je znatno uža. Zakon govori o „odgovornom licu u pravnom licu" kojem se za prekršaje može izreći novčana kazna od 30 EUR do 1500 EUR[43], i, tek u slučaju ponavljanja, zabrana obavljanja dužnosti u trajanju od tri do šest mjeseci.[44]

Operativni akti, kao i prateći podzakonski akti, tek treba da se donesu. Iako je rok za imenovanje predsjednika i članova Savjeta Agencije za sajber bezbednost istekao u februaru ove godine, Vlada Crne Gore to do danas nije učinila. Agencija za sajber bezbjednost nema ni vršioca dužnosti direktora, iako je odluku o njenom osnivanju Vlada donijela 19. decembra prošle godine. Zakonom je predviđeno da se direktor imenuje u roku od 90 dana od dana izbora Savjeta Agencije, dok bi do tada poslove direktora obavljao vršilac dužnosti, koga, na predlog ministra javne uprave, imenuje Vlada.[45] Do tada, novi standardi ostaju na deklaratornom nivou. Pomak predstavlja uvođenje sistema rane detekcije incidenata, što podiže prag za masovno širenje dezinformacija. Ipak, dok mehanizam prijavljivanja incidenata može brzo osvijetliti napadnu površinu, bez efikasnih sankcija i obavezne upravljačke kontrole ostaje rizik da ključni subjekti plate prekršaj i nastave sa minimalističkim mjerama zaštite.

Drugi relevantni propisi - EU i Crna Gora

Crnogorski Zakon o audiovizuelnim medijskim uslugama[46] prenosi revidiranu AVMS direktivu[47] i daje Agenciji za audiovizuelne medijske usluge (u daljem tekstu: AMU) nadzor nad platformama za dijeljenje video sadržaja.

Ovaj zakon prvi put uvodi sveobuhvatna pravila za platforme za razmjenu video sadržaja - svaka takva platforma mora se najprije upisati u poseban registar kod AMU-a.[48] Nakon upisa dužna je da uspostavi jasne mehanizme za označavanje i prijavljivanje nezakonitog ili štetnog materijala, da taj sadržaj po službenom nalogu AMU-a ukloni ili ograniči njegovo prikazivanje u Crnoj Gori, te da vodi transparentnu evidenciju o preduzetim radnjama[49].

[43] Članovi 68-70.
[44] Član 70 stav 7.
[45] Više o ovome je dostupno u članku u nastavku: Vlada kasni sa imenovanjima u Agenciji za sajber bezbjednost | BIRN Crna Gora
[46] Službeni listu CG, br. 54/2024, tekst dostupan na linku u nastavku: Zakon o audiovizuelnim medijskim uslugama | PROPISINET.ME | Svi propisi Crne Gore online
[47] Pun naziv - Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, tekst dostupan na linku u nastavku: Directive - 2018/1808 - EN - EUR-Lex
[48] Članovi 124 – 126.
[49] Članovi 128 – 130.

Istovremeno, platforma mora omogućiti verifikaciju uzrasta, roditeljske kontrole i postupak prigovora korisnika, čime se maloljetnici štite od dezinformacija i drugog potencijalno opasnog sadržaja.[50] AMU je ovlašćen da u nadzornom postupku ocijeni da li su preduzete odgovarajuće mere iz člana 130 i, po potrebi, izrekne nalog za uklanjanje spornog videa ili onemogućavanje pristupa crnogorskim korisnicima.

Zakon takođe pooštrava režim reklama – zabranjene su prikrivene i prevarne komercijalne audiovizuelne komunikacije.[51] Obaveza AMU-a da promoviše i preduzima mjere za razvoj medijske pismenosti[52] dodaje preventivni sloj borbi protiv manipulativnih narativa. Ipak, propis i dalje ne sadrži pravila o transparentnosti političkih oglasa, ne uvodi algoritamsku odgovornost platformi i propisuje kaznene raspone koji su daleko ispod onih koje uspostavlaju propisi EU, pa puni odvraćajući efekat ostaje nedostižan.

Za razliku od važećeg režima audiovizuelnih usluga, koji pokriva klasičan video sadržaj i reklamne formate, Zakon o digitalnim uslugama Evropske unije (Digital Services Act, u daljem tekstu: DSA[53]) zahvata same infrastrukturalne procese platformi - obavezuje ih da mapiraju algoritme preporuka, procijene i ublaže „sistemske rizike“ i da objedine sve oglase u javno pretraživoj bazi u kojoj se vide sponzor, budžet i kriterijumi targetiranja. Koliko su zemlje Zapadnog Balkana spremne za takva pravila pokazala je prošlogodišnja regionalna studija[54] koja je analizirala zakone i kapacitete svih WB6 država. Zaključak za Crnu Goru je da, iako formalno najdalje u pregovorima, još nema definisanog budućeg Koordinatora digitalnih usluga, kao ni budžet za nadzor velikih platformi. DSA obaveze u praksi će se preplitati sa Zakonom o digitalnim tržištima Evropske unije (Digital Markets Act, u daljem tekstu: DMA), koji ograničava antikonkurentske prakse „gejtikipera“ i otvara prostor za alternativne, transparentnije preporučivačke sisteme. Crna Gora tek treba da se uskladi sa ovim propisima.

Najzad, Uredba (EU) 2024/900 o transparentnosti političkog oglašavanja postavlja obaveznu oznaku „politička reklama“, javni registar oglasa i zabranu targetiranja na osnovu posebnih vrsta podataka o ličnosti. Nijedan crnogorski propis još ne preuzima te odredbe, pa „tamni“ politički oglasi mogu da ostanu nevidljivi regulatoru i javnosti.

[50] Član 130.
[51] Član 68 stav 2.
[52] Član 141.
[53] Pun naziv - Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), tekst dostupan na linku u nastavku: Regulation - 2022/2065 - EN - DSA - EUR-Lex
[54] „Towards a Feasible Implementation of the Digital Services Act in the Western Balkans”, koju su objavili Partneri Srbija. Studija je dostupna na linku u nastavku, deo relevantan za Crnu Goru dosupan je na stranicama 76-85 - dsa-wb-new.pdf

Preporuke

Na osnovu navedenog pregleda domaćih i relevantnih EU propisa, u nastavku dajemo set preporuka za različite društvene aktere, a u cilju unapređenja zaštite od dezinformacija zasnovanih na profilisanju, i zloupotrebi podataka o ličnosti građana.

1. Preporuke za državne institucije (Vlada, Skupština, ministarstva):

- Uskladiti zakone sa EU regulativom:
- Hitno usvojiti novi Zakon o zaštiti podataka o ličnosti u skladu sa GDPR-om.
- Uskladiti propise sa DSA/DMA i Uredbom (EU) 2024/900 o političkom oglašavanju, imajući u vidu lokalni kontekst i specifičnosti.

- Ojačati institucionalne kapacitete:
- Osigurati finansijsku i kadrovsku nezavisnost Agencije za zaštitu podataka.
- Izraditi jasan plan zapošljavanja, budžeta i obuke zaposlenih.
- Obezbijediti operativnost Agencije za sajber bezbednost.

- Uvesti obavezne preventivne mehanizme
- Uvesti obavezu izrade procjene uticaja na zaštitu podataka (DPIA) za sve obrade podataka sa visokim rizikom (profilisanje, biometrija, političko targetiranje).
- Uspostaviti obavezan mehanizam za prijavu povrede podataka u kratkom roku.

- Reformisati nadzor nad političkim oglašavanjem:
- Zabrana targetiranja na osnovu posebnih podataka (vjera, etnicitet, seksualna orijentacija).
- Uspostavljanje obaveze označavanja političkih reklama i javnog registra političkih oglasa.

2. Preporuke za nezavisna regulatorna tijela (AZLP, AMU, CIRT)

- Proaktivna kontrola rizičnih obrada:
- Sprovođenje inspekcija na osnovu DPIA izveštaja.
- Uspostavljanje mehanizama za dijeljenje podataka o zloupotrebama između AZLP, AMU i CIRT-a.

- Jačanje algoritamske i medijske transparentnosti:
- AMU bi trebalo da zahtijeva da platforme objavljuju informacije o algoritmima preporuke i targetiranju.
- Pratiti kako mediji i digitalni servisi prikupljaju i koriste podatke za oglašavanje i personalizaciju sadržaja.

- Kreirati nacionalni sistem ranog upozoravanja:
- Uspostaviti digitalni alert sistem koji uključuje medijske regulatore, CIRT, AZLP, tužilaštvo i telekome.

3. Preporuke za medije i civilno društvo

- Obuke za prepoznavanje zloupotreba podataka i dezinformacija
- Organizovati kontinuirane treninge za novinare, urednike i aktiviste o:
  – GDPR i lokalnim zakonima,
  – Mikrotargetiranju i prikrivenim oglasima,
  – Tehnikama osnaživanja digitalne pismenosti.

- Aktivno zagovaranje transparentnosti:
- OCD i novinari da zahtijevaju objavljivanje DPIA izveštaja za kampanje sa javnim uticajem.
- Javna kontrola političkih oglašivača – npr. kroz watchdog projekte.

- Učešće u formiranju regionalnog sistema
- OCD iz Crne Gore treba da intenziviraju saradnju sa partnerima u Srbiji, BiH, Albaniji itd. na uspostavljanju regionale mreže za brzo upozoravanje o dezinformacionim kampanjama.

4. Preporuke za međunarodne aktere (EU, donatori, tech kompanije)

- Tehnička i finansijska podrška reformama:
- Prioritetna podrška u implementaciji GDPR i DSA/DMA kroz ekspertsku pomoć i IT rješenja.
- Podrška opremanju i obuci nadzornih tijela.

- Regionalna saradnja i pritisak na platforme:
- Podstaći velike platforme da primijene DSA standarde i u „malim tržištima“ poput Crne Gore.
- Uključiti Zapadni Balkan u evropske standarde za političko oglašavanje i algoritamsku odgovornost.
- Kreirati mehanizam regionalnog rapid-alert sistema za obavještavanje i razmjenu informacija o prekograničnim kampanjama dezinformacija.


25
GODINA
CDT
BRANIMO
DEMOKRATIJU


PARTNERI
SRBIJA