

ANALIZA DIGITALNA PRAVA I SLOBODE - IZAZOVI I PRIJETNJE

MEDIJSKA ASOCIJACIJA JUGOISTOČNE EVROPE
AUTOR: ADVOKAT VESELIN RADULOVIĆ



Reporting

**Digital Rights
& Freedoms**



Funded by
the European Union

ANALIZA

DIGITALNA PRAVA I SLOBODE - IZAZOVI I PRIJETNJE

CRNA GORA

Autor: Advokat Veselin Radulović

April 2025. godine

O autoru

Advokat Veselin Radulović položio je Pravosudni ispit u Podgorici pred Komsijom Ministarstva pravde Crne Gore u februaru 2003. godine. U periodu od juna 1994. godine do maja 2000. godine radio je u Ministarstvu unutrašnjih poslova Crne Gore kao inspektor za suzbijanje privrednog kriminaliteta i kao inspektor za suzbijanje krivičnih djela krađe. U periodu od 18.01.2005. godine do 07.06.2007. godine radio je u organima lokalne samouprave Glavnog grada na poslovima šefa pravne službe i inspektora za drumski saobraćaj. Od juna 2007. godine bavi se advokaturom u oblastima krivičnog, građanskog, prekršajnog, ustavnog i upravnog prava. Za vrijeme bavljenja advokaturom branio je i zastupao više pravnih i fizičkih lica u krivičnim, parničnim, prekršajnim, ustavnosudskim, upravnim i upravnosudskim postupcima.

U 2013. godini bio je pravni savjetnik Anketnog odbora Skupštine Crne Gore, formiranog radi parlamentarne istrage povodom afere „Snimak“. Autor ili ko-autor je više desetina istraživanja u stručnoj oblasti, a kao pravni savjetnik ili konsultant učestovao je u brojnim projektima monitoringa postupanja pravosuđa.

Izdavač: Medijska Asocijacija Jugoistočne Evrope
Trg Nezavisnosti BB, 81000 Podgorica
www.masee.org

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of MASE and do not necessarily reflect the views of the EU.



UVOD

Dezinformacije i strani uticaji predstavljaju ozbiljne izazove i prijetnje za crnogorsko društvo. Nedovoljni mehanizmi zaštite omogućavaju ugrožavanje državne bezbjednosti, ograničavanje digitalnih sloboda, ali i njihovu zloupotrebu koja se manifestuje kroz ugrožavanje privatnosti, govor mržnje, ugrožavanje sigurnosti i pozivanje na nasilje.

Digitalna prava i slobode u savremenom društvu su postali neophodni za jačanje osnovnih ljudskih prava u virtuelnom prostoru. Međutim, u društvu poput crnogorskog, sa izraženim političkim podjelama i tenzijama, digitalni prostor sve više se koristi za podsticanje i širenje dezinformacija, govora mržnje, ali i podsticanje sukoba i nasilja.

Dakle, ubrzan razvoj digitalnih medija omogućava bržu razmjenu informacija i globalnu dostupnost sadržaja, ali donosi sa sobom i nove izazove jer istovremeno omogućava nove načine i metode ugrožavanja državne bezbjednosti i vitalnih interesa, doprinosi lakšem širenju govora mržnje, propagandama, podsticanju podjela, pa čak i promovisanju nasilja i pozivanju na nasilje.

U digitalnoj eri, gdje se javna komunikacija i dijeljenje informacija velikim dijelom ostvaruju putem interneta i društvenih mreža, zaštita slobode izražavanja dobija dodatno na značaju. Na današnjem stepenu digitalnog i tehnološkog razvoja, ne samo novinari i mediji, već i svaki pojedinac, mogu javno širiti i dobijati informacije. Ipak, tako je i mogućnost zloupotrebe prava na slobodu izražavanja značajno veća.

Društvene mreže su preuzele glavnu ulogu u dijeljenju informacija i javnom govoru. To nameće veću odgovornost digitalnih platformi kod javnog objavljivanja nekog sadržaja, odnosno uspostavljanje djelotvornih mehanizama za moderaciju i provjeru činjenica. Ova odgovornost podrazumijeva sprječavanje širenja lažnih vijesti i suzbijanje govora mržnje i sajber prijetnji.

Zato rad digitalnih medija treba regulisati na način koji štiti slobodu izražavanja, ali i osigurava odgovornost u komunikaciji i prenosu informacija, kako bi se uspostavio balans između slobode govora, zaštite privatnosti, suzbijanja govora mržnje i širenja dezinformacija.

SADRŽAJ

1. Sajber bezbjednost i digitalne slobode	6
2. Sloboda izražavanja	14
3. Pravo na privatnost i zaštita ličnih podataka	21
4. Preporuke za unapređenje	26

1.

SAJBER BEZBJEDNOST I DIGITALNE SLOBODE

Glavni propisi koji definišu oblast sajber bezbjednosti u Crnoj Gori su: Zakon o informacionoj bezbjednosti, Zakon o tajnosti podataka, Zakonik o krivičnom postupku, Zakon o potvrđivanju Konvencije o računarskom kriminalu, Zakon o agenciji za nacionalnu bezbjednost, Krivični zakonik, Zakon o elektronskom potpisu, Zakon o elektronskim komunikacijama, Zakon o elektronskoj trgovini, tri strategije sajber bezbjednosti Crne Gore koje se primjenjuju u periodu od 2013. do 2026. godine, Strategija nacionalne bezbjednosti i Strategija odbrane.

Za pitanje sajber bezbjednosti od posebnog su značaja Strategija sajber bezbjednosti (2022-2026) koju je usvojila Vlada Crne Gore u decembru 2021. godine i novi Zakon o informacionoj bezbjednosti koji je stupio na snagu 5.12.2024. godine, a koji je usklađen je sa Direktivom (EU) 2022/2555 Evropskog parlamenta i Savjeta od 14. decembra 2022. godine o mjerama za visoki zajednički nivo sajber bezbjednosti u Uniji, izmjeni Regulative (EU) br. 910/2014 i Direktive (EU) 2018/1972 i prestanku važenja Direktive (EU) 2016/1148 (Direktiva NIS2).

Strategija sajber bezbjednosti Crne Gore 2022-2026 kao operativni cilj koji se odnosi na poboljšanje odgovora na sajber kriminal predviđa izmjene i dopune Krivičnog zakonika kojim bi se sankcionisalo širenje i prenošenje lažnih vijesti i dezinformacija i izmjene i dopune Zakonika o krivičnom postupku, kojim bi se unaprijedio i olakšao istražni postupak. Međutim, izmjenama Krivičnog zakonika iz decembra 2023. godine izmijenjena je radnja krivičnog djela izazivanje panike i nereda^[1] na način kojim se iznošenje ili prenošenje lažnih vijesti ili tvrđenja više ne definiše kao radnja izvršenja krivičnog djela. Tako je širenje dezinformacija faktički dekriminalizovano, iako je kao cilj bilo navedeno da se sankcioniše.

Zakon o informacionoj bezbjednosti propisuje mjere informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema, uključujući sajber bezbjednost, određivanje ključnih i važnih subjekata, upravljanje sajber bezbjednošću, kao i druga pitanja od značaja za informacionu bezbjednost.^[2]

Osnovni principi informacione bezbjednosti su povjerljivost, cjelovitost, dostupnost i zaštita podataka, kao i sajber bezbjednost.^[3]

Zakonom je predviđeno osnivanje Agencije za sajber bezbjednost koja vrši zaštitu mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata, osim organa državne uprave od sajber prijetnji, ozbiljnih sajber prijetnji i incidenata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti kod tih organa i drugih subjekata.^[4] Odluka o osnivanju Agencije donosi se u roku od 15 dana od dana stupanja na snagu zakona,^[5] predsjednik i članovi Savjeta Agencije imenuju se u roku od 60 dana od dana stupanja na snagu zakona,^[6] dok će se imanovanje direktora izvršiti u roku od 90 dana od dana izbora Savjeta Agencije.^[7]

Shodno navedenom, Vlada Crne Gore donijela je Odluku o osnivanju Agencije za sajber bezbjednost^[8] koja obavlja sljedeće poslove:

- 1) prati i analizira primjenu propisa, strategija i akcionih planova u oblasti informacione bezbjednosti i daje predloge i preporuke za unapređenje informacione bezbjednosti;
- 2) prati i analizira propise Evropske unije i država članica Sjevernoatlantskog saveza u oblasti informacione bezbjednosti;
- 3) vrši proaktivno skeniranje mrežnih i informacionih sistema ključnih i važnih subjekata koji nijesu organi državne uprave, uz njihovu prethodnu saglasnost;
- 4) donosi uputstva i procedure koje se sprovode prilikom procjene informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, osim organa državne uprave;
- 5) daje upozorenja, najave i informacije o rizicima i incidentima organima i drugim subjektima, osim organa državne uprave;
- 6) postupa po prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;
- 7) vodi evidenciju o prijavljenim incidentima na mrežnim i informacionim sistemima organa i drugih subjekata, osim organa državne uprave;
- 8) vrši stručni nadzor nad primjenom mjera informacione bezbjednosti kod organa i drugih subjekata, osim organa državne uprave;
- 9) vrši stručni nadzor utvrđivanjem da li ključni subjekti posjeduju sertifikat o ispunjenosti uslova u skladu sa važećim crnogorskim standardom za upravljanje informacionom bezbjednošću MEST ISO/IEC 27001 i da li su zahtijevali periodičnu provjeru ispunjenosti uslova u skladu sa tim standardom;
- 10) učestvuje u implementaciji međunarodnih projekata u oblasti informacione bezbjednosti;
- 11) vrši edukaciju zaposlenih u organima i drugim subjektima u cilju jačanja informacione bezbjednosti;
- 12) sarađuje sa Ministarstvom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize, u skladu sa ovim zakonom;
- 13) u cilju unapređenja informacione bezbjednosti sarađuje sa domaćim i međunarodnim institucijama i organizacijama, kao i privatnim i civilnim sektorom;
- 14) dostavlja Vladi izvještaj o stanju informacione bezbjednosti mrežnih i informacionih sistema organa i drugih subjekata, a naročito ključnih i važnih subjekata koji nijesu organi državne uprave, najmanje jednom godišnje.^[9]

Skupština Crne Gore donijela je i Strategiju nacionalne bezbjednosti^[10] koja, kao jedan od stratejskih interesa Crne Gore, definiše i kontinuirano unapređenje sistema sajber odbrane, bezbjednosti i sigurnosti. Ova Strategija među bezbjednosne izazove rizike i prijetnje navodi i sajber prijetnje kao kompleksno područje koje zahtijeva potpunu sinergiju svih činilaca sistema nacionalne bezbjednosti i potpunu kooperativnost svih imalaca sistema i provajdera usluga.

Skupština Crne Gore donijela je i Strategiju odbrane^[11] koja takođe posebno izdvaja sajber prijetnje kao dio izazova, rizika i prijetnji koji mogu imati implikacije na odbranu. Strategija odbrane prepoznaje da savremeni trendovi ukazuju na porast uticaja sajber i hibridnih izazova i prijetnji, da su sajber napadi posebno kompleksni, s obzirom na to da sajber prostor ne poznaje granice i državni suverenitet, da hibridne prijetnje, koje obuhvataju sinhronizaciju različitih metoda destruktivnog djelovanja, predstavljaju, takođe, značajan rizik i da je njihov cilj destabilizacija i pokušaj diskreditacije demokratskog i ekonomskog razvoja, te ugrožavanje stabilnosti i bezbjednosti zemlje i regiona. Predviđeno je da se planom odbrane definišu mjere i mehanizme za unapređenje sajber bezbjednosti i otpornosti na hibridne prijetnje.

Dalje, 2012. godine formiran je nacionalni Tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore (CIRT.ME) koji je postao član FIRST-a (Forum of Incident Response and Security Teams). Shodno novom Zakonu o informacionoj bezbjednosti, CIRT je inkorporiran u novu Agenciju za sajber bezbjednost koja preuzima i službenike CIRT-a.

Crna Gora je donijela i Zakon o potvrđivanju Konvencije o računarskom kriminalu Savjeta Evrope (Budimpeštanska konvencija), ratifikovala je dodatni Protokol o rasizmu i ksenofobiji (CETS 189), kao i Konvenciju o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja (CETS 201). Nakon ratifikacije Crna Gora je uskladila svoje krivično zakonodavstvo sa odredbama ovih Konvencija, kao i sa Okvirnom odlukom Savjeta

2005/222/ o napadima na informacione sisteme i Okvirnom odlukom Savjeta 32000D0375 o suzbijanju dječije pornografije na internetu. U tom kontekstu Ustav Crne Gore propisuje da su ratifikovani i objavljeni međunarodni ugovori i opšteprihvaćena pravila međunarodnog prava sastavni dio unutrašnjeg pravnog poretka, imaju primat nad domaćim zakonodavstvom i neposredno se primjenjuju kada odnose regulišu drugačije od unutrašnjeg zakonodavstva.^[12]

Međutim, pored napretka u normativnom usvajanju evropskih standarda po pitanju sajber bezbjednosti, Crna Gora i dalje ne posjeduje adekvatne mehanizme za detektovanje sajber prijetnji, kao ni mehanizme za dovoljno brz odgovor, odnosno oporavak od sajber napada. Dodatno, nedostatak eksperata iz oblasti sajber bezbjednosti je prepoznat kao globalan problem, dok je u Crnoj Gori zbog ograničenih ljudskih resursa ovaj problem još izraženiji.^[13]

Crna Gora nema tehničku mogućnost, pravni osnov i nadležni organ koji bi analizirao i blokirao na internetu neki nedozvoljeni sadržaj, odnosno sajtove koji se koriste za vršenje krivičnih djela poput dječije pornografije, terorizma, govora mržnje, ucjenjivanja putem društvenih mreža i sl. Takođe, crnogorski internet servis provajderi nemaju mogućnost gašenja subdomena, odnosno onemogućavanja pristupa stranicama na internetu sa kojih se vrše krivična djela.^[14]

Tzv. medijski zakoni, uključujući i novi Zakon o medijima,^[15] ne bave se problemom dezinformacija, njihovog nekontrolisanog širenja i načina suzbijanja.

U Glavi XXVIII Krivičnog zakonika propisana su krivična djela protiv bezbjednosti računarskih podataka čiji objekt radnje su računarski podatak ili računarski program i sistem i to: oštećenje računarskih podataka i prigrama,^[16] ometanje računarskog sistema,^[17] pravljenje i unošenje računarskih virusa,^[18] računarska prevara,^[19] neovlašćeni pristup računarskom sistemu^[20] i zloupotreba

uređaja i programa.^[21] Tako se i krivičnim pravom štiti korišćenje informacione tehnologije i pruža zaštita njenom funkcionisanju. Za ovu vrstu kriminaliteta koristi se termin kompjuterski kriminalitet i “sajber kriminal”. Ova krivična djela propisana su u Krivičnom zakoniku izmjenama i dopunama zakonika iz 2010. godine^[22] nakon što je Crna Gora 2009. godine donijela Zakon o potvrđivanju Konvencije Savjeta Evrope o računarskom kriminalu (“cyber crime”) iz 2001. godine.^[23] Istovremeno, donešen je i Zakon o potvrđivanju Dodatnog protokola uz ovu Konvenciju^[24] koji sadrži obavezu kažnjavanja akata rasizma i ksenofobije učinjenih putem kompjutera iz 2003. godine.

Međutim, ograničeni kapaciteti institucija i otkrivanju ovih krivičnih djela i identifikaciji njihovih izvršilaca razlog je što 15 godina nakon propisivanja ovih krivičnih djela ne možemo govoriti o značajnijim rezultatima kada je u pitanju suzbijanje ove vrste kriminaliteta.

Napredak tehnologije, digitalnih medija i značaj društvenih mreža u primanju i širenju informacija za posljedicu je imao u praksi i veću i lakšu mogućnost širenja govora mržnje i dezinformacija. Ono što Crnu Goru čini dodatno ranjivom i podložnom širenju govora mržnje, dezinformacija i malignim stranim uticajima jesu nedostatak demokratskih kapaciteta, nedostatak funkcionalnih institucija, nedostatak stručnih kadrovskih kapaciteta, nedovoljna digitalna i medijska pismenost građana, politička nestabilnost i podjele.

U Crnoj Gori ima više medija što je poželjno sa aspekta dalje demokratizacije društva. Ipak, uređivačka politika medija vodi se na osnovu političke i ideološke orijentacije vlasnika od kojih su neki iz drugih država, najčešće iz Srbije. EU je zbog agresije na Ukrajinu uvela sankcije Ruskoj Federaciji koje su obuhvatile i suspenziju emitovanja nekih propagandnih medija. Kao kandidat za članstvo u EU, Crna Gora je suspendovala emitovanje tv kanala Russia Today i Sputnik.^[25] Međutim, zabilježeno je da je Javni medijski servis – Radio televizija Crne Gore u više navrata širio proruske narative i

dezinformacije, dok je portal RTCG bez kritičkog osvrta preuzimao informacije iz ruskih medijskih izvora.^[26] Takođe, na Radiju Crne Gore sukob u Ukrajini ocijenjen je kao proxy posrednički rat dvije velike imperije, Rusije i SAD, koji se preliva preko evropskog prostora i dovedena je u pitanje Rezolucija izglasana u Crnogorskom parlamentu, kojom se osuđuje napad Rusije na Ukrajinu i naglašena ekonomska neisplativost uvođenja sankcija Rusiji.^[27]

Takođe, srpska TV Happy, čiji sadržaj se emituje u Crnoj Gori, primjer je širenja proruske i ratnohušakačke propagande, te govora mržnje, netrpeljivosti i diskriminacije Crnogoraca zbog čega je Savjet Agencije za elektronske medije 2020. godine na tri mjeseca ograničio emitovanje tri emisije te televizije.^[28] Međutim, ovi programi su i dalje mogli da se prate na društvenim mrežama i YouTube kanalu televizije.^[29]

Ovi primjeri pokazuju nedostatke u pravnom i institucionalnom okviru koji onemogućavaju djelotvornu i efikasnu borbu protiv stranog uticaja, širenja dezinformacija i propagande, uključujući i ratnu propagandu, govora mržnje, podržavanja i podsticanja na nasilje.

[1] Član 398. Krivičnog zakonika

[2] Član 1.

[3] Član 3.

[4] Član 6.

[5] Član 74.

[6] Član 75.

[7] Član 76. stav 1.

[8] Odluka je objavljena u "Službenom listu CG", br. 125/2024 od 26.12.2024. godine, a stupila je na snagu 27.12.2024. godine

[9] Član 40. Zakona o informacionoj bezbjednosti i član 3. Odluke o osnivanju Agencije za sajber bezbjednost

[10] "Službeni list CG", br. 85/2018 od 27.12.2018. godine

[11] "Službeni list CG", br. 37/2019 od 1.7.2019. godine

[12] Član 9. Ustava Crne Gore

[13] Izvor: Strategija sajber bezbjednosti 2022–2026, str. 16

[14] Ibid: str. 25

[15] Objavljen u "Službenom listu CG", br. 54/2024 od 11.6.2024. godine, a stupio je na snagu 19.6.2024. godine

[16] Član 349.

- [17] Član 350.
- [18] Član 351.
- [19] Član 352.
- [20] Član 353.
- [21] Član 354.
- [22] "Službenom listu CG", br. 25/2010 od 5.5.2010. godine
- [23] Zakon je objavljen u "Službenom listu CG - Međunarodni ugovori", br. 4/2009 od 20.10.2009. godine
- [24] Ibid
- [25] <https://www.slobodnaevropa.org/a/crna-gora-zabranila-emitovanje-russia-today-i-sputnik/31813054.html>
- [26] Izvor: Komparativna studija Digitalno forenzičkog centra (DFC) „Mehanizmi za borbu protiv dezinformacija“, jun 2024. godine, strana 37, dostupna na: <https://dfc.me/wp-content/uploads/Studija-CG-3.pdf>
- [27] Ibid, strana 38
- [28] Ibid, strana 39
- [29] Ibid, strana 44

2.

SLOBODA IZRAŽAVANJA

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda u članu 10. garantuje pravo na slobodu izražavanja i istovremeno propisuje da se to pravo može podvrgnuti formalnostima, uslovima, ograničenjima ili kaznama propisanim zakonom i neophodnim u demokratskom društvu u interesu nacionalne bezbjednosti, teritorijalnog integriteta ili javne bezbjednosti, radi sprječavanja nereda ili kriminala, zaštite zdravlja ili morala, zaštite ugleda ili prava drugih, sprječavanja otkrivanja obavještenja dobijenih u povjerenju, ili radi očuvanja autoriteta ili nepristrasnosti sudstva.

Ustav Crne Gore propisuje da svako ima pravo na slobodu izražavanja govorom, pisanom riječju, slikom ili na drugi način i da se pravo na slobodu izražavanja može ograničiti samo pravom drugoga na dostojanstvo, ugled i čast i ako se ugrožava javni moral ili bezbjednost Crne Gore.^[1]

Ustav Crne Gore propisuje zabranu izazivanja ili podsticanja mržnje ili netrpeljivosti po bilo kom osnovu^[2] i ova zabrana ne može se ukinuti ili ograničiti ni u vrijeme ratnog ili vanrednog stanja.^[3] Takođe, shodno Ustavu Crne Gore nadležni sud može spriječiti širenje informacija i ideja putem sredstava javnog obavješćavanja, između ostalog, ako je to neophodno radi sprječavanja propagiranja rasne, nacionalne i vjerske mržnje ili diskriminacije.^[4] Zabranjeno je i djelovanje političkih i drugih organizacija koje je usmjereno, između ostalog, na kršenje zajamčenih sloboda i prava ili izazivanje nacionalne, rasne, vjerske i druge mržnje i netrpeljivosti.^[5]

Ustav propisuje i zabranu diskriminacije,^[6] zaštitu privatnosti^[7] i moguća ograničenja slobode izražavanja pravom drugoga na dostojanstvo, ugled i čast, kao i kada se ugrožava javni moral i bezbjednost Crne Gore.^[8] Država garantuje ravnopravnost žene i muškarca i razvija politiku jednakih mogućnosti ovih subjekata,^[9] a posebno su garantovana prava manjinskim narodima i nacionalnim zajednicama na izražavanje, čuvanje, razvijanje i javno ispoljavanje nacionalne, etničke, kulturne i vjerske posebnosti.^[10]

Zakon o elektronskim medijima zabranjuje pružanje audiovizuelnih medijskih usluga kojima se podstiču mržnja ili diskriminacija.^[11] U slučaju kršenja ove zabrane i podsticanja mržnje i diskriminacije moguće je ograničenje emitovanja programa iz Crne Gore, kao i reemitovanje programa iz drugih država.^[12] Takođe, posredstvom komercijalne audiovizuelne komunikacije zabranjeno je promovisanje mržnje ili diskriminacije.^[13] Agencija za elektronske medije vrši nadzor nad primjenom ovog zakona u skladu sa zakonom kojim se uređuje inspeksijski nadzor,^[14] pa može pokrenuti i prekršajni postupak.^[15]

Bitno je istaći da izborna zakonodavstvo ne propisuje nikakve sankcije za učesnike predizbornih kampanja koji u značajnom dijelu političke poruke šalju putem interneta i društvenih mreža i pri tome ne poštuju Ustav i zakone, odnosno koriste govor mržnje, uvreda, kleveta i netolerancije.

Novi Zakon o medijima predstavlja napredak u odnosu na raniji tekst jer je definisano da se primjenjuje na medije koji su osnovani u Crnoj Gori, bez obzira gdje se donose uređivačke odluke.^[16] Tako je izbjegnuta ranija mogućnost da primjenu zakona i odgovornost izbjegnu mediji koji su osnovani u Crnoj Gori, ali kod kojih se uređivačke odluke donose u inostranstvu.

Novi Zakon o medijima po prvi put definiše pojam novinara. Novinarem se smatra fizičko lice koje se bavi prikupljanjem, obradom, oblikovanjem, razvrstavanjem, uređivanjem ili drugom

vrstom intervencije na informacijama koje se objavljuju u medijima, a koje novinarsku djelatnost obavlja kao zaposleni ili na drugi način angažovani u mediju ili kod osnivača medija u Crnoj Gori ili inostranstvu ili koje tu djelatnost obavlja kao slobodno zanimanje. [17] Tako se od stupanja na snagu ovog zakona novinare smatraju i tzv. frilenseri (freelancer) koji posao obavljaju primarno preko interneta i ovaj zakon primjenjuje se i na njih.

Nadležni sud može, na predlog državnog tužioca ili lica koje traži zaštitu prava zbog nezakonito objavljenog sadržaja [18] kojim se krše zakonom zaštićena prava, zabraniti dalje širenje medijskog sadržaja samo u slučajevima kad je to neophodno u interesu zaštite nacionalne bezbjednosti i teritorijalnog integriteta Crne Gore, radi sprečavanja nereda ili vršenja krivičnih djela, zaštite zdravlja i morala, zaštite ugleda ili prava drugih, sprečavanja odavanja povjerljivih informacija ili radi očuvanja autoriteta i nepristrasnosti sudstva. [19] U tom slučaju, sud će zabraniti dalje širenje medijskog sadržaja i naložiti njegovo uklanjanje ili ograničavanje dostupnosti. [20]

Takođe, osnivač internetske publikacije dužan je da ukloni komentar koji predstavlja očigledno nezakonit sadržaj ili kojim se krše zakonom zaštićena prava, bez odlaganja, a najkasnije u roku od 60 minuta od saznanja ili od dobijanja prijave drugog lica da taj komentar predstavlja očigledno nezakonit sadržaj ili da se tim komentarom krše zakonom zaštićena prava. Ako osnivač internetske publikacije ne ukloni takav komentar, lice na koje se odnosi taj komentar može tražiti uklanjanje komentara od nadležnog suda. [21]

U tom kontekstu treba ukazati i da je sud u Strazburu razmatrao i situacije odgovornosti internet portala za komentare koje čitaoci javno postavljaju ispod tekstova. U jednom od takvih predmeta [22] Sud je našao da su u skladu sa standardima domaće pravne mjere koje unaprijed jasno određuju da izdavač medijskog portala osnovanog za komercijalne svrhe može biti odgovoran za očigledno nezakonit sadržaj objavljen na njegovom portalu. Kako je presuda u

ovom predmetu izazvala posebnu pažnju i nedoumice, u drugom predmetu^[23] na istu temu Sud u Strazburu je prikazao okolnosti koje je uzeo kao naročito bitne kad je procjenjivao eventualnu odgovornost izdavača Internet portala za objavljen sadržaj. Te okolnosti odnosile su se na: kontekst u kojem su komentari postavljeni, sadržaj samih komentara, mogućnost odgovornosti autora komentara, mjere preduzete od strane portala (uklanjanje komentara), ponašanje onoga čija su prava eventualno povrijeđena (prijavljivanje, traženje uklanjanja komentara) i posljedice koje je trpio onaj čija su prava povrijeđena komentarom i posljedice koje sankcionisanjem trpi portal, odnosno, njegov izdavač.

Sud u Strazburu takođe je utvrdio da nije u suprotnosti sa standardima slobode izražavanja sankcionisanje političara koji je propustio da obriše javno dostupne komentare napisane na otvorenom Facebook nalogu koji je on koristio za svoju izbornu kampanju, a koji su sadržali govor mržnje.^[24]

Na kraju, postoje i krivična djela koja predstavljaju zloupotrebu prava na slobodu izražavanja i koja se mogu izvršiti putem interneta. Tako Krivični zakonik propisuje krivično djelo povreda ravnopravnosti^[25] koje čini onaj ko zbog nacionalne ili etničke pripadnosti, pripadnosti rasi ili vjeroispovijesti ili zbog odsustva te pripadnosti ili zbog razlika u pogledu političkog ili drugog ubjeđenja, pola, jezika, obrazovanja, društvenog položaja, socijalnog porijekla, seksualne orijentacije, rodnog identiteta, invaliditeta, imovnog stanja ili nekog drugog ličnog svojstva, drugome uskrati ili ograniči ljudska prava i slobode utvrđene Ustavom, zakonima ili drugim propisima ili opštim aktima ili potvrđenim međunarodnim ugovorima ili mu na osnovu ove razlike daje povlastice ili pogodnosti. Teži oblici ovog krivičnog djela postoje ako je djelo učinjeno zbog mržnje prema pripadniku grupe određene na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti i ako to učini službeno lice u vršenju službe.

Krivični zakonik propisuje krivično djelo izazivanje nacionalne, rasne i vjerske mržnje,^[26] koje čini onaj ko javno podstiče na nasilje

ili mržnju prema grupi ili članu grupe koja je određena na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti. Isto djelo postoji i kada se javno odobrava, negira postojanje ili značajno umanjuje težina krivičnih djela genocida, zločina protiv čovječnosti i ratnih zločina učinjenih protiv grupe ili člana grupe koja je određena na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti, na način koji može dovesti do nasilja ili izazvati mržnju prema grupi lica ili članu takve grupe, ukoliko su ta krivična djela utvrđena pravnosnažnom presudom suda u Crnoj Gori ili međunarodnog krivičnog suda. Postoji i teži oblik ovog krivičnog djela s obzirom na sredstvo i način izvršenja^[27] i najteži oblik koji se vrši zloupotrebom položaja ili koji dovede do određenih posljedica.^[28]

Krivični zakonik propisuje i krivično djelo rasne i druge diskriminacije^[29] koje čini onaj ko zbog nacionalne ili etničke pripadnosti, pripadnosti rasi ili vjeroispovijesti ili zbog odsustva te pripadnosti ili zbog razlika u pogledu političkog ili drugog ubjeđenja, pola, jezika, obrazovanja, društvenog položaja, socijalnog porijekla, seksualne orijentacije, rodnog identiteta, invaliditeta, imovnog stanja ili nekog drugog ličnog svojstva krši osnovna ljudska prava i slobode zajamčena opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima od strane Crne Gore. Ovo krivično djelo čini i onaj ko vrši proganjanje organizacija ili pojedinaca zbog njihovog zalaganja za ravnopravnost ljudi ili ko širi ideje o superiornosti jedne rase nad drugom ili propagira mržnju ili netrpeljivost po osnovu rase, pola, invaliditeta, seksualne orijentacije, rodnog identiteta ili drugog ličnog svojstva ili podstiče na rasnu ili drugu diskriminaciju. Krivični zakonik posebno propisuje da ovo krivično djelo postoji kada se putem računarskog sistema čuva, širi ili na drugi način čini dostupnim materijal koji je namijenjen širenju ideja o superiornosti jedne rase nad drugom ili propagiranju mržnje ili netrpeljivosti po osnovu rase, pola, invaliditeta, seksualne orijentacije, rodnog identiteta ili drugog ličnog svojstva ili podsticanju na rasnu ili drugu diskriminaciju. Teži oblik postoji kada se neko djelo izvrši

zloupotrebom položaja ili ako je usljed tih djela došlo do nereda ili nasilja.

U definisanju značenja izraza Krivični zakonik definiše zlonamjerni računarski program kao program koji je napravljen da nanese štetu računaru, računarskoj mreži ili računarskim podacima, koji se bez saglasnosti korisnika ubacuje u računar sa namjerom ugrožavanja povjerljivosti, cjelovitosti ili dostupnosti računarskih podataka, aplikacija ili operativnih sistema ili na neki drugi način ometa rad računara ili računarske mreže.^[30]

Tokom parlamentarnih izbora 2016. godine nekoliko veb-stranica bilo je meta sajber napada, a sistemi za praćenje utvrdili su da su napadi dolazili s velikog broja različitih IP adresa iz više zemalja. Na dan izbora, Agencija za elektronske komunikacije i poštansku djelatnost naložila je svim operaterima da privremeno obustave rad aplikacija za razmjenu poruka Viber i WhatsApp, sa pozivom na Zakon o elektronskim komunikacijama i sa obrazloženjem da je preko ovih aplikacija građanima prosljeđivana neželjena pošta ili nezakoniti marketinški materijal. Ustavni sud Crne Gore je 2019. godine donio odluku kojom je utvrđeno da je nesaglasna sa Ustavom odredba Zakona o elektronskim komunikacijama koji Agenciji za elektronske komunikacije i poštansku djelatnost omogućava da naloži operaterima da obustave internetske i telefonske komunikacije u neograničenom obimu ako smatra da je to „opravdano u slučajevima prevare ili zloupotrebe“. Objavljivanjem odluke Ustavnog suda ta odredba zakona prestala je da važi. Šesnaest građana koji su, kao predstavnici civilnog sektora, bili akreditovani posmatrači parlamentarnih izbora, zbog toga je protiv Agencije za elektronske komunikacije i poštansku djelatnost pokrenulo postupak pred sudom radi naknade nematerijalne štete zbog povrede prava ličnosti, odnosno kršenja prava na slobodu izražavanja i slobodu primanja i širenja informacija poslovne i privatne prirode i onemogućavanja rada na praćenju izbora, dokumentovanja i prijavljivanja nepravilnosti i krivičnih djela, ali i onemogućavanja privatne komunikacije sa porodicom i prijateljima.

Pravnosnažnom presudom Osnovnog suda u Cetinju^[31] usvojen je tužbeni zahtjev ovih građana.

[1] Član 47.

[2] Član 7.

[3] Član 25.

[4] Član 50. stav 2.

[5] Član 55. stav 1.

[6] Član 8.

[7] Član 40.

[8] Član 47.

[9] Član 18.

[10] Član 79.

[11] Član 48. stav 2.

[12] Član 6.

[13] Član 85. stav 3. tačka 2.

[14] Član 12. tačka 9 i član 138.

[15] Član 15. stav 2. Zakona o inspekcijском nadzoru

[16] Član 2.

[17] Član 3. stav 4.

[18] Sadržaj kojim se:

1) podstiče ili omogućava podsticanje nasilnog ugrožavanja ili nezakonite promjene ustavnog uređenja,

2) može ugroziti javno zdravlje ili koji predstavlja ozbiljan rizik po javno zdravlje;

3) može ugroziti ili dovesti u pitanje javna bezbjednost ili koji predstavlja ozbiljan rizik po javnu bezbjednost, nacionalnu bezbjednost i odbranu;

4) javno podstiče izvršenje krivičnog djela terorizma;

5) omogućava ili vrši ratna propaganda i

6) čije je objavljivanje u mediju zabranjeno u skladu sa zakonom

[19] Član 54. stav 1. Zakona o medijima

[20] Član 54. stav 2. Zakona o medijima

[21] Član 44. stav 5 i 6 Zakona o medijima

[22] Delfi AS protiv Estonije, predstavka br. 64569/09

[23] Magyar Tartalomszolgáltatás Egyesülete and Index.hu Zrt protiv Mađarske, predstavka br. 22947/13.

[24] Sanchez protiv Francuske, predstavka br. 45581/15

[25] Član 159. Krivičnog zakonika

[26] Član 370.

[27] Ako je učinjeno prinudom, zlostavljanjem, ugrožavanjem sigurnosti, izlaganjem poruzi nacionalnih, etničkih ili vjerskih simbola, oštećenjem tuđih stvari, sknavljenjem spomenika, spomenobilježja ili grobova

[28] Ako je usljed tih djela došlo do nereda, nasilja ili drugih teških posljedica za zajednički život naroda, nacionalnih manjina ili etičnih grupa koje žive u Crnoj Gori

[29] Član 443.

[30] Član 142. stav 22.

[31] P.br.450/2017 od 16.12.2019. godine

3.

PRAVO NA PRIVATNOST I ZAŠTITA LIČNIH PODATAKA

Kada je u pitanju ova oblast, Crna Gora svoje zakonodavstvo nije uskladila sa Opštom uredbom o zaštiti ličnih podataka - GDPR 2016/679, zbog čega se ne može smatrati da je omogućen nivo zaštite ličnih podataka i ostvarivanje prava na privatnost na način koji imaju građani Evropske unije.^[1]

Za zaštitu ličnih podataka od značaja su odredbe Ustava Crne Gore, ratifikovanih međunarodnih ugovora, Krivičnog zakonika, Zakona o zaštiti podataka o ličnosti, Zakona o slobodnom pristupu informacijama i Zakona o obligacionim odnosima u dijelu propisivanja obaveze naknade štete zbog povrede prava ličnosti.

Nadzornu ulogu u oblasti zaštite ličnih podataka vrši Agencija za zaštitu ličnih podataka i slobodan pristup informacijama.

Izmjenama Krivičnog zakonika iz 2023. godine propisano je novo krivično djelo zloupotreba tuđeg snimka, fotografije, portreta, audio zapisa ili spisa sa seksualno eksplicitnim sadržajem^[2] čiji izvršilac je onaj ko učini dostupnim trećem licu video ili drugi snimak, fotografiju, portret, audio zapis ili spis sa seksualno eksplicitnim sadržajem, bez pristanka lica na koje se spis odnosi, odnosno bez pristanka lica koje je prikazano na snimku, fotografiji ili portretu ili čiji je glas snimljen na audio zapisu. Jedan od težih oblika ovog krivičnog djela postoji kada se djelo učini posredstvom

informaciono-komunikacionih tehnologija ili na drugi način zbog čega su video ili drugi snimak, fotografija, portret, audio zapis ili spis sa seksualno eksplicitnim sadržajem postali dostupni većem broju lica. Od izvršioca ovog krivičnog djela oduzeće se video ili drugi snimci, fotografije, portreti, audio zapisi i spisi, kao i posebni uređaji kojima je učinjeno krivično djelo.

Krivični zakonik propisuje i krivično djelo mamljenje djeteta mlađeg od 14 godina u cilju vršenja krivičnih djela protiv polne slobode.^[3] Izvršilac ovog krivičnog djela je punoljetno lice koje u namjeri izvršenja krivičnih djela silovanja djeteta mlađeg od 14 godina, obljube djeteta mlađeg od 14 godina koje ima duševno oboljenje, zaostali duševni razvoj, drugu duševnu poremećenost, nemoć ili kakvo drugo stanje usljed kojeg ono nije sposobno za otpor, obljube sa djetetom mlađim od 14 godina, obljube djeteta mlađeg od 14 godina zloupotrebom položaja, nedozvoljene polne radnje, podvođenje i omogućavanje vršenja polnog odnosa, posredovanje u vršenju prostitucije i iskorišćavanje djece i maloljetnika za pornografiju, koristeći sredstva informaciono-komunikacionih tehnologija ili na drugi način dogovori susret sa djetetom mlađim od četrnaest godina i preduzme radnje da do tog susreta dođe.

Međutim, primjena ovih krivičnopravnih odredbi u praksi ne pruža potpunu i djelotvornu zaštitu žrtvama jer, kako je već navedeno, Crna Gora nema tehničku mogućnost, pravni osnov i nadležni organ koji bi analizirao i nezavisno od pokretanja i okončanja krivičnog postupka blokirao na internetu neki nedozvoljeni sadržaj, odnosno sajtove koji se koriste za vršenje ovih i drugih krivičnih djela putem društvenih mreža i tako spriječio dalje nastupanje štetnih posljedica za žrtvu.

Još od 2013. godine Krivični zakonik propisuje i krivično djelo neovlašćeno prikupljanje i korišćenje ličnih podataka,^[4] ali se ne definiše posebno slučaj ako se lični podaci prikupe zloupotrebom interneta i informaciono-komunikacionih tehnologija.

Pred crnogorskim sudovima bilo je više stotina tužbenih zahtjeva radi naknade štete zbog kršenja prava na privatnost i objavljivanja identiteta osoba koje su bile pod mjerama samoizolacije zbog COVIDa-19 u proljeće 2020. godine, a što je Ustavni sud ocijenio kao kršenje ustavnog prava na privatnost. Tada su organi vlasti javno objavili lične podatke najmanje 2.000 lica.^[5] Prvom pravosnažnom presudom utvrđena je povreda prava i dosuđena naknada nematerijalne štete građaninu čiji podaci su nezakonito objavljeni u iznosu od 200 eura. Ipak, nadzorni organ – Agencija za zaštitu ličnih podataka ranije nije smatrala da se radi o kršenju prava na privatnost i nezakonitom objavljivanju ličnih podataka.

U aprilu 2021. godine objavljena su imena i prezimena, kao i matični brojevi 62 osobe iz Podgorice koje su zaražene koronavirusom. Protiv jednog zaposlenog Doma zdravlja Podgorica pokrenut je krivični postupak, ali je i on oslobođen optužbi jer je u postupku utvrđeno da su određene kategorije ličnih podataka poslate van zdravstvenog informacionog sistema putem imejla, bez ikakve zaštite putem enkripcije.

Protiv nekadašnjeg direktora Agencije za nacionalnu bezbjednost vodi se krivični postupak zbog zloupotrebe službenog položaja, odnosno nezakonitog prisluškivanja i nadzora političara, sveštenika i novinara u periodu od januara do septembra 2020. godine.

Tokom 2015 i 2016 godine državni organi su se nezakonito miješali u pravo na privatnost građana naredbama za izuzimanje podataka iz telekomunikacionog saobraćaja. Naime, Agencija za zaštitu ličnih podataka po službenoj dužnosti je izvršila inspekcijski nadzor kod mobilnih operatora i utvrdila da su tokom 2015 i 2016 godine sudije za istragu svim mobilnim operatorima u Crnoj Gori dostavili više desetina naloga za izuzimanje tzv. listinga telefonskog saobraćaja za cijelu Crnu Goru ili za pojedine opštine. Nakon obavljenog inspekcijskog nadzora, Savjet Agencije za zaštitu ličnih podataka donio je preporuku da ovakav način izuzimanja zadržanih podataka na osnovu naredbi sudija za istragu koje se odnose na podatke za teritoriju cijele Crne Gore ili pojedine opštine ne

odgovara načelu srazmjernosti i svrsishodnosti, suprotan je pravnom poretku Crne Gore, neetički je i nezakonit. Savjet Agencije je preporučio preispitivanje ovakvog postupanja kako bi se na utemeljen pravno-sistemski način garantovalo ostvarenje ljudskih prava.^[6]

Nakon toga i Vrhovni sud Crne Gore zauzeo je pravni stav^[7] da sudija istragu ne može izdati naredbu za dostavljanje podataka o elektronskom komunikacijskom saobraćaju za teritoriju cijele Crne Gore ili pojedine opštine.

Dakle, s obzirom na sadržaj podataka o tzv. listinzima, tokom dvije godine masovno i proizvoljno su prikupljeni podaci o tome sa kime su građani Crne Gore u određeno vrijeme komunicirali, kojim sredstvom, u kom vremenu, koliko je učestala njihova komunikacija sa određenim licima, kao i o lokaciji na kojoj su se građani u određenom vremenu nalazili, dok im nije bilo dostupno nikakvo sredstvo zaštite od tako proizvoljnog miješanja u njihova prava.

Zbog nezakonitog prikupljanja podataka o privatnom životu, odnosno samoinicijativnog miješanja u pravo na privatnost bez ikakvog obavještenja o mjerama koje se preduzimaju i bez omogućavanja bilo kakve djelotvorne kontrole, četrnaest građana je podnijelo tužbu protiv države Crne Gore radi naknade nematerijalne štete. Pravnosnažnom presudom Višeg suda u Podgorici njima je dosuđena naknada u iznosu od po 200,00 eura.^[8]

Prethodno, dana 7.2.2014. godine Agencija za nacionalnu bezbjednost i Ministarstvo unutrašnjih poslova zaključili su Sporazum o načinu pristupa elektronskoj bazi podataka Ministarstva unutrašnjih poslova,^[9] po kome je Agencija za nacionalnu bezbjednost imala pristup svim evidencijama i registrima Ministarstva unutrašnjih poslova. Prema Sporazumu je Agenciji za nacionalnu bezbjednost omogućen neograničen i stalan pristup svim evidencijama i registrima koje Ministarstvo unutrašnjih poslova vodi, odnosno neograničen i stalan pristup

ličnim i drugim podacima sadržanim u elektronskoj bazi podataka MUP-a bez ikakve kontrole ili bilo kakvog uslova. MUP se obavezao da službenicima ANB-a omogućiti neprekidan pristup službenim evidencijama u kojima su sadržani brojni lični podaci, kao i da izda potreban broj digitanih sertifikata za više službenika ANB-a koji imaju neograničen i stalan pristup ličnim podacima svih građana, bez djelotvorne kontrole na koju građani imaju pravo po vladavini zakona. Pravnosnažnom presudom Osnovnog suda u Podgorici^[10] od 7.6.2019. godine, utvrđeno je da je ovaj sporazum ništavan jer je suprotan prinudnim propisima i to Ustavu Crne Gore, Evropskoj Konvenciji za zaštitu ljudskih prava i sloboda, Zakonu o zaštiti podataka o ličnosti i Zakonu o obligacionim odnosima, kao i stavovima Evropskog suda za ljudska prava.

Svi ovi slučajevi pokazuju da je i sistem zaštite ličnih podataka neefikasan i da nadležni organi, umjesto zaštite prava svih građana, nerijetko preduzimaju radnje kojima se ta prava masovno krše.

[1] Izvor: Strategija sajber bezbjednosti 2022-2026, str. 17

[2] Član 175a

[3] Član 211b

[4] Član 176.

[5] <https://www.vijesti.me/vijesti/drustvo/574937/drzava-krsila-pravo-na-privatnost>

[6] Preporuka Savjeta Agencije za zaštitu ličnih podataka br.06-29-2840-1/16 od 25.05.2016. godine

[7] Su.V.br.413/16 od 13.9.2016. godine

[8] Gž.br.5122/19-17 od 22.12.2020. godine

[9] Sporazum zaveden kod Agencije za nacionalnu bezbjednost pod brojem 250/14-08-11-7 od 07.02.2014. godine

[10] Pbr.1104/19

4.

PREPORUKE ZA UNAPREĐENJE

Set preporuka koje je potrebno sprovesti kako bi se poboljšalo stanje u oblasti digitalnih prava uključuje unapređenje pravnog, regulatornog i institucionalnog okvira, praksi, ali i jačanje svijesti.

1.

Neophodno je aktivnije raditi na podizanju svijesti da je sajber bezbjednost pitanje ljudskih prava i na promovisanju otvorenog, slobodnog i bezbjednog sajber prostora. Poboljšanjem pravnog i institucionalnog okvira treba obezbijediti veći stepen vladavine prava u ovoj oblasti, kao i bolju i djelotvorniju zaštitu ljudskih prava i osnovnih sloboda. U tom smislu treba omogućiti djelotvornu i efikasnu zaštitu od blokade i uskraćivanja pristupa internetu, kako bi se građanima obezbijedilo pravo na slobodan pristup informacijama i pravo na slobodno izražavanje mišljenja.

2.

Istovremeno, jačanjem pravnog i institucionalnog okvira neophodno je povećati i odgovornost za ponašanje u sajber prostoru, obezbijediti djelotvornu zaštitu od nasilja, diskriminacije i govora mržnje na internetu, odnosno blagovremeno i efikasno procesuiranje izvršilaca krivičnih djela. Zakonodavni okvir i njegova primjena u praksi, uz jačanje tehničkih i kadrovskih kapaciteta, treba da omoguće sankcionisanje krivičnih djela koja se vrše putem interneta,

sankcionisanje govora mržnje i pozivanje na nasilje, ali ne i sankcionisanje drugih neistinitih izjava nijesu govor mržnje i poziv na nasilje, jer bi to vodilo nedozvoljenom ograničavanju prava na slobodu izražavanja.

3.

Ojačati stručne kapacitete policije i tužilaštva u cilju otkrivanja krivičnih djela protiv bezbjednosti računarskih podataka i identifikacije njihovih izvršilaca.

4.

Izvršiti detaljnu reviziju zakona i drugih propisa koji regulišu pitanja sajber bezbjednosti i ljudskih prava, uporediti ih sa najboljim standardima i dobrim uporednim praksama i pripremiti konkretne preporuke za unapređenje zakonodavnog okvira. U strateškim dokumentima i javnim inicijativama već su date ideje o tome kako poboljšati krivično, medijsko, izborno i drugo zakonodavstvo u kontekstu hibridnih prijetnji, dezinformacija i pokušaja miješanja od strane stranih aktera. U realizaciji tih inicijativa neophodno je uspostaviti balans sa zaštitom osnovnih ljudskih prava i sloboda. Takođe, neophodno je unaprijediti zakonodavstvo koje štiti lične podatke, kao i zakone koji garantuju pristup informacijama.

5.

Izmijeniti zakonodavni okvir na način kojim će se uspostaviti nadležni organ za analizu i blokadu/gašenje internet stranica koje se koriste za vršenje krivičnih djela, posebno dječje pornografije, ksenofobije, terorizma, širenja vjerske i nacionalne mržnje, kao i za vršenje krivičnih djela kojima se ugrožava državna bezbjednost. Na taj način ograničiti i pristup propagandnim medijima i platformama koje šire govor mržnje, podstiču na nasilje i promovišu

ratnu propagandu, kao i pristup sajtovima i sadržajima koji su prijetnja za nacionalnu bezbjednost.

6.

Definisati odgovornost i sankcije za medije, odnosno on line portale koji nijesu registrovani i promovisati obuke za medije i novinare za prepoznavanje dezinformacija, propagande i govora mržnje.

7.

U zakonskim tekstovima treba definisati pojam dezinformacija i načine borbe protiv dezinformacija, te izraditi strategiju i osposobiti državne institucije za borbu protiv širenja dezinformacija.

8.

Uspostaviti insitucionalni nadzor nad internet publikacijama i portalima i propisati izricanje sankcija za širenje govora koji ne uživa zaštitu.

9.

Neophodno je raditi na poboljšanju medijske pismenosti svih građana i novinara posebno, kao i na edukaciji građana i novinara radi većeg stepena njihove bezbjednosti na internetu. Promijeniti zakonodavni i institucionalni okvir koji će omogućiti da svi vlasnici informacionih sistema budu obavezni da sprovode mjere bezbjednosti kako bi spriječili napade.

10.

Pojačati saradnju i koordinaciju između vlade, privatnog sektora i svih segmenata društva kako bi se pravovremeno i efikasno odgovorilo na sve izazove. Takođe, povećati iznos

finansijskih sredstava namijenjenih za poboljšanje sajber bezbjednosti i uspostavljanje mehanizama za otkrivanje sajber prijetnji, brz odgovor i oporavak nakon sajber napada

11.

Izvršiti analizu prakse Uprave policije, Državnog tužilaštva, te redovnih sudova i sudova za prekršaje u slučajevima širenja mržnje, diskriminacije, ksenofobije i dezinformacija na internetu. U skladu sa tim, uraditi preporuke radi efikasnijeg suzbijanja svih kažnjivih djela iz ove oblasti.

12.

Sprovesti javne kampanje radi ohrabrivanja građana da prijave sve incidente, radi njihove edukacije u cilju zaštite ličnih podataka i bezbjednosti uređaja koje koriste, te zaštite osnovnih ljudskih prava i sloboda, borbi protiv govora mržnje, diskriminacije i nasilja.

13.

Uskladiti zakonodavstvo s opštim propisom EU u oblasti zaštite ličnih podataka – Uredbom o zaštiti ličnih podataka (GDPR 2016/679), kako bi građani Crne Gore imali isti nivo zaštite ličnih podataka ili mogućnosti ostvarivanja prava na privatnost kao građani EU.

14.

Ojačati stručne kapacitete nadzornog organa za oblast zaštite ličnih podataka – Agencije za zaštitu ličnih podataka i slobodan pristup informacijama.