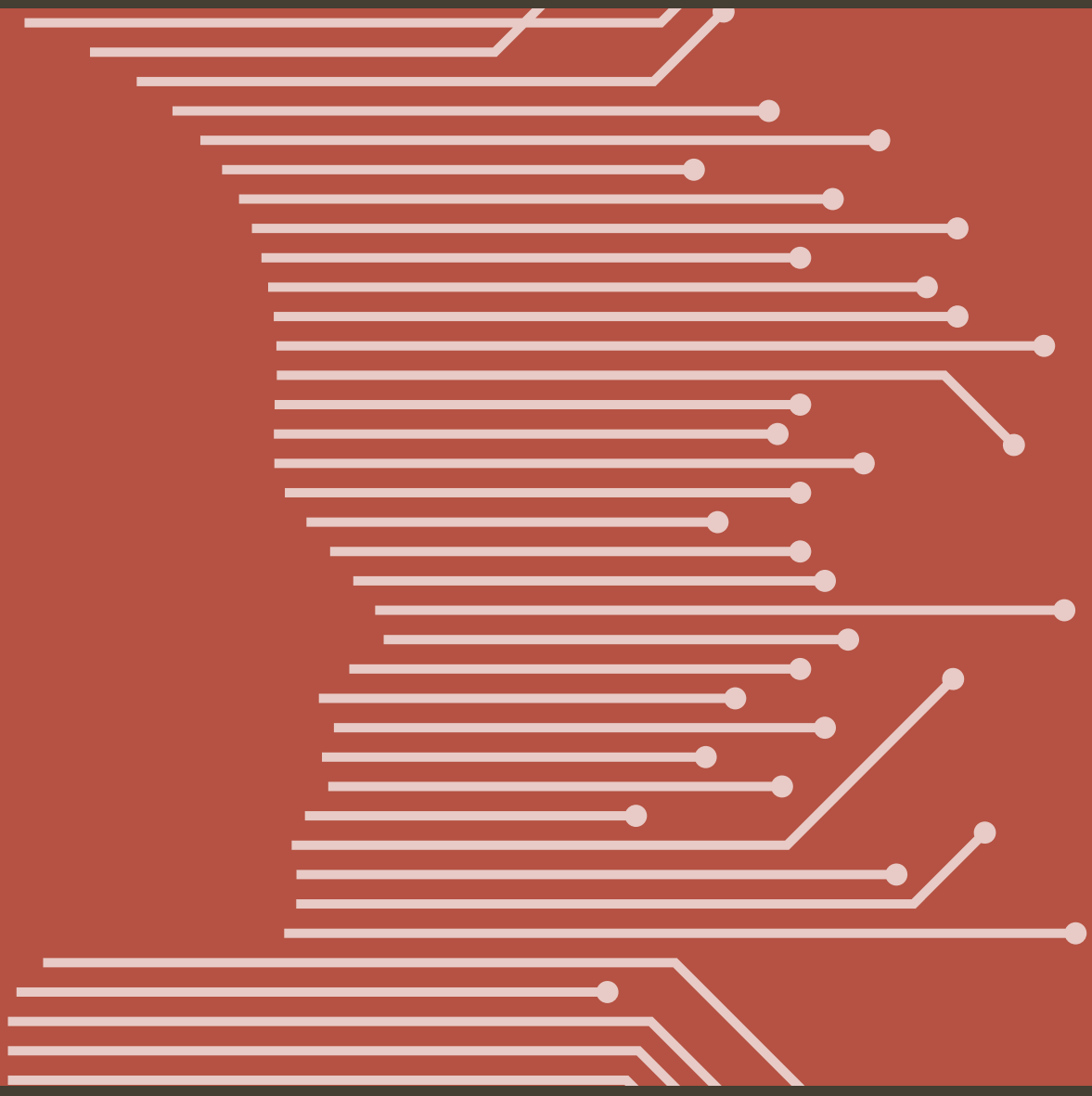
Sajber bezbjednost i ljudska prava na Zapadnom Balkanu

MAPIRANJE NAČINA UPRAVLJANJA I KLJUČNIH AKTERA

Mreža za istraživanje sajber bezbjednosti Zapadnog Balkana



22 GODINE CENTAR ZA DEMOKRATSKU TRANZICIJU

DCAF Geneva Centre for Security Sector Governance

Foreign, Commonwealth & Development Office

Inicijativa DCAF-a – Ženevskog centra za upravljanje sektorom bezbjednosti, u okviru projekta „Dobro upravljanje u sajber bezbjednosti na Zapadnom Balkanu“, podržanog od strane Kancelarije Ujedinjenog Kraljevstva za vanjske poslove, Komonvelt i razvoj (FCDO)

Lajlo Merali i Ena Bavčić | DCAF

DCAF

UVOD

OKVIRI ANALIZE LJUDSKIH PRAVA I SAJBER BEZBJEDNOSTI

OKVIRI ANALIZE LJUDSKIH PRAVA I SAJBER BEZBJEDNOSTI

Baš kako kaže i poslovna izreka, „ne možete ni upravljati onim što ne možete izmjeriti“, tako važi i da „ne možete promijeniti ono što ne mapirate“. Ova važna stvarnost relevantna je za tumačenje veze između sajber bezbjednosti i ljudskih prava na Zapadnom Balkanu.

Definicije sajber bezbjednosti naglasak obično stavljaju na zaštitu imovine države i drugih institucija, kao i na digitalno okruženje.[1] Međutim, ovakve definicije zanemaruju brojne sigurnosne izazove s kojima se pojedinci suočavaju u onlajn okruženju. Ova publikacija istražuje nacionalne politike sajber bezbjednosti u ekonomijama Zapadnog Balkana kroz pristup u smjeren na čovjeka i ocjenjuje nivoe sajber bezbjednosti u smislu zaštite ljudskih prava. Drugim riječima, sajber bezbjednost zavređuje analitički pristup koji je više usmjeren na čovjeka i koji naglasak stavlja ne samo probleme koji utiču na državne aktere, već i na probleme koje ti akteri izazivaju građanima.

Ovakav pristup sajber bezbjednosti, koji je usmjeren na čovjeka, proističe iz šire teorije dobrog upravljanja sektorom bezbjednosti.[2] Dobro upravljanje fokusira se na zaštitu ne samo državnih mreža, sistema i stabilnosti, već i na prava pojedinaca unutar demokratskog društva. Ono obuhvata principe kao što su odgovornost, participacija tj. učešće, inkluzivnost, efektivnost, efikasnost i transparentnost. Ovo vodi ka boljem pružanju usluga koje se tiču bezbjednosti i omogućava demokratski nadzor nad istima, čime se, zauzvrat, sprečava zloupotreba ovlašćenja od strane onih koji su zaduženi da osiguraju bezbjednost. „Sajber bezbjednost” se, stoga, može definisati kao bezbjednost ljudi i njihovih ljudskih prava na internetu, te kao bezbjednost mreža i usluga koje su ključne za ostvarivanje ovog cilja, a koje zajedno štite demokratski poredak i vladavinu prava.

1. Definicija sajber bezbjednosti Međunarodne unije za telekomunikacije (ITU).
2. DCAF, Guide to Good Governance in Cybersecurity [*Vodič za dobro upravljanje u sajber bezbjednosti*] Geneva: Geneva Centre for Security Sector Governance (DCAF); 2021

Dostupan je veliki broj istraživanja o vezama između sajber bezbjednosti i ljudskih prava.[3] Decenijama unazad, aktivisti, članovi akademske zajednice i predstavnici vlada i privatnog sektora rade na tome da definišu šta podrazumijevamo pod „ljudskim pravima u onlajn okruženju", „ljudskim pravima na internetu" i „sajber bezbjednošću i ljudskim pravima".[4] Analizama koje se bave pitanjem sajber bezbjednosti u različitim zemljama takođe se redovno procjenjuje na koji način vlade integrišu postojeće standarde ljudskih prava u onlajn sferu.[5]

U ovoj publikaciji, autori različitih profila razmatraju u kojoj mjeri se ljudska prava trenutno ostvaruju u šest ekonomija Zapadnog Balkana: **Albaniji, Bosni i Hercegovini, Kosovu, Crnoj Gori, Sjevernoj Makedoniji i Srbiji.** U slučajevima gdje su u pogledu određenih prava evidentni izazovi, pomenute analize postavljaju pitanje zašto je to slučaj i ispituju na koji način se principi dobrog upravljanja primjenjuju u svakoj od ekonomija. U analizama se posebno sagledavaju zakoni, prakse i kapaciteti ključnih aktera (sajber) bezbjednosti i aktera koji su predmet nadzora. Zbog čega onda stalno dolazi do kršenja, uključujući i ona na sistemskom nivou, ako imamo međunarodne standarde koji definišu kako ljudska prava treba primjenjivati na nacionalnom nivou? Da li takvi standardi nisu dovoljno jasni ili nisu dovoljno detaljno razrađeni da bi se omogućila njihova primjena u različitim nacionalnim kontekstima? Ili, bolje rečeno, zar se ovi standardi ne razumiju? Kako je moguće da država može da izvrši transponovanje standarda u zakon, a da se isti nakon toga ne primjenjuju?

Kao jedna od vodećih inicijativa projekta DCAF „Dobro upravljanje u sajber bezbjednosti na Zapadnom Balkanu", koji podržava Kancelarija Ujedinjenog Kraljevstva za vanjske poslove, Komonvelt i razvoj (FCDO), Istraživačka mreža za sajber bezbjednost Zapadnog Balkana započela je važnu misiju sprovođenja revolucionarnih istraživanja čiji je cilj da rasvijetli ovu materiju, a koja počinje ovim skupom analiza. Ova publikacija fokus stavlja na mapiranje mogućnosti i izazova u pogledu ljudskih prava u vezi sa sajber bezbjednošću i predstavlja oblast koja u ovom regionu nije nedovoljno istražena.

3. Publikacije organizacije Global Partners Digital (GPD) na CybilPortal.
4. Microsoft's initiative on technology and human rights. [Majkrosoftova inicijativa o tehnologiji i ljudskim pravima].
5. Freedom House Freedom on the Net.

Sam dokument čini šest poglavlja – po jedno za svaku od ekonomija Zapadnog Balkana. Svako od poglavlja počinje osnovnim konceptualnim informacijama o sajber bezbjednosti i kontekstu ljudskih prava u svakoj od ekonomija. Nakon toga, u svakom od poglavlja istražuju se četiri ključna tematska pitanja: sajber bezbjednost i pravo na privatnost, sajber bezbjednost i sloboda izražavanja, sajber bezbjednost i sloboda mirnog okupljanja (i, kad je to relevantno – sloboda udruživanja), te sajber bezbjednost i anti-diskriminacija. Na kraju svakog od poglavlja predstavljene su mogućnosti u pogledu daljih koraka koji se mogu preduzeti, s konkretnim preporukama za ključne aktere.

Koja su to konkretna prioritetna pitanja koja su predmet ovih analiza? Mnogo ih je, ali su u nastavku navedeni neki od primjera.

- **Kad je riječ o Albaniji, Megi Reči i Sara Keljmendi iz Instituta za demokratiju i medijaciju (IDM)** razmatrale su, u načelu jak pravni okvir zemlje u smislu mjera sajber bezbjednosti (čiji je cilj usklađivanje s regulativom EU), kao i njene slabosti u pogledu saradnje u domenu sajber bezbjednosti i razvoju kapaciteta. U ovom poglavlju akcenat se stavlja na različite zakonodavne odredbe koje se odnose na ljudska prava u ovoj zemlji, ali se takođe i skreće pažnja na to da dimenzija sajber bezbjednosti u kontekstu ovih prava ponekad nije razvijena onoliko eksplicitno koliko je potrebno. Neke od preporuka u ovom poglavlju usmjerene su na javne aktere, na primjer, u vezi s neophodnim izmjenama propisa ili specifičnim mjerama koje se odnose na zaštitu podataka, dok su druge usmjerene na aktere koji ne pripadaju javnom sektoru, na primjer – na ulogu koju civilno društvo igra u praćenju kršenja prava i podizanju svijesti.

- **Kad je riječ o Bosni i Hercegovini, Aida Mahmutović i Aida Trepanić iz Balkanske istraživačke mreže (BIRN BiH)** opisuju višestruke prepreke koje su rezultat složenosti pravosudnog sistema u zemlji, a koje građanima otežavaju ostvarivanje ljudskih prava u vezi sa sajber bezbjednošću i dovode do urušavanja povjerenja. One ističu potrebu da lideri u domenu javnih politika prošire svoje razumijevanje ovog koncepta kako bi na bolji način razmotrili implikacije pitanja sajber bezbjednosti na ljudska prava, potrebu da institucije efikasnije sarađuju, kako na domaćem tako i na međunarodnom planu (naročito vladine institucije, ali i civilno društvo), i potrebu za daljom edukacijom aktera u pravosudnom sistemu. Ovo poglavlje govori i o prostoru koji je potrebno otvoriti za dijalog kako bi se pospješila saradnja između zainteresovanih strana.

- **Kad je riječ o Kosovu, Ljuljzim Peci i Valdrin Ukšini iz Kosovskog instituta za politiku i istraživanja (KIPRED)** pojašnjavaju evoluciju pravnog i okvira javnih politika ove države od njenog proglašenja nezavisnosti 2008. godine, iako je pravni okvir i dalje nepotpun, a smjernice u vidu javnih politika pate od manjka konkretnosti. Autori opisuju kako na Kosovu postoji potreba za znatnim razvojem kapaciteta ove države za sajber bezbjednost uopšte i njene veze s ljudskim pravima, te navode da su glavne žrtve sajber kriminala žene, LGBTQI+ zajednica, pripadnici manjinske romske zajednice i druge ranjive grupe. U ovom poglavlju predstavljene su preporuke za kontinuirani institucionalni razvoj Kosova u cilju jačanja poštovanja ljudskih prava u oblasti sajber bezbjednosti.

- **Kad je riječ o Crnoj Gori, Milica Kovačević i Tijana Velimirović iz Centra za demokratsku tranziciju (CDT)** ističu potrebu za podizanjem svijesti o dimenzijama sajber bezbjednosti koje se tiču ljudskih prava, a koje potencijalno mogu predstavljati osnovu za razvoj normi ljudskih prava. Osim toga, autorke primjećuju potrebu za detaljnijim stručnim pregledom zakona i propisa o sajber bezbjednosti koji imaju uticaja na ljudska prava, te za poređenjem istih s dobrim praksama u drugim zemljama. U ovom poglavlju se, takođe, ispituju veze između, s jedne strane, odbrane od hibridnih sajber prijetnji i osiguravanja da se takvim radnjama istovremeno štite ljudska prava, s druge, uključujući sudske, medijske, izborne i druge kontekste koji imaju svoju sajber dimenziju. Takođe, autorke ispituju i implikacije u vezi s iznalaženjem finansijskih sredstava.

- **Kad je riječ o Sjevernoj Makedoniji, Bardil Jašari, Goce Arsovski i Elida Zilbeari iz Metamorfozis fondacije** daju pregled svrsishodnih koraka koje ova zemlja preduzima kako bi unaprijedila sajber bezbjednost, uključujući pravne i političke aspekte usklađivanja sa standardima EU, ali i opisuju slabosti u pogledu implementacije istih. Autori iznose preporuke kako bi se osiguralo snažnije uključivanje komponente ljudskih prava u zakone o sajber bezbjednosti, uz inicijative za obuku i podizanje svijesti i angažman civilnog društva, medija i drugih nevladinih aktera.

- **Kad je riječ o Srbiji, Maja Bjeloš i Marija Pavlović iz Beogradskog centra za bezbednosnu politiku (BCBP)** ukazuju na relativno snažan pravni okvir u vezi sa sajber bezbjednošću u ovoj zemlji, ali primjećuju izazove u pogledu nedostatka kvalifikovanog osoblja i nedostatka obuke, što znači da se ne ide ukorak s napredovanjem tehnologije, te da se država mora baviti brojnim prioritetima koji se nameću kao prioritetni. U poglavlju se napominje da se u dokumentima koji se odnose na sajber bezbjednost, u veoma ograničenoj mjeri pominju žene, LGBTQI osobe, branioci ljudskih prava i novinari i novinarke što svjedoči o kontekstu nedovoljnog razumijevanja inkluzivnih procesa. Uz to, ovo poglavlje opisuje kako se kršenja digitalnih prava građana često tolerišu u vezi sa sajber bezbjednošću, što može imati uticaja na zaštitu ljudskih prava.

Tematski gledano, analiziraju se četiri glavna horizontalna pitanja.

- **Sajber bezbjednost i pravo na privatnost:** Ovo je jedno od pitanja koja se najčešće postavljaju u vezi s ljudskim pravima u domenu sajber bezbjednosti. Autori istražuju da li je došlo do kršenja podataka od strane javnih i/ili aktera koji ne pripadaju javnom sektoru u ekonomiji o kojoj je riječ, kako uredno definisana pravila i norme u pogledu sajber bezbjednosti mogu doprinijeti povećanju prava na privatnost, te kakav je opšti nivo otpornosti na kršenja takvih prava.

- **Sajber bezbjednost i sloboda izražavanja:** Preciznije rečeno – civilna društva u regionu doživljavaju probleme s onlajn cenzurom, klevetom i dezinformacijama, što dovodi do sajber nasilja. Autori istražuju odgovore državnih institucija na ovakva kršenja, kao i potencijalnu uključenost privatnog sektora, akademske zajednice, međunarodnih organizacija i lokalnih organizacija civilnog društva (OCD).

- **Sajber bezbjednost i sloboda mirnog okupljanja i udruživanja:** Autori istražuju u kojoj mjeri su problemi kao što su video nadzor i tehnologije za prepoznavanje lica, gašenja interneta/mobilnih mreža, sajber prijetnje i nasilje nad aktivistima, te problemi s onlajn skupovima bili prisutni u zemljama Zapadnog Balkana. U slučajevima gdje su takvi problemi bili primijećeni, autori dalje istražuju da li su se odnosili na određene vrste okupljanja, koji su akteri bili uključeni i kakav je bio odgovor.

- **Sajber bezbjednost i anti-diskriminacija:** Autori istražuju da li su kršenja sajber bezbjednosti bila ciljano usmjerena na određene grupe i da li su se reakcije razlikovale u slučaju da je riječ o grupama koje su nedovoljno zastupljene. Istraživanje ima za cilj da istraži koliko grupe koje su diskriminisane imaju pristup zaštiti njihove sajber bezbjednosti uopšte.

Ukupno gledano, cilj poglavlja u ovoj publikaciji jeste da pospiješe razumijevanje kapaciteta sajber bezbjednosti u odnosu na specifična prava – prava na privatnost, slobodu izražavanja, slobodu okupljanja i udruživanja, i anti-diskriminaciju – u različitim ekonomijama Zapadnog Balkana. Studija u cjelini ima za cilj da ponudi preporuke za uključivanje standarda ljudskih prava u upravljanje sajber bezbjednošću i za bolju implementaciju normi koje se tiču sajber bezbjednosti u okvirima ljudskih prava u regionu Zapadnog Balkana. A u nastavku ovog dokumenta dajemo pregled za Crnu Goru.

Autorke:
Milica Kovačević i Tijana Velimirović
Centar za demokratsku tranziciju (CDT)

POGLAVLJE 4

CRNA GORA – Podizanje svijesti kao temelj za prilagođavanje pristupa

POGLAVLJE 4

CRNA GORA – Podizanje svijesti kao temelj za prilagođavanje pristupa

OPŠTI KONTEKST SAJBER BEZBJEDNOSTI

Sajber bezbjednost i zaštita podataka u Crnoj Gori regulisani su Zakonom o informacionoj bezbjednosti[6] i Uredbom o mjerama informacione bezbjednosti, koji su usvojeni u decembru 2021. godine. Digitalna transformacija društva dovela je do značajnog povećanja broja slučajeva sajber napada, što je dodatno ukazalo na važnost uspostavljanja adekvatne zaštite kritične infrastrukture i preduzimanja odlučnih koraka u oblasti sajber bezbjednosti, u vidu jačanja nacionalnih kapaciteta za sajber odbranu i odgovor na sajber kriminal.[7]

Crna Gora je posljednjih godina uspostavila niz strateških okvira i organizacionih struktura u oblasti sajber bezbjednosti. Strategija nacionalne bezbjednosti Crne Gore i Strategija odbrane Crne Gore usvojene su u februaru 2020. godine.[8] Nova Strategija sajber bezbjednosti pokriva period 2022–2026, i kao takva dolazi nakon dvije slične strategije koje su implementirane u periodima 2013–2017 i 2018–2021. Najnovija Strategija sajber bezbjednosti Vojske Crne Gore obuhvata period 2019–2022. Nacionalni centar za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore – CIRT (CIRT.ME) formiran je 2012. godine i član je globalnog Foruma za reagovanje na incidente i timove za bezbjednost (FIRST). Uz to, uspostavljena je i mreža CIRT-ova na lokalnom nivou. U Ministarstvu odbrane uspostavljena je organizaciona jedinica za sajber odbranu i odgovor na incidente u vezi s računarskom tehnologijom; ojačani su kapaciteti Agencije za nacionalnu bezbjednost (ANB) i Uprave policije, a osnovan je i Savjet za informacionu bezbjednost.[9]

6. https://www.gov.me/dokumenta/fbb730c5-8c62-47e3-863f-cfaae9631b8d
7. https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0
8. https://www.gov.me/dokumenta/08cb12b5-395e-4047-a1cd-ff884683b9e3
9. https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0

Organi državne uprave koji su prepoznati nacionalnom strategijom sajber bezbjednosti su ANB, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Uprava policije, Direkcija za zaštitu tajnih podataka, CIRT.ME, Ministarstvo prosvjete, nauke, kulture i sporta, Ministarstvo javne uprave, digitalnog društva i medija, te Ministarstvo vanjskih poslova. Predviđene su izmjene i dopune Zakona o informacionoj bezbjednosti i dodatno usklađivanje s Direktivom Evropske unije o bezbjednosti mrežnih i informacionih sistema (NIS Direktiva), kao i osnivanje nove Agencije za sajber bezbjednost.

Agencija za nacionalnu bezbjednost je u strateškim dokumentima prepoznata kao jedna od ključnih institucija odgovornih za kontrolu u oblasti sajber prostora u Crnoj Gori, u skladu sa svojim primarnim fokusom na zaštitu nacionalnih interesa i bezbjednosti. Zakonom kojim se uređuje rad ANB definisane su nadležnosti agencije, koje se prvenstveno odnose na prikupljanje i obradu podataka od značaja za nacionalnu bezbjednost, kao i njen rad u oblasti kontraobavještajne djelatnosti i zaštite važnih objekata i lica.

Tim CIRT-a odgovoran je za postupanje u slučajevima sigurnosnih incidenata koji uključuju računarsku tehnologiju u sajber prostoru Crne Gore. Formiran je 2012. godine kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne unije za telekomunikacije (ITU). CIRT je do novembra 2020. godine bio u sastavu Ministarstva javne uprave, ali je od tada, nakon izmjena Zakona o tajnosti podataka, u nadležnosti Direkcije za zaštitu tajnih podataka. Funkcija nacionalnog CIRT-a je da zaštiti nacionalne mreže od incidenata u vezi sa računarskom bezbjednošću koji proističu sa interneta i drugih rizika u vezi s bezbjednošću informacija. On takođe predstavlja i centralnu tačku kontakta na nacionalnom i međunarodnom nivou za sve incidente u vezi s računarskom bezbjednošću gdje barem jedna od uključenih strana ima sjedište u Crnoj Gori. CIRT radi na rješavanju incidenata, reagovanju i koordinaciji, priprema bezbjednosna upozorenja i savjete za korisnike, te radi na podizanju svijesti i edukaciji korisnika.

Savjet za informacionu bezbjednost ima za cilj praćenje i koordinaciju aktivnosti u oblasti sajber bezbjednosti i rad na predlaganju propisa

Vlada Crne Gore je 2019. godine donijela Odluku kojom je naloženo formiranje Savjeta za informacionu bezbjednost, čiji bi cilj bio praćenje i koordinacija aktivnosti u oblasti sajber bezbjednosti i predlaganje mjera za unapređenje politika, propisa i prakse u ovoj oblasti.[10] Nalazi analize obavljene na nivou Savjeta, uz pomoć strateških partnera, ukazuju je na potrebu za temeljnom reorganizacijom nacionalnog CIRT-a u cilju centralizacije sajber ekspertize, smanjenja odliva stručnjaka, omogućavanja efikasnijeg odgovora na sajber napade i zaštite kritične informacione infrastrukture.[11]

Od pristupanja Crne Gore NATO-u 2017. godine do danas, Ministarstvo odbrane i Vojska Crne Gore uložili su značajne napore u pogledu unapređenja informacione bezbjednosti, naročito u pogledu izgradnje kapaciteta u domenu sajber odbrane, u skladu s nacionalnim i strateškim ciljevima NATO-a. U tom kontekstu, izvršene su promjene u organizacionim strukturama i unutar vojske i u samom ministarstvu, čime se jasno prepoznaje potre ba za jačanjem sajber kapaciteta u odbrambenoj areni.

Ministarstvo javne uprave, digitalnog društva i medija, između ostalog, zaduženo je i za predlaganje i implementaciju politike usmjerene na razvoj informacionog društva; priprema predloge zakona i drugih propisa iz oblasti informacione bezbjednosti; i pruža stručnu pomoć za primjenu informaciono-komunikacionih tehnologija (IKT) u državnoj upravi i drugim državnim organima. Ministarstvo trenutno radi na uspostavljanju okvira za upravljanje informacionim sistemima unutar takvih organa, u skladu s međunarodnim standardima; uspostavlja tehnološku i sigurnosno-informacionu infrastrukturu za ove državne organe; i utvrđuje tehnička i druga pravila koja regulišu njihovo korišćenje IKT.

Crna Gora je ratifikovala niz međunarodno obavezujućih konvencija, pristupila Ujedinjenim nacijama, Organizaciji za evropsku bezbjednost i saradnju (OEBS), NATO-u i FIRST-u, i učestvovala u inicijativama i platformama čiji je cilj jačanje kapaciteta za sajber odbranu. Crna Gora je, takođe, članica Evropskog centra izvrsnosti za suzbijanje hibridnih prijetnji (Hybrid CoE) i NATO-ovog centra izvrsnosti za kooperativnu sajber odbranu (CCDCOE) sa sjedištem u Estoniji, i uzela učešća u brojnim međunarodnim zajedničkim

10. https://www.gov.me/dokumenta/5b254c61-683f-45fa-8925-30d2df8ecb63
11. https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0

vježbama, obukama, sastancima, forumima i konferencijama. Njeno članstvo u pomenutim konvencijama i organizacijama predstavljalo je značajan faktor u oblikovanju nacionalnog pristupa sajber bezbjednosti. Prvi NATO kontrahibridni tim za podršku koji se bavi hibridnim prijetnjama posjetio je Crnu Goru u novembru 2020. godine kako bi pomogao u jačanju sposobnosti zemlje i odgovoru na hibridne izazove.[12] Crna Gora se uključila u EU istraživanje hibridnih rizika, s ciljem identifikovanja sistemskih ranjivosti daljeg konkretnijeg usmjeravanja pomoći koju EU pruža u ovoj oblasti.[13]

Država, međutim, još uvijek nema strategiju za borbu protiv hibridnih prijetnji. Ista je najavljena 2019. godine, ali je nakon promjene vlasti 2020. godine obustavljen rad na ovom strateškom dokumentu. U međuvremenu, naši sagovornici navode da trenutni nivoi zaštite definitivno nisu dovoljni, s obzirom na visoku zastupljenost hibridnih prijetnji, a time i sajber prijetnji. Pojedinci nemaju visok nivo svijesti o sajber prijetnjama i najranjiviji su na društveni inženjering. Ukazano je na potrebu edukacije građana kako bi se povećao stepen njihove bezbjednosti na internetu uopšte, ali je i naglašeno da svi vlasnici informacionih sistema moraju sprovoditi mjere bezbjednosti kako bi spriječili napade.

Postoji očigledna potreba za tijesnom saradnjom u oblasti sajber bezbjednosti između vlade i privatnog sektora, te je neophodna koordinacija svih segmenata društva kako bi se pravovremeno i efikasno odgovorilo na izazove koji postoje u sajber domenu. Vladina strategija sajber bezbjednosti i prateći akcioni plan prepoznaju da su neophodne i veća saradnja i poboljšanje mjera za prevenciju i edukaciju o sajber bezbjednosti u javnom i privatnom sektoru. Strategija skreće pažnju na to da postojeće platforme koje okupljaju privatni i javni sektor (kao što je Naučno-tehnološki park Crne Gore) treba dalje jačati kako bi se obezbijedila obuka, razmjena stručnosti i podsticala saradnja u istraživanjima i razvoju u oblasti sajber bezbjednosti.

12. https://balkans.aljazeera.net/news/balkan/2020/1/17/tim-nato-u-crnoj-gori-zbog-prijetnje-od-ruskih-hibridnih-napada
13. Izvještaj Evropske komisije o napretku Crne Gore za 2021. godinu

I pored postojanja institucionalnog i strateškog okvira, identifikovan je niz izazova koji se tiču implementacije i ostvarivanja rezultata. Ono što je prepoznato kao ključni izazov jeste nedostatak finansijskih sredstava za implementaciju strategije što je posljedica nedovoljne svijesti donosilaca odluka o važnosti ulaganja u sajber bezbjednost. Drugi problem prestavlja nedostatak eksperata i stručnog kadra u ovoj oblasti, koji je naročito izražen u Crnoj Gori kao zemlji sa izuzetno ograničenim ljudskim resursima. U strateškim dokumentima otvoreno stoji da Crnoj Gori nedostaju odgovarajući mehanizmi za otkrivanje sajber prijetnji i mehanizmi za dovoljno brz odgovor ili oporavak nakon napada.

Počinioce sajber kriminala često je teško identifikovati i krivično goniti. Shodno tome, državni organi često djeluju nemoćni u pokušajima da otkriju odakle dolaze napadi i javnosti objasne ko stoji iza njih. Na primjer, u aprilu 2022. godine Crna Gora je bila preplavljena lažnim dojavama da su u zgrade javnih ustanova postavljene bombe, što je dovelo do evakuisanja svih škola u zemlji i izazvalo veliku zabrinutost javnosti. Osim poruka opšteg karaktera koje su nadležni uputili kako bi razuvjerili javnost, rečeno je samo da su „mejlovi poslati sa domena čiji su serveri u inostranstvu, te da nadležni rade na identifikaciji pošiljalaca“.[14]

Crna Gora ne raspolaže niti zakonskim okvirom niti mehanizmima koji su potrebni za blokiranje sadržaja s interneta, čak i kada se čini da su onlajn aktivnosti nedvosmisleno kriminalne prirode, kao što su govor mržnje, prijetnje, promovisanje terorizma, širenje vjerske ili etničke mržnje i dezinformacije, dječja pornografija i slično. Ovaj problem prepoznat je u novoj strategiji, te rješenjima za isti treba dati prioritet, naročito imajući u vidu značajan porast širenja mržnje, diskriminacije, ksenofobije i dezinformacija na internetu, s ciljem podrivanja bezbjednosti i društvene kohezije.

14. https://www.slobodnaevropa.org/a/crna-gora-skole-dojava-bomba-evakuacija/31823151.html

SAJBER BEZBJEDNOST I OKVIRI LJUDSKIH PRAVA

Crna Gora je započela proces uspostavljanja zakonskog okvira za istraživanje slučajeva visokotehnološkog računarskog i sajber kriminala i sankcionisanje počinilaca

Crna Gora je započela proces uspostavljanja zakonodavnog okvira za sprečavanje remećenja rada informaciono-komunikacionih tehnologija, za istragu slučajeva visokotehnološkog računarskog i sajber kriminala, te sankcionisanje počinilaca reformisanjem svog krivičnog zakonodavstva. Osim toga, Ustav Crne Gore, konkretno član 9, precizira da ratifikovani i objavljeni međunarodni ugovori i opšteprihvaćena pravila međunarodnog prava čine sastavni dio unutrašnjeg pravnog poretka, i da imaju primat nad domaćim zakonodavstvom i da su direktno primjenjivi kada odnose regulišu drugačije od domaćeg zakonodavstva.

Godine 2009, u Crnoj Gori je usvojen Zakon o potvrđivanju Konvencije Savjeta Evrope o visokotehnološkom kriminalu (Budimpeštanska konvencija), a istovremeno su potvrđeni i Dodatni protokol o rasizmu i ksenofobiji (CETS 189) i Konvencija o zaštiti djece od seksualnog iskorišćavanja i seksualnog zlostavljanja (CETS 201). Pored toga, Crna Gora je počela da usklađuje svoj nacionalni pravni okvir s odredbama sadržanim u ovim konvencijama.

Nadležni organ za utvrđivanje pravnog okvira i politike sajber bezbjednosti u Crnoj Gori je Ministarstvo javne uprave, digitalnog društva i medija. Pravni akti koji čine osnovu savremenog koncepta sajber bezbjednosti i načina na koji on funkcioniše u Crnoj Gori su:

- Zakon o informacionoj bezbjednosti [15]
- Zakon o tajnosti podataka [16]
- Uredba o mjerama informacione bezbjednos [17]
- Zakonik o krivičnom postupku [18]

15. https://www.gov.me/dokumenta/fbb730c5-8c62-47e3-863f-cfaae9631b8d
16. https://www.gov.me/dokumenta/c1ac4c4d-e914-47f7-8f61-49d1bf85560e
17. https://www.gov.me/dokumenta/c3b1ba84-8d7b-4baf-914c-3913b358bb2d
18. https://www.paragraf.me/propisi-crnegore/zakonik-o-krivicnom-postupku.html

- Zakon o potvrđivanju Konvencije o računarskom kriminalu[19]
- Zakon o Agenciji za nacionalnu bezbjednost[20]
- Krivični zakonik[21]
- Zakon o elektronskom potpisu[22]
- Zakon o elektronskim komunikacijama[23]
- Zakon o elektronskoj trgovini[24]
- Strategija sajber bezbjednosti Crne Gore 2013–2017, 2018–2021 i 2022–2026[25]

Nacionalni CIRT svakodnevno dobija prijave o incidentima različite vrste (napadi na veb-stranice, prevare putem interneta, zloupotrebe profila na društvenim mrežama itd.), ali u CIRT-u smatraju da je pravi broj sajber incidenata mnogo veći od onog koji se prijavljuje, s obzirom na to da su korisnici obično ne prijavljuju uznemirujuće incidente na internetu zvaničnim organima.

CIRT ohrabruje građane da prijave incidente posredstvom njegove veb-stranice, te izdaje obavještenja i upozorenja o internet prevarama i sajber napadima. Tokom 2021, CIRT je vodio je javne kampanje upozoravajući na fišing (phishing, tj. pokušaj krađe identiteta i podataka), važnost zaštite podataka i bezbjednosti uređaja, te potrebu za oprezom prilikom kupovine putem interneta. Pored toga, CIRT je ranije vodio i kampanje usmjerene na zaštitu djece i mladih. Međutim, iz javno dostupnih izvora jasno je da je bilo veoma malo posebnih kampanja (ako ih je uopšte i bilo) čiji je fokus bio na ljudskim pravim, diskriminaciji ili nasilju.

19. https://wapi.gov.me/download/fe845b44-f208-444b-9ff1-3a96b6ce0983?version=1.0
20. http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=194322&rType=2&file=ZAKON%20O%20ANB.pdf
21. https://www.gov.me/dokumenta/5bd66a1b-ad2a-4801-ae8a-e025016691f0
22. https://www.gov.me/dokumenta/040e9f79-f385-49bd-9773-6a77cb7e8f40
23. https://www.gov.me/dokumenta/207dd619-58fc-4d2e-a033-e31642675807
24. https://www.gov.me/dokumenta/c46f2c6b-a0bc-459c-8086-00c618d3a4be
25. https://www.gov.me/dokumenta/8a2de214-c58e-4524-9196-c08886f5829b

Za različite izazove tek treba da se iznađu rešenja koja bi zadovoljila standarde EU i međunarodne zajednice. Jedan primjer je taj da su u EU pravila o zaštiti ličnih podataka veoma stroga. Iako je je sajber prostor idealna arena za zloupotrebu ličnih podataka, u EU se takva zloupotreba ozbiljno kažnjava. Međutim, Crna Gora nije uskladila svoje zakonodavstvo s opštim propisom EU u ovoj oblasti – Uredbom o zaštiti ličnih podataka (GDPR 2016/679), zbog čega se ne može smatrati da građani Crne Gore imaju isti nivo zaštite ličnih podataka ili mogućnosti ostvarivanja prava na privatnost kao građani zemalja EU.[26]

Osim toga, ljudska prava se još uvijek ne uzimaju adekvatno u obzir prilikom razvoja regulatornog okvira za sajber bezbjednost. Čak ni nova strategija ne prepoznaje da je sajber bezbjednost u suštini pitanje ljudskih prava i da je treba tretirati na taj način. Kad je riječ o prepoznatim problemima, govor mržnje i širenje etničke i vjerske mržnje pominju se na nekoliko mjesta na stranicama strategije, ali na konceptualnom planu strategija ne pokazuje nikakvu ambiciju da primijeni pristupe zasnovane na zaštiti ljudskih prava na zakone, politike i prakse koje se tiču sajber bezbjednosti.

SAJBER BEZBJEDNOST I PRAVO NA PRIVATNOST

Zaštita podataka o ličnosti u Crnoj Gori garantovana je Ustavom, ratifikovanim međunarodnim ugovorima i nacionalnim zakonodavstvom, a prije svega odredbama sadržanim u Zakonu o zaštiti podataka o ličnosti i Zakonu o slobodnom pristupu informacijama.

Namjera je da se novi Zakon o zaštiti podataka o ličnosti uskladi sa GDPR-om, te da lični podaci građana Crne Gore budu zaštićeni na isti način kao u EU. Međutim, Crna Gora još nije potpisala Protokol Savjeta Evrope iz 2018. godine o izmjenama i dopunama Konvencije za zaštitu pojedinaca u vezi sa automatskom obradom ličnih podataka.[27]

Nadzorna uloga u oblasti zaštite podataka o ličnosti nadležnost je Agencije za zaštitu ličnih podataka i slobodan pristup informacijama,[28] čije administrativne kapacitete treba dodatno ojačati.[29]

26. https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0
27. Izvještaj Evropske komisije o napretku Crne Gore za 2021. godinu
28. https://www.azlp.me/me/agencija
29. Izvještaj Evropske komisije o napretku Crne Gore za 2021. godinu

Za ilustraciju izazova s kojima se ovaj sektor suočava poslužiće primjer iz marta 2020. godine, kad je sama vlada prekršila pravo na privatnost i zaštitu ličnih podataka objavljivanjem spiskova lica u samoizolaciji tokom pandemije kovida-19. Prema podacima nevladine organizacije Akcija za ljudska prava (HRA), objavljeni su lični podaci najmanje 2.000 lica.[30] Nakon što je Vlada objavila imena i adrese onih koji su bili pod zdravstvenim nadzorom, pojavila se aplikacija (https://crnagorakorona.com/home) nepoznatih autora, putem koje je bilo moguće utvrditi lokaciju lica koja su se nalazila u samoizolaciji. Spiskove lica u samoizolaciji objavili su i pojedini štampani i elektronski mediji. Sistem zaštite ličnih podataka je u ovom slučaju očigledno zakazao, a Agencija za zaštitu ličnih podataka je podržala radnje Vlade u ovom pogledu. Po objavljivanju spiskova, Zaštitnik ljudskih prava i sloboda Crne Gore – Ombudsman, saopštio je da „nije bilo mogućnosti da se reaguje“ i da „ne može da se miješa u rad drugih nezavisnih i samostalnih organa“. Ipak, svega dva mjeseca kasnije zatražio je od Ministarstva javne uprave da sprovede detaljnu istragu.[31] U oktobru 2021. godine, Viši sud u Bijelom Polju donio je prvu pravosnažnu presudu da je država objavljivanjem spiskova lica u samoizolaciji povrijedila pravo na privatnost i zaštitu ličnih podataka.

Početkom aprila 2021. godine objavljen je spisak od 62 osobe iz Podgorice koje su zaražene koronavirusom, zajedno s njihovim matičnim brojevima. Kao posljedica toga, samo jedan radnik Doma zdravlja Podgorica procesuiran je pred nadležnim organima, ali je i on oslobođen optužbi prvostepenom presudom. U toku krivičnog postupka dokazano je da su određene kategorije ličnih podataka poslate van zdravstvenog informacionog sistema putem imejla, bez ikakve zaštite putem enkripcije, što je suprotno važećim propisima.[32]

ANB je takođe optužena za neopravdano kršenje prava na privatnost. Protiv bivšeg direktora Agencije, Dejana Peruničića, 2021. godine podnesena je krivična prijava zbog zloupotrebe službenog položaja, nezakonitog prisluškivanja i nadzora nad nekoliko tadašnjih lidera opozicije, mitropolita Srpske pravoslavne crkve i dvojice novinara koji su bili kritički nastrojeni prema bivšoj vladi, u periodu od januara do septembra 2020. godine.[33]

30. https://www.vijesti.me/vijesti/drustvo/574937/drzava-krsila-pravo-na-privatnost
31. https://www.vijesti.me/vijesti/drustvo/543643/bivsa-vlada-masovno-krsila-pravo-na-privatnost
32. https://www.vijesti.me/vijesti/drustvo/543643/bivsa-vlada-masovno-krsila-pravo-na-privatnost
33. U.S. Department of State, 2021 Country Reports on Human Rights Practices: Montenegro [Državni izvještaji o praksi ljudskih prava za 2021. godinu: Crna Gora], Bureau of Democracy, Human Rights, and Labor: 2021

Zakonom o tajnosti podataka propisuje se sistem za utvrđivanje povjerljivosti podataka, i reguliše pristup tajnim podacima, čuvanje, zaštita i korišćenje tih podataka, kao i vođenje evidencije. Tajni podaci su u zakonu definisani kao podaci čijim bi otkrivanjem nepozvanom licu nastupile ili mogle nastupiti štetne posljedice za bezbjednost i odbranu, vanjsku, monetarnu i ekonomsku politiku Crne Gore. Ovaj zakon utvrđuje uslove i određuje šta se smatra povjerljivim podacima. Povjerljivim se smatraju i podaci strane države i međunarodne organizacije koji su kao takvi označeni i dostavljeni nadležnim organima u Crnoj Gori.[34]

Organizacije civilnog društva (OCD) već godinama upozoravaju da se u Crnoj Gori oznake tajnosti neopravdano koriste za ograničavanje pristupa javnim informacijama. Osim toga, izmjenama i dopunama Zakona o slobodnom pristupu informacijama iz 2017. godine degradirano je pravo javnosti na pristup informacijama. ANB i Ministarstvo odbrane informacije od javnog značaja mogu proglasiti tajnim bez ikakve sudske kontrole. NVO MANS je pozvala novu vladu da ukine ova ograničenja i vrati se prethodnim otvorenijim rješenjima.[35]

SAJBER BEZBJEDNOST I SLOBODA IZRAŽAVANJA

Nova strategija sajber bezbjednosti prioritet daje izmjenama i dopunama Krivičnog zakonika i Zakonika o krivičnom postupku Crne Gore. Izmjene i dopune Krivičnog zakonika pomoći će u sankcionisanju krivičnog djela širenja i prenošenja lažnih vijesti i dezinformacija, dok bi izmjene i dopune Zakonika o krivičnom postupku trebalo da unaprijede i olakšaju istražne postupke.

Crna Gora nema organ koji je u stanju da analizira i ugasi sajtove s kojih se vrše krivična djela, a naročito krivična djela koja se tiču dječje pornografije, ksenofobije, terorizma i širenja vjerske i nacionalne mržnje, te krivična djela u vezi sa sivom ekonomijom. Internet provajderi u Crnoj Gori ne mogu da ugase poddomene niti da onemoguće pristup sajtovima s kojih se vrše krivična djela.

34. https://www.gov.me/dokumenta/c1ac4c4d-e914-47f7-8f61-49d1bf85560e
35. https://www.vijesti.me/vijesti/politika/608778/mans-pozvao-vladu-da-hitno-usvoji-izmjene-zakona-o-slobodnom-pristupu-informacijama

Nova strategija predviđa izmjene i dopune postojećeg Zakona o elektronskim komunikacijama, kako bi se identifikovale tehničke mogućnosti za gašenje ili blokiranje poddomena, odnosno onemogućavanje pristupa veb-stranicama s kojih se vrše krivična djela ili koje krše odredbe Krivičnog zakonika. Međutim, ovo nije samo tehničko već i pravno pitanje, a posebnu pažnju treba posvetiti definisanju pravnog osnova za ove radnje i pažljivom određivanju organa čije odluke će omogućiti blokiranje sadržaja na internetu.

Strategijom se predviđaju i izmjene i dopune Krivičnog zakonika u cilju prepoznavanja i sankcionisanja krivičnog djela kreiranja i širenja lažnih vijesti i dezinformacija putem interneta. Posljednjih godina hapšeni su brojni novinari i drugi pojedinci zbog navodnog objavljivanja lažnih vijesti pri čemu su optuživani za „izazivanje panike i nereda“. Međutim, ovi postupci bili su selektivne prirode i nisu svi autori lažnih vijesti tretirani na isti način. NVO HRA je 2020. godine Ustavnom sudu Crne Gore podnijela inicijativu za ocjenu ustavnosti ovog člana Krivičnog zakonika, tvrdeći da je neprecizan i da je dozvoljeno njegovo proizvoljno tumačenje, na štetu ljudskih prava i slobode izražavanja.[36] Iako upravo zbog ove nepreciznosti treba pažljivo razmotriti propisivanje ovog krivičnog djela, i u ovom slučaju treba voditi računa o tome da se pojedinci ne procesuiraju za netačne izjave koje ne pozivaju na nasilje i ne predstavljaju govor mržnje, jer bi to predstavljalo pretjerano ograničavanje slobode izražavanja što je suprotno evropskim standardima ljudskih prava.

SAJBER BEZBJEDNOST I SLOBODA OKUPLJANJA

Sajber napadi na medijske portale česta su pojava, a na meti su gotovo svi portali koji se češće koriste u posljednjih nekoliko godina. Pored medija, najnovija Procjena opasnosti od teškog i organizovanog kriminala (SOCTA 2022), čiji je autor Europol, procjenjuje da su distribuirani napadi uskraćivanjem usluga (DDoS) na informacione sisteme državnih organa i pravnih lica, vladine veb-stranice i portale, i veb-stranice političkih stranaka, česta pojava.[37]

36. https://www.pobjeda.me/clanak/hra-trazi-ocjenu-ustavnosti-krivicnog-djela-kojim-se-sankcionisu-lazne-vijesti
37. https://www.vijesti.me/vijesti/crna-hronika/603933/socta-2022-raste-sajber-kriminal-sve-vise-prisutno-dijeljenje-snimaka-seksualnog-zlostavljanja-djece

Sagovornici su naveli dva nedavna incidenta kad su hakeri remetili događaje koje su organizovali mediji. Hakeri su „upali“ na dva hibridna događaja i puštali muziku, prikazivali neprikladne grafičke sadržaje i ometali rad. Ispostavilo se da oba ova događaja imaju zajedničku karakteristiku u smislu da su pozivi za učešće objavljivani na internetu putem društvenih mreža. Organizatori su reagovali i riješili probleme, ali su propustili da prijave ove incidente jer su zatečeni nepripremljeni.

Naši sagovornici su istakli da se o digitalnoj bezbjednosti novinara rijetko govori i da se veoma malo ulaže u edukaciju novinara i drugih medijskih poslenika. Jasno je da je u ovoj oblasti potrebna tehnička pomoć i podrška edukaciji. Međutim, zbog važnosti novinarstva za demokratiju i ljudska prava, te činjenice da su mediji prepoznati kao grupa koja je posebno osjetljiva na sajber prijetnje, strateški i politički dokumenti bi trebalo i da razmotre mogućnost intervencije države u vidu posebne podrške medijima, kako bi im se pomoglo da se odupru ovim prijetnjama.

Tokom parlamentarnih izbora 2016. godine, nekoliko važnih veb-stranica bilo je meta sajber napada, uključujući informativne portale i veb-stranice političkih stranaka i nevladinih organizacija. Veb-stranica Centra za demokratsku tranziciju (CDT), nevladine organizacije koja je imala akreditovane posmatrače izbora širom zemlje, bila je predmet kontinuiranih DDoS napada danima uoči samog izbornog dana. Sistemi za praćenje utvrdili da su napadi dolazili s velikog broja različitih IP adresa iz više zemalja.

Na sam dan izbora, Agencija za elektronske komunikacije i poštansku djelatnost (EKIP) naložila je svim operaterima da privremeno obustave rad aplikacija za razmjenu poruka Viber i WhatsApp. Zvanični razlog koji je saopšten bio je da je putem ovih servisa slata neželjena pošta ili nezakoniti marketinški materijal. OCD su kritikovale ovu odluku kao suprotnu pravu na slobodu izražavanja i Ustavu. Ustavni sud je 2019. godine presudio da je član Zakona o elektronskim komunikacijama koji EKIP-u omogućava da naloži operaterima da obustave internetske i telefonske komunikacije u neograničenom obimu ako smatra da je to „opravdano u slučajevima prevare ili zloupotrebe“ neustavan i naložio da se ta odredba ukine.

Različite profašističke grupe u Crnoj Gori širile su govor mržnje na ekstremno desničarskim portalima, u komentarima ispod članaka i objava na društvenim mrežama, kritikujući aktiviste, građane, ali i čitave narode za sve što smatraju da nije u skladu s njihovim sistemom vrijednosti. Obično ovakve ekstremističke grupe pokreću talase stigmatizacije i zlostavljanja

koji su usmjereni na pojedince i grupe ljudi, čineći to objavama koje podstiču etničku i vjersku mržnju, rasnu i drugu diskriminaciju i nasilje nad onima koji su predmet njihovih napada.[38]

Ovakvi pozivi na sajber linč često ciljaju određenu osobu i tako je izlažu prijetnji nasiljem u stvarnom životu. Osim toga, ne postoje efikasne, proporcionalne ili odvraćajuće sankcije za borbu protiv govora mržnje i zločina motivisanog mržnjom. Tužioci takve slučajeve često klasifikuju kao lakši prekršaj protiv javnog reda i mira, čime se zanemaruju – bilo slučajno ili namjerno – motivi takvih napada, a problem gura „pod tepih" kad je riječ o statistici o prekršajima, koja ne prepoznaje etničku ili vjersku mržnju kao motiv.

Prema podacima Sudskog savjeta, u periodu od 2017. do 2020. godine donesena je jedna pravosnažna presuda za krivično djelo izazivanje nacionalne, rasne i vjerske mržnje, a počinilac je osuđen na uslovnu kaznu. Prekršaj je počinjen putem društvenih mreža. U 2021. godini, pred sudovima je pokrenuto ukupno 15 predmeta protiv lica optuženih za izazivanje nacionalne, vjerske i rasne mržnje, od kojih je šest vezano za događaje iz 2021. godine. Do kraja 2021. godine postupci su vođeni u ukupno 11 predmeta, a njih osam je u potpunosti okončano. Od ovog broja, postupak je obustavljen u četiri slučaja, a osuđujuće presude izračene su u ostala četiri.[39]

Iako su onlajn mediji i internet komunikacija godinama prepoznati kao kanali za širenje govora mržnje, dezinformacija i propagande, sama oblast onlajn medija u Crnoj Gori nije bila regulisana sve do nedavnog usvajanja Zakona o medijima. Izmjenama i dopunama ovog zakona internetska publikacija (informativni portal) definiše se kao medij čiji se sadržaj dijeli putem interneta i koji se upisuje u Evidenciju medija koju vodi Ministarstvo kulture. Portali su u obavezi da prijave svoje pravne informacije i podatke o vlasničkoj strukturi, da propišu pravila za komentare čitalaca i uklanjaju nezakoniti sadržaj i sl. Međutim, još uvijek nema sankcija ako portal nije registrovan, niti su pronađena rješenja u slučajevima kad portali dijele nezakonit sadržaj.[40] [41]

38. https://www.cdtmn.org/wp-content/uploads/2021/03/Rast-desnicarskog-ekstremizma-u-Crnoj-Gori_WEB-Preview-3.pdf
39. https://www.cdtmn.org/2022/04/20/na-zataskavati-slucajeve-izazivanja-mrznje/
40. https://seenpm.org/wp-content/uploads/2021/01/Resilience-research-publication-2-Montenegro_Nationall-language.pdf
41. Zakon o medijima (Sl. list CG, br. 46/2010, 40/2011 – dr. zakon, 53/2011, 6/2013, 55/2016, 92/2017 i 82/2020 – dr. zakon).

SAJBER BEZBJEDNOST I ANTIDISKRIMINACIJA

Crnogorsko zakonodavstvo sajber bezbjednost i diskriminaciju rijetko tretira kao srodne teme. Zakon o zabrani diskriminacije propisuje da se uznemiravanje putem audio i video nadzora, mobilnih uređaja, društvenih mreža i interneta, koje ima za cilj ili čija je posljedica povreda ličnog dostojanstva, izazivanje straha, osjećaja poniženosti ili uvrijeđenosti ili stvaranje neprijateljskog, ponižavajućeg ili uvredljivog okruženja smatra diskriminacijom.[42] Krivični Zakonik Crne Gore predviđa niz krivičnih djela koja se tiču povrede ravnopravnosti i slobode izražavanja nacionalne ili etničke pripadnosti.

Definicija krivičnog djela „izazivanje nacionalne, rasne i vjerske mržnje“ obuhvata zabranu javnog podsticanja nasilja ili mržnje prema grupi ili članu grupe koja je određena na osnovu rase, boje kože, religije, porijekla, državne ili nacionalne pripadnosti. Zakonodavac je istim članom obuhvatio i zabranu javnog odobravanja, negiranja postojanja ili značajnog umanjenja težine krivičnih djela genocida, zločina protiv čovječnosti i ratnih zločina, na način koji može dovesti do nasilja ili izazvati mržnju prema grupi lica ili članu grupe, ukoliko su ta krivična djela utvrđena pravosnažnom presudom suda u Crnoj Gori ili međunarodnog krivičnog suda.

Zakonom o zabrani diskriminacije govor mržnje je definisan kao „svaki oblik izražavanja ideja, tvrdnji, informacija i mišljenja koji širi, raspiruje, podstiče ili pravda diskriminaciju, mržnju ili nasilje protiv lica ili grupe lica zbog njihovog ličnog svojstva, ksenofobiju, rasnu mržnju, antisemitizam ili ostale oblike mržnje zasnovane na netoleranciji, uključujući i netoleranciju izraženu u formi nacionalizma, diskriminacije i neprijateljstva protiv manjina.“ Za upotrebu govora mržnje predviđena je prekršajna odgovornost, i to novčana kazna.

Romi su najugroženija manjinska zajednica u Crnoj Gori i oni se, kao takvi, suočavaju s ogromnim rizicima od diskriminacije. Veliki procenat romskih domaćinstava ne posjeduje osnovne uslove za pristojan porodični život. Na primjer, u jednom nedavnom istraživačkom izvještaju (Socio-ekonomski položaj Roma i Egipćana u Crnoj Gori, Ministarstvo pravde, ljudskih i manjinskih prava, 2020),[43] 9,8% ispitanika Roma navelo je da njihovo domaćinstvo nema struju, a 11,6% da nema vodu (13,8% nema tekuću vodu).

42. https://www.ombudsman.co.me/docs/1612165541_zakon-o-zabrani-diskriminacije.pdf
43. https://www.gov.me/dokumenta/ac3e91ce-6f24-4aad-b648-70d51de2559e

Osamdeset odsto domaćinstava nije imalo računar koji je bio potreban za učenje na daljinu tokom pandemije kovida-19. Svega 65,5% domaćinstava imalo je neki vid pristupa internetu (putem mobilnog telefona, Wi-Fi rutera ili na neki drugi način), dok je samo 55,1% ispitanika koristilo internet svakog dana.

Sagovornici iz romske organizacije mladih Phiren Amenca (Koračajte s nama) rekli su nam da je bilo mnogo neetičkog izvještavanja i ekstremnog govora mržnje protiv romske i egipćanske zajednice na internetu, ali da ne raspolažu nikakvim konkretnim podacima o povredama sajber bezbjednosti kad su u pitanju njihove zajednice.

Na početku pandemije koronavirusa diskriminacija Roma bila je vrlo vidljiva. Govor mržnje korisnika društvenih mreža obično je uključivao tvrdnje da su Romi bili prvi zaraženi koronavirusom zbog lošeg načina života i loše higijene. Od početka pandemije mnogi Romi ostali su bez prihoda ili pristupa obrazovanju i socijalnoj i zdravstvenoj zaštiti. Međutim, neka romska naselja ni godinama prije toga nisu imala pristup tekućoj vodi.

Kad je riječ o slučajevima pred Ombudsmanom, 2020. godine u postupku je bilo 19 predmeta koji su uključivali diskriminaciju na osnovu etničke pripadnosti i povezanosti s manjinskim narodom ili manjinskom nacionalnom zajednicom.[44]

Govor mržnje usmjeren prema LGBTIQA+ populaciji takođe je česta pojava u medijskom i informativnom prostoru. Od 2013. godine do danas održano je devet Montenegro Pride šetnji, ali je u društvu i dalje široko rasprostranjena diskriminacija. LGBTIQA+ osobe suočavaju se s uvredljivim napadima na društvenim mrežama, koje često prate i prijetnje nasiljem. LGBTIQA+ zajednica se godinama bavi govorom mržnje i javnim prijetnjama, posebno na društvenim mrežama kao što su Facebook i Instagram. Predstavnici organizacije Queer Montenegro kažu da su napadi najizraženiji u vrijeme održavanja Montenegro Pride šetnje, kada se LGBTIQA+ osobe suočavaju s najgorim vrstama komentara i prijetnji, kako putem javnih tako i putem privatnih profila. Često se suočavaju sa slikovitim opisima nasilja usmjerenog prema njima ili njihovim porodicama, popraćenim riječima poput „znam gdje mogu da te nađem“, te bivaju primorani da izbrišu svoje profile, s obzirom na to da je takve vrste prijetnji teško izdržati.

44. https://www.ombudsman.co.me/docs/1619074992_izvjestaj_01042021.pdf

Zakon o životnom partnerstvu lica istog pola, koji je u Skupštini Crne Gore izglasan 1. jula 2020. godine[45] takođe je bio predmet napada i govora mržnje. Opasnost od napada za ovu zajednicu donose i aplikacije za upoznavanje, koje se uveliko koriste u Crnoj Gori. Kako su objasnili iz organizacije Queer Montenegro, zlostavljači se često registruju na takvim sajtovima samo da bi pronašli pojedinca i zaprijetili mu, u nekim slučajevima praveći skrinšot komunikacije prijeteći da će ga objaviti i javno „autovati" osobu, tj. obznaniti njen identitet. Takođe je prilično uobičajeno da pojedinci upadnu u kancelarije organizacije i upućuju direktne prijetnje onima koje tamo zateknu.

Jedna trećina građana Crne Gore ne želi da živi u istoj zemlji kao LGBTIQA+ osobe, a skoro 43 odsto smatra da LGBTIQA+ osobe ne bi trebalo da imaju ista prava kao ostali građani, pokazalo je istraživanje EU i Savjeta Evrope koje je sproveo Centar za demokratiju i ljudska prava (CEDEM) 2020. godine.[46]

Izvještavanje o migrantima u crnogorskim medijima uglavnom se odvija putem članaka i izvještaja koji se kopiraju i doslovce prenose iz regionalnih medija; vrlo malo toga zasniva se na originalnim istraživanjima. To znači da se, u lokalnom kontekstu, izvještaji o migrantima uglavnom odnose na određeni događaj. Analiza narativa koji sadrži govor mržnje i dezinformacije, koju su zajednički objavili Institut za medije Crne Gore (Podgorica), SEENPM (Tirana) i Mirovni institut (Ljubljana),[47] otkriva da komentari čitalaca, koji su identifikovani kao problematičan segment onlajn medija, uključuju pozive na fizičko nasilje nad migrantima, sadržaj koji ismijava njihovu situaciju i širenje teorija zavjere kao što je ona da je cilj kretanja izbjeglica „islamizacija Evrope".

Onlajn nasilje nad ženama nije izolovana pojava, već dio šireg društvenog konteksta rodne nejednakosti i diskriminacije žena i djevojčica. Kako bismo razumjeli digitalno nasilje, ključno je da zastanemo kako bismo ispitali šta je rodno zasnovano nasilje, jer agresija i napadi koje žene doživljavaju u svojim onlajn interakcijama nije ništa drugo do produžetak nasilja koje ih već dugi niz godina pogađa u svim sferama njihovog života.[48] U Crnoj Gori, na primjer, žene koje se usude da se uključe u politiku i da iznose svoje mišljenje često

45. https://www.slobodnaevropa.org/a/30701060.html
46. https://www.portalanalitika.me/clanak/trecina-crnogorskih-gradana-ne-zeli-da-zivi-u-istoj-drzavi-sa-lgbti-osobama
47. https://seenpm.org/wp-content/uploads/2021/01/Resilience-research-publication-2-Montenegro_Nationall-language.pdf
48. Organization of American States (OAS), Online gender-based violence against women and girls: Guide of basic concepts, digital security tools, and response strategies [Onlajn rodno zasnovano nasilje nad ženama i djevojčicama: Vodič za osnovne koncepte, digitalne bezbjednosne alate i strategije odgovora] (OAS, 2021).

su na meti zlostavljanja i mizoginih napada. Nedavno se pojavila nova vrsta obrasca: uvredljivi, ponižavajući, zlostavljački i seksistički komentari usmjereni na gotovo svaku ženu koja se usudi da misli drugačije od većine, uključujući i one koje obavljaju visoke državne funkcije.[49]

DALJI KORACI

U Crnoj Gori je, prije svega, potrebno aktivno raditi na podizanju svijesti o činjenici da je sajber bezbjednost pitanje ljudskih prava. Postoji potreba za promovisanjem otvorenog, slobodnog i stabilnog sajber prostora u kome bi se vladavina prava primjenjivala u potpunosti, a ljudska prava i osnovne slobode poštovale. To znači zaštitu od gašenja interneta kojom se ljudima uskraćuje pristup informacijama i mogućnost izražavanja mišljenja. To, takođe, znači i preuzimanje odgovornosti za ponašanje u sajber prostoru i zaštitu od nasilja, diskriminacije i govora mržnje na internetu.

Shodno tome, potrebna je stručna revizija postojećih zakona i drugih propisa koji regulišu pitanja na presjeku sajber bezbjednosti i ljudskih prava, kako bi se isti uporedili s najboljim standardima i dobroj praksi u ovoj oblasti i kako bi se dale preporuke za unapređenje zakonodavnog okvira. U strateškim dokumentima i javnim inicijativama već su iznesene ideje o tome kako poboljšati krivično, medijsko, izborno i drugo zakonodavstvo u kontekstu hibridnih prijetnji, dezinformacija i pokušaja miješanja od strane stranih aktera. Sve ove inicijative treba posmatrati kroz prizmu ljudskih prava. Takođe, neophodno je unaprijediti zakonodavstvo koje štiti lične podatke, uz zakone koji garantuju pristup informacijama.

Neophodno je obezbijediti dovoljna finansijska sredstva za sprovođenje postojećih strateških dokumenata i zakona, što do sada nije bio slučaj. Ovo je posebno važno u svjetlu nedostatka eksperata i stručnog kadra u oblasti sajber bezbjednosti. Postojaće stalna potreba za ulaganjem u zapošljavanje, edukaciju i unapređenje vještina takvog kadra.

49. https://docs.google.com/viewerng/viewer?url=https://www.cdtmn.org/wp-content/uploads/2022/05/WEB_Vidimo-li-slona- MNE-1.pdf&hl=en

Neophodno je raditi na poboljšanju medijske pismenosti. Po riječima jednog sagovornika – „Ljudi treba da nauče da se u sajber prostoru ponašaju kao što se ponašaju u fizičkom prostoru, samo uz mnogo više pažnje i obzira prema svom okruženju."

Država mora da uspostavi zakonodavni okvir i ojača kapacitete nadležnih za taj okvir, kao i da ojača partnerstva između javnog i privatnog sektora.

Pored pomenutog, za ostvarivanje ovih ciljeva potrebno je izgraditi okruženje koje počiva na povjerenju. Ovo je naročito potrebno kako bi se dao doprinos izgradnji partnerstva između države i privatnog sektora. To je proces koji zahtijeva puno vremena i truda, kao aktivan pristup komunikaciji, koordinaciji i edukaciji.

Autorka: Franciska Klopfer | DCAF

DCAF

ZAKLJUČAK

Ka boljem uključivanju perspektive ljudskih prava u dobro upravljanje sajber bezbjednošću

Ka boljem uključivanju perspektive ljudskih prava u dobro upravljanje sajber bezbjednošću

Demokratiju, ljudska prava ili vladavinu zakona ne možemo uzimati zdravo za gotovo: riječ je o dobrima koja treba štititi i njegovati. Tokom posljednjih nekoliko decenija, kako se sve veći dio naših života selio na internet, učili smo kako demokratija, ljudska prava i vladavina prava mogu napredovati uz i kroz tehnologiju. Rani zagovornici prednosti interneta najavljivali su ga kao do tada nezabilježenu priliku za prava kao što je sloboda govora i govorili o novoj eri za demokratiju. Ove pretpostavke nisu bile u potpunosti pogrešne, ali smo bili i svjedoci toga da tehnologija i život na internetu sa sobom nose niz svojevrsnih izazova.

Studije slučaja uključene u ovu publikaciju to vrlo dobro ilustruju. Autori su analizirali situaciju u vezi s ljudskim pravima – uključujući prava koja su neophodna za demokratsku participaciju, kao što su sloboda izražavanja, sloboda informacija i sloboda okupljanja – kao i situaciju u vezi sa sajber bezbjednošću u šest ekonomija Zapadnog Balkana. U njihovim analizama poseban fokus stavlja se na strukture upravljanja, a cilj im je da ukažu na to kako nedostaci u upravljanju – u zakonu; u njegovoj implementaciji; u uspostavljanju, funkcionisanju i saradnji institucija; kao i u upravljanju i nadzoru nad institucijama – mogu dovesti do izazova za ljudska prava i sajber bezbjednost.

Autori su prilikom definisanja sajber bezbjednosti s namjerom zauzeli pristup koji je usmjeren na čovjeka. To znači fokus koji prevazilazi temu bezbjednosti mreža i usluga, već i kako te mreže i usluge mogu da se bezbjedno koriste od strane svih članova društva.

U šest poglavlja integralnog izvještaja ukazuje se na jasne trendove u svakoj od pomenutih ekonomija; na primjer, važni zakoni i strukture koji se tiču sajber bezbjednosti uvedeni su u posljednjoj deceniji, a mnogo je uloženo i postignuto u pogledu bezbjednosti mreža i usluga. Međutim, one kao takve

još uvijek nisu potpuno bezbjedne i ostaju ranjive na napade i krađu podataka. Ovo je imalo štetne efekte na brojna ljudska prava. Ne radi se dovoljno na rješavanju pitanja rastuće nebezbjednosti na internetu, naročito onlajn nasilja. Takođe, povećan je broj pokušaja korišćenja tehnologije za ograničavanje ljudskih prava.

U većini od šest poglavlja prisutna je slika ekonomija koje su uložile velike napore da razviju zakonske i regulatorne okvire za sajber bezbjednost. Bosna i Hercegovina, koja u 2022. godini još uvijek nema nacionalnu strategiju za sajber bezbjednosti niti zakon o sajber bezbjednosti, izuzetak je od ovog pravila. Druge ekonomije već razvijaju svoju drugu ili treću iteraciju nacionalne strategije sajber bezbjednosti i usklađuju svoja nacionalna zakonodavstva s najnovijim standardima EU, kao što je ažurirana Direktiva o bezbjednosti mrežnih i informacionih sistema, tzv. NIS2 direktiva. Procesi EU integracija bili su prvi i važan pokretač za razvoj zakonodavstva o sajber bezbjednosti u ovom regionu. Digitalizacija je bila drugi. I zaista, EU promoviše digitalizaciju u regionu, a to se može vidjeti na primjeru Digitalne agende za Zapadni Balkan.

POZIV NA PRISTUP SAJBER BEZBJEDNOSTI KOJI JE USMJEREN NA LJUDE

Činjenica da su digitalizacija i EU integracije glavni pokretači donošenja politika o sajber bezbjednosti nije lišena svojevrsnih problema, ističu autori. U stvari, čini se da postoji vrlo malo drugih principa koji oblikuju aktivnosti u ovoj areni. Nijedna od šest ekonomija nije se čvrsto obavezala na poštovanje ljudskih prava u svojoj politici sajber bezbjednosti, već se cilj sajber bezbjednosti prije definiše kao zaštita mreža i sistema. Iako se može pretpostaviti da je takav cilj u interesu zaštite nacionalne bezbjednosti, demokratskog poretka i ljudskih prava svih, to se rijetko eksplicitno navodi. Ovo je problematično, jer to znači da će ionako ograničeni resursi dostupni za sajber bezbjednost biti usmjereni su na bezbjednost tehničkih sistema, te da nacionalne strategije nemaju za cilj analiziranje ili zaštitu prava korisnika – pri čemu je izuzetak stavljanje fokusa na zaštitu djece, koja predstavlja istaknuti element trenutne nacionalne strategije sajber bezbjednosti Albanije. Nekoliko autora ukazuje na ove nedostatke i poziva na pristup sajber bezbjednosti koji je više usmjeren na čovjeka (za razliku od pristupa usmjerenog na državu ili tehnologiju).

PRIJETNJE LJUDSKIM PRAVIMA PREDSTAVLJAJU PRIJETNJU BEZBJEDNOSTI LJUDI I DEGRADIRANJE DEMOKRATIJE NA INTERNETU

Sagledavanje sajber bezbjednosti kroz prizmu dobrog upravljanja pomaže da se pokaže kako prijetnje ljudskim pravima na internetu mogu prerasti u sistemske prijetnje demokratiji na internetu. Autori i autorke šest poglavlja integralnog izvještaja osvrnuli su se na temu zaštite i promocije ljudskih prava na internetu u ekonomijama Zapadnog Balkana. U slučajevima u kojima su otkriveni izazovi u pogledu poštovanja ljudskih prava, autori su analizirali sisteme upravljanja. Na taj način pružena je veoma informativna slika o tome zašto dolazi do zloupotreba i kako i zašto zakoni, institucije ili tehnički sistemi ne uspijevaju da ostvare svoje ciljeve ili zaostaju po ovom pitanju.

U šest poglavlja identifikovan je niz izazova za ljudska prava na internetu u ekonomijama Zapadnog Balkana. Jedan od najčešćih je onlajn nasilje. Zapravo, onlajn maltretiranje, uznemiravanje, uhođenje, prijetnje i drugi napadi na bezbjednost pojedinaca i grupa postali su široko rasprostranjena pojava. Ovi izazovi su uglavnom usmjereni protiv grupa koje već doživljavaju diskriminaciju i nasilje u oflajn svijetu: žena, manjina (naročito romske zajednice), migranata i LGBTIQA+ osoba.[50] Onlajn nasilje zauzima značajno mjesto u svih šest studija slučaja, i kao takvo ima štetan uticaj na brojna ljudska prava.

Onlajn nasilje takođe ima štetan efekat na slobodu izražavanja, pravo na informacije i slobodu okupljanja, naročito kad se pojedincima na internetu prijeti s ciljem da se ućutkaju i obeshrabre da budu prisutne ili da se izraze i budu politički, društveno ili kulturno aktivni, bilo da je riječ o onlajn ili oflajn okruženju. Studije slučaja jasno pokazuju da ova pojava više nije ograničena na situacije gdje pojedinac biva predmet vrijeđanja ili agresije. Umjesto toga, sve češće primjećujemo pojavu sajber mafije[51] – organizovanih grupa koje koriste različite tehnike da ućutkaju pojedince, naročito novinare, aktiviste i

50. Poglavlje 6: Srbija – Povlačenje veza s ljudskim pravima i ulaganje u ljude', 117; „Poglavlje 3: Kosovo – Jačanje novih temelja i institucija", 65, 71; „Poglavlje 5: Sjeverna Makedonija – Pokretanje implementacije za jačanje uključivanja zainteresovanih strana", 105; „Poglavlje 4: Crna Gora – Podizanje svijesti kao temelj za prilagođavanje pristupa", 87.
51. Poglavlje 4: Crna Gora – Podizanje svijesti kao temelj za prilagođavanje pristupa", 85.

branioce ljudskih prava.[52] Mnoge takve grupe mogu biti povezane s ideološkim ili političkim grupama. Povremeno se spekuliše da iza ovakvih organizovanih kampanja stoje vladini akteri ili drugi domaći ili strani centri političke moći.[53] Jasno je da namjera ovakvih napada nije samo da se izrazi neslaganje s određenim pojedincima ili grupama, već da se isti zastraše i spriječe da učestvuju u društvenom, kulturnom i političkom životu. Autori poglavlja o Bosni i Hercegovini organizovano sajber nasilje povezuju s fenomenom govora mržnje – govorom čija je namjera da podstiče mržnju i nasilje. Ovo pokazuje da je nasilje koje se vrši onlajn povezano s onim što se dešava u oflajn, tj. fizičkom svijetu.

PROMJENE U POGLEDU UPRAVLJANJA NEOPHODNE SU ZA PREVAZILAŽENJE IZAZOVA ONLAJN NASILJA

Nažalost, Zapadni Balkan nije jedini region u kome je sajber nasilje postalo široko rasprostranjeno, organizovano i štetno po prava i demokratsku participaciju pojedinaca. Studije slučaja pokazuju zašto se to dešava u ovih šest ekonomija i šta treba učiniti da se ova pitanja riješe.

Čini se da u jednom broju ekonomija zakon ne pokriva pitanje sajber nasilja na adekvatan način. Kako ističu autori, sve ekonomije su ratifikovale, odnosno izvršile usklađivanje s relevantnim međunarodnim standardima, kao što su npr. Konvencija Savjeta Evrope o visokotehnološkom kriminalu (Budimpeštanska konvencija) ili Konvencija o sprečavanju i borbi protiv nasilja nad ženama i nasilja u porodici (Istanbulska konvencija). Međutim, iako zakoni u načelu pokrivaju diskriminaciju ili govor mržnje, onlajn diskriminacija i nasilje još uvijek nisu u potpunosti pokriveni kao pitanja.[54] Štaviše, šest poglavlja analize obiluje primjerima slučajeva u kojima organi za sprovođenje zakona i pravosuđe nisu bili u mogućnosti ili nisu htjeli da

52. „Poglavlje 6: Srbija – Povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 130; „Poglavlje 4: Crna Gora – Podizanje svijesti kao temelj za prilagođavanje pristupa“, 83; „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 28.
53. „Poglavlje 6: Srbija – Povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 121, „Poglavlje 2: Bosna i Hercegovina – Kretanje kroz pravni sistem i promovisanje dobre prakse“, 43.
54. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 14; „Poglavlje 6: Srbija – povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 111.

istraže, krivično gone i donose presude u slučajevima onlajn nasilja. U nekim slučajevima postoji jasno odbijanje da se vidi da onlajn nasilje može imati slične efekte kao i fizičko nasilje.[55] U drugim slučajevima, čini se da policija, tužioci i sudije nisu dovoljno obučeni za adekvatno postupanje u takvim slučajevima.

SAJBER BEZBJEDNOST, MJERE PROTIV GOVORA MRŽNJE I MJERE PROTIV DEZINFORMACIJA KOJE VODE UTIŠAVANJU GLASOVA OPOZICIJE

Autori takođe navode brojne slučajeve u kojima su vlasti možda prekoračile mjeru u primjeni zakona protiv dezinformacija i govora mržnje kako bi utišale glasove opozicije. Korisnici društvenih mreža nalaze se pod istragom zbog objava na internetu. Glasovi koji kritikuju vladine odgovore na vanredne situacije kao što su zemljotres ili kovid-19 doveli su do krivičnog gonjenja novinara ili gašenja veb-stranica pod izgovorom „širenja dezinformacija“ ili „izazivanja panike i nereda“.[56]

ZAŠTITA PODATAKA I BEZBJEDNOST MREŽA I SISTEMA

Poglavlja koja se odnose na Albaniju i Sjevernu Makedoniju ilustruju kako velika krađa podataka u posjedu javnih institucija može narušiti pravo na privatnost građana i narušiti njihovo povjerenje u institucije i demokratske procedure. Sajber napadi velikih razmjera postali su češći u Evropi, uključujući i Zapadni Balkan. Takođe, u ovom regionu postoji stvarni ili percipirani porast slučajeva zloupotrebe, curenja ili krađe podataka. Kako autori objašnjavaju, to je rezultat i sve veće digitalizacije javnih usluga,[57] što znači da se u mrežama javnih institucija pohranjuje više podataka o građanima. U poglavlju o Albaniji istražuje se nekoliko slučajeva koji uključuju krađu ili

55. „Poglavlje 2: Bosna i Hercegovina – Kretanje kroz pravni sistem i promovisanje dobre prakse“, 53; „Poglavlje 4: Crna Gora – Podizanje svijesti kao temelj za prilagođavanje pristupa“, 86-87; „Poglavlje 3: Kosovo – Jačanje novih temelja i institucija“, 71.
56. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 22; Crna Gora – Unapređenje svijesti kao osnova za prilagođavanje pristupa” 85; „Poglavlje 6: Srbija – povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 124.
57. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 23.

curenje podataka građana, i ukazuje se na to da se čini da sistemi nisu uspostavljeni tako da ih prate dovoljne mjere bezbjednosti. Čini se i da nedostaju odgovarajuća tehnička rješenja i procedure za zaštitu podataka od kriminalaca.

Brojni sajber napadi visokog profila čiji su predmet bile javne institucije u regionu Zapadnog Balkana pokazuju koliko je važno zaštititi sisteme i servise.[58] Ako se to ne učini, ekonomije u regionu su u riziku da budu žrtve prekida rada kritične nacionalne infrastrukture i javnih usluga, gubitka podataka, kao i gubitka povjerenja javnosti. Sajber napadi mogu imati štetne posljedice po nacionalnu bezbjednost i prava svih građana, a naročito po pravo na privatnost (u slučaju krađe ili curenja podataka) i pravo građana na pristup javnim uslugama. Studije slučaja ukazuju na to da praktično ni u jednoj od ekonomija nema dovoljno stručnjaka za sajber bezbjednost koji rade u javnom sektoru i da infrastrukturu sajber bezbjednosti tek treba ojačati. Na primjer, lični podaci bivaju izgubljeni zbog tehničkih propusta javnih ili privatnih aktera koji nisu u stanju da pravilno zaštite sisteme u kojima se podaci pohranjuju.[59] Ljudska prava, stoga, mogu biti zaštićena samo ako se prevaziđu ovi izazovi koji se tiču upravljanja.

NEDOSTACI U POGLEDU UPRAVLJANJA UGROŽAVAJU ZAŠTITU PODATAKA I BEZBJEDNOST MREŽE

Šest studija slučaja detaljno ispituje nedostatak stručnog kadra za sajber bezbjednost u javnom sektoru i razloge za to. Poglavlje o Albaniji donosi dobro poznatu priču: kad je došlo do velikog curenja podataka o građanima, pokazalo se da je teško utvrditi koja je institucija bila kriva.[60] Ovo ukazuje na nekoliko potencijalnih problema. Čini se da uloge i odgovornosti između različitih državnih institucija nisu jasno raspodijeljene, a u nekim slučajevima takva jasnoća ne postoji ni i između državnih organa i privatnih aktera koji pružaju usluge zaštite podataka. U Albaniji, kao i u sličnim slučajevima u ovom regionu, nije sačinjen nikakav konačan izvještaj, niti su izvedeni zaključci na osnovu kojih bi se relevantne institucije ili pojedinci pozvali na

58. Kajošević, Samir, Zapadni Balkan pozvan da se pripremi za porast sajber-napada, BIRN, 12. septembar 2022
59. „Poglavlje 6: Srbija – Povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 119.
60. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 16-17.

odgovornost. To, zauzvrat, dovodi do gubitka povjerenja u vlade i onlajn usluge koje one pružaju.[61] Pored izazova koji se tiču koordinacije, nedostatak kvalifikovanog kadra za sajber bezbjednost koji bi se bavio zaštitom sistema podataka doprinosi ranjivosti javno pohranjenih podataka.[62] Ekonomije regiona moraju više ulagati u obrazovanje, obuku, zapošljavanje i zadržavanje stručnjaka za sajber bezbjednost u javnom sektoru.

Čini se i da manjka parlamentarnog nadzora nad sajber bezbjednošću. Parlamenti rijetko nadziru aktivnosti vlade u vezi sa sajber bezbjednošću i moguće je da im nedostaje znanja da budu učinkoviti u takvom svom radu.[63] Što se tiče samostalnih državnih organa koji bi mogli da vrše nadzor nad sajber bezbjednošću, odgovarajuće institucije za takvu vrstu aktivnosti uglavnom nisu uspostavljene. S jedne strane su institucije zadužene za sajber bezbjednost, a s druge organi (državni ili nedržavni) koji se bave zaštitom ljudskih prava. Kada su im se obratili autori različitih poglavlja, predstavnici ministarstava ili državnih agencija odgovornih za sajber bezbjednost isticali su da ljudska prava nisu dio njihovog mandata. Organi zaduženi za ljudska prava navode da im nedostaje stručnosti u pogledu sajber bezbjednosti, pri čemu su neki saopštili da smatraju da je riječ o oblasti koja zahtijeva pažnju.[64]

POSTOJE OPASNOSTI U TEHNOLOGIJAMA KOJE ZADIRU U PRAVA LJUDI I DEGRADIRAJU DEMOKRATIJU

Čini se da sve veća dostupnost tehnologija koje omogućavaju lakše praćenje ljudi, gotovo bilo gdje i bilo kada, predstavlja preveliko iskušenje za vlade, čak i one koje se smatraju demokratskim i poštuju ljudska prava.[65] Kao što pokazuju studije slučaja, vlade u regionu Zapadnog Balkana koriste ove tehnologije – i više nije riječ o povremenoj upotrebi, s obzirom na to da je u nekim ekonomijama takva upotreba postala sistematska. Studija slučaja u Srbiji objašnjava kako je vlada pokušala da odobri agencijama za sprovođenje zakona da prošire opseg korišćenja uređaja za nadzor, ali da je nacrt

61. „Poglavlje 5: Sjeverna Makedonija – Pokretanje implementacije za jačanje uključivanja zainteresovanih strana“, 97.
62. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 10.
63. „Poglavlje 6: Srbija – Povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 113.
64. „Poglavlje 1: Albanija – Premošćivanje jaza između fragmentacije sajber politike i ljudskih prava“, 23; „Poglavlje 5: Sjeverna Makedonija – Pokretanje implementacije za jačanje uključivanja zainteresovanih strana“, 113.
65. The Guardian, The Pegasus project. [Projekat Pegasus]

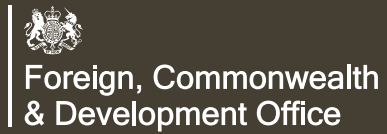
zakona povučen nakon brojnih protesta civilnog društva. Ovaj primjer pokazuje koliko je važno biti oprezan kad je u pitanju upotreba i regulacija tehnologija za nadzor. Usklađenost zakonodavstva s međunarodnim standardima ljudskih prava je ključna. Međutim, čak i kad se tehnologije za nadzor koriste u skladu s domaćim zakonodavstvom i međunarodnim standardima, njihova upotreba može imati efekat obeshrabrivanja i odvraćanja u pogledu ljudskih prava. Primjeri iz Srbije i Bosne i Hercegovine pokazuju da su građani počeli da zaziru od odlazaka na javne proteste jer se plaše da će biti praćeni i nadzirani.[66]

POTREBNO JE VIŠE ISTRAŽIVANJA I PODIZANJA SVIJESTI KAKO BI DOŠLO DO ODRŽIVIH PROMJENA

Kao što je ova publikacija pokazala, postoje realni izazovi za ljudska prava u sajber bezbjednosti u regionu Zapadnog Balkana. Istraživanje ovih izazova omogućava detaljno ispitivanje načina na koji IKT mogu uticati na uživanje prava, demokratsku participaciju i demokratski poredak. Sagledavanjem ovih izazova kroz prizmu dobrog upravljanja i sagledavanjem neuspjeha u pogledu upravljanja koji su doveli do tih izazova, iste možemo bolje razumjeti i početi da tražimo rješenja. Studije slučaja u ovoj publikaciji pokazuju da je potrebno mnogo više istraživanja i podizanja svijesti o izazovima koji se tiču upravljanja. Naročito su potrebna dalja istraživanja na nacionalnom nivou o ulogama i odgovornostima različitih aktera u rješavanju pitanja ljudskih prava i sajber bezbjednosti, kao i istraživanja o institucionalnim preprekama za prevazilaženje ovih izazova.

Polazeći od ove analize ljudskih prava i sajber bezbjednosti, u daljem radu koji planira Istraživačka mreža za sajber bezbjednost Zapadnog Balkana poseban fokus će biti na rodnim pitanjima i sajber bezbjednosti. Ova publikacija utire put za takav rad, u smislu metodologije i identifikovanja ključnih aktera i pitanja koja se, u većoj ili manjoj mjeri, odnose i na rodna pitanja. Ovim će biti načinjen važan iskorak ka sveobuhvatnom nizu publikacija o najvažnijim pitanjima u vezi s dobrim upravljanjem u domenu sajber bezbjednosti, kako na regionalnom nivou, tako i konkretno u vezi s ekonomijama Zapadnog Balkana.

66. „Poglavlje 6: Srbija – Povlačenje veza sa ljudskim pravima i ulaganje u ljude“, 125-126; „Poglavlje 2: Bosna i Hercegovina – Kretanje kroz pravni sistem i promovisanje dobre prakse“, 51.



DCAF
Ženevski centar za upravljanje sektorom bezbjednosti
Maison de la Paix, Chemin Eugène-Rigot 2E
CH-1202, Ženeva, Švajcarska

Tel: +41 22 730 94 00
Email: info@dcaf.ch
Website: www.dcaf.ch
Twitter @DCAF_Geneva