Uloga civilnog društva i medija u zaštiti digitalnih prava i bezbjednosti novinara i aktivista u Republici Srpskoj

SErvis za Medijsku Profesionalnu Edukaciju i Razvoj

Reporting Digital Rights & Freedoms

Sadržaj

Uloga civilnog društva i medija u zaštiti digitalnih prava i bezbjednosti novinara i aktivista u Republici Srpskoj

Sažetak

Ovaj izvještaj predstavlja empirijske nalaze i analitički pregled stanja digitalnih prava u Republici Srpskoj, s fokusom na bezbjednost novinara, aktivista i građana. Korišteni su: (1) baza podataka prikupljena putem online upitnika (N = 13 incidenata), (2) polustrukturisani intervjui/odgovori pravnih i tehnoloških stručnjaka, te (3) desk-research i priložene studije slučaja (hakerski napadi na medije i građanske inicijative). Najzastupljenije forme kršenja su online uznemiravanje/govor mržnje, dezinformacije, online cenzura, neovlašćen pristup/zloupotreba podataka i prijetnje. U preko 60% slučajeva počinilac nije poznat. Dominantni kanali su društvene mreže (posebno Facebook i X/Twitter) i online portali. Intervjuirani eksperti ukazuju na: (a) slabosti tehničke i institucionalne zaštite ličnih podataka i digitalne bezbjednosti, (b) normativni raskorak i potrebu za operacionalizacijom novih propisa, te (c) porast algoritamske moderacije i ograničenja oglašavanja koja utiču na vidljivost novinarskog sadržaja.

1. Uvod

U posljednjih deset godina digitalni prostor u Republici Srpskoj i Bosni i Hercegovini postao je ključna arena za političku komunikaciju, građanski aktivizam, ali i za širenje dezinformacija, govor mržnje i koordinisane napade na novinare i aktiviste. Internet i društvene mreže omogućili su široj javnosti da slobodno iznosi stavove i dijeli informacije, ali su istovremeno otvorili i prostor za nove oblike ugrožavanja ljudskih prava i demokratskih sloboda. Digitalna prava – koja obuhvataju pravo na privatnost, slobodu izražavanja, bezbjednost podataka i pristup informacijama – danas predstavljaju temelj bez kojeg se ne može govoriti o funkcionalnoj demokratiji niti o slobodnom društvu.

Ovaj izvještaj nastao je kao rezultat višemjesečnog istraživanja u kojem su kombinovane kvantitativne i kvalitativne metode: online upitnik kojim su prikupljeni podaci o konkretnim slučajevima kršenja digitalnih prava, intervjui sa pravnim i tehničkim ekspertima, te analiza dokumentovanih slučajeva hakerskih napada i kampanja online uznemiravanja. Time je obezbijeđen uvid u višeslojnu prirodu problema – od individualnih iskustava građana do šireg institucionalnog i zakonodavnog konteksta.

Uvodno poglavlje ima za cilj da prikaže širi društveni okvir u kojem se kršenja digitalnih prava dešavaju. Republika Srpska, kao i ostatak BiH, suočava se s izazovima slabe institucionalne zaštite, nedovoljno razvijenih mehanizama digitalne bezbjednosti, kao i niskim nivoom digitalne pismenosti kod građana. Odsustvo jasnih procedura i nedovoljna proaktivnost nadležnih institucija dodatno doprinose osjećaju nesigurnosti kod novinara, aktivista i običnih korisnika interneta.

Posebno je važno istaći da digitalna prava nisu apstraktan koncept, već imaju direktne posljedice po život i rad pojedinaca. Kada novinar doživi prijetnje putem društvenih mreža, ili kada aktivističkoj platformi bude obrisan sadržaj bez jasnog objašnjenja, to ne utiče samo na njihovu ličnu bezbjednost, već i na pravo javnosti da bude informisana. Upravo iz tog razloga,

ovaj izvještaj pokušava da objedini kvantitativne podatke, lične priče i ekspertske analize u jednu cjelinu, kako bi se bolje razumjela dinamika digitalnih prijetnji i kako bi se ponudile konkretne preporuke za njihovo prevazilaženje.

Cilj ovog dokumenta nije samo da prikaže obim i prirodu kršenja digitalnih prava, već i da posluži kao alat za zagovaranje promjena – od jačanja kapaciteta institucija i zakonodavnih reformi, preko unapređenja tehničkih mehanizama zaštite, do razvoja kulture digitalne pismenosti i solidarnosti među novinarima, aktivistima i građanima. Drugim riječima, uvod postavlja osnovu za razmatranje digitalnih prava ne samo kao pitanja zaštite pojedinaca, već i kao strateškog preduslova za demokratizaciju i evropske integracije Bosne i Hercegovine.

2. Metodologija

Metodološki okvir ovog istraživanja osmišljen je tako da omogući sveobuhvatno razumijevanje fenomena kršenja digitalnih prava i bezbjednosti novinara, aktivista i građana u Republici Srpskoj. Uvažena je složenost problema, koji obuhvata tehničke, pravne, društvene i političke dimenzije, pa je istraživanje kombinovalo kvantitativne i kvalitativne pristupe kako bi se dobila cjelovita i višeslojna slika.

2.1. Kvantitativna komponenta

Kvantitativni dio istraživanja oslonio se prvenstveno na analizu baze podataka kreirane putem online upitnika. Upitnik je bio otvoren tokom cijelog perioda istraživanja i distribuiran kroz mreže organizacija civilnog društva, novinarska udruženja, kao i lično. Pitanja su bila strukturisana tako da obuhvate osnovne parametre svakog incidenta:

- datum i lokaciju incidenta,
- vrstu kršenja (npr. govor mržnje, online uznemiravanje, neovlašteni upad u nalog, cenzuru, dezinformacije, prijetnje fizičkim nasiljem),
- platformu ili medij na kojem se incident dogodio,
- odnos žrtve prema počiniocu (poznat/ nepoznat),
- posljedice incidenta (psihološke, profesionalne, bezbjednosne).

Ova baza omogućila je kvantifikaciju fenomena – mjerenje učestalosti različitih tipova kršenja, njihovog geografskog rasprostiranja, kao i identifikaciju najčešće korištenih digitalnih platformi kao prostora ugrožavanja prava. Statistička analiza obuhvatila je frekvencije, procente i vremenske trendove, čime je omogućeno poređenje sa sličnim istraživanjima u regionu i Evropi.

2.2. Kvalitativna komponenta

Kvalitativni dio istraživanja obuhvatio je:

1. Polustrukturisane intervjue sa stručnjacima iz oblasti prava, informacionih tehnologija i digitalne bezbjednosti. Posebno su značajni uvidi profesora Mirka Sajića (informatika i sajber bezbjednost), Dejana Lučke (ljudska prava i pravna regulativa), Aleksandra Mastilovića (digitalna transformacija i sigurnost) i Borislava Vukojevića (medijska i

informacijska pismenost). Njihovi stavovi pružili su ekspertski okvir za razumijevanje institucionalnih i društvenih slabosti u zaštiti digitalnih prava.

2. Analizu dokumentovanih slučajeva digitalnog nasilja, hakerskih napada i online kampanja dezinformacija, koji su bili medijski zabilježeni ili su došli do istraživačkog tima kroz prijave učesnika. Uključeni su slučajevi poput hakerskih napada na portale *Capital* i *Istraga*, targetiranja aktivista zbog ekoloških protesta, ili organizovanih kampanja govora mržnje na društvenim mrežama.
3. Studije slučaja (case studies), gdje su pojedini incidenti detaljno analizirani u pogledu posljedica po žrtvu, reakcije institucija i šireg društvenog odjeka. Ovaj pristup omogućio je razumijevanje fenomena ne samo kao zbirke izolovanih događaja, već i kao dio šire strukture političkih i društvenih odnosa.

2.3. Dokumentaciona i komparativna analiza

Kako bi se rezultati istraživanja stavili u širi kontekst, korištena je i analiza zakonodavnog okvira Republike Srpske i Bosne i Hercegovine, sa posebnim osvrtom na usklađenost sa standardima Evropske unije (npr. GDPR, Digital Services Act, Direktiva o bezbjednosti mrežnih i informacionih sistema – NIS2). Ova analiza dopunjena je poređenjem sa regionalnim praksama u Srbiji i Hrvatskoj, kako bi se identifikovali modeli koji mogu biti primjenjivi u domaćem kontekstu.

2.4. Etika istraživanja

Posebna pažnja posvećena je etici istraživanja, imajući u vidu da su učesnici upitnika i intervjua dijelili iskustva o prijetnjama, zastrašivanju i uznemiravanju. Svi podaci su obrađeni anonimno, a identitet ispitanika zaštićen. Cilj nije bio izlaganje pojedinaca dodatnim rizicima, već kreiranje baze podataka koja će služiti kao alat za zagovaranje i izgradnju sigurnijeg digitalnog okruženja.

2.5. Ograničenja istraživanja

Istraživanje se suočilo i sa određenim ograničenjima. Prvo, samo-selekcija ispitanika znači da podaci mogu odražavati iskustva onih koji su već senzibilisani za ovu temu, dok incidenti koji nisu prijavljeni ostaju izvan baze. Drugo, nedostatak institucionalne transparentnosti otežao je pribavljanje zvaničnih podataka o procesuiranju digitalnih prijetnji i napada. Treće, prisutna je dinamičnost digitalnog prostora – priroda prijetnji i napada brzo se mijenja, pa rezultati daju trenutni presjek, ali ne i konačnu sliku.

3. Teorijski i regulatorni okvir

Razumijevanje kršenja digitalnih prava i bezbjednosti novinara i aktivista u Republici Srpskoj zahtijeva postavljanje istraživanja u širi teorijski i regulatorni okvir. Time se obezbjeđuje povezivanje konkretnih empirijskih nalaza sa postojećim naučnim spoznajama i pravnim normama koje oblikuju digitalni prostor, kako u lokalnom, tako i u globalnom kontekstu.

3.1. Digitalna prava kao ljudska prava

Digitalna prava u savremenoj literaturi sve češće se posmatraju kao sastavni dio osnovnih ljudskih prava, a ne kao njihov tehnički dodatak. Pojavom interneta i digitalnih tehnologija

došlo je do radikalne transformacije društvenih odnosa, političke participacije i komunikacijskih obrazaca, što je zahtijevalo proširenje postojećih normativnih okvira. U tom smislu, digitalna prava čine most između tradicionalnih građanskih sloboda i novog društveno-tehnološkog poretka.

Prema Oomen i van den Berg (2014), koncept digitalnih prava može se posmatrati kao "nova generacija prava" koja proizlazi iz već postojećih normi, ali je prilagođena digitalnom okruženju. Primjeri uključuju:

- Pravo na privatnost: u digitalnom prostoru ovo se odnosi na zaštitu ličnih podataka, komunikacija i digitalnog identiteta;
- Sloboda izražavanja: obuhvata pravo na nesmetano širenje i razmjenu mišljenja putem digitalnih platformi, ali i zaštitu od cenzure i algoritamskih ograničenja;
- Pravo na sigurnost: podrazumijeva zaštitu od digitalnog nasilja, nadzora, neovlaštenih upada i krađe identiteta.

Ova prava nisu nova u suštini, ali digitalni kontekst stvara specifične izazove: masovno prikupljanje podataka, algoritamsko odlučivanje, transnacionalne platforme i globalne mreže nadzora.

Autori poput Manuela Castellsa (2009) i Shoshane Zuboff (2019) naglašavaju da digitalni prostor nije neutralan, već duboko politički određen. Internet je postao nova javna sfera u kojoj se oblikuje moć, ali i razvijaju društveni pokreti. Ako u toj sferi nisu garantovana prava građana, demokratija gubi ključni prostor djelovanja.

Castells digitalna prava povezuje sa mogućnošću građana da učestvuju u mrežama komunikacije i da na taj način oblikuju društveno-političke procese.

Zuboff kroz koncept „nadzirane ekonomije" (surveillance capitalism) ukazuje da bez adekvatne zaštite, digitalni prostor postaje alat za komercijalnu i političku manipulaciju.

Za Bosnu i Hercegovinu i Republiku Srpsku, gdje su tradicionalni mediji često pod političkim pritiscima, digitalni prostor predstavlja jednu od rijetkih platformi za slobodnu debatu. Upravo zato je zaštita digitalnih prava nužna za očuvanje pluralizma i javnog interesa.

U literaturi o ljudskim pravima ponekad se govori o "generacijama prava"[1]:

1. Građanska i politička prava (pravo na život, slobodu, sigurnost, slobodu izražavanja);
2. Ekonomska, socijalna i kulturna prava (pravo na rad, obrazovanje, zdravstvo);
3. Kolektivna prava (pravo na razvoj, pravo na mir, pravo na zdravu životnu sredinu);
4. Digitalna prava (pravo na internet, zaštita podataka, digitalna sigurnost, pravo na pristup informacijama).

[1] Koncept „generacija prava" u literaturi o ljudskim pravima prvi je uveo Karel Vasak 1977. godine, razlikujući prvu generaciju (građanska i politička prava), drugu generaciju (ekonomska, socijalna i kulturna prava) i treću generaciju (kolektivna prava). Tokom posljednjih decenija, dio akademske zajednice i stručnjaka predložio je proširenje ovog okvira na četvrtu generaciju, koja obuhvata digitalna prava – pravo na pristup internetu, zaštitu podataka, digitalnu sigurnost i pristup informacijama. Ova interpretacija nije univerzalno usvojena, ali odražava rastući značaj digitalnog prostora za zaštitu osnovnih ljudskih sloboda (Becker, 2019, Benedek, 2007).

Ova četvrta generacija prava i dalje nije univerzalno prihvaćena, ali je sve prisutnija u akademskom diskursu, naročito u Evropi, gdje se razvija koncept "digitalnog građanstva". On podrazumijeva da građani ne samo da koriste digitalne alate, nego i da uživaju zaštitu, odgovornost i mogućnost učešća u kreiranju digitalnih politika.

Jedno od ključnih pitanja u teorijskom okviru jeste balans između prava na privatnost i potrebe za sigurnošću. Kao što naglašava Aleksandar Mastilović (intervju, 2025), čak i u EU dolazi do tenzija između direktiva koje omogućavaju zadržavanje i presretanje podataka u cilju borbe protiv terorizma i presuda Evropskog suda za ljudska prava koje naglašavaju da se radi o nesrazmjernom zadiranju u privatnost.

U Republici Srpskoj i BiH, taj balans je dodatno narušen jer su bezbjednosni mehanizmi slabi, dok se represivni instrumenti često koriste selektivno. To otvara prostor za zloupotrebe – nadzor se ne koristi primarno za zaštitu građana, već za kontrolu neistomišljenika.

Neki autori (Hintz, Dencik i Wahl-Jorgensen, 2019) digitalna prava povezuju sa širim konceptom društvene pravde. Pristup internetu, digitalna pismenost i zaštita od nadzora nisu privilegija, već preduslov ravnopravnog učešća u društvu. U kontekstu RS i BiH, gdje je digitalna pismenost niska, a nejednakost visoka, neadekvatna zaštita digitalnih prava produbljuje društvene razlike.

Digitalna prava nisu samo tehničko pitanje, već fundamentalni preduslov demokratije, ljudskog dostojanstva i društvene jednakosti. U BiH i RS, gdje političke strukture često koriste digitalni prostor za kontrolu i manipulaciju, nužno je posmatrati digitalna prava kao integralni dio borbe za osnovna ljudska prava.

3.2. Međunarodni regulatorni okvir

Razumijevanje digitalnih prava i bezbjednosti novinara i aktivista u Republici Srpskoj ne može se sagledati izolovano od međunarodnih normativnih tokova. Globalni regulatorni okvir predstavlja temeljni referentni okvir, koji određuje standarde zaštite ljudskih prava u digitalnom prostoru i kojem se državni i entitetski sistemi trebaju prilagoditi. Ovaj okvir razvija se kroz dokumente Ujedinjenih nacija, Savjeta Evrope, Evropske unije i drugih međunarodnih organizacija, a ujedno je oblikovan i praksom međunarodnih sudova i specijalizovanih tijela.

Na najširem nivou, digitalna prava se posmatraju kao dio univerzalnih ljudskih prava.

- Univerzalna deklaracija o ljudskim pravima (1948) i Međunarodni pakt o građanskim i političkim pravima (1966) garantuju slobodu izražavanja, pravo na privatnost i pravo na pristup informacijama. Iako ovi dokumenti ne koriste termin „digitalna prava", njihova primjena u digitalnoj sferi postaje očigledna s razvojem interneta.
- Rezolucija UN-a o promociji, zaštiti i uživanju ljudskih prava na internetu (2012) eksplicitno potvrđuje da su prava ljudi offline jednaka onima online, čime se digitalna dimenzija formalno uvrštava u globalnu agendu ljudskih prava.
- Rad Specijalnih izvjestilaca UN-a za slobodu izražavanja i privatnost dodatno naglašava da digitalni prostor mora ostati slobodan od proizvoljnog nadzora, masovnog prikupljanja podataka i neosnovane cenzure.

Evropski kontinent je posebno relevantan za BiH i RS, budući da članstvo u Savjetu Evrope nameće određene obaveze.

- Evropska konvencija o ljudskim pravima (ECHR, 1950) garantuje slobodu izražavanja (član 10) i pravo na privatni i porodični život (član 8). Evropski sud za ljudska prava (ECHR) razvio je bogatu praksu u vezi sa zloupotrebom digitalnog prostora, uključujući presude o neovlaštenom nadzoru i ograničavanju online sadržaja.
- Konvencija 108+ o zaštiti pojedinaca u vezi s automatskom obradom ličnih podataka (1981, revidirana 2018) predstavlja prvi i do danas jedini globalno obavezujući instrument u oblasti zaštite podataka. BiH je potpisnica, ali implementacija u praksi i dalje je fragmentarna.
- Preporuke Savjeta Evrope – poput *CM/Rec(2022)16 o zaštiti novinara i drugih aktera u digitalnom okruženju* – eksplicitno pozivaju države članice da tretiraju online napade na novinare kao prijetnju slobodi medija, naglašavajući institucionalnu odgovornost u prevenciji i reakciji.

Za Bosnu i Hercegovinu, kao zemlju koja teži članstvu u EU, evropski pravni okvir je najvažniji orijentir.

- Opšta uredba o zaštiti podataka (GDPR, 2018) postavlja visoke standarde zaštite ličnih podataka, uključujući pravo na brisanje („pravo na zaborav“), transparentnost obrade i snažne obaveze za institucije i privatni sektor. Iako BiH tek treba da uskladi svoj zakonodavni okvir sa GDPR-om, on ostaje ključni model.
- Direktiva o bezbjednosti mrežnih i informacionih sistema (NIS2, 2023) uvodi obaveze za države članice da razviju nacionalne strategije sajber sigurnosti, osnuju CERT/CSIRT timove i zaštite kritičnu infrastrukturu, uključujući medijske i komunikacione sisteme.
- Digital Services Act (DSA, 2022) i Digital Markets Act (DMA, 2022) predstavljaju prekretnicu u regulaciji digitalnih platformi. DSA, posebno, uspostavlja obaveze velikih platformi da uklanjaju nezakonit sadržaj, ali i da obezbijede transparentne mehanizme žalbi i zaštitu korisnika od arbitrarnog uklanjanja sadržaja.
- EU Kodeks dobre prakse protiv dezinformacija (2018, revidiran 2022), iako dobrovoljan, postao je ključni instrument saradnje između institucija EU, platformi i civilnog društva u borbi protiv širenja lažnih vijesti i manipulativnog sadržaja.

Pored univerzalnih i evropskih instrumenata, značajno je posmatrati i regionalne inicijative. Organizacija za evropsku bezbjednost i saradnju (OSCE) putem svog Predstavnika za slobodu medija aktivno zagovara sigurnost novinara online, dok OECD i NATO razvijaju standarde za zaštitu infrastrukture i borbu protiv hibridnih prijetnji, uključujući dezinformacije.

BiH, iako formalno članica Savjeta Evrope i potpisnica Konvencije 108+, u praksi i dalje kasni u implementaciji međunarodnih standarda. Neusklađenost sa GDPR-om, nepostojanje jasnog zakona o cyber nasilju, slabi kapaciteti za implementaciju NIS2 direktive i odsustvo strategije digitalne bezbjednosti na državnom nivou stvaraju regulatorni vakuum. To dovodi do situacije u kojoj međunarodni okvir služi više kao deklarativna obaveza, nego kao operativni alat za zaštitu novinara i aktivista.

3.3. Regionalni i nacionalni regulatorni okvir

Razumijevanje stanja digitalnih prava u Republici Srpskoj zahtijeva analizu kako regionalnih normativnih procesa u jugoistočnoj Evropi, tako i državnog i entitetskog pravnog okvira u

Bosni i Hercegovini. Ova dimenzija je posebno važna jer pokazuje jaz između deklarativnih obaveza prema međunarodnim standardima i njihove stvarne implementacije u domaćem pravnom i institucionalnom sistemu.

U regionu zapadnog Balkana države se nalaze u različitim fazama usklađivanja sa evropskim standardima zaštite digitalnih prava.

- Srbija je usvojila Zakon o zaštiti podataka o ličnosti (2019) koji je djelimično harmonizovan sa Opštom uredbom EU o zaštiti podataka (GDPR). Ipak, kako ukazuje Dejan Lučka, zakon je ostao u raskoraku sa drugim propisima, pa zaštita ličnih podataka građana nije u potpunosti obezbijeđena.
- Crna Gora i Sjeverna Makedonija, kao kandidati za članstvo u EU, preduzele su značajne korake u izgradnji pravnog okvira za sajber sigurnost i zaštitu podataka, uključujući osnivanje CERT/CSIRT timova i donošenje strategija informacione bezbjednosti.
- Albanija je 2020. doživjela jedan od najvećih cyber napada u regionu, što je ubrzalo donošenje Zakona o kibernetičkoj bezbjednosti i saradnju s NATO-om i EU na jačanju zaštite kritične infrastrukture.

Regionalni trend ukazuje da države prepoznaju digitalnu bezbjednost i prava kao dio šire agende evropskih integracija, ali i kao instrument zaštite od hibridnih prijetnji i dezinformacija koje dolaze iznutra i spolja.

Što se BiH tiče, na državnom nivou, pravni okvir koji se odnosi na digitalna prava i bezbjednost građana je fragmentiran, nedovoljno usklađen i često zastario.

1. Bosna i Hercegovina je ove godine usvojila novi zakon o zaštiti ličnih podataka, za koji zakonodavci tvrde da je usklađen s pravnom tekovinom EU. Ipak, efikasna zaštita podataka zahtijeva i prilagođavanje drugih propisa te promjene u praksi brojnih institucija. U stvarnosti, mnogi organi zaštitu podataka ne tretiraju kao prioritet, što se vidi kroz nedostatak informisanja građana i rijetko proaktivno obavještavanje o incidentima.
2. Krivični zakoni BiH i entiteta – pojedinačno sadrže odredbe koje se mogu primijeniti na digitalno nasilje, ugrožavanje bezbjednosti i govor mržnje, ali ne postoji jedinstveno i jasno definisano krivično djelo *nasilje na internetu* ili *cyber bullying*, što stvara pravnu prazninu i omogućava različita tumačenja.
3. Strategije i institucionalni kapaciteti – iako postoji CERT tim na državnom nivou (BH-CERT), njegov fokus je dominantno tehnički i infrastrukturni. Ne postoji koordinisani sistemski odgovor na napade usmjerene protiv novinara, aktivista i medija, što stvara osjećaj institucionalnog vakuuma.
4. Zakon o komunikacijama (2003) – uređuje rad Regulatorne agencije za komunikacije (RAK), ali je zastario u odnosu na brze promjene u digitalnom ekosistemu. Posebno je problematično što ne predviđa specifične mehanizme zaštite digitalnih prava građana u online prostoru.

Na nivou Republike Srpske dodatni problem predstavlja uvođenje normi koje potencijalno ugrožavaju slobodu izražavanja, pod plaštom regulacije digitalnog prostora:

- Izmjene Krivičnog zakonika RS (2023) ponovo su kriminalizovale uvredu i klevetu, što je naišlo na snažnu kritiku domaćih i međunarodnih aktera. Ove odredbe mogu poslužiti kao instrument za zastrašivanje novinara i aktivista, naročito u digitalnoj sferi, gdje se objave na društvenim mrežama mogu kvalifikovati kao krivična djela.
- Nedostatak specifičnih zakona o cyber bezbjednosti – iako se povremeno spominje potreba za donošenjem zakona o informacionoj bezbjednosti, RS do sada nije razvila sveobuhvatan okvir koji bi bio u skladu s direktivama EU (npr. NIS2).
- Institucionalna pasivnost – CERT RS je formalno uspostavljen, ali njegova nadležnost je ograničena uglavnom na zaštitu informacionih sistema javne uprave. U slučajevima kada su mete napada pojedinci ili mediji, CERT se ne uključuje, što potvrđuje i Aleksandar Mastilović (intervju, 2025).

Analiza pokazuje da u Bosni i Hercegovini, a naročito u Republici Srpskoj, postoji značajan raskorak između:

- formalnog postojanja normi (zakoni o zaštiti podataka, krivične odredbe o ugrožavanju bezbjednosti), i
- njihove primjene u praksi (nedostatak kapaciteta, politički pritisci, nekažnjivost počinilaca).

Na primjer, iako postoje pravne odredbe koje se mogu primijeniti na govor mržnje na internetu, u praksi je malo presuda koje sankcionišu digitalno nasilje. Institucije često odgovaraju da „nema elemenata krivičnog djela“, a žrtvama se savjetuje da „blokiraju naloge“ umjesto da dobiju pravnu i tehničku zaštitu.

Nacionalni i entitetski okvir, u poređenju s međunarodnim i EU standardima, pokazuje nekoliko ključnih slabosti:

1. Fragmentacija i neusklađenost zakona – odsustvo koordinisanog pristupa na nivou BiH i RS;
2. Zastarjelost propisa – mnogi zakoni doneseni su u vrijeme prije društvenih mreža i savremenih digitalnih prijetnji;
3. Politička zloupotreba – norme poput kriminalizacije klevete mogu se koristiti protiv novinara i aktivista;
4. Slabi kapaciteti regulatornih tijela – Agencija za zaštitu ličnih podataka, RAK i CERT timovi imaju ograničene resurse;
5. Nedostatak edukacije i svijesti – kako kod građana, tako i kod službenika koji rukuju osjetljivim podacima.

Zaključno, regionalni i nacionalni regulatorni okvir pokazuje da su digitalna prava u Republici Srpskoj i BiH često pravno deklarisana, ali faktički nezaštićena. U poređenju s međunarodnim i EU standardima, BiH zaostaje u izgradnji sveobuhvatnog i funkcionalnog sistema zaštite, što ostavlja novinare i aktiviste ranjivim na digitalne prijetnje i represiju.

3.4. Tehnološki i društveni aspekti regulacije

Regulacija digitalnog prostora ne odvija se isključivo kroz zakone i formalne institucije – značajan uticaj imaju tehnološke arhitekture i društveni obrasci upotrebe digitalnih platformi. Na to ukazuje i teorija Lawrencea Lessiga (2006) o „četiri modaliteta regulacije“ – pravo, tržište, društvene norme i arhitektura (kod, algoritmi). Kada se ova teorija primijeni na digitalna prava u Republici Srpskoj i BiH, postaje jasno da pravna regulacija čini samo jedan dio šireg ekosistema u kojem građani, mediji i institucije egzistiraju.

Jedan od ključnih tehnoloških aspekata regulacije je činjenica da algoritmi digitalnih platformi (Facebook, X/Twitter, YouTube, TikTok) oblikuju ono što korisnici vide, dijele i percipiraju kao „važnu informaciju“.

- Algoritamska cenzura: sadržaji koji sadrže određene ključne riječi, simbole ili hashtage mogu biti uklonjeni ili potisnuti bez jasnog objašnjenja. Primjeri iz BiH pokazuju da su novinarske objave uklanjane zbog „kršenja pravila zajednice“ iako su se bavile legitimnim temama od javnog interesa.
- Shadow banning i ograničavanje dosega: sadržaj nije eksplicitno obrisan, ali je njegov doseg znatno umanjen, čime se utiče na vidljivost kritičkih narativa. To ima ozbiljne posljedice po medije i organizacije civilnog društva koji zavise od digitalne publike za distribuciju sadržaja.
- Komercijalna pristrasnost: algoritmi prioritetno plasiraju sadržaje koji generišu klikove i angažman, što često favorizuje senzacionalizam, dok ozbiljan novinarski sadržaj ostaje u drugom planu.

U ovakvom kontekstu, regulacija digitalnih prava ne svodi se samo na pravne norme, već i na borbu za transparentnost algoritama i uvođenje mehanizama kontrole i odgovornosti velikih tehnoloških kompanija.

Tehnološki razvoj donosi i nove mehanizme zaštite, ali i sofisticiranije prijetnje:

- Zaštita: enkripcija komunikacije (npr. Signal, WhatsApp end-to-end), višefaktorska autentifikacija, VPN alati i softveri za anonimnost (Tor) omogućavaju korisnicima i novinarima veću privatnost i bezbjednost;
- Prijetnje: istovremeno, razvoj *deepfake* tehnologija, phishing napada i malvera usmjerenih na novinare i aktiviste pokazuje da digitalna bezbjednost nikada nije statična. Mastilović (intervju, 2025) naglašava da upravo sofisticirani napadi poput lažnih identiteta stvaraju nove oblike ugrožavanja kredibiliteta i bezbjednosti;
- Infrastrukturna zavisnost: regionalni mediji i organizacije civilnog društva često koriste besplatne ili jeftine platforme, što ih čini zavisnim od spoljnih servera, cloud servisa i komercijalnih alata. Kada dođe do napada (npr. DDoS na portale), lokalni kapaciteti za zaštitu su nedovoljni.

Društveni faktori igraju presudnu ulogu u oblikovanju digitalnog prostora:

- Niska digitalna pismenost: građani često nisu upoznati s osnovnim mehanizmima zaštite podataka, niti prepoznaju opasnosti od lažnih vijesti i online manipulacija. To ih čini ranjivima i prema institucionalnim zloupotrebama i prema napadima drugih korisnika;

- Normalizacija nasilja na internetu: u RS i BiH se online prijetnje često doživljavaju kao „retorički eksces“, a ne kao ozbiljna povreda prava. Takav društveni stav odražava se i na rad institucija, koje rijetko procesuiraju digitalno nasilje;
- Politički kontekst: u polarizovanom društvu, društvene mreže postaju produžena ruka političke borbe, gdje se koriste bot mreže, koordinisane kampanje i dezinformacije kako bi se oblikovalo javno mnijenje. U takvom ambijentu novinari i aktivisti postaju legitimna meta napada, dok institucije ostaju pasivne.

Treći dimenzionalni sloj regulacije čini tržište. Platforme i pružaoci digitalnih usluga imaju profitne motive, koji oblikuju pravila igre:

- Dominacija oglašavanja zasnovanog na podacima (targeted ads) podstiče masovno prikupljanje i obradu podataka o korisnicima, što direktno ugrožava pravo na privatnost;
- Lokalni mediji i organizacije civilnog društva, kako navodi Kerim Hodžić iz BIRN-a (intervju, 2025), suočeni su s ograničenjima sponzorisanja i targetiranja publike na globalnim platformama, što smanjuje njihovu vidljivost i ekonomske mogućnosti.
- Digitalna tržišta u regionu su nedovoljno regulisana, pa građani i organizacije nemaju mehanizme za žalbu ili kompenzaciju u slučaju zloupotrebe.

Sve navedeno ukazuje na raskorak između pravne regulacije i tehnološke stvarnosti:

- Zakoni u RS i BiH rijetko adresiraju pitanja algoritamske transparentnosti, online uznemiravanja ili digitalne diskriminacije;
- Tehnološke platforme primjenjuju sopstvena pravila, često zasnovana na globalnim politikama, koje ne prepoznaju lokalne specifičnosti jezika, političkog konteksta i kulturnih normi;
- Društvena svijest o digitalnim pravima i dalje je niska, što dodatno otežava javni pritisak na institucije i kompanije da osiguraju veći stepen zaštite.

Generalno gledano, tehnološki i društveni aspekti regulacije digitalnog prostora pokazuju da prava građana u Republici Srpskoj nisu ugrožena samo nedostatkom pravnog okvira, već i strukturnim dinamikama tehnološkog razvoja i društvenim normama komunikacije. Algoritamska cenzura, nevidljivi oblici ograničavanja sadržaja, masovno prikupljanje podataka i normalizacija online nasilja stvaraju složen ambijent u kojem formalna pravna zaštita ostaje tek djelimično efikasna. Stoga, istinska zaštita digitalnih prava mora kombinovati pravnu regulaciju sa zahtjevima za transparentnost platformi, jačanje digitalne pismenosti i promjenu društvenih normi u online komunikaciji.

3.5. Normativno–praktični raskorak

Iako Bosna i Hercegovina, a time i Republika Srpska, formalno raspolažu zakonima i strategijama koje obuhvataju pitanja digitalnih prava, u praksi se pokazuje značajan jaz između onoga što je propisano i onoga što se primjenjuje. Ovaj raskorak je jedan od ključnih razloga zbog kojeg novinari, aktivisti i građani ostaju nezaštićeni u online prostoru.

Na normativnom nivou, u BiH postoje zakoni o zaštiti ličnih podataka, krivične i prekršajne odredbe koje obuhvataju prijetnje i govor mržnje, te strateški dokumenti o informacionoj bezbjednosti. Međutim, u praksi:

- institucije rijetko reaguju na prijave digitalnog nasilja, govoreći da „nema elemenata krivičnog djela“;
- pravni postupci traju predugo, pa žrtve odustaju ili se suočavaju sa dodatnim sekundarnim viktimizacijama;
- kazne su minimalne ili simbolične, što šalje poruku nekažnjivosti i podstiče dalje napade.

Ova diskrepancija obeshrabruje građane da prijavljuju incidente, a napadače ohrabruje da nastave s praksama uznemiravanja i prijetnji.

Još jedna dimenzija raskoraka je selektivna primjena propisa. Dok se u slučajevima koji se tiču političkih interesa i vlasti zakoni često koriste brzo i represivno (npr. pokretanje procesa protiv građana zbog uvredljivih komentara na društvenim mrežama), u slučajevima kada su žrtve novinari, aktivisti ili kritički orijentisani građani, institucije pokazuju nevoljkost da zaštite njihove interese. Time se zakon ne koristi kao neutralni instrument zaštite, već kao alat političke kontrole i pritiska.

Formalno postojanje propisa ne znači mnogo ukoliko institucije nemaju kapacitete da ih provode. U BiH i RS-u evidentan je:

- nedostatak stručnih kadrova obučenih za digitalnu forenziku, analizu online prijetnji i zaštitu podataka;
- slaba koordinacija između institucija (npr. policije, tužilaštava, agencije za zaštitu podataka i regulatornih tijela);
- nedostatak tehničke opreme za praćenje i procesuiranje sofisticiranih cyber napada.

To stvara situaciju u kojoj i najbolji zakonski okvir ostaje mrtvo slovo na papiru jer se njegovo provođenje ne može osigurati u praksi.

Bosna i Hercegovina je potpisnica brojnih međunarodnih dokumenata (Konvencija 108+, Budimpeštanska konvencija, ECHR), a u procesu evropskih integracija postoji i obaveza usklađivanja sa GDPR-om i DSA-om. Međutim, lokalna realnost pokazuje da ti standardi nisu operacionalizovani:

- pravna terminologija je često zastarjela i ne prati nove oblike digitalnog nasilja;
- međunarodne obaveze se sprovode formalno, bez edukacije službenika ili ulaganja u tehničke kapacitete;
- izvještaji o napadima na novinare i aktiviste rijetko rezultiraju sudskim epilogom, iako bi po EU standardima institucije morale reagovati hitno i proaktivno.

Ovaj jaz proizvodi niz negativnih posljedica:

1. Nekažnjivost počinilaca – stvaranje percepcije da je online nasilje dozvoljeno i bezopasno, iako ostavlja ozbiljne posljedice po žrtve;
2. Autocenzura žrtava – novinari i aktivisti povlače se iz javnog prostora ili izbjegavaju određene teme iz straha od napada;

3. Slabljenje povjerenja u institucije – građani gube vjeru da će pravni sistem zaštititi njihova prava;
4. Erozija demokratije – kada su digitalni prostori nesigurni, sloboda izražavanja i učešće u javnom životu su ograničeni.

Prevazilaženje ovog jaza zahtijeva tri paralelna procesa:

- Normativnu reformu – usklađivanje zakona sa međunarodnim standardima i jasno prepoznavanje novih oblika digitalnog nasilja;
- Jačanje institucija – obuka kadrova, ulaganje u tehničke resurse, bolja koordinacija između različitih nivoa vlasti;
- Promjenu institucionalne kulture – prelazak sa pasivnog na proaktivni pristup, gdje institucije ne čekaju prijave žrtava, već same prate i sankcionišu zloupotrebe u digitalnom prostoru.

Ukratko, normativno–praktični raskorak u Republici Srpskoj i BiH pokazuje da postojanje zakona nije dovoljno: ključna prepreka je njihova selektivna, spora i nedosljedna primjena. Dok se taj jaz ne prevaziđe, digitalna prava ostaju deklarativna, a građani nezaštićeni.

4. Rezultati empirijskog istraživanja

Empirijsko istraživanje sprovedeno u okviru ovog projekta imalo je za cilj da pruži uvid u oblike, učestalost i posljedice kršenja digitalnih prava novinara, aktivista i građana u Republici Srpskoj, kao i u institucionalne reakcije na takve pojave. Podaci su prikupljeni kombinacijom kvantitativnih i kvalitativnih metoda: analizom slučajeva iz baze podataka, polustrukturisanim intervjuima sa stručnjacima (Dejan Lučka, Mirko Sajić, Borislav Vukojević, Aleksandar Mastilović), te pregledom dostupnih medijskih izvještaja i dokumenata organizacija civilnog društva. Rezultati ukazuju na širok spektar kršenja digitalnih prava koji obuhvata online uznemiravanje, govor mržnje, neovlašteni pristup podacima, cenzuru i hakerske napade.

4.1. Struktura i rasprostranjenost incidenata

Analiza baze podataka o kršenjima digitalnih prava pokazala je da je tokom perioda istraživanja zabilježeno više incidenata različite prirode, pri čemu se izdvajaju sljedeći obrasci:

- Online uznemiravanje i govor mržnje – najčešći oblik kršenja, čineći više od trećine svih zabilježenih slučajeva. Žrtve su prvenstveno novinari i aktivisti, koji su targetirani putem društvenih mreža (Facebook, X/Twitter) i lokalnih portala. Napadi su uključivali uvrede na nacionalnoj i rodnoj osnovi, prijetnje fizičkim nasiljem, kao i seksualizovane prijetnje;
- Dezinformacije i diskreditacija – svaki četvrti slučaj odnosio se na organizovane kampanje dezinformacija, gdje su novinari i javne ličnosti (npr. Srđan Puhalo) bili meta koordinisanih hajki i manipulacija. Ove kampanje su često vođene bot nalozima ili putem portala bez impresuma, što otežava identifikaciju počinilaca;
- Neovlašteni pristup podacima i zloupotreba identiteta – u više slučajeva evidentirano je hakovanje email naloga i lažne online transakcije s ciljem krađe ličnih i finansijskih

podataka. Posebno zabrinjavaju slučajevi u kojima su lični podaci novinara završili u rukama državnih institucija, što ukazuje na institucionalnu zloupotrebu;

- Hakerski napadi na medije i aktivističke grupe – portali poput Capitala i Istrage, kao i aktivistička grupa BOJkot.ba, bili su mete sofisticiranih DDoS i phishing napada, često koordinisanih iz inostranstva. Ovi napadi su se dešavali u trenucima objavljivanja istraživačkih tekstova ili tokom organizovanja protesta, što ukazuje na njihovu političku pozadinu;
- Online cenzura i algoritamska ograničenja – novinari i aktivisti izvijestili su o uklanjanju objava i smanjivanju vidljivosti sadržaja na Facebooku, najčešće bez obrazloženja i mogućnosti efikasne žalbe. Ovo stvara dodatnu neizvjesnost i podstiče autocenzuru.

4.2. Profil počinilaca

Istraživanje ukazuje da su počinioci online napada raznoliki:

- anonimni korisnici društvenih mreža i bot nalozi;
- javni zvaničnici (npr. pojedini politički funkcioneri) koji koriste institucionalni autoritet da targetiraju novinare;
- organizovane grupe povezane sa ekonomskim i političkim interesima;
- hakerske mreže koje djeluju izvan BiH, koristeći servere u Singapuru, Holandiji i drugim zemljama kako bi prikrile tragove.

4.3. Posljedice po žrtve

Empirijski podaci jasno ukazuju na višeslojne posljedice kršenja digitalnih prava:

- psihološke – žrtve prijavljuju osjećaj straha, anksioznosti, pa čak i simptome PTSP-a, naročito kada su napadi uključivali prijetnje članovima porodice;
- profesionalne – prisutna je autocenzura, selekcija tema i odustajanje od osjetljivih istraživačkih priča, što dugoročno ugrožava kvalitet novinarstva;
- društvene – učestalo targetiranje aktivista dovodi do njihovog povlačenja iz javnog života i smanjenja povjerenja građana u medije;
- bezbjednosne – zloupotreba ličnih podataka povećava rizik od krađe identiteta, finansijskih prevara i fizičkog ugrožavanja.

4.4. Institucionalni odgovor

Rezultati pokazuju da je institucionalni odgovor izrazito slab. Policija i tužilaštva u većini slučajeva minimiziraju težinu digitalnog nasilja, tretirajući ga kao „uvrede“ ili „lične sukobe“. CERT RS fokusiran je prvenstveno na infrastrukturne incidente, dok se napadi na pojedince i medije ignorišu. Agencija za zaštitu ličnih podataka BiH djeluje formalno i sa ograničenim kapacitetima, dok Ombudsman uglavnom izdaje preporuke koje institucije ne moraju da implementiraju. Time se stvara institucionalni vakuum, gdje se digitalna prava priznaju na papiru, ali ostaju nezaštićena u praksi.

4.5. Uporedni uvid

Podaci iz RS-a uklapaju se u širi regionalni obrazac. Prema BIRN izvještajima i studijama European Centre for Press and Media Freedom, online napadi na novinare u Jugoistočnoj Evropi imaju visoku učestalost, uz mali broj procesuiranih slučajeva. BiH se tako pridružuje zemljama u kojima digitalni prostor postaje instrument političkog pritiska, a ne prostor slobode izražavanja.

4.6. Sinteza empirijskih nalaza

Rezultati empirijskog istraživanja ukazuju na nekoliko ključnih zaključaka:

1. Digitalni napadi su sistemski i učestali, posebno usmjereni na novinare i aktiviste;
2. Najčešći oblici kršenja su online uznemiravanje, govor mržnje i hakerski napadi, ali sve veću opasnost predstavljaju i algoritamska ograničenja;
3. Institucionalni odgovor je nedovoljan, što produbljuje jaz između formalnih normi i njihove primjene;
4. Posljedice po društvo su višestruke – od autocenzure i profesionalne degradacije novinarstva do slabljenja demokratije i povjerenja građana u institucije.

Ovim rezultatima potvrđuje se centralna teza projekta – da je digitalni prostor u Republici Srpskoj neregulisan, nesiguran i često zloupotrebljen, te da je uloga civilnog društva i medija ključna u dokumentovanju, praćenju i zagovaranju promjena u oblasti digitalnih prava.

5. Studije slučaja

Kako bi se kvantitativni nalazi iz baze podataka dopunili i osnažili konkretnim primjerima iz prakse, u ovom poglavlju analiziraju se studije slučaja dokumentovane kroz medijske izvještaje, prijave civilnog društva i ekspertske komentare. Ove studije pružaju narativni i kontekstualni okvir za razumijevanje šire slike o tome kako digitalna prava u Republici Srpskoj i Bosni i Hercegovini bivaju ugrožena, kakve posljedice trpe novinari i aktivisti, te na koji način reaguju institucije i platforme.

5.1. Hakerski napad na BOJkot.ba (februar 2025)

Tokom dvodnevnog građanskog bojkota trgovinskih lanaca u BiH (7–9. februar 2025), organizatori okupljeni oko inicijative BOJkot.ba suočili su se sa ozbiljnim digitalnim napadima.

- Priroda napada: hakovanje Facebook stranice i masovno uklanjanje objava koje su sadržavale pozive na bojkot.
- Posljedice: gubitak komunikacijskog kanala prema javnosti u ključnim satima akcije, što je smanjilo mobilizacijski potencijal inicijative i unijelo nesigurnost među organizatore.
- Širi značaj: ovaj slučaj pokazuje kako digitalni napadi na aktivističke grupe imaju direktne posljedice na slobodu udruživanja i pravo građana na protest, jer onemogućavaju artikulisanje društvenog nezadovoljstva u javnoj sferi.

- Institucionalni odgovor: izostao; inicijatori su se oslonili na sopstvene pokušaje vraćanja kontrole nad stranicom i komunikaciju preko alternativnih kanala (WhatsApp grupe, Telegram).

5.2. Napadi na medije: Capital (mart 2025) i Istraga (april 2025)

U martu 2025. portal Capital.ba, poznat po istraživačkim tekstovima o korupciji i zloupotrebama javnih resursa, bio je meta DDoS napada koji je trajao više sati. Mjesec dana kasnije, slični napadi pogodili su i portal Istraga.ba.

- Priroda napada: masovno slanje zahtjeva prema serverima portala, što je dovelo do prekida rada i nemogućnosti pristupa sadržaju. U slučaju Istrage, napadi su koincidirali s objavljivanjem tekstova o vezama političkih elita i kriminalnih struktura.
- Posljedice: oba portala su imala pad čitanosti, dok su novinari bili pod dodatnim pritiskom zbog nemogućnosti da pravovremeno informišu javnost.
- Širi značaj: ovi slučajevi ilustrativno pokazuju kako se tehnički napadi koriste kao oblik digitalne cenzure. Napadači ne pokušavaju samo zastrašiti novinare, već im oduzimaju osnovno sredstvo rada – platformu za objavljivanje.
- Institucionalni odgovor: sveden na konstataciju da se radi o „tehničkom problemu“; nije bilo konkretnih istraga koje bi vodile ka identifikaciji počinilaca, iako su tragovi napada vodili ka inostranim serverima (Singapur, Holandija).

5.3. Online hajke i prijetnje eko-aktivistima (slučaj Ozren)

Putem fejsbuk naloga Ozren na dlanu, te lokalnih dobojskih portala Olovka.ba i RTV Doboj, kao i portala Tanjug Srpske, vodila se hajka na eko aktiviste i portale Antikorupcija.ba i Odgovorno.ba zbog kritika načina i dodjele koncesija na geološka istraživanja na Ozrenu. Čak je objavljena i šema čime se, kako je navedeno u anketi, crtala meta na čelo eko aktivistima i novinarima koji kritički pišu o navedenoj temi.

Inače, radi se o napadima koji su se dešavali unazad godinu i po dana, a eko aktivisti Ozrenskog studenca i Ozren Gostilj su podnijeli u januaru 2025. godine krivičnu prijavu OJT Doboj, na koju su iz OJT odgovorili u maju 2025. godine. U prijavi je navedeno da je predmet kod MUP-a, odnosno da ništa nije učinjeno na procesuiranju.

- Priroda napada: kampanje na društvenim mrežama i lokalnim portalima, u kojima su aktivisti označavani kao „izdajnici“, „strani plaćenici“ i „neprijatelji RS“. U pojedinim slučajevima prijetnje su uključivale i pozive na fizičko nasilje.
- Posljedice: dio aktivista se povukao iz javnog angažmana.
- Širi značaj: ovaj slučaj pokazuje kako digitalni prostor postaje nastavak offline represije i sredstvo za gušenje građanskog aktivizma. Sistematske hajke stvaraju atmosferu straha i obeshrabruju građane da se uključe u javne debate.
- Institucionalni odgovor: policija i tužilaštvo nisu pokrenuli istrage. Time je poslana poruka da su ovakve prijetnje nekažnjive.

5.4. Seksualizovane prijetnje na društvenim mrežama

Najteži slučaj u istraživanju zabilježen je u martu 2025. godine kada je putem društvene mreže X jedna osoba prijetila silovanjem djeteta. Ovaj slučaj prevazilazi dimenzije individualne ugroženosti i otvara pitanje sistemske ranjivosti digitalnog prostora u Republici Srpskoj i Bosni i Hercegovini. Seksualizovane prijetnje, naročito kada su usmjerene prema porodici novinara ili aktivista, imaju dalekosežan psihološki i društveni uticaj: one ne samo da targetiraju pojedinca već pokušavaju da ga diskredituju i zastraše kroz prijetnje najintimnijem dijelu njegovog života. Time se nasilje pomjera s profesionalne na privatnu sferu, pojačavajući efekat pritiska i povećavajući vjerovatnoću autocenzure.

- Priroda napada: korištenje anonimnih profila za slanje vulgarnih i prijetećih poruka.
- Posljedice: psihološki pritisak, autocenzura i povlačenje sa društvenih mreža.
- Širi značaj: ovakav vid prijetnji predstavlja indikator duboke normalizacije digitalnog nasilja, gdje anonimnost i nekažnjivost na mrežama postaju podloga za najekstremnije oblike zastrašivanja. Posebno zabrinjava činjenica da institucije često ne reaguju adekvatno ili da istrage stagniraju, što šalje poruku da su čak i najteže prijetnje – uključujući one koje se odnose na djecu – tolerisane. Time se podriva povjerenje građana u pravni sistem i ostavlja prostor za dalju eskalaciju nasilja.
- Institucionalni odgovor: ispitanik je naveo da zbog interesa istrage koju vode policija RS i okružni tužilac u Banjaluci ne može govoriti o identitetima jer nije siguran u imena.

5.5. Cenzura i ograničenja vidljivosti na društvenim mrežama

Pojedini novinari i aktivisti izvijestili su da su im objave uklanjane ili da im je onemogućeno sponzorisanje sadržaja na Facebooku, posebno kada su teme bile politički i društveno osjetljive (npr. objave sa hashtagom #UDT u slučaju BIRN-a).

- Priroda problema: algoritamske odluke platformi bez jasnog obrazloženja i bez mogućnosti brze žalbe.
- Posljedice: smanjena vidljivost sadržaja i gubitak mogućnosti da se informacije od javnog interesa prošire do šire publike.
- Širi značaj: ovaj slučaj pokazuje da cenzura ne dolazi uvijek od države, već i od privatnih platformi koje kroz netransparentne algoritme oblikuju javni diskurs.
- Institucionalni odgovor: potpuno odsutan, jer domaće regulatorne agencije nemaju ingerencije nad globalnim platformama.

5.6. Zaključna zapažanja iz studija slučaja

Analiza konkretnih incidenata potvrđuje nekoliko važnih uvida:

1. Napadi su ciljano usmjereni – najčešće protiv onih koji istražuju korupciju, kritikuju vlast ili se bave ekološkim i društvenim aktivizmom;
2. Spektar metoda je širok – od tehničkih (DDoS, hakovanja) preko psiholoških (uvrede, prijetnje) do strukturnih (algoritamska ograničenja);

3. Institucionalni odgovor je minimalan ili selektivan, što potvrđuje nalaz o normativno–praktičnom raskoraku;
4. Posljedice su višeslojne – osim što utiču na pojedince, napadi erodiraju javni interes, umanjuju slobodu izražavanja i dovode do autocenzure.

Ove studije slučaja jasno pokazuju da je digitalni prostor u RS i BiH ne samo tehnički, već i politički konstruisan, te da se zloupotrebljava za gušenje kritičkog diskursa i obeshrabrivanje građanske participacije.

6. Diskusija

Diskusija ima za cilj da objedini nalaze iz kvantitativne baze, kvalitativnih intervjua i studija slučaja te da ih stavi u širi teorijski, društveni i politički okvir. Na taj način se otkriva kako se različiti nivoi ugrožavanja digitalnih prava – od individualnih incidenata do institucionalne inertnosti – prepliću i stvaraju složen ambijent nesigurnosti u digitalnom prostoru Republike Srpske i Bosne i Hercegovine.

6.1. Povezanost kvantitativnih i kvalitativnih nalaza

Kvantitativna baza pokazuje da su online uznemiravanje i govor mržnje najčešći oblici kršenja (nešto više od trećine slučajeva), dok kvalitativni podaci dopunjuju ovu sliku opisima rodno zasnovanih prijetnji, targetiranjem novinara, kao i orkestriranih kampanja diskreditacije. Slučajevi hakerskih napada na portale Capital i Istragu pokazuju da digitalni napadi nisu nasumični, već se intenziviraju u trenucima političke osjetljivosti – tokom istraživačkih objava ili organizovanja protesta.

Ovo upućuje na obrazac u kojem digitalna kršenja ne nastaju samo kao „spontano nasilje“, već kao dio šire strategije zastrašivanja, disciplinovanja i ograničavanja javne debate.

6.2. Normativno–praktični raskorak u fokusu

Jedan od najizraženijih zaključaka jeste postojanje dubokog jaza između zakona i njihove primjene. Formalno, BiH i RS imaju propise o zaštiti podataka, prekršaje za uvrede i krivične odredbe koje obuhvataju prijetnje, ali u praksi institucije:

- minimiziraju prijave, tretirajući ih kao „lične sukobe“,
- rijetko sprovode istrage ili podižu optužnice,
- a kazne su minimalne i bez preventivnog efekta.

Ova neusklađenost šalje dvostruku poruku: napadači osjećaju nekažnjivost, dok žrtve gube povjerenje u sistem. Time se digitalni prostor pretvara u „sivu zonu“ gdje pravila postoje, ali se selektivno ili nikako ne primjenjuju.

6.3. Institucionalni vakuum i pasivnost

Mora se naglasiti i institucionalni vakuum: CERT RS je ograničen na tehničke incidente u javnim sistemima; Agencija za zaštitu ličnih podataka ima nedovoljne resurse; policija i tužilaštva ne pokazuju spremnost da tretiraju digitalno nasilje kao ozbiljnu prijetnju. U tom

kontekstu, napadi na novinare i aktiviste prolaze bez posljedica, dok globalne platforme (Facebook, X) djeluju po vlastitim pravilima, nerijetko uklanjajući sadržaje od javnog interesa.

Ovaj paralelizam – nemoć lokalnih institucija i samovolja globalnih platformi – dodatno sužava prostor slobode izražavanja.

6.4. Društveni i politički kontekst

Rezultati pokazuju da digitalni napadi nisu izolovani, već da odražavaju širi društveni i politički ambijent. U polarizovanom društvu kakvo je u RS i BiH:

- političke elite koriste digitalni prostor za targetiranje kritičara, dok njihovi simpatizeri nastavljaju hajke na društvenim mrežama;
- građani normalizuju nasilje online, tretirajući ga kao neizbježni „dio javne debate“;
- novinari i aktivisti internalizuju pritisak, pribjegavaju autocenzuri i povlačenju s mreža.

Ovakav ambijent vodi ka eroziji javnog interesa i demokratije: ako su oni koji ukazuju na zloupotrebe i društvene probleme kontinuirano mete, društvo gubi kapacitet da kritički preispituje vlast i institucije.

6.5. Tehnološki izazovi i algoritamska neprozirnost

Kombinacija ljudskih i algoritamskih faktora stvara složeni okvir. S jedne strane, napadači koriste društvene mreže, bot mreže i hakerske alate. S druge strane, algoritmi platformi dodatno oblikuju javni diskurs:

- uklanjaju se objave sa društveno važnim sadržajem,
- ograničava se doseg novinarskih izvještaja,
- dok se sadržaji koji izazivaju „engagement“ (npr. senzacionalistički sadržaji) podstiču i šire.

Ovaj fenomen algoritamske „regulacije kroz arhitekturu“ stavlja novinare i aktiviste u dvostruko nepovoljan položaj: napadaju ih anonimni korisnici i interesne grupe, a istovremeno platforme smanjuju vidljivost njihovog rada.

6.6. Regionalni i evropski kontekst

Nalazi iz RS u velikoj mjeri odražavaju šire trendove u regionu i EU. Istraživanja BIRN-a i ECPMF-a pokazuju da je online nasilje protiv novinara sve prisutnije, a institucionalne reakcije slabe. Međutim, razlika je u stepenu institucionalne proaktivnosti: dok u nekim zemljama EU postoje specijalizovane policijske jedinice za cyber kriminal i programi podrške novinarima, u BiH taj sistem tek treba izgraditi.

Drugim riječima, BiH i RS se nalaze u svojevrsnom „regulatornom limbu“: vezane su međunarodnim obavezama, ali nemaju kapacitete niti političku volju da ih sprovedu.

6.7. Sinteza diskusije i nalaza

Diskusija jasno pokazuje da se u Republici Srpskoj formirao sistem digitalne nesigurnosti u kojem:

1. Institucije zakazuju – zakoni postoje, ali nisu efikasno implementirani;
2. Platforme dominiraju – algoritmi oblikuju javni diskurs, često na štetu slobode izražavanja;
3. Društvo normalizuje nasilje – građani i javnost ne prepoznaju digitalno nasilje kao ozbiljan problem;
4. Žrtve se povlače – novinari i aktivisti postaju izolovani, što osiromašuje javni prostor.

Sveukupno, diskusija potvrđuje da kršenja digitalnih prava u RS nisu slučajna niti pojedinačna, već da predstavljaju strukturalni problem u kojem se prepliću politički interesi, institucionalna pasivnost, tehnološki izazovi i društvene norme. Ako se ovi obrasci ne adresiraju sistemski, digitalni prostor će postati još nesigurniji i zatvoreniji, čime se ugrožava ne samo sloboda izražavanja, već i temelji demokratije.

7. Preporuke

Na osnovu kvantitativnih i kvalitativnih nalaza, studija slučaja i šire teorijske analize, moguće je izdvojiti set preporuka koje ciljaju tri nivoa aktera: institucije Republike Srpske i Bosne i Hercegovine, organizacije civilnog društva i medije, te globalne digitalne platforme i međunarodne partnere. Preporuke su usmjerene ka smanjenju normativno–praktičnog raskoraka, jačanju institucionalnih kapaciteta, unapređenju sigurnosti novinara i aktivista, te uspostavljanju transparentnijeg i pravednijeg digitalnog okruženja.

7.1. Preporuke za institucije u RS i BiH

1. Normativno usklađivanje sa EU standardima
    - Hitno usklađivanje Zakona o zaštiti ličnih podataka sa GDPR-om, uz uvođenje mehanizama poput prava na zaborav, obaveze prijavljivanja povrede podataka i jačanja funkcije službenika za zaštitu podataka (DPO).
    - Donošenje posebnih odredbi u Krivičnim zakonima koje jasno prepoznaju *cyber bullying*, online prijetnje i digitalno nasilje kao zasebna krivična djela.
2. Jačanje institucionalnih kapaciteta
    - Osnivanje specijalizovanih jedinica u policiji i tužilaštvu za procesuiranje digitalnog nasilja i online prijetnji.
    - Razvoj kapaciteta CERT timova na entitetskom i državnom nivou kako bi, osim zaštite infrastrukture, obuhvatili i zaštitu pojedinaca, medija i OCD-a.
    - Povećanje budžetskih sredstava i stručnog osoblja u Agenciji za zaštitu ličnih podataka BiH.
3. Proaktivna zaštita i transparentnost
    - Uvođenje obaveze institucija da vode javno dostupne statistike o prijavljenim slučajevima digitalnog nasilja i zloupotreba, te da redovno objavljuju izvještaje.

- Uspostavljanje nacionalnih i entitetskih *helpline* kontakt tačaka (24/7) za hitnu podršku novinarima i aktivistima koji se suoče sa prijetnjama.
- Edukacija javnih službenika o sigurnom rukovanju ličnim podacima i odgovornosti u digitalnom prostoru.

4. Politička odgovornost
    - Jasna distanca političkih institucija i funkcionera od orkestriranih kampanja mržnje i prijetnji, uz usvajanje kodeksa ponašanja javnih zvaničnika u online prostoru.

7.2. Preporuke za civilno društvo i medije

1. Jačanje digitalne sigurnosti u redakcijama i OCD-ima
    - Uvođenje standardizovanih procedura zaštite (dvofaktorska autentifikacija, šifrirana komunikacija, upravljanje lozinkama, redovan backup podataka).
    - Formiranje internih timova ili „bezbjednosnih koordinatora“ koji će pratiti potencijalne digitalne prijetnje i obučavati kolege.
2. Obuka i svijest
    - Organizacija kontinuiranih treninga za novinare i aktiviste o prepoznavanju digitalnih prijetnji (phishing, deepfake, malware) i o digitalnoj higijeni.
    - Povećanje digitalne i medijske pismenosti građana kroz radionice, kurseve i javne kampanje, sa naglaskom na zaštitu privatnosti i kritičko čitanje online sadržaja.
3. Solidarnost i dokumentovanje slučajeva
    - Umrežavanje novinara i aktivista radi brze razmjene informacija i koordinisanih reakcija u slučaju napada.
    - Sistematsko dokumentovanje svih prijetnji i napada u zajedničkim bazama podataka koje se mogu koristiti za zagovaranje promjena i pritisak na institucije.
    - Razvijanje *peer-to-peer* podrške (psihološke, pravne i tehničke) za one koji postaju mete napada.
4. Diversifikacija kanala distribucije sadržaja
    - Pored oslanjanja na društvene mreže, mediji i organizacije civilnog društva trebaju jačati direktne kanale komunikacije sa publikom (newsletter, podkasti, vlastite aplikacije), kako bi smanjili zavisnost od algoritamske kontrole globalnih platformi.

7.3. Preporuke za digitalne platforme i međunarodne aktere

1. Veća transparentnost digitalnih platformi
    - Uvođenje jasnih i razumljivih obrazloženja prilikom uklanjanja sadržaja, sa brzim i efikasnim mehanizmima žalbi.

- Lokalizacija algoritama i moderacijskih politika tako da prepoznaju specifičnosti jezika i političkog konteksta u BiH i regionu.

2. Međunarodni pritisak i podrška

    - Uključivanje pitanja digitalne bezbjednosti u EU izvještaje o napretku BiH i uslovljavanje evropskih integracija napretkom u ovoj oblasti.
    - Aktivna podrška međunarodnih organizacija (OSCE, UNESCO, ECPMF, IPI) u vidu tehničke pomoći, treninga i fondova za bezbjednost novinara i organizacija civilnog sdruštva.
    - Saradnja sa evropskim tijelima radi primjene instrumenata poput *Digital Services Acta* i *Kodeksa dobre prakse protiv dezinformacija* u lokalnom kontekstu.

7.4. Preporuke u širem društvenom kontekstu

1. Promjena društvenih normi

    - Pokretanje javnih kampanja koje osuđuju online nasilje i ističu posljedice po žrtve.
    - Uključivanje pitanja digitalnih prava u obrazovni sistem – od osnovnih škola do univerziteta, kroz predmete o medijskoj i digitalnoj pismenosti.

2. Rodna perspektiva

    - Razvijanje posebnih programa zaštite novinarki i aktivistkinja, koje su posebno izložene seksualizovanom i rodno zasnovanom digitalnom nasilju.

3. Psihološka podrška

    - Uspostavljanje servisa za mentalno zdravlje novinara i aktivista pogođenih digitalnim prijetnjama, kako bi se smanjile dugoročne posljedice (stres, anksioznost, PTSP).

Najvažnija poruka ovih preporuka jeste da digitalna prava ne mogu biti zaštićena parcijalno. Potreban je holistički pristup koji uključuje:

- zakonsku reformu i institucionalno jačanje,
- edukaciju i osnaživanje novinara, aktivista i građana,
- transparentnost i odgovornost digitalnih platformi,
- promjenu društvenih normi i izgradnju kulture nulte tolerancije prema online nasilju.

Samo kombinacijom ovih mjera moguće je stvoriti sigurno digitalno okruženje koje će omogućiti novinarima i građanima da slobodno izražavaju mišljenja, a društvu da koristi puni potencijal digitalne sfere za demokratizaciju i napredak.

8. Zaključak

Nalazi ovog istraživanja jasno pokazuju da su digitalna prava u Republici Srpskoj i Bosni i Hercegovini ozbiljno ugrožena i da se građani, novinari i aktivisti suočavaju sa kontinuiranim izazovima u online prostoru. Kombinacijom kvantitativnih podataka, intervjua sa stručnjacima i studija slučaja pokazano je da digitalni prostor, iako formalno zamišljen kao slobodna i demokratska arena komunikacije, u praksi postaje polje represije, zloupotreba i institucionalne pasivnosti.

8.1. Ključni nalazi

- Učestalost i oblici napada: Najzastupljeniji oblici kršenja digitalnih prava su online uznemiravanje, govor mržnje i dezinformacije, dok tehnički sofisticiraniji napadi (DDoS, hakovanja, phishing) ciljano pogađaju medije i organizacije civilnog društva u trenucima kada objavljuju osjetljive informacije.
- Anonimnost i nekažnjivost: Više od dvije trećine napada dolazi od anonimnih ili pseudonimnih počinilaca, što u kombinaciji sa institucionalnom inertnošću stvara atmosferu nekažnjivosti.
- Institucionalni vakuum: Postojanje zakona ne garantuje zaštitu, jer su institucije nedovoljno opremljene, pasivne ili selektivne u primjeni. Normativno–praktični raskorak jedan je od ključnih generatora nesigurnosti u digitalnoj sferi.
- Algoritamska cenzura i platformska zavisnost: Globalne platforme kroz svoje algoritme oblikuju javni diskurs, često uklanjajući sadržaje od javnog interesa ili smanjujući njihovu vidljivost. Time se stvara dvostruki pritisak – od napadača i od samih platformi.

8.2. Šire implikacije

Ovakvo stanje ima višestruke posljedice:

- na pojedince – psihološki pritisak, autocenzura, povlačenje sa mreža, pa čak i profesionalno napuštanje novinarstva ili aktivizma;
- na medije i organizacije civilnog društva – smanjenje vidljivosti, gubitak publike i resursa, otežan rad u javnom interesu;
- na društvo u cjelini – erozija slobode izražavanja, smanjenje pluralizma i demokratije, normalizacija nasilja i nepovjerenje u institucije.

Drugim riječima, digitalna nesigurnost nije izolovan problem novinara i aktivista, već sistemski izazov koji pogađa sve građane i dugoročno ugrožava društveni razvoj i evropske integracije BiH.

8.3. Perspektiva

Izvještaj pokazuje da je zaštita digitalnih prava strateški prioritet za BiH i RS, i to iz tri ključna razloga:

1. Demokratski kapacitet – bez slobodnog i sigurnog digitalnog prostora nema stvarnog pluralizma niti kritičkog preispitivanja vlasti;

2. Evropske integracije – usklađivanje sa GDPR-om, DSA-om i NIS2 direktivom predstavlja neophodan uslov na putu ka EU;
3. Društvena kohezija i povjerenje – samo sistemska zaštita može povratiti povjerenje građana u institucije i omogućiti uključivanje šire javnosti u digitalne procese.

Digitalna prava nisu apstraktan pravni koncept, već konkretna ljudska prava u digitalnom dobu. U Republici Srpskoj i BiH, ona se svakodnevno testiraju kroz prijetnje, napade i cenzuru. Ovaj izvještaj jasno pokazuje da trenutni sistem zaštite nije dovoljan – potrebna je kombinacija zakonskih reformi, institucionalnog jačanja, međunarodne podrške i društvene solidarnosti.

Ako se ovi izazovi ne adresiraju, digitalni prostor će postati trajno obilježen strahom, manipulacijama i ograničenom slobodom. Suprotno tome, ako se preporuke iz ovog izvještaja implementiraju, digitalna sfera može postati ključni instrument demokratizacije, zaštite novinara i aktivista, te osnaživanja građana da slobodno učestvuju u javnom životu.

Reference

1. Becker, M. (2019). *Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy*. **Ethics Inf Technol 21**, 307–317.
2. Benedek, W. (2007). **Understanding Human Rights: Manual on Human Rights Education**. European Training and Research Centre for Human Rights and Democracy (ETC), Graz.
3. BIRN. (2025). **Surveillance and Censorship Worsening in Western Balkans: BIRN Report**. Balkan Insight.
4. BIRN. (2025). **Digital Rights Review: Online Abuses, Deepfakes and Scams Proliferate**. Balkan Insight.
5. BIRN. (2025). **Digital Rights Review: Governments and Big Tech 'Enabling' Online Violations**. Balkan Insight.
6. BIRN. (2025). **Digital Rights Review: AI-Driven Violations Go Unchecked in South-East Europe**. Balkan Insight.
7. Castells, M. (2009). **Communication Power**. Oxford University Press.
8. European Centre for Press and Media Freedom (ECPMF). (2023). **Annual report on threats to journalists in the EU**. Leipzig: ECPMF.
9. Evropska komisija. (2022). **Digital Services Act (Regulation (EU) 2022/2065)**. Official Journal of the European Union.
10. Evropska komisija. (2023). **Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)**. Official Journal of the European Union.
11. Evropski sud za ljudska prava. (1976). **Handyside v. United Kingdom, Application no. 5493/72**.
12. Gerila. (2025). **Digitalna prava: Nevidljiva granica slobode u online svijetu**. Gerila.info.
13. Gerila. (2025). **„Digitalna paljba": Kako prijetnje i uvrede na mrežama ciljaju novinare i aktiviste**. Gerila.info.
14. Gerila. (2025). **Digitalna (ne)zaštićenost: Širenje dezinformacija u Republici Srpskoj**. Gerila.info.

15. Gerila. (2025). **Lični podaci kao oružje: Novinari i aktivisti u Republici Srpskoj na meti neovlašćenih upada u digitalni identitet**. Gerila.info.
16. Gerila. (2025). **Sloboda izražavanja pod algoritamskim nadzorom: Gdje prestaje moderacija, a počinje cenzura**. Gerila.info.
17. Hintz, A., Dencik, L., & Wahl-Jørgensen, K. (2019). **Digital citizenship in a datafied society**. Cambridge: Polity Press.
18. Hodžić, K. (2025). Intervju za Gerila.info.
19. Kancelarija za demokratske institucije i ljudska prava (ODIHR). (2022). **Safety of journalists guidebook**. OSCE.
20. Lessig, L. (2006). **Code: And other laws of cyberspace (Version 2.0)**. New York: Basic Books.
21. Lučka, D. (2025). Intervju za Gerila.info.
22. Mastilović, A. (2025). Intervju za Gerila.info.
23. Oomen, B., & van den Berg, E. (2014). *Human rights cities: Urban actors as pragmatic idealistic human rights users*. **Human Rights & International Legal Discourse**, 8(2), 160–185.
24. Puhalo, S. (2025). Izjava u okviru istraživanja Gerila.info.
25. Reporteri bez granica. (2024). **World Press Freedom Index 2024: Bosnia and Herzegovina**. Reporters Without Borders.
26. Sajić, M. (2025). Intervju za Gerila.info.
27. Ujedinjene nacije. (1948). **Universal Declaration of Human Rights**. General Assembly Resolution 217 A (III).
28. Ujedinjene nacije. (1966). **International Covenant on Civil and Political Rights**. General Assembly Resolution 2200A (XXI).
29. Vasak, K. (1977). **Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights**. UNESCO Courier, 30(11), 29–32.
30. Vukojević, B. (2025). Intervju za Gerila.info.
31. Zuboff, S. (2019). **The age of surveillance capitalism: The fight for a human future at the new frontier of power. First edition**. New York: PublicAffairs.

Funded by
the European Union

Projekat: Osnaživanje novinarstva u digitalnom dobu - Jačanje digitalne bezbjednosti i kapaciteta medija i organizacija civilnog društva na Zapadnom Balkanu

Autor: Servis za medijsku profesionalnu edukaciju i razvoj SEMPER

Septembar 2025.

Ova publikacija je proizvedena uz finansijsku podršku Evropske unije. Sadržaj ovog materijala je isključiva odgovornost SEMPER-a i ne odražava nužno stavove Evropske unije.

Reporting Digital Rights & Freedoms