

ZLOUPORABA DRUSTVENIH MREŽA KROZ ONLINE NASILJE U BOSNI I HERCEGOVINI

DOI: 10.70329/2744-2403.2026.6.11.5

Pregledni članak

Atina Perković, PhDc

Sažetak:

Zlouporaba društvenih mreža kroz online nasilje predstavlja sve izraženiji problem suvremenog digitalnog društva, osobito među djecom i mladima koji su najaktivniji korisnici digitalnih platformi. Analiziranjem fenomena online nasilja, njegovih oblika, uzroka i posljedica, kao i zakonodavnog okvira u Bosni i Hercegovini koji se odnosi na ovu problematiku. Pregledom relevantne znanstvene i stručne literature te analizi važećih zakonskih akata, rezultati ukazuju da online nasilje uključuje različite oblike ponašanja, poput vrijeđanja, prijetnji, širenja dezinformacija, narušavanja privatnosti i govora mržnje. Uviđa se da takvi oblici nasilja imaju značajne psihološke, socijalne i akademske posljedice, uključujući anksioznost, depresiju i socijalnu izolaciju. Posebno je naglašena uloga digitalnih platformi, čije karakteristike poput anonimnosti i viralnosti doprinose širenju nasilja. Analiza zakonodavnog okvira pokazala je da Bosna i Hercegovina nema specifičan zakon koji izravno regulira online nasilje, već se ovaj fenomen regulira kroz opće kaznenopravne odredbe, što često otežava njegovu učinkovitu primjenu. Rad ističe potrebu za unapređenjem zakonodavstva, jačanjem institucionalnih kapaciteta i razvojem preventivnih mjera, osobito u području obrazovanja i digitalne pismenosti.

Ključne riječi: *online nasilje, društvene mreže, cyberbullying, Bosna i Hercegovina, digitalna pismenost*

UVOD

Razvoj digitalnih tehnologija i ubrzana ekspanzija društvenih mreža značajno su promijenili način komunikacije, interakcije i razmjene informacija u suvremenom društvu. Platforme poput Facebooka, Instagrama, TikToka i drugih omogućuju korisnicima brzu i jednostavnu komunikaciju, ali istodobno otvaraju prostor za različite oblike zloporabe. Jedan od najizraženijih negativnih fenomena koji se javlja u digitalnom okruženju jest online nasilje (engl. *cyberbullying*), koje predstavlja ozbiljan društveni i javnozdravstveni problem (Zhu et al., 2021). Online nasilje obuhvaća različite oblike agresivnog ponašanja putem digitalnih medija, uključujući vrijeđanje, prijetnje, širenje lažnih informacija i neovlašteno dijeljenje privatnih sadržaja. Za razliku od tradicionalnog nasilja, online nasilje karakterizira anonimnost počinitelja, širok doseg publike i trajnost sadržaja, što dodatno pojačava njegove negativne učinke (Giumetti & Kowalski, 2022). Posebno su ranjiva djeca i mladi, koji su ujedno i najaktivniji korisnici društvenih mreža, što povećava njihovu izloženost rizicima digitalnog nasilja (Craig et al., 2020). U kontekstu Bosne i Hercegovine, problem online nasilja dodatno je složen zbog nedovoljno razvijenog zakonodavnog okvira i ograničenih institucionalnih kapaciteta za njegovo učinkovito suzbijanje. Iako postoje određene zakonske odredbe koje se mogu primijeniti na digitalno nasilje, one često nisu specifično usmjerene na ovaj fenomen, što otežava pravnu zaštitu žrtava (Muratbegović et al., 2017). Sve izraženija zloporaba društvenih mreža kroz različite oblike online nasilja i nedovoljna učinkovitost postojećih mehanizama prevencije i zaštite predstavlja zanačajan problem za bosansko-hercegovačko društvo. Unatoč rastućoj prisutnosti ovog problema, još uvijek postoji nedostatak sustavnog pristupa u njegovom razumijevanju, osobito u kontekstu Bosne i Hercegovine. Poseban problem predstavlja činjenica da online nasilje ima ozbiljne psihološke, socijalne i akademske posljedice za žrtve, uključujući anksioznost, depresiju, smanjeno samopoštovanje i socijalnu izolaciju (Kwan et al., 2020). Istovremeno, anonimnost i dostupnost digitalnih platformi olakšavaju počiniteljima provođenje nasilja bez neposrednih posljedica, što dodatno otežava njegovo suzbijanje. Analiziranjem fenomena zloporabe društvenih mreža kroz online nasilje, identificirati njegove uzroke, oblike i posljedice te ispitati postojeći zakonodavni okvir u Bosni i Hercegovini koji se odnosi na ovu problematiku. Svrha rada je pružiti cjelovit pregled relevantne literature i zakonskih regulativa kako bi se doprinijelo boljem razumijevanju ovog problema te predložile smjernice za njegovo učinkovitije suzbijanje. Rad također ima za cilj ukazati na potrebu unapređenja pravnog i institucionalnog okvira u cilju zaštite korisnika, osobito djece i mladih.

1. Društvene mreže u suvremenom društvu

Društvene mreže predstavljaju jedan od najznačajnijih fenomena suvremenog digitalnog društva, koji je temeljito transformirao način na koji ljudi komuniciraju, razmjenjuju informacije i oblikuju društvene odnose. Njihova sveprisutnost i dostupnost putem pametnih uređaja omogućile su kontinuiranu povezanost korisnika, bez obzira na prostorne i vremenske granice. U tom kontekstu, društvene mreže imaju ključnu ulogu u svakodnevnom životu pojedinaca, osobito mladih, ali istodobno nose i određene rizike povezane s njihovom zlouporabom (Garett et al., 2016). Društvene mreže mogu se definirati kao digitalne platforme koje omogućuju korisnicima stvaranje osobnih profila, povezivanje s drugim korisnicima te razmjenu sadržaja u različitim oblicima, uključujući tekst, slike i videozapise. Njihov razvoj započinje početkom 21. stoljeća pojavom platformi poput MySpacea i kasnije Facebooka, koje su postavile temelje modernih društvenih mreža. Tijekom godina, društvene mreže su evoluirale od jednostavnih komunikacijskih alata u kompleksne digitalne ekosustave koji uključuju funkcije poput dijeljenja multimedijalnog sadržaja, oglašavanja, poslovne komunikacije i informiranja javnosti. Razvoj tehnologije, osobito mobilnih uređaja i brzog interneta, dodatno je ubrzao njihovu popularizaciju i globalnu rasprostranjenost (Kowalski et al., 2012).

U suvremenom digitalnom okruženju dominiraju platforme poput Facebooka, Instagrama, TikToka, Snapchata, YouTubea i X-a, koje okupljaju milijarde korisnika diljem svijeta. Svaka od ovih platformi ima specifične funkcionalnosti i ciljne skupine korisnika, ali zajednički im je cilj omogućavanje interakcije i dijeljenja sadržaja. Način korištenja društvenih mreža značajno se razlikuje ovisno o dobi korisnika, interesima i društvenom kontekstu. Mladi korisnici najčešće koriste društvene mreže za komunikaciju s vršnjacima, zabavu i izražavanje identiteta, dok starije generacije češće koriste ove platforme za informiranje i održavanje društvenih kontakata. Međutim, intenzivna i dugotrajna uporaba društvenih mreža povezuje se s povećanim rizikom izloženosti negativnim sadržajima, uključujući online nasilje (Craig et al., 2020). Društvene mreže imaju brojne pozitivne aspekte, među kojima se ističu mogućnost brze komunikacije, pristup informacijama, razvoj digitalnih kompetencija te poticanje društvene uključenosti. One omogućuju korisnicima izražavanje mišljenja, sudjelovanje u društvenim i političkim procesima te stvaranje novih oblika zajednica i mreža podrške. S druge strane, negativni aspekti uključuju ovisnost o društvenim mrežama, smanjenu kvalitetu međuljudskih odnosa, izloženost neprimjerenim sadržajima te povećani rizik od online nasilja. Poseban problem predstavlja širenje dezinformacija i govor mržnje, koji mogu imati ozbiljne društvene posljedice. Također, istraživanja ukazuju na povezanost intenzivne uporabe društvenih mreža s narušenim mentalnim zdravljem, uključujući simptome depresije i anksioznosti (Giumetti & Kowalski, 2022; Nixon, 2014).

Društvene mreže imaju izuzetno važnu ulogu u komunikaciji mladih, budući da predstavljaju primarni kanal njihove svakodnevne interakcije. Putem ovih platformi mladi razvijaju socijalne vještine, grade identitet i održavaju odnose s vršnjacima. Digitalna komunikacija omogućuje im brzu razmjenu informacija i kontinuiranu povezanost, što značajno utječe na njihove društvene obrasce ponašanja. Međutim, upravo zbog intenzivne uporabe društvenih mreža, mladi su posebno izloženi rizicima poput cyberbullyinga, socijalnog pritiska i potrebe za stalnim online prisustvom. Istraživanja pokazuju da su adolescenti jedna od najranjivijih skupina kada je riječ o online nasilju, što dodatno naglašava potrebu za edukacijom, prevencijom i zaštitom u digitalnom okruženju (Vejmelka et al., 2017; Kwan et al., 2020).

2. Pojam i oblici online nasilja

Online nasilje predstavlja jedan od najozbiljnijih izazova suvremenog digitalnog društva. Razvoj društvenih mreža i digitalnih komunikacijskih alata omogućio je nove oblike interakcije, ali istodobno i pojavu novih oblika nasilnog ponašanja. Za razliku od tradicionalnih oblika nasilja, online nasilje karakterizira stalna dostupnost, anonimnost i mogućnost brzog širenja sadržaja, što dodatno povećava njegov negativni utjecaj na žrtve (Zhu et al., 2021). Online nasilje ili cyberbullying definira se kao namjerno i ponavljano agresivno ponašanje koje se provodi putem digitalnih tehnologija, s ciljem nanošenja štete drugoj osobi. Ono uključuje korištenje društvenih mreža, poruka, e-mailova i drugih digitalnih platformi za uznemiravanje, vrijeđanje ili zastrašivanje pojedinca (Kowalski et al., 2012). Ključne karakteristike online nasilja su namjera nanošenja štete, ponavljanost i neravnoteža moći između počinitelja i žrtve. Međutim, za razliku od tradicionalnog nasilja, čak i jednokratna objava može imati dugotrajan učinak zbog mogućnosti njezinog trajnog prisustva u digitalnom prostoru (Nixon, 2014).

Iako online nasilje dijeli određene karakteristike s tradicionalnim nasiljem, postoje značajne razlike koje ga čine specifičnim. Prije svega, online nasilje može se odvijati u bilo koje vrijeme i na bilo kojem mjestu, što znači da žrtve nemaju „sigurno mjesto“ gdje bi izbjegle nasilje. Također, anonimnost počinitelja otežava identifikaciju i sankcioniranje, što može potaknuti agresivnije ponašanje (Giumetti & Kowalski, 2022). Dodatno, digitalni sadržaj može biti brzo distribuiran velikom broju ljudi, čime se povećava intenzitet i trajanje nasilja. Za razliku od tradicionalnog nasilja koje je često ograničeno na određeni prostor (npr. škola), online nasilje ima potencijal globalnog dosega (Craig et al., 2020).

Online nasilje može se manifestirati u različitim oblicima, ovisno o načinu komunikacije i vrsti sadržaja koji se koristi. Najčešći oblici uključuju verbalno zlostavljanje, širenje dezinformacija, narušavanje privatnosti i govor mržnje.

Jedan od najčešćih oblika online nasilja jest vrijeđanje i upućivanje prijetnji putem digitalnih platformi. Ovaj oblik uključuje uvredljive komentare, ponižavanje, ismijavanje i zastrašivanje žrtve. Takvo ponašanje može imati ozbiljne psihološke posljedice, osobito kod mladih koji su osjetljiviji na društvenu percepciju (Kwan et al., 2020). Širenje lažnih ili manipulativnih informacija predstavlja još jedan oblik online nasilja. Ovaj oblik uključuje namjerno plasiranje netočnih informacija s ciljem narušavanja ugleda pojedinca. Dezinformacije se brzo šire putem društvenih mreža, što dodatno otežava njihovu kontrolu i ispravljanje (Garett et al., 2016). Objavljivanje privatnih fotografija, videozapisa ili osobnih podataka bez pristanka osobe predstavlja ozbiljno kršenje privatnosti i čest oblik digitalnog nasilja. Ovaj oblik nasilja može imati dugoročne posljedice za žrtvu, uključujući emocionalnu traumu i društvenu stigmatizaciju. Cyberstalking podrazumijeva kontinuirano praćenje, uznemiravanje i kontroliranje žrtve putem digitalnih sredstava. To može uključivati slanje prijetećih poruka, praćenje aktivnosti na društvenim mrežama i prikupljanje osobnih informacija. Ovaj oblik nasilja često izaziva osjećaj straha i nesigurnosti kod žrtava (Nixon, 2014). Govor mržnje odnosi se na izražavanje netrpeljivosti i diskriminacije prema određenim skupinama na temelju njihove nacionalnosti, religije, spola ili drugih obilježja. Na društvenim mrežama govor mržnje može imati širok doseg i potaknuti daljnje nasilno ponašanje, čime postaje ozbiljan društveni problem (European Union Agency for Fundamental Rights, 2023).

Uzroci online nasilja su kompleksni i uključuju individualne, društvene i tehnološke čimbenike. Među najčešćim motivima počinitelja ističu se želja za dominacijom, potreba za pažnjom, frustracija i nedostatak empatije. Anonimnost digitalnog okruženja dodatno potiče nasilno ponašanje jer smanjuje osjećaj odgovornosti za vlastite postupke (Zhu et al., 2021). Također, društveni pritisak i želja za prihvaćanjem u vršnjačkim skupinama mogu potaknuti pojedince na sudjelovanje u nasilju. Nedostatak digitalne pismenosti i svijesti o posljedicama vlastitih postupaka dodatno doprinosi ovom problemu. Istraživanja pokazuju da su djeca i adolescenti najčešće žrtve online nasilja, ali i najčešći počinitelji. Žrtve su često osobe koje se na neki način razlikuju od većine, bilo po izgledu, ponašanju ili društvenom statusu. Također, osobe s nižim samopoštovanjem i slabijom socijalnom podrškom podložnije su viktimizaciji (Vejmelka et al., 2017). S druge strane, počinitelji online nasilja često pokazuju sklonost agresivnom ponašanju, nedostatak empatije i potrebu za kontrolom. U nekim slučajevima, počinitelji mogu istovremeno biti i žrtve nasilja, što ukazuje na složenost ovog fenomena (Kowalski et al., 2012).

3. Posljedice online nasilja

Online nasilje ima brojne i složene posljedice koje se odražavaju na psihološko, socijalno i funkcionalno stanje žrtava. Za razliku od tradicionalnih oblika nasilja, njegove posljedice mogu biti intenzivnije zbog stalne izloženosti, anonimnosti počinitelja i širokog dosega publike. Digitalno okruženje omogućuje trajnost sadržaja, što dodatno produbljuje osjećaj bespomoćnosti kod žrtava i otežava oporavak (Zhu et al., 2021). Istraživanja pokazuju da online nasilje značajno utječe na kvalitetu života, osobito kod djece i adolescenata koji su najčešće izloženi ovom obliku nasilja (Kwan et al., 2020). Jedna od najozbiljnijih posljedica online nasilja odnosi se na psihološko zdravlje žrtava. Izloženost uvredama, prijetnjama i javnom poniženju može dovesti do razvoja anksioznosti, depresije i kroničnog stresa. Žrtve često razvijaju osjećaj straha, nesigurnosti i gubitka kontrole nad vlastitim životom (Nixon, 2014). Dugotrajna izloženost nasilju može rezultirati smanjenim samopoštovanjem i negativnom slikom o sebi, što dodatno pogoršava psihičko stanje. U težim slučajevima, online nasilje povezuje se s pojavom suicidalnih misli i ponašanja, osobito među adolescentima (Giumetti & Kowalski, 2022). Zbog stalne dostupnosti digitalnih platformi, žrtve često nemaju mogućnost „bijega“ od nasilja, što dodatno povećava razinu stresa. Osim psiholoških, online nasilje ima i značajne socijalne posljedice. Žrtve se često povlače iz društvenih interakcija kako bi izbjegle daljnje uznemiravanje, što dovodi do socijalne izolacije. Takvo povlačenje može negativno utjecati na razvoj socijalnih vještina i sposobnost uspostavljanja zdravih međuljudskih odnosa (Vejmelka et al., 2017). Online nasilje također može narušiti odnose s vršnjacima, obitelji i širom društvenom zajednicom. Širenje dezinformacija ili kompromitirajućih sadržaja može dovesti do gubitka povjerenja i stigmatizacije žrtve, čime se dodatno produbljuje osjećaj usamljenosti i društvene isključenosti (Craig et al., 2020). Posljedice online nasilja često se odražavaju i na akademski i profesionalni život žrtava. Kod učenika i studenata može doći do smanjene koncentracije, pada motivacije za učenje te slabijih obrazovnih rezultata. Strah od ismijavanja ili uznemiravanja može dovesti do izbjegavanja školskog okruženja, što dodatno pogoršava akademski uspjeh (Kwan et al., 2020). U profesionalnom kontekstu, online nasilje može utjecati na radnu učinkovitost, profesionalnu reputaciju i mogućnosti zapošljavanja. Objavljivanje kompromitirajućih sadržaja ili širenje lažnih informacija može imati dugoročne posljedice na karijeru pojedinca, osobito u digitalno povezanom društvu gdje informacije ostaju trajno dostupne. Dugoročne posljedice online nasilja mogu biti izrazito ozbiljne i trajne. Istraživanja pokazuju da osobe koje su bile izložene cyberbullyingu u mladosti imaju povećan rizik od razvoja kroničnih mentalnih poremećaja u odrasloj dobi, uključujući depresiju, anksiozne poremećaje i posttraumatski stresni poremećaj (Zhu et al., 2021). Također, iskustvo online nasilja može dugoročno utjecati na samopouzdanje, interpersonalne odnose i opću kvalitetu života. Negativna iskustva iz digitalnog okruženja mogu oblikovati percepciju sigurnosti i

povjerenja u društvo, što dodatno naglašava važnost pravovremene intervencije i prevencije (Giumetti & Kowalski, 2022).

4. Zloupotreba društvenih mreža

Zloupotreba društvenih mreža predstavlja kompleksan fenomen koji proizlazi iz načina na koji su digitalne platforme dizajnirane i korištene. Iako društvene mreže nude brojne mogućnosti za komunikaciju i razmjenu informacija, njihove tehničke i društvene karakteristike mogu biti iskorištene za širenje nasilja, dezinformacija i drugih oblika štetnog ponašanja. Zloupotreba se očituje kroz različite oblike online nasilja, ali i kroz manipulaciju sadržajem, narušavanje privatnosti i poticanje negativnih društvenih obrazaca (Garett et al., 2016).

Jedan od ključnih mehanizama zloupotrebe društvenih mreža jest anonimnost korisnika. Mogućnost skrivanja identiteta smanjuje osjećaj odgovornosti za vlastite postupke i potiče agresivnije ponašanje. Korisnici se često osjećaju sigurnije u izražavanju negativnih stavova ili provođenju nasilja kada vjeruju da neće snositi posljedice (Zhu et al., 2021). Viralnost sadržaja predstavlja dodatni problem jer omogućuje brzo i masovno širenje informacija, uključujući uvredljive ili lažne sadržaje. Jednom objavljen sadržaj može dosegnuti velik broj korisnika u vrlo kratkom vremenu, čime se intenzivira negativni učinak na žrtvu. Algoritmi društvenih mreža također igraju značajnu ulogu u zloupotrebi. Oni su dizajnirani tako da promoviraju sadržaj koji izaziva snažne emocionalne reakcije, što često uključuje kontroverzne ili negativne objave. Time se povećava vidljivost problematičnih sadržaja i potencijalno potiče daljnje nasilno ponašanje (Giumetti & Kowalski, 2022).

Digitalna pismenost predstavlja ključni faktor u prevenciji zloupotrebe društvenih mreža. Ona uključuje sposobnost kritičkog razumijevanja digitalnog sadržaja, prepoznavanja rizičnih situacija i odgovornog ponašanja u online okruženju. Nedostatak digitalne pismenosti može dovesti do neprimjerenog korištenja društvenih mreža, uključujući sudjelovanje u nasilju ili širenje dezinformacija (UNESCO, 2022). Edukacija korisnika, osobito mladih, o sigurnom i odgovornom korištenju digitalnih tehnologija može značajno smanjiti rizik od zloupotrebe. Digitalna pismenost također uključuje razumijevanje posljedica online ponašanja, što može potaknuti razvoj empatije i odgovornosti kod korisnika.

Mediji i popularna kultura imaju značajnu ulogu u oblikovanju stavova i ponašanja korisnika društvenih mreža. Česta izloženost nasilnim sadržajima, govor mržnje i agresivnoj komunikaciji može dovesti do normalizacije takvog ponašanja. Kada se nasilje prikazuje kao prihvatljivo ili čak zabavno, postoji veća vjerojatnost da će ga pojedinci imitirati u digitalnom okruženju (European Union Agency for Fundamental Rights, 2023). Društvene mreže dodatno pojačavaju

ovaj efekt jer omogućuju brzo širenje sadržaja bez adekvatne kontrole. Kultura „lajkova“ i dijeljenja može potaknuti korisnike na stvaranje provokativnih ili negativnih sadržaja kako bi privukli pažnju, što doprinosi širenju nasilja i netrpeljivosti.

Mladi predstavljaju najranjiviju skupinu kada je riječ o zlouporabi društvenih mreža. Njihova visoka razina uključenosti u digitalno okruženje, zajedno s nedovoljno razvijenim mehanizmima samokontrole i kritičkog mišljenja, povećava rizik od izloženosti i sudjelovanja u online nasilju (Craig et al., 2020). Specifičnost zlouporabe među mladima očituje se u snažnom utjecaju vršnjačkih odnosa i potrebe za društvenim prihvaćanjem. Mladi često sudjeluju u online nasilju kako bi stekli status u grupi ili izbjegli vlastitu viktimizaciju. Istovremeno, strah od osude ili gubitka društvenog statusa može ih spriječiti u prijavljivanju nasilja. Zbog svega navedenog, prevencija zlouporabe društvenih mreža među mladima zahtijeva sveobuhvatan pristup koji uključuje edukaciju, podršku obitelji i institucija te razvoj sigurnog digitalnog okruženja (Kwan et al., 2020).

5. Zakonska regulativa u Bosni i Hercegovini

Zakonodavni okvir Bosne i Hercegovine u području zaštite od online nasilja karakterizira složena struktura koja proizlazi iz ustavnog uređenja države. Ne postoji jedinstveni zakon koji izravno regulira cyberbullying, već se zaštita ostvaruje kroz kombinaciju kaznenopravnih, građanskopravnih i administrativnih propisa. Takav fragmentiran pristup često otežava učinkovitu primjenu zakona i zaštitu žrtava u digitalnom okruženju (Muratbegović et al., 2017).

Opći pravni okvir zaštite od nasilja u Bosni i Hercegovini temelji se na ustavnim odredbama koje jamče zaštitu dostojanstva, privatnosti i sigurnosti pojedinca. Ova prava dodatno su razrađena kroz različite zakone i podzakonske akte na razini entiteta i Brčko distrikta. Iako zakonodavstvo prepoznaje različite oblike nasilja, online nasilje nije uvijek jasno definirano kao posebna kategorija. Stoga se u praksi primjenjuju postojeće pravne norme koje reguliraju srodna kaznena djela, što može dovesti do pravne nesigurnosti i neujednačene sudske prakse (OSCE, 2023).

Kaznenopravna regulativa u Bosni i Hercegovini podijeljena je između entiteta i Brčko distrikta, što znači da postoje tri relevantna kaznena zakona koji uređuju ovu oblast. Krivični zakon Federacije BiH sadrži odredbe koje se mogu primijeniti na online nasilje, iako ono nije izričito imenovano. Kaznena djela poput ugrožavanja sigurnosti, klevete i neovlaštenog snimanja mogu se primijeniti na ponašanja koja se odvijaju putem digitalnih platformi (Krivični

zakon FBiH¹). Slično zakonodavstvu Federacije BiH, Krivični zakonik Republike Srpske također regulira kaznena djela koja se mogu povezati s online nasiljem. U novijim izmjenama posebna pažnja posvećena je zaštiti od govora mržnje i sigurnosti građana u digitalnom prostoru (Krivični zakonik RS²). Krivični zakon Brčko distrikta³ također predviđa sankcioniranje kaznenih djela relevantnih za online nasilje, uključujući povrede privatnosti i sigurnosti. Međutim, kao i u drugim dijelovima BiH, nedostaje specifična regulacija cyberbullyinga kao posebnog kaznenog djela.

Iako online nasilje nije posebno definirano, određena kaznena djela iz postojećih zakona mogu se primijeniti na digitalno okruženje:

- Ugrožavanje sigurnosti - Ovo kazneno djelo uključuje prijetnje koje mogu izazvati osjećaj straha i nesigurnosti kod žrtve. U kontekstu online nasilja, prijetnje putem društvenih mreža ili poruka mogu se kvalificirati kao ugrožavanje sigurnosti.
- Neovlašteno snimanje i objavljivanje - Objavljivanje fotografija, videozapisa ili drugih osobnih podataka bez pristanka predstavlja ozbiljno kršenje privatnosti i može biti sankcionirano prema kaznenim zakonima.
- Kleveta i uvreda - Širenje lažnih informacija ili uvredljivih sadržaja putem društvenih mreža može se kvalificirati kao kleveta ili uvreda, ovisno o težini i posljedicama takvog ponašanja.
- Govor mržnje - Govor mržnje, osobito kada potiče nasilje ili diskriminaciju, predstavlja ozbiljno kazneno djelo koje se sve češće pojavljuje u online prostoru. Njegova regulacija u BiH još uvijek je u razvoju i suočava se s brojnim izazovima (European Union Agency for Fundamental Rights, 2023).

U kontekstu online nasilja, posebno je značajno kazneno djelo neovlaštenog dijeljenja spolno eksplicitnih snimaka bez pristanka osobe na koju se sadržaj odnosi, koje predstavlja ozbiljan oblik povrede privatnosti i dostojanstva pojedinca. Novije izmjene kaznenog zakonodavstva u Federaciji Bosne i Hercegovine prepoznaju ovaj oblik zlouporabe digitalnih tehnologija te

¹ Krivični zakon FBiH ("Sl. novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017, 31/2023 i 58/2025)

² Krivični zakonik RS ("Sl. glasnik RS", br. 64/2017, 104/2018 - odluka US, 15/2021, 89/2021, 73/2023, "Sl. glasnik BiH", br. 9/2024 - odluka US BiH, "Sl. glasnik RS" 105/2024 - odluka US, 19/2025, "Sl. glasnik BiH", br. 14/2025 - odluka US BiH i "Sl. glasnik RS", br. 31/2025, 85/2025 - odluka US i 25/2026)

³ Krivični zakon Brčko distrikta BiH ("Sl. glasnik Brčko distrikta BiH", br. 19/2020 - prečišćen tekst, 3/2024 i 14/2024)

predviđaju kazne zatvora za počinitelje, osobito u slučajevima kada se takvi sadržaji učine dostupnima većem broju osoba ili kada uključuju maloljetnike. Ovakva pravna regulacija predstavlja važan iskorak u prilagodbi zakonodavstva suvremenim oblicima online nasilja, budući da jasno sankcionira ponašanja koja su sve prisutnija na društvenim mrežama i drugim digitalnim platformama (Hercegovina.info, 2025).

Zakon o zaštiti osobnih podataka Bosne i Hercegovine⁴ predstavlja ključni pravni instrument za zaštitu privatnosti u digitalnom okruženju. Ovaj zakon regulira prikupljanje, obradu i korištenje osobnih podataka te propisuje prava pojedinaca u vezi s njihovim osobnim informacijama. U kontekstu online nasilja, zakon je posebno važan jer omogućuje sankcioniranje neovlaštenog dijeljenja osobnih podataka i sadržaja. Međutim, njegova primjena u praksi često je ograničena zbog nedostatka svijesti i institucionalnih kapaciteta.

U suzbijanju online nasilja ključnu ulogu imaju različite institucije koje djeluju na nacionalnoj i lokalnoj razini. Policija je odgovorna za prijem prijava i provođenje istraga u slučajevima kaznenih djela povezanih s online nasiljem. Sudovi donose presude i određuju sankcije za počinitelje, čime osiguravaju pravnu zaštitu žrtava. Posebno važnu ulogu ima Agencija za zaštitu osobnih podataka u BiH, koja nadzire primjenu zakona o zaštiti osobnih podataka i pruža smjernice za zaštitu privatnosti u digitalnom okruženju. Unatoč postojećem pravnom okviru, zakonodavstvo Bosne i Hercegovine suočava se s brojnim izazovima u regulaciji online nasilja. Glavni problem predstavlja nedostatak specifičnih zakonskih odredbi koje bi izravno regulirale cyberbullying. Dodatni izazovi uključuju neujednačenu primjenu zakona, nedovoljnu edukaciju pravosudnih tijela i sporu prilagodbu zakonodavstva tehnološkim promjenama. Također, prekogranična priroda digitalnog nasilja otežava njegovo procesuiranje i zahtijeva međunarodnu suradnju (OSCE, 2023).

Širenje sadržaja i iznošenje neistinitih ili uvredljivih komentara putem anonimnih i lažnih profila ima izravan negativan učinak na žrtvu, ostavljajući ozbiljne psihološke i društvene posljedice. Online nasilje na društvenim mrežama u velikoj se mjeri upravo i širi putem takvih profila, koji omogućuju počiniteljima djelovanje bez odgovornosti i straha od sankcija. U zakonodavstvu Bosne i Hercegovine, kao i Federacije Bosne i Hercegovine, prepoznata su određena kaznena djela poput neovlaštenog dijeljenja eksplicitnog sadržaja, što predstavlja važan korak u zaštiti žrtava. Međutim, i dalje ne postoji jasno definiran i specifičan pravni okvir koji bi sustavno regulirao zlouporabu anonimnih profila i lažno komentiranje s ciljem uznemiravanja, klevete i digitalnog nasilja. Stoga je nužno hitno uvesti zakonske izmjene koje će precizno definirati odgovornost za djelovanje putem anonimnih korisničkih računa, omogućiti učinkovitu

⁴ Zakon o zaštiti ličnih podataka BiH ("Sl. glasnik BiH", br. 12/2025)

identifikaciju počinitelja u slučajevima zlouporabe te osigurati adekvatne sankcije. Time bi se doprinijelo stvaranju sigurnijeg digitalnog prostora, smanjenju zlouporabe društvenih mreža i jačanju zaštite žrtava online nasilja. Zaštita dostojanstva, privatnosti i mentalnog zdravlja pojedinca mora biti prioritet i u digitalnom okruženju, jednako kao i u stvarnom životu (European Union Agency for Fundamental Rights, 2023; Zhu et al., 2021).

S obzirom na sve izraženije zlouporabe društvenih mreža, posebno kroz anonimne profile i nekontrolirano širenje štetnih sadržaja, nameće se hitna potreba za dodatnim izmjenama i dopunama zakonodavstva u Bosni i Hercegovini. Anonimnost korisnika omogućuje počiniteljima da bez straha od sankcija objavljuju uvredljive komentare, šire dezinformacije i narušavaju ugled drugih osoba, pri čemu je često otežano ili gotovo nemoguće utvrditi njihov identitet. Takvo okruženje potiče neodgovorno ponašanje i doprinosi normalizaciji online nasilja, što može imati ozbiljne posljedice po mentalno zdravlje žrtava, uključujući duševnu bol, osjećaj nesigurnosti i narušavanje osobnog identiteta. Stoga je nužno razviti učinkovitije pravne mehanizme koji će omogućiti bržu identifikaciju počinitelja, veću odgovornost digitalnih platformi te snažniju zaštitu korisnika u online prostoru (European Union Agency for Fundamental Rights, 2023; Zhu et al., 2021).

Bosna i Hercegovina nastoji uskladiti svoje zakonodavstvo s međunarodnim standardima, osobito kroz implementaciju konvencija i preporuka međunarodnih organizacija. Konvencije Vijeća Europe, uključujući Konvenciju o kibernetičkom kriminalu (Budimpeštanska konvencija), predstavljaju važan okvir za borbu protiv digitalnog kriminala i online nasilja. Također, iako Bosna i Hercegovina nije članica Europske unije, nastoji se približiti europskim pravnim standardima kroz usklađivanje s relevantnim direktivama i regulativama EU. Međutim, proces usklađivanja još uvijek traje i zahtijeva dodatne napore u cilju stvaranja učinkovitijeg sustava zaštite korisnika u digitalnom okruženju.

6. Prevencija i suzbijanje online nasilja

Prevencija i suzbijanje online nasilja zahtijevaju sveobuhvatan i interdisciplinarni pristup koji uključuje obrazovne institucije, obitelj, zakonodavstvo, tehnološke kompanije i širu društvenu zajednicu. S obzirom na kompleksnost digitalnog okruženja i brz razvoj tehnologije, učinkovite mjere prevencije moraju biti usmjerene na edukaciju korisnika, razvoj odgovornog ponašanja te unapređenje institucionalnih i tehnoloških mehanizama zaštite (UNESCO, 2022). Obrazovni sustav ima ključnu ulogu u prevenciji online nasilja jer predstavlja primarno okruženje za razvoj znanja, vrijednosti i socijalnih vještina kod djece i mladih. Uvođenje edukativnih programa koji obuhvaćaju digitalnu sigurnost, odgovorno

ponašanje na internetu i prepoznavanje nasilja može značajno doprinijeti smanjenju rizika od cyberbullyinga. Škole također imaju važnu ulogu u stvaranju sigurnog i poticajnog okruženja u kojem se učenici osjećaju zaštićeno i podržano. Razvoj školskih politika protiv nasilja, edukacija nastavnika i suradnja s roditeljima ključni su elementi učinkovite prevencije (Polanin et al., 2021). Roditelji i obitelj imaju nezamjenjivu ulogu u oblikovanju ponašanja djece u digitalnom okruženju. Aktivno praćenje online aktivnosti djece, otvorena komunikacija i pružanje podrške ključni su za prepoznavanje i sprječavanje online nasilja. Istraživanja pokazuju da djeca koja imaju kvalitetnu komunikaciju s roditeljima rjeđe postaju žrtve ili počinitelji online nasilja. Roditelji također trebaju razvijati vlastite digitalne kompetencije kako bi mogli adekvatno reagirati na izazove digitalnog okruženja (Kowalski et al., 2012).

Digitalna i medijska pismenost predstavljaju temeljne alate za prevenciju online nasilja. One uključuju sposobnost kritičkog vrednovanja informacija, razumijevanje načina funkcioniranja digitalnih platformi te odgovorno korištenje interneta. Razvijanje digitalne pismenosti omogućuje korisnicima prepoznavanje rizičnih situacija, zaštitu vlastite privatnosti i odgovorno ponašanje prema drugima. Edukacija u ovom području posebno je važna za mlade, ali i za odrasle koji sudjeluju u digitalnom okruženju (UNESCO, 2022). Tehnološke kompanije i platforme društvenih mreža imaju značajnu odgovornost u suzbijanju online nasilja. Razvoj i implementacija mehanizama za prijavu neprimjerenog sadržaja, moderiranje objava i uklanjanje štetnih sadržaja ključni su za zaštitu korisnika. Algoritmi i sustavi umjetne inteligencije mogu pomoći u prepoznavanju nasilnog sadržaja, ali njihova učinkovitost ovisi o transparentnosti i odgovornosti kompanija. Osim toga, platforme trebaju kontinuirano unapređivati svoje politike korištenja i surađivati s institucijama kako bi osigurale sigurnije digitalno okruženje (European Union Agency for Fundamental Rights, 2023). Preventivni programi i javne kampanje imaju važnu ulogu u podizanju svijesti o problemu online nasilja i poticanju odgovornog ponašanja. Kampanje usmjerene na edukaciju korisnika, osobito mladih, mogu značajno doprinijeti smanjenju nasilja u digitalnom prostoru. Primjeri dobre prakse uključuju edukativne radionice, online platforme za pomoć žrtvama i nacionalne strategije za borbu protiv nasilja. Uspješni programi temelje se na suradnji različitih sektora, uključujući obrazovanje, zdravstvo, pravosuđe i civilno društvo (World Health Organization, 2024).

ZAKLJUČAK

Online nasilje kao oblik zlouporabe društvenih mreža predstavlja ozbiljan društveni problem koji zahtijeva sustavan i koordiniran pristup različitih društvenih aktera. Razvoj digitalnih tehnologija donio je brojne prednosti, ali i nove izazove u području zaštite pojedinaca, osobito djece i mladih. U ovom radu analizirani su ključni aspekti online nasilja, uključujući njegove oblike, uzroke, posljedice i zakonodavni okvir u Bosni i Hercegovini. Analiza literature pokazala je da je online nasilje sve prisutniji fenomen koji ima značajne negativne posljedice na psihološko, socijalno i funkcionalno stanje žrtava. Posebno su istaknute karakteristike digitalnog okruženja, poput anonimnosti i viralnosti sadržaja, koje doprinose intenzitetu i širenju nasilja (Zhu et al., 2021). Utvrđeno je da su djeca i mladi najranjivija skupina, te da su izloženi različitim oblicima online nasilja, uključujući vrijeđanje, prijetnje, govor mržnje i narušavanje privatnosti. Posljedice takvih iskustava uključuju anksioznost, depresiju i socijalnu izolaciju (Kwan et al., 2020). Također je utvrđeno da zakonodavni okvir u Bosni i Hercegovini nije u potpunosti prilagođen specifičnostima digitalnog nasilja, što predstavlja značajan izazov u njegovom suzbijanju (Muratbegović et al., 2017).

Na temelju dobivenih nalaza, moguće je formulirati nekoliko preporuka za unapređenje zakonodavstva i prakse u Bosni i Hercegovini. Prije svega, potrebno je razviti specifične zakonske odredbe koje će jasno definirati i sankcionirati online nasilje kao poseban oblik kaznenog djela. Također je važno unaprijediti suradnju između institucija, uključujući policiju, pravosuđe i regulatorna tijela, kako bi se osigurala učinkovitija primjena postojećih propisa. Edukacija stručnjaka koji rade na ovim slučajevima, kao i podizanje svijesti građana o pravima i načinima zaštite, ključni su za uspješnu borbu protiv online nasilja. Dodatno, potrebno je uskladiti zakonodavstvo s međunarodnim standardima koje promiču organizacije poput Vijeće Europe, kako bi se osigurala učinkovitija zaštita korisnika u digitalnom okruženju.

S obzirom na dinamičan razvoj digitalnih tehnologija, buduća istraživanja trebala bi se usmjeriti na detaljniju analizu novih oblika online nasilja i njihovih posljedica. Poseban naglasak potrebno je staviti na empirijska istraživanja u kontekstu Bosne i Hercegovine, kako bi se bolje razumjele lokalne specifičnosti i potrebe. Također, preporučuje se istraživanje učinkovitosti preventivnih programa i zakonodavnih mjera, kao i uloge tehnoloških kompanija u suzbijanju nasilja. Razvoj interdisciplinarnih pristupa koji uključuju psihologiju, pravo, sociologiju i informacijske tehnologije može značajno doprinijeti sveobuhvatnom razumijevanju ovog fenomena.

LITERATURA

1. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health*, 9, 634909. <https://doi.org/10.3389/fpubh.2021.634909>
2. Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. *Current Opinion in Psychology*, 45, 101314. <https://doi.org/10.1016/j.copsyc.2022.101314>
3. Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., et al. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, 66(6), S100–S108. <https://doi.org/10.1016/j.jadohealth.2020.03.006>
4. Kwan, I., Dickson, K., Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., et al. (2020). Cyberbullying and children and young people's mental health: A systematic map of systematic reviews. *Cyberpsychology, Behavior, and Social Networking*, 23(2), 72–82. <https://doi.org/10.1089/cyber.2019.0370>
5. Polanin, J. R., Espelage, D. L., Grotzinger, J. K., Ingram, K. M., Michaelson, L., Spinney, E., et al. (2021). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science*, 22, 102–112. <https://doi.org/10.1007/s11121-020-01151-3>
6. Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. <https://doi.org/10.2147/AHMT.S36456>

7. Garrett, R., Lord, L. R., & Young, S. D. (2016). Associations between social media and cyberbullying: A review of the literature. *mHealth*, 2, 46. <https://doi.org/10.21037/mhealth.2016.12.01>
8. Vejmelka, L., Strabić, N., & Jazvo, M. (2017). Online aktivnosti i rizična ponašanja adolescenata u virtualnom okruženju. *Društvena istraživanja*, 26(1), 59–78.
9. Jeleč, V. (2020). Elektroničko nasilje među djecom i mladima: Pregled preventivnih programa. *Kriminologija i socijalna integracija*, 28(2), 235–252.
10. Pavlović, V., Vinogradac, M., & Sudar, D. (2019). Načini reagiranja i razlozi nereagiranja adolescenata u situacijama nasilja na društvenim mrežama. *Ljetopis socijalnog rada*, 26(3), 347–368.
11. Buljan Flander, G., Durman Marijanović, Z., & Ćorić Špoljarić, R. (2015). Odnos elektroničkog nasilja, samopoštovanja i roditeljskih oblika ponašanja. *Društvena istraživanja*, 24(2), 239–259.
12. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley-Blackwell.
13. World Health Organization. (2024). *A focus on adolescent peer violence and bullying in Europe*. WHO.
14. World Health Organization. (2021). *Violence against children online*. WHO.
15. UNICEF. (2023). *Tackling online violence against children*. UNICEF.
16. UNESCO. (2022). *Tackling cyberbullying and other forms of online violence involving children and young people*. UNESCO.
17. Council of Europe. (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*.

18. European Union Agency for Fundamental Rights. (2023). *Online content moderation: Challenges in detecting hate speech.*
19. Muratbegović, E., et al. (2017). *Smjernice za postupanje u slučaju nasilja nad djecom u digitalnom okruženju u Bosni i Hercegovini.* Međunarodni forum solidarnosti – EMMAUS.
20. Sarajevski otvoreni centar. (2024). *Izveštaj o online nasilju i govoru mržnje u Bosni i Hercegovini.*
21. Organization for Security and Co-operation in Europe. (2023). *Hate crime reporting in Bosnia and Herzegovina.* OSCE Mission to BiH.
22. Zakon o zaštiti ličnih podataka Bosne i Hercegovine. (2025). *Službeni glasnik BiH*, br. 12/25.

ABUSE OF SOCIAL NETWORKS THROUGH ONLINE VIOLENCE IN BOSNIA AND HERZEGOVINA

DOI: 10.70329/2744-2403.2026.6.11.5

Review article

Atina Perković, PhDc

Abstract

The misuse of social media through online violence represents an increasingly prominent problem in modern digital society, particularly among children and young people who are the most active users of digital platforms. By analyzing the phenomenon of online violence, its forms, causes, and consequences, as well as the legislative framework in Bosnia and Herzegovina related to this issue, this paper provides a comprehensive overview of the topic. A review of relevant scientific and professional literature, along with an analysis of applicable legal acts, indicates that online violence includes various forms of behavior such as insults, threats, the spread of misinformation, violations of privacy, and hate speech. It is evident that such forms of violence have significant psychological, social, and academic consequences, including anxiety, depression, and social isolation. The role of digital platforms is particularly emphasized, as their characteristics—such as anonymity and virality—contribute to the spread of violent behavior. The analysis of the legislative framework shows that Bosnia and Herzegovina does not have a specific law that directly regulates online violence; instead, this phenomenon is addressed through general criminal law provisions, which often complicates its effective implementation. The paper highlights the need to improve legislation, strengthen institutional capacities, and develop preventive measures, especially in the fields of education and digital literacy.

Keywords: *online violence, social media, cyberbullying, Bosnia and Herzegovina, digital literacy*

INTRODUCTION

The development of digital technologies and the rapid expansion of social media have significantly changed the way communication, interaction, and information exchange take place in modern society. Platforms such as Facebook, Instagram, TikTok, and others enable fast and easy communication, but at the same time create space for various forms of misuse. One of the most prominent negative phenomena emerging in the digital environment is online violence (cyberbullying), which represents a serious social and public health issue (Zhu et al., 2021).

Online violence includes various forms of aggressive behavior through digital media, such as insults, threats, the spread of false information, and unauthorized sharing of private content. Unlike traditional forms of violence, online violence is characterized by the anonymity of perpetrators, a wide audience reach, and the permanence of content, which further intensifies its negative effects (Giumetti & Kowalski, 2022).

Children and young people are particularly vulnerable, as they are also the most active users of social media, which increases their exposure to the risks of digital violence (Craig et al., 2020). In the context of Bosnia and Herzegovina, the issue of online violence is further complicated by an underdeveloped legislative framework and limited institutional capacities for its effective suppression. Although certain legal provisions can be applied to digital violence, they are often not specifically tailored to this phenomenon, making legal protection for victims more difficult (Muratbegović et al., 2017).

The growing misuse of social media through various forms of online violence, along with the insufficient effectiveness of existing prevention and protection mechanisms, represents a significant problem for Bosnian society. Despite the increasing presence of this issue, there is still a lack of a systematic approach to understanding it, particularly in the context of Bosnia and Herzegovina.

A particular concern is that online violence has serious psychological, social, and academic consequences for victims, including anxiety, depression, reduced self-esteem, and social isolation (Kwan et al., 2020). At the same time, the anonymity and accessibility of digital platforms make it easier for perpetrators to engage in abusive behavior without immediate consequences, which further complicates efforts to combat it.

By analyzing the phenomenon of social media misuse through online violence, this paper aims to identify its causes, forms, and consequences, as well as to examine the existing legislative framework in Bosnia and Herzegovina related to this issue. The purpose of the paper is to provide a comprehensive overview of relevant literature and legal regulations in order to contribute to a better understanding of this problem and to propose guidelines for its more effective prevention and suppression. The paper also aims to highlight the need to improve the legal and institutional framework in order to better protect users, especially children and young people.

1. Social networks in modern society

Social networks represent one of the most significant phenomena of modern digital society, fundamentally transforming the way people communicate, exchange information, and shape social relationships. Their widespread presence and accessibility through smart devices have enabled continuous connectivity among users, regardless of spatial and temporal boundaries. In this context, social networks play a key role in the everyday lives of individuals, especially young people, but at the same time they carry certain risks associated with their misuse (Garett et al., 2016).

Social networks can be defined as digital platforms that allow users to create personal profiles, connect with other users, and share content in various forms, including text, images, and videos. Their development began in the early 21st century with the emergence of platforms such as MySpace and later Facebook, which laid the foundation for modern social networks. Over time, these platforms have evolved from simple communication tools into complex digital ecosystems that include functions such as multimedia sharing, advertising, business communication, and public information dissemination. The development of technology, particularly mobile devices and high-speed internet, has further accelerated their popularization and global expansion (Kowalski et al., 2012).

In the contemporary digital environment, platforms such as Facebook, Instagram, TikTok, Snapchat, YouTube, and X dominate, gathering billions of users worldwide. Each of these platforms has specific functionalities and target user groups, but they share the common goal of enabling interaction and content sharing.

The way social networks are used varies significantly depending on users' age, interests, and social context. Young users most often use social media for communication with peers, entertainment, and identity expression, while older

generations tend to use these platforms for information and maintaining social connections. However, intensive and prolonged use of social networks is associated with an increased risk of exposure to negative content, including online violence (Craig et al., 2020).

Social networks have numerous positive aspects, including the ability to communicate quickly, access information, develop digital competencies, and promote social inclusion. They enable users to express opinions, participate in social and political processes, and create new forms of communities and support networks. On the other hand, negative aspects include addiction to social media, reduced quality of interpersonal relationships, exposure to inappropriate content, and an increased risk of online violence. A particular concern is the spread of misinformation and hate speech, which can have serious social consequences. Research also indicates a link between intensive use of social networks and impaired mental health, including symptoms of depression and anxiety (Giumetti & Kowalski, 2022; Nixon, 2014).

Social networks play an extremely important role in youth communication, as they represent the primary channel of their daily interaction. Through these platforms, young people develop social skills, build their identity, and maintain relationships with peers. Digital communication enables fast information exchange and continuous connectivity, significantly influencing their social behavior patterns. However, due to the intensive use of social media, young people are particularly exposed to risks such as cyberbullying, social pressure, and the need for constant online presence. Research shows that adolescents are one of the most vulnerable groups when it comes to online violence, which further emphasizes the need for education, prevention, and protection in the digital environment (Vejmelka et al., 2017; Kwan et al., 2020).

2. The concept and forms of online violence

Online violence represents one of the most serious challenges of the modern digital society. The development of social networks and digital communication tools has enabled new forms of interaction, but at the same time the emergence of new forms of violent behavior. Unlike traditional forms of violence, online violence is characterized by constant availability, anonymity, and the ability to rapidly spread content, which further increases its negative impact on victims (Zhu et al., 2021).

Online violence, or cyberbullying, is defined as intentional and repeated aggressive behavior carried out through digital technologies with the aim of

harming another person. It includes the use of social networks, messages, emails, and other digital platforms to harass, insult, or intimidate an individual (Kowalski et al., 2012). The key characteristics of online violence are the intent to cause harm, repetition, and an imbalance of power between the perpetrator and the victim. However, unlike traditional violence, even a single post can have long-lasting effects due to its potential permanence in the digital space (Nixon, 2014).

Although online violence shares certain characteristics with traditional violence, there are significant differences that make it specific. First of all, online violence can occur at any time and in any place, meaning that victims do not have a “safe space” where they can escape it. Additionally, the anonymity of perpetrators makes identification and sanctioning more difficult, which can encourage more aggressive behavior (Giumetti & Kowalski, 2022). Furthermore, digital content can be rapidly distributed to a large number of people, increasing both the intensity and duration of the violence. Unlike traditional violence, which is often limited to a specific location (e.g., school), online violence has the potential for a global reach (Craig et al., 2020).

Online violence can manifest in various forms, depending on the mode of communication and the type of content used. The most common forms include verbal abuse, the spread of misinformation, violations of privacy, and hate speech. One of the most common forms is insulting and threatening individuals through digital platforms. This includes offensive comments, humiliation, ridicule, and intimidation of the victim. Such behavior can have serious psychological consequences, especially for young people who are more sensitive to social perception (Kwan et al., 2020).

The spread of false or manipulative information represents another form of online violence. This includes the intentional dissemination of inaccurate information with the aim of damaging an individual’s reputation. Misinformation spreads rapidly through social networks, making it difficult to control and correct (Garett et al., 2016).

Publishing private photos, videos, or personal data without consent represents a serious violation of privacy and a common form of digital violence. This type of abuse can have long-term consequences for the victim, including emotional trauma and social stigmatization. Cyberstalking refers to continuous monitoring, harassment, and control of a victim through digital means. This may include sending threatening messages, tracking social media activity, and collecting personal information. This form of violence often creates a sense of fear and insecurity among victims (Nixon, 2014).

Hate speech refers to the expression of intolerance and discrimination against certain groups based on their nationality, religion, gender, or other characteristics. On social networks, hate speech can reach a wide audience and incite further violent behavior, making it a serious social issue (European Union Agency for Fundamental Rights, 2023).

The causes of online violence are complex and include individual, social, and technological factors. Among the most common motives of perpetrators are the desire for dominance, the need for attention, frustration, and a lack of empathy. The anonymity of the digital environment further encourages violent behavior by reducing the sense of responsibility for one's actions (Zhu et al., 2021). Social pressure and the desire for acceptance within peer groups can also motivate individuals to engage in such behavior. A lack of digital literacy and awareness of the consequences of one's actions further contributes to the problem.

Research shows that children and adolescents are the most frequent victims of online violence, but also among the most common perpetrators. Victims are often individuals who differ in some way from the majority, whether in appearance, behavior, or social status. Additionally, individuals with lower self-esteem and weaker social support are more vulnerable to victimization (Vejmelka et al., 2017). On the other hand, perpetrators of online violence often exhibit tendencies toward aggressive behavior, lack of empathy, and a need for control. In some cases, perpetrators may also be victims themselves, which highlights the complexity of this phenomenon (Kowalski et al., 2012).

3. Consequences of online violence

Online violence has numerous and complex consequences that affect the psychological, social, and functional well-being of victims. Unlike traditional forms of violence, its effects can be more intense due to constant exposure, the anonymity of perpetrators, and the wide reach of the audience. The digital environment enables the permanence of content, which further deepens the feeling of helplessness among victims and complicates recovery (Zhu et al., 2021). Research shows that online violence significantly impacts quality of life, especially among children and adolescents who are most frequently exposed to this form of abuse (Kwan et al., 2020).

One of the most serious consequences of online violence relates to the psychological health of victims. Exposure to insults, threats, and public humiliation can lead to the development of anxiety, depression, and chronic stress. Victims often develop feelings of fear, insecurity, and loss of control over their own lives (Nixon, 2014). Prolonged exposure to violence may result in decreased self-esteem and a negative self-image, further worsening mental health.

In more severe cases, online violence is associated with suicidal thoughts and behaviors, particularly among adolescents (Giumetti & Kowalski, 2022). Due to the constant availability of digital platforms, victims often have no possibility of “escape,” which further increases stress levels.

In addition to psychological effects, online violence also has significant social consequences. Victims often withdraw from social interactions to avoid further harassment, leading to social isolation. Such withdrawal can negatively affect the development of social skills and the ability to establish healthy interpersonal relationships (Vejmelka et al., 2017). Online violence can also damage relationships with peers, family members, and the wider community. The spread of misinformation or compromising content can lead to a loss of trust and stigmatization of the victim, further deepening feelings of loneliness and social exclusion (Craig et al., 2020).

The consequences of online violence are also reflected in the academic and professional lives of victims. Among pupils and students, it can lead to decreased concentration, reduced motivation to learn, and poorer academic performance. Fear of ridicule or harassment may result in avoidance of the school environment, further worsening educational outcomes (Kwan et al., 2020). In a professional context, online violence can affect work performance, professional reputation, and employment opportunities. The publication of compromising content or the spread of false information can have long-term consequences for an individual's career, especially in a digitally connected society where information remains permanently accessible.

The long-term consequences of online violence can be particularly severe and lasting. Research indicates that individuals who were exposed to cyberbullying in their youth have an increased risk of developing chronic mental health disorders in adulthood, including depression, anxiety disorders, and post-traumatic stress disorder (Zhu et al., 2021). Additionally, the experience of online violence can have long-term effects on self-confidence, interpersonal relationships, and overall quality of life. Negative experiences in the digital environment may shape perceptions of safety and trust in society, further emphasizing the importance of timely intervention and prevention (Giumetti & Kowalski, 2022).

4. Social media abuse

The misuse of social media represents a complex phenomenon arising from the way digital platforms are designed and used. Although social networks offer numerous opportunities for communication and information exchange, their

technical and social characteristics can be exploited for the spread of violence, misinformation, and other forms of harmful behavior. Misuse is manifested through various forms of online violence, as well as through content manipulation, violations of privacy, and the encouragement of negative social patterns (Garett et al., 2016).

One of the key mechanisms of social media misuse is user anonymity. The ability to conceal one's identity reduces the sense of responsibility for one's actions and encourages more aggressive behavior. Users often feel safer expressing negative attitudes or engaging in harmful conduct when they believe they will not face consequences (Zhu et al., 2021). The virality of content represents an additional issue, as it enables the rapid and widespread dissemination of information, including offensive or false content. Once published, content can reach a large number of users in a very short time, intensifying its negative impact on victims. Social media algorithms also play a significant role in misuse. They are designed to promote content that generates strong emotional reactions, which often includes controversial or negative posts. This increases the visibility of problematic content and may further encourage harmful behavior (Giumetti & Kowalski, 2022).

Digital literacy is a key factor in preventing the misuse of social media. It includes the ability to critically understand digital content, recognize risky situations, and behave responsibly in an online environment. A lack of digital literacy can lead to inappropriate use of social networks, including participation in online violence or the spread of misinformation (UNESCO, 2022). Educating users, especially young people, about the safe and responsible use of digital technologies can significantly reduce the risk of misuse. Digital literacy also involves understanding the consequences of online behavior, which can foster the development of empathy and responsibility among users.

Media and popular culture play a significant role in shaping the attitudes and behaviors of social media users. Frequent exposure to violent content, hate speech, and aggressive communication can lead to the normalization of such behavior. When violence is portrayed as acceptable or even entertaining, individuals are more likely to imitate it in the digital environment (European Union Agency for Fundamental Rights, 2023). Social networks further amplify this effect by enabling the rapid spread of content without adequate control. The culture of "likes" and sharing can encourage users to create provocative or negative content in order to attract attention, thereby contributing to the spread of violence and intolerance.

Young people represent the most vulnerable group when it comes to the misuse of social media. Their high level of engagement in the digital environment,

combined with underdeveloped mechanisms of self-control and critical thinking, increases the risk of both exposure to and participation in online violence (Craig et al., 2020). The specificity of misuse among youth is reflected in the strong influence of peer relationships and the need for social acceptance. Young individuals often engage in online violence to gain status within a group or to avoid becoming victims themselves. At the same time, fear of judgment or loss of social status may prevent them from reporting violence. For these reasons, preventing the misuse of social media among young people requires a comprehensive approach that includes education, support from families and institutions, and the development of a safe digital environment (Kwan et al., 2020).

5. Legislation in Bosnia and Herzegovina

The legislative framework of Bosnia and Herzegovina in the field of protection against online violence is characterized by a complex structure arising from the constitutional organization of the state. There is no single law that directly regulates cyberbullying; instead, protection is achieved through a combination of criminal, civil, and administrative regulations. Such a fragmented approach often complicates the effective implementation of laws and the protection of victims in the digital environment (Muratbegović et al., 2017).

The general legal framework for protection against violence in Bosnia and Herzegovina is based on constitutional provisions that guarantee the protection of dignity, privacy, and individual security. These rights are further elaborated through various laws and by-laws at the entity level and in the Brčko District. Although legislation recognizes different forms of violence, online violence is not always clearly defined as a separate category. Therefore, in practice, existing legal norms regulating related criminal offenses are applied, which may lead to legal uncertainty and inconsistent judicial practice (OSCE, 2023).

Criminal legislation in Bosnia and Herzegovina is divided between the entities and the Brčko District, meaning that there are three relevant criminal codes governing this area. The Criminal Code of the Federation of Bosnia and Herzegovina contains provisions that can be applied to online violence, although it is not explicitly named. Criminal offenses such as endangering security, defamation, and unauthorized recording can be applied to behaviors occurring through digital platforms. Similarly, the Criminal Code of the Republic of Srpska regulates offenses that may be associated with online violence. In its more recent amendments, particular attention has been given to protection against hate speech and the safety of citizens in the digital space. The Criminal Code of the Brčko

District also provides for sanctions related to offenses relevant to online violence, including violations of privacy and security. However, as in other parts of Bosnia and Herzegovina, there is still no specific regulation of cyberbullying as a distinct criminal offense.

Although online violence is not specifically defined, certain criminal offenses from existing legislation can be applied to the digital environment:

- **Endangering security** – This offense includes threats that may cause fear and insecurity in the victim. In the context of online violence, threats made via social networks or messages may qualify as endangering security.
- **Unauthorized recording and publishing** – Publishing photos, videos, or other personal data without consent constitutes a serious violation of privacy and may be sanctioned under criminal law.
- **Defamation and insult** – The dissemination of false information or offensive content via social networks may be classified as defamation or insult, depending on the severity and consequences.
- **Hate speech** – Hate speech, especially when it incites violence or discrimination, represents a serious criminal offense that is increasingly present in the online environment. Its regulation in Bosnia and Herzegovina is still evolving and faces numerous challenges (European Union Agency for Fundamental Rights, 2023).

In the context of online violence, a particularly significant offense is the unauthorized sharing of sexually explicit material without the consent of the person concerned, which constitutes a serious violation of privacy and dignity. Recent amendments to criminal legislation in the Federation of Bosnia and Herzegovina recognize this form of digital abuse and предусматрива imprisonment for perpetrators, especially in cases where such content is made available to a wider audience or involves minors. This represents an important step toward adapting legislation to modern forms of online violence, as it clearly sanctions behaviors increasingly present on social networks and other digital platforms (Hercegovina.info, 2025).

The Law on Personal Data Protection of Bosnia and Herzegovina represents a key legal instrument for the protection of privacy in the digital environment. This law regulates the collection, processing, and use of personal data and defines the rights of individuals regarding their personal information. In the context of online violence, it is particularly important as it enables the sanctioning of unauthorized sharing of personal data and content. However, its practical application is often limited due to a lack of awareness and insufficient institutional capacities.

Various institutions at national and local levels play a crucial role in combating online violence. The police are responsible for receiving reports and conducting investigations in cases involving criminal offenses related to online violence. Courts issue judgments and determine sanctions for perpetrators, thereby ensuring legal protection for victims. A particularly important role is played by the Personal Data Protection Agency of Bosnia and Herzegovina, which oversees the implementation of data protection laws and provides guidelines for privacy protection in the digital environment. Despite the existing legal framework, Bosnia and Herzegovina faces numerous challenges in regulating online violence. The main issue is the lack of specific legal provisions directly addressing cyberbullying. Additional challenges include inconsistent application of laws, insufficient training of judicial authorities, and the slow adaptation of legislation to technological changes. Furthermore, the cross-border nature of digital violence complicates prosecution and requires international cooperation (OSCE, 2023).

The dissemination of content and the posting of false or offensive comments through anonymous and fake profiles have a direct negative impact on victims, leaving serious psychological and social consequences. Online violence on social networks is largely spread through such profiles, which allow perpetrators to act without accountability or fear of sanctions. In the legislation of Bosnia and Herzegovina, as well as the Federation of Bosnia and Herzegovina, certain criminal offenses such as unauthorized sharing of explicit content have been recognized, representing an important step in victim protection. However, there is still no clearly defined and specific legal framework that systematically regulates the misuse of anonymous profiles and fake commenting for the purpose of harassment, defamation, and digital violence. Therefore, it is necessary to urgently introduce legal amendments that would precisely define responsibility for actions conducted through anonymous user accounts, enable effective identification of perpetrators in cases of misuse, and ensure appropriate sanctions. This would contribute to creating a safer digital environment, reducing the misuse of social networks, and strengthening the protection of victims of online violence. The protection of dignity, privacy, and mental health must be a priority in the digital environment, just as it is in real life (European Union Agency for Fundamental Rights, 2023; Zhu et al., 2021).

Given the increasing misuse of social networks, particularly through anonymous profiles and the uncontrolled spread of harmful content, there is an urgent need for further amendments and improvements to legislation in Bosnia and Herzegovina. User anonymity allows perpetrators to post offensive comments, spread misinformation, and damage the reputation of others without fear of sanctions, while their identification is often difficult or nearly impossible. Such an environment encourages irresponsible behavior and contributes to the normalization of online violence, which can have serious consequences for

victims' mental health, including emotional distress, feelings of insecurity, and damage to personal identity. Therefore, it is necessary to develop more effective legal mechanisms that will enable faster identification of perpetrators, greater accountability of digital platforms, and stronger protection of users in the online space (European Union Agency for Fundamental Rights, 2023; Zhu et al., 2021).

Bosnia and Herzegovina strives to harmonize its legislation with international standards, particularly through the implementation of conventions and recommendations of international organizations. Council of Europe conventions, including the Convention on Cybercrime (Budapest Convention), represent an important framework for combating digital crime and online violence. Although Bosnia and Herzegovina is not a member of the European Union, it seeks to align its legal system with EU standards through harmonization with relevant directives and regulations. However, this process is still ongoing and requires additional efforts to establish a more effective system for protecting users in the digital environment.

6. Prevention and suppression of online violence

The prevention and suppression of online violence require a comprehensive and interdisciplinary approach involving educational institutions, families, legislation, technology companies, and the broader social community. Given the complexity of the digital environment and the rapid development of technology, effective preventive measures must focus on user education, the development of responsible behavior, and the improvement of institutional and technological protection mechanisms (UNESCO, 2022).

The education system plays a key role in preventing online violence, as it represents the primary environment for the development of knowledge, values, and social skills among children and young people. The introduction of educational programs covering digital safety, responsible online behavior, and the recognition of violence can significantly reduce the risk of cyberbullying. Schools also play an important role in creating a safe and supportive environment in which students feel protected and encouraged. The development of school anti-violence policies, teacher training, and cooperation with parents are essential elements of effective prevention (Polanin et al., 2021).

Parents and families have an irreplaceable role in shaping children's behavior in the digital environment. Active monitoring of children's online activities, open communication, and providing support are crucial for recognizing and preventing online violence. Research shows that children who have quality communication

with their parents are less likely to become victims or perpetrators of online violence. Parents should also develop their own digital competencies in order to adequately respond to the challenges of the digital environment (Kowalski et al., 2012).

Digital and media literacy represent fundamental tools for preventing online violence. They include the ability to critically evaluate information, understand how digital platforms function, and use the internet responsibly. Developing digital literacy enables users to recognize risky situations, protect their privacy, and behave responsibly toward others. Education in this area is especially important for young people, but also for adults who participate in the digital environment (UNESCO, 2022).

Technology companies and social media platforms bear significant responsibility in combating online violence. The development and implementation of mechanisms for reporting inappropriate content, moderating posts, and removing harmful content are essential for user protection. Algorithms and artificial intelligence systems can help identify violent content, but their effectiveness depends on the transparency and accountability of the companies. In addition, platforms should continuously improve their usage policies and cooperate with institutions to ensure a safer digital environment (European Union Agency for Fundamental Rights, 2023).

Preventive programs and public awareness campaigns play an important role in raising awareness about the issue of online violence and encouraging responsible behavior. Campaigns aimed at educating users, especially young people, can significantly contribute to reducing violence in the digital space. Examples of good practice include educational workshops, online platforms for victim support, and national strategies for combating violence. Successful programs are based on cooperation between various sectors, including education, healthcare, the judiciary, and civil society (World Health Organization, 2024).

CONCLUSION

Online violence as a form of social media abuse represents a serious societal issue that requires a systematic and coordinated approach by various social actors. The development of digital technologies has brought numerous advantages, but also new challenges in the field of individual protection, particularly for children and young people. This paper analyzes the key aspects of online violence, including its forms, causes, consequences, and the legislative framework in Bosnia and Herzegovina. The literature review indicates that online violence is an increasingly prevalent phenomenon with significant negative effects on the psychological, social, and functional well-being of victims. Particular emphasis is placed on the characteristics of the digital environment, such as anonymity and content virality, which contribute to the intensity and spread of violence (Zhu et al., 2021). It has been established that children and young people are the most vulnerable group and are exposed to various forms of online violence, including insults, threats, hate speech, and violations of privacy. The consequences of such experiences include anxiety, depression, and social isolation (Kwan et al., 2020). It has also been found that the legislative framework in Bosnia and Herzegovina is not fully adapted to the specific nature of digital violence, which represents a significant challenge in combating this issue (Muratbegović et al., 2017).

Based on the findings, several recommendations can be formulated to improve legislation and practice in Bosnia and Herzegovina. First, it is necessary to develop specific legal provisions that clearly define and sanction online violence as a distinct criminal offense. It is also important to enhance cooperation between institutions, including the police, judiciary, and regulatory bodies, in order to ensure more effective implementation of existing regulations. The education of professionals working on these cases, as well as raising public awareness about rights and protection mechanisms, are essential for successfully combating online violence. Additionally, it is necessary to harmonize legislation with international standards promoted by organizations such as the Council of Europe, in order to ensure more effective protection of users in the digital environment.

Given the dynamic development of digital technologies, future research should focus on a more detailed analysis of emerging forms of online violence and their consequences. Particular emphasis should be placed on empirical research in the context of Bosnia and Herzegovina, in order to better understand local specificities and needs. Furthermore, it is recommended to examine the effectiveness of preventive programs and legislative measures, as well as the role of technology companies in combating online violence. The development of interdisciplinary approaches involving psychology, law, sociology, and information technology can significantly contribute to a comprehensive understanding of this phenomenon.

LITERATURE

13. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health*, 9, 634909. <https://doi.org/10.3389/fpubh.2021.634909>
14. Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. *Current Opinion in Psychology*, 45, 101314. <https://doi.org/10.1016/j.copsyc.2022.101314>
15. Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., et al. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health*, 66(6), S100–S108. <https://doi.org/10.1016/j.jadohealth.2020.03.006>
16. Kwan, I., Dickson, K., Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., et al. (2020). Cyberbullying and children and young people's mental health: A systematic map of systematic reviews. *Cyberpsychology, Behavior, and Social Networking*, 23(2), 72–82. <https://doi.org/10.1089/cyber.2019.0370>
17. Polanin, J. R., Espelage, D. L., Grotz, J. K., Ingram, K. M., Michaelson, L., Spinney, E., et al. (2021). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science*, 22, 102–112. <https://doi.org/10.1007/s11121-020-01151-3>
18. Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, 5, 143–158. <https://doi.org/10.2147/AHMT.S36456>

19. Garrett, R., Lord, L. R., & Young, S. D. (2016). Associations between social media and cyberbullying: A review of the literature. *mHealth*, 2, 46. <https://doi.org/10.21037/mhealth.2016.12.01>
20. Vejmelka, L., Strabić, N., & Jazvo, M. (2017). Online aktivnosti i rizična ponašanja adolescenata u virtualnom okruženju. *Društvena istraživanja*, 26(1), 59–78.
21. Jeleč, V. (2020). Elektroničko nasilje među djecom i mladima: Pregled preventivnih programa. *Kriminologija i socijalna integracija*, 28(2), 235–252.
22. Pavlović, V., Vinogradac, M., & Sudar, D. (2019). Načini reagiranja i razlozi nereagiranja adolescenata u situacijama nasilja na društvenim mrežama. *Ljetopis socijalnog rada*, 26(3), 347–368.
23. Buljan Flander, G., Durman Marijanović, Z., & Ćorić Špoljarić, R. (2015). Odnos elektroničkog nasilja, samopoštovanja i roditeljskih oblika ponašanja. *Društvena istraživanja*, 24(2), 239–259.
24. Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley-Blackwell.
19. World Health Organization. (2024). *A focus on adolescent peer violence and bullying in Europe*. WHO.
20. World Health Organization. (2021). *Violence against children online*. WHO.
21. UNICEF. (2023). *Tackling online violence against children*. UNICEF.
22. UNESCO. (2022). *Tackling cyberbullying and other forms of online violence involving children and young people*. UNESCO.
23. Council of Europe. (2018). *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*.

24. European Union Agency for Fundamental Rights. (2023). *Online content moderation: Challenges in detecting hate speech*.
22. Muratbegović, E., et al. (2017). *Smjernice za postupanje u slučaju nasilja nad djecom u digitalnom okruženju u Bosni i Hercegovini*. Međunarodni forum solidarnosti – EMMAUS.
23. Sarajevski otvoreni centar. (2024). *Izveštaj o online nasilju i govoru mržnje u Bosni i Hercegovini*.
24. Organization for Security and Co-operation in Europe. (2023). *Hate crime reporting in Bosnia and Herzegovina*. OSCE Mission to BiH.
23. Zakon o zaštiti ličnih podataka Bosne i Hercegovine. (2025). *Službeni glasnik BiH*, br. 12/25.