Kreiranje sigurnog digitalnog prostora potiče od nas kao krajnjih korisnika i korisnica

Pretposljednje predavanje petog ciklusa javnih razgovora i predavanja "Neko je rekao feminizam", koje organizuju Sarajevski otvoreni centar i Fondacija Friedrich Ebert u Bosni i Hercegovini, održano je u utorak, 17. oktobra, u Muzeju književnosti i pozorišne umjetnosti u Sarajevu. Amina Beriša Liora govorila je o temi "Cyber nasilje i feminizam"

Amina Beriša Liora, magistrica sigurnosti i mirovnih studija na Fakultetu političkih nauka, koja radi u Institutu za društvena istraživanja Fakulteta političkih nauka, na odjelu Informacijske sigurnosti, govorila je o temi cyber nasilja i feminizma u sklopu još jednog predavanja ciklusa "Neko je rekao feminizam". Amina ima dugogodišnje iskustvo u području informacijsko-komunikacijskih tehnologija (IKT), a na početku predavanja istaknula je da je u modernom dobu potrebno ostvariti senzibilniji pristup prema krajnjim korisnicima/cama IKT-a, te u isto vrijeme uzeti u obzir sigurnost individue u digitalnom prostoru. Definišući nasilje kao svjesno, maliciozno ponašanje protiv druge osobe, koje postoji u digitalnom prostoru ili u stvarnom životu, te može biti usmjereno protiv različitih ranjivih društvenih grupa, Amina je napomenula da nasilje ima četiri najizraženije forme (ekonomsko, psihološko, fizičko i seksualno), ali da sve četiri forme bivaju takoreći združene u cyber nasilju.

"Digitalna era nam je donijela razne izazove na koje moramo biti spremni/e. U BiH se digitalno posmatra kao nerealno i samim tim sva nasilja koja se dešavaju u digitalnoj sferi ostaju neprimijećena. Posebno post-konfliktna i tranziciona društva još uvijek

nemaju dovoljno dobre zakone koji bi uzeli u obzir IKT i njihov razvoj, te vrste nasilja i moguće maliciozne aktivnosti usmjerene prema krajnjim korisnicima/cama", rekla je Amina. Informacijsko-komunikacijske tehnologije danas svi nosimo u džepu i koristimo kao jedan vid pomagala u svakodnevnom životu. One većinom služe za umrežavanje korisnika/ca u svrhu komunikacije preko tehnoloških uređaja, medija i mreža. Samim tim je protok informacija koji se dešava u digitalnoj eri ogroman, a iako postoje benefiti od toga, postoje i posljedice po krajnje korisnike/ce. "Cyber bullying, to jest cyber ili digitalno nasilje, je digitalna realizacija nasilja koje se dešava i u stvarnom životu, sa ciljem različitih psiholoških malicioznih manevara nad drugom osobom. U BiH se cyber nasilje najčešće smatra nerealnim nasiljem koje ne ostavlja nikakve posljedice ni tragove, te se smatra da samo jednim blokom možemo zaustaviti nasilnika/cu u njegovim/njenim daljnjim namjerama. Često se i u kuloarima cyber sigurnosnog sektora i IT sektora banalizuje pojam cyber nasilja", pojasnila je Amina.

Flaming, outing, stalking, sexting

Često cyber nasiljem bivaju pogođeni i kompletni kolektivi, a pogotovo ranjive grupe, najčešće žene i djeca. "Forme nasilja u digitalnom prostoru su čudno raspoređene. One nisu i ne moraju biti jasno vidljive kao svo fizičko, psihološko, ekonomsko, pogotovo seksualno nasilje u stvarnom prostoru. Nasilje u digitalnom prostoru poprima sasvim novu dimenziju." Najčešća forma cyber nasilja je verbalno/tekstualno/grafičko zlostavljanje osobe, u svrhu dobijanja različite koristi. Tzv. *flaming*, *roasting* ili *trolling* je vid nanošenja štete kroz humoristični karakter, gdje nasilnici/e "ulaze u rat" sa osobom, pri čemu žrtva odgovara na napadanje, te se tako konflikt produžava dok jedno od njih ne odustane. Tzv. *outing* je slučaj kada nasilnik/ca obznanjuje sve podatke o žrtvi na društvenim mrežama i putem kanala komunikacije, te time nanosi direktnu ili indirektnu štetu žrtvi. To se najčešće dešava u svrhu zlostavljanja žrtve, i tome su najpodložnije žene koje izlaze iz (nasilnih) veza. Amina je u tom kontekstu spomenula Facebook grupu "Sarajevo Glamour", na kojoj su se muškarci svetili bivšim djevojkama objavljujući njihove fotografije, dok je od stranica u svijetu jedna od poznatijih bila Pink Mat, stranica koja se nalazila na dubokom webu, gdje su muškarci prodavali fotografije bivših djevojaka i žena.

U digitalnom prostoru je često i lažno predstavljanje, u svrhu dobijanja koristi. Jedna od najčešćih formi je lažno predstavljanje sebe u idealnom maniru, što je uvertira u neki od oblika cyber nasilja. Lažno predstavljanje je podložno Krivičnom zakonu BiH, ali do sada nije bilo presuda vezanih za to. Još jedna vrsta cyber bullyinga je digitalno praćenje (*stalking*), koje postaje maliciozno kada napadač/ica namjerno prikuplja što veći broj informacija o određenoj osobi u svrhu iznude, dobijanja materijalne ili psihičke koristi, ili emotivne, odnosno seksualne koristi. Ucjene spadaju pod cyber kriminal, ali posjeduju i dimenziju cyber nasilja. U pitanju je cyber ekonomsko nasilje poput tzv. Ponzijevih shema, koje podrazumijevaju finansijsko iznuđivanje, odnosno dobivanje ekonomske koristi u digitalnom prostoru od strane IT stručnjaka/inja koji/e djeluju ilegalno.

Forme nasilja u cyber prostoru mogu se posmatrati indirektno, gdje žrtva ne primjećuje da se nad njom vrši cyber nasilje. To npr. može biti digitalno praćenje (*stalking*), jer žrtva tek kasnije može otkriti šta se dešavalo. Iza te tehnološke strukture postoji osoba koja je povrijeđena, i kojoj treba pružiti pomoć prije nego što se kanali komunikacije poprave i ponovo osiguraju. U slučaju direktnog digitalnog nasilja, žrtva je svjesna da se

nad njom vrši nasilje, i da postoji problem čiji se uzrok najčešće nalazi u samom napadaču/ici. Treći oblik se najčešće smatra latentnim oblikom nasilja, i najviše obuhvata žene – kada se napadač predstavlja kao najbolja osoba, a na kraju ispada psihomanični bolesnik koji ženu uništava na sve moguće načine. Ovaj pristup najčešće na internetu koriste seksualni predatori i pedofili.

Kada mediji govore o cyber nasilju i kriminalu, najčešći profil počinioca koji daju je hacker, osoba potpuno prekrivena duksericom koja pokušava provaliti u nečiji Facebook profil. Amina ističe da to uopće nije slučaj i da svi/e mogu biti i cyber zlostavljači/ce i žrtve. "Medijska slika prema kojoj su hackeri jedini zlostavljači u digitalnoj sferi je apsolutno pogrešna. Takav medijski diskurs nam ne pomaže da raspoznamo prave cyber zlostavljače/ice, jer to može biti dijete, profesor, uglađeni biznismen ili biznismenka, osoba koja ima neku moć u društvu i koja je javna ličnost." Amina je navela nedavni primjer kada je Hana Hadžiavdagić Tabaković poručila Hrvatici Luciji Lugomer da je predebela, i da zbog toga sebe ne može nazivati nikakvim plus-size modelom. "To je jedan vid cyber bullyinga. Ako javna ličnost šalje poruku nasilja osobama koje gledaju njen Instagram profil, onda ona potpiruje val cyber nasilja kao nečeg normalnog što se podvodi pod slobodu govora. To nije sloboda govora", rekla je Amina.

Cyber nasilje se ne smatra stvarnim nasiljem

Kada se govori o psihološkom profilu počinioca, zlostavljač/ica je često senzitivna osoba koja je u prošlosti iskusila nasilje u kući, školi, i sl. Amina je istaknula da je digitalna era sa sobom donijela anonimnost, tako da nikada ne možemo znati ko je cyber zlostavljač/ica dok se ne pregleda apsolutno sve u mrežnoj komunikaciji. "U slučaju cyber nasilja, zlostavljač/ica je osoba niskog samopouzdanja, koja radi zadovoljavanja psihičke koristi i sopstvenog ega, i, nažalost, najčešće maskuliniteta, želi da nanese štetu drugom korisniku/ici, jer će se on osjećati dobro. Problem je u tome što sam profil odgovara svakome, a u suštini ne odgovara nikome. To je psihološki manevar koji je trenutno nemoguće dovesti do jedinstvenog spektra, ali postoje neke karakteristike koje su povezane sa svim počiniocima i počiniteljicama cyber nasilja. U realnosti, takve osobe su često prijatne, vedre, nasmijane, i ne pokazuju znakove nasilja."

Kada je u pitanju profil žrtve, sam počinioc žrtvu posmatra u određenom periodu da bi donio odluku o zlostavljanju. To se često ne uklapa u manevar klasičnog nasilja, jer je fizičko nasilje direktan čin, a u cyber svijetu osoba pravi puni profil žrtve: ko je, kakve probleme ima, da li ima određenih stvari koje treba riješiti u budućem periodu, i sl. Oni često biraju ranjive osobe, o čemu odluke donose na osnovu subjektivne percepcije. "Naprimjer, zlostavljač će naići na neku ženu koja će mu otresito reći da ne želi s njim da priča, blokirat će ga, i to je to. U isto vrijeme, on će pokušati da se približi toj ženi sa 10 različitih profila, i u jednom momentu će i uspjeti." Ako su imale visoko samopouzdanje prije cyber nasilja, žrtve najčešće tokom cyber nasilja postaju osobe sa niskim samopouzdanjem. To je posebno slučaj kada je u pitanju kontinuirano nasilje, koje podrazumijeva da će zlostavljač/ica na sve načine pokušati da žrtvi nanese nasilje i u stvarnom životu.

"Životni ciklus cyber nasilja je poprilično konfuzan i difuzan, te ne može nikada biti centralizovan na samo dva kompjutera, odnosno dva IKT-a, već je u pitanju disperzivno djelovanje koje podrazumijeva da se moraju pratiti sve moguće komunikacije te osobe, da bi se u konačnici zaključilo ko je zlostavljač/ica i da bi se on/a profilirao/la", objasnila je Amina. Nasilnici/e će često na sve načine pokušati da uđu u neku grupu, u kojoj će se nastojati prikazati kao relevantan faktor, da bi kasnije ispoljili/e nasilno ponašanje prema individui s kojom nisu u dobrim odnosima (to može biti kolega/ica sa posla, drugar/ica iz škole…) Kontinuirano nasilno ponašanje podrazumijeva stalno slanje verbalnog, grafičkog, tekstualnog i drugog sadržaja, bez prethodnog odobravanja žrtve. Jedan od primjera je *sexting* (slanje poruka seksualnog sadržaja), bez intencije žrtve da učestvuje u njemu, ili slanje grafičkog materijala na otvorenim chatovima sa web kamerama. "Primijetila sam da žene na to uopšte ne reaguju. Smatra se apsolutno normalnim da neko prikazuje intimne dijelove svog tijela, bez intencije žrtve, i da je rješenje samo blokirati osobu. To nije rješenje. To je jedan oblik cyber nasilja, i to je cyber seksualno nasilje. Svako namjerno maliciozno ponašanje napadača, bez prethodnog odobravanja žrtve u tom kontekstu, jeste cyber seksualno nasilje."

U BiH sigurnosne službe, škole, edukativni centri i slično zapostavljaju temu cyber nasilja jer je ne smatraju realnom, istaknula je Amina. No, nereagovanje okoline može dovesti do autodestrukcije osobe koja je žrtva nasilja. Ljudi koji su upoznati sa cyber nasiljem to možda neće smatrati prijetnjom, ali posebno ranjiva kategorija u ovom spektru su djeca. "Psihološke posljedice cyber nasilja su dosad odnijele mnogo života. Djeca širom svijeta su počinila suicid, ili su postala veoma autodestruktivna, što je vodilo ka fazama predsuicida, poput samopovređivanja. To se dešavalo zbog nereagovanja okoline i neprepoznavanja cyber nasilja koje je završavalo autodestrukcijom i fizičkim ili seksualnim nasiljem nad djecom." Ako vidimo da u digitalnoj sferi postoji makar jedan trag nasilja, koji može dovesti do daljnjeg nasilja, potrebno je reagovati. "To ne mora biti fizička rekacija – ona može biti i digitalna. Kada se nasilniku/ici neko suprotstavi u realnom životu, on/a u najvećem broju slučajeva odustaje od te namjere. Svi mi možemo zaustaviti cyber nasilje kada ga vidimo. Jednim komentarom ili prijavom administratorima možemo barem malo prekinuti taj lanac nasilja."

U BiH još uvijek ne postoje centri koji bi se ozbiljno pozabavili cyber nasiljem. "Nasilnici/e se nadaju da nikada neće biti pronađeni/e niti sankcionisani/e. U njihovim glavama ne postoji kazna, jer je to digitalna sfera i oni/e ostaju anonimni/e. Mi moramo prepoznati koje bi bile najbolje sankcije, i kao civilno društvo postaviti neke uvjete, i dati

daljnje smjernice zakonodavnoj vlasti, kako bismo kreirali/e sigurno društveno i digitalno okruženje za sve", kaže Amina. No, najveći problem u prepoznavanju nasilja jeste njegovo sakrivanje od strane same žrtve. To se dešava i pri stvarnom nasilju, daje veću moć nasilnicima/cama i ohrabruje ih u daljnjim namjerama. "Ako kod djece prepoznamo neki vid zbunjenosti, ako brzo zatvaraju laptop, ili izbrišu Facebook profil, to može biti jedan znak cyber nasilja. Osoba ne može podnijeti psihološku presiju, ne može podnijeti da je neko omalovažava i da se ta vijest širi. Digitalne komunikacije imaju *share* i *like*, i te informacije rapidnom brzinom kruže svim mogućim društvenim mrežama."

Žene i djeca kao ranjive individue

Još jedan problem koji se dešava je razlika između tzv. *digital natives* i *digital migrants*. *Digital natives* su osobe koje su rođene u periodu digitalne sfere, dok su *digital migrants* osobe koje su se u jednom momentu svog života susrele sa digitalnom tehnologijom. "Potrebno je naći sredinu koja će odgovarati i prvima i drugima, kako bismo iznašli/e jedinstven okvir za djelovanje i u digitalnom prostoru, ali i u stvarnom životu i zakonodavstvu. Digitalno se smatra nerealnim, i moramo pronaći paradigmu koja će dokazati da je digitalno javno, da je stvarno, i da nanosi štetu određenim osobama." Ranjive grupe koje su podložne cyber nasilju su često osobe koje nemaju ili imaju vrlo malo prava u državi u kojoj žive. To su često osobe prema kojima društvo ima stereotipe koji mogu dovesti do kontinuiranog grupnog nasilja. Ranjive individue su najčešće žene i djeca. "Prema statističkim podacima koji sam čula na Cyber Security Forumu 2017 koji je 13. oktobra održan na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije, u BiH je svako drugo dijete ostvarilo kontakt sa nepoznatom osobom na internetu. Zamislite spektar situacija u kojima svako drugo dijete kontaktira sa potencijalno malicioznom osobom, što može prerasti u nasilje poput fizičkog ili seksualnog. 11 % djece u BiH se sastalo sa nepoznatom starijom osobom koju je upoznalo putem interneta. Ovo nećemo pronaći u medijima kao relevantnu informaciju, jer to biva zapostavljeno zbog političkih i drugih tema s kojima se naša država suočava. U svijetu je 8 od 10 žena na različite načine svakodnevno zlostavljano preko IKT-a, putem sextinga, slanja grafičkog pornografskog sadržaja, ucjena, prijetnji od strane bivših ili trenutnih partnera, ili od ljudi s kojima su odlučile prekinuti odnose." Amina ističe da je posebno brinu komentari o LGBT populaciji koji podržavaju korektivno silovanje.

Muškarci se najčešće pretvaraju da nisu žrtve nasilja, bilo u stvarnom životu, ili na internetu, zbog tako izgrađenog društvenog konstrukta. "U digitalnoj sferi, koja je poprilično rodno i spolno neutralna, moramo uzeti u obzir da i muškarci trebaju da budu u mogućnosti da kažu ukoliko je došlo do digitalnog nasilja, i da ga smiju prijaviti, jer je to narušavanje njihovog prvog digitalnog ljudskog prava: ne šteti krajnjem korisniku/ici i nemoj mu/joj uništiti opremu." Sve manjinske grupe u društvu su često žrtve nasilja u postkonfliktnim i tranzicijskim društvima, kakvo je i bosanskohercegovačko. U digitalno nasilje prema grupama spadaju homofobne izjave, vrijeđanje na osnovu rase, spola, etniciteta, religije, političkih svjetonazora, itd. "Kada pričamo o slobodi govora, svi/e je moramo imati, jer je to neupitno ljudsko pravo, ali u slobodi govora mora biti uzeto u obzir da mišljenje nužno ne moramo dijeliti, ali se moramo poštovati. Ako se poštujemo, tek onda možemo da kažemo da smo postigli/e svijest kojoj svi težimo."

Statistika za BiH o međuvršnjačkom nasilju, u kojoj je uzeto u obzir i cyber nasilje, kaže da je 6957 ispitanika/ca u osnovnim i srednjim školama dobijalo različite vidove prijetnji ili su bili/e direktne žrtve nasilja od kolega/ica u razredu. Njih 2339 je bilo podložno fizičkom nasilju od strane kolega/ica. 702 se nije nikome obratilo za pomoć ili je u konačnici reklo roditeljima ili nastavnom osoblju da su bili žrtva određene forme nasilja. Samo 66 se obratilo policiji za pomoć. Od tih 66 slučajeva nije bilo krivičnih prijava. Podaci su preuzeti sa web sitea Dan ružičastih majica, kampanje koja se bori protiv međuvršnjačkog nasilja. "Mi, kao individue , se zarad naše sigurnosti moramo poštovati i kreirati siguran prostor. Ako inicijativa za to ne krene od civilnog društva i samog stanovništva, neće sigurno krenuti sa vrhova vlasti. U zakonskoj regulativi BiH ne postoji jasna distinkcija između digitalnog nasilja i ostalih formi nasilja. U zakonu BiH je sve podvedeno pod krivični zakon Federacije BiH, Republike Srpske i Brčko Distrikta, mada se sada desila izmjena u zakonu RS-a, koji nalaže da je svaki oblik nasilja podložan krivičnom djelu, čak i cyber nasilje. Zakon u BiH koji se bori protiv cyber kriminala ni u jednom članu ne podrazumijeva cyber nasilje kao formu cyber kriminala."

U digitalnoj sferi niko nije siguran

Amra smatra da je potrebna hitna izmjena zakona, kao i istraživanje relevantnih stakeholdera: od akademije, NGO sektora, vladinih institucija, kako bi postojao jasan uvid u statističke podatke o tome koliko je bilo žrtava cyber nasilja, u kojem vremenskom periodu, kakav je profil napadača i žrtava u BiH, itd. Ona također smatra da je najpotrebnije osnovati centar posvećen prevenciji cyber nasilja, koji će voditi registar osoba koje su preživjele cyber nasilje. "Intervencija je krajnji element životnog ciklusa cyber nasilja. Ona podrazumijeva namjerni prekid nasilja od strane trećeg lica ili same žrtve, u vidu kontakta s napadačem. Najčešće žrtva sama odlučuje da prekine ciklus nasilja, i ona u potpunosti prestaje koristiti IK tehnologije, jer se boji da se ne ponovi ista situacija. Kako pomoći žrtvi da prekine krug nasilja? Taj ciklus je prilično sličan prekidu stvarnog nasilja i on podrazumijeva ohrabrivanje, kontinuiranu edukaciju od osnovnih i srednjih škola, sve do fakulteta, te stalnu psihološku podršku i podršku sigurnosnih službi."

Država sigurnost više ne posmatra samo kao isključivo nacionalnu, te je individualna sigurnost u digitalnom prostoru od izrazite važnosti. Sve društvene mreže imaju jasnu strategiju za borbu protiv cyber nasilja, bilo sa tehnološke ili psihološke strane. No, u BiH često digitalni dokazi ne bivaju uzeti u obzir, te su zapostavljeni. "Uvijek i u svakom momentu morate osiguravati svoj IKT, jer privatnost ne smije biti narušena u digitalnom prostoru. To podrazumijeva da roditelji imaju monitoring uređaja i korištenja interneta i drugih komunikacija od strane djece. To se postiže jeftinim ili besplatnim softverima koji imaju roditeljski nadzor, i enkripcijom osjetljivih podataka. Ukoliko imate slike svoje djece na internetu, ukoliko mislite da se može desiti neko maliciozno postupanje sa njima na društvenim mrežama, prebacite postavke na privatne i samim tim ste se koliko-toliko zaštitili. Naravno, ne treba prihvatati nepoznate ljude kao prijatelje i ostvarivati komunikaciju s ljudima koji pokazuju tendenciju da taj razgovor preraste u nešto nasilno. Kreiranje sigurnog digitalnog prostora potiče od nas kao krajnjih korisnika/ca. Ukoliko mi budemo dobar primjer i praksa kolegama/icama i

prijateljima/icama, moći ćemo da vidimo šta smo uradili u svrhu zaustavljanja i prevencije cyber nasilja."

Bitno je napomenuti da u digitalnoj sferi skoro niko nije siguran, čak i ako je sve enkriptovano, jer IKT jako brzo napreduje. BiH će morati kreirati jasnu strategiju o cyber nasilju, gdje će prevencija i protekcija, te sankcija počinitelja/ica, biti osnova, smatra Amina. Sve vrste nasilja će se morati posmatrati realnima, pogotovo u kontekstu zaštite ranjivih, visoko ranjivih i marginaliziranih grupa u BiH. "Cyber nasilje jeste realno, digitalno jeste realno, i mi kao svakodnevni konzumenti/ce postajemo kreatori/ce digitalnog svijeta. Kreirajte sigurno okruženje za svaku osobu s kojom stupate u komunikaciju. Podizanje svijesti o cyber nasilju je ono što mi kao individue i društvo možemo uraditi u svru ohrabrivanja žrtve, slabljenja nasilnika/ca i stvaranja budućnosti u kojoj će svako uživati svoja digitalna ljudska prava i slobode. Razvijanje svijesti od malih nogu će pomoći da izrastemo u kvalitetno i osposobljeno informacijsko-komunikacijsko društvo koje će moći držati korak sa digitalnim promjenama." U tom kontekstu, feminizam u cyber sferi je veoma bitan, jer se bori i protiv patrijarhata u digitalnom svijetu, ali i daje mogućnost svima koji su zlostavljani/e ili su imali/e problema sa nasiljem, da pronađu utočište, da se osjećaju sigurno i da nauče o tome šta je nasilje. "Kada se desi problem, bilo u digitalnoj sferi ili u stvarnom životu, prva instanca jesu feminističke i ženske organizacije. Ako feminizam smatramo saveznikom u borbi protiv malilcioznosti u informacijsko-komunikacijskim tehnologijama i IT sektorima, postići ćemo balans. U čitavom svijetu je samo 11% žena zastupljeno u IKT-u. U BiH mislim da taj postotak iznosi 2%. To dovoljno govori zašto je feminizam potreban. Ali u slučaju cyber nasilja, feminizam može kreirati sigurno okruženje, kako za djecu, tako i za odrasle ljude."

Piše: Masha Durkalić

Oktobar 20, 2017