



Pojmovnik

rodno zasnovanog

nasilja počinjenog

posredstvom tehnologije

bodyright

05

Čemu ovaj pojmovnik i kako ga koristiti?

12

Odmazda zbog podrške osobama koje su preživele nasilje

Kleveta u onlajn prostoru

Seksualno nasilje u digitalnom okruženju

Zlostavljanje posredstvom vizuelnog sadržaja

07

Krovne definicije rodno zasnovanog nasilja počinjenog posredstvom tehnologije

13

Podsuknjavanje i perverznačko fotografisanje

Pornografija bez saglasnosti i iznuda na seksualnoj osnovi

Sintetički seksualni mediji, dipfejkovi i lažna (dipfejk) pornografija

09

Oblici rodno zasnovanog nasilja počinjenog posredstvom tehnologije

14

Seksting i zlostavljački sexting

Sajber egzibicionizam, neželjena pornografija i dikpik fotografije / neželjene fotografije penisa

10

Sajber (ili digitalno) nasilje i rodno zasnovano onlajn uznemiravanje

Umreženo uznemiravanje i uznemiravanje na različitim platformama

15

Snimanje i/ili emitovanje seksualnih napada i silovanja

Grumovanje u onlajn prostoru

Neželjena seksualna iskustva uživo omogućena tehnologijom

11

Rodni i seksistički govor mržnje

Seks posramljivanje onlajn

Trolovanje, trolovanje na osnovu roda, potpirivanje i trolovanje u cilju zastrašivanja

Elektronski potpomognuta trgovina ljudima i vrbovanje

16

**Ugrožavanje privatnosti i bezbednosti
posredstvom tehnologije**

Doksovanje, dednejmovanje
i autovanje bez saglasnosti

20

Lažne optužbe za bogohuljenje

Posthumno trolovanje i trolovanje
na osnovu šoka i žalosti

Svotovanje

Trovanje heštega

17

Lažno predstavljanje i ketfišing

Ograničavanje ili kontrolisanje
pomoću tehnologije

Finansijsko zlostavljanje
elektronskim putem

21

Pojmovi iz domena tehnologije

18

Sajber proganjanje i opsesivno
praćenje na internetu

Napadi „u stvarnom životu“

Onlajn pretnje

Bombardovanje na Guglu i Zumu

19

Napad uskraćivanjem pristupa
i napad uskraćivanjem usluga

**Drugi oblici nasilja
u digitalnom okruženju**

Astroturfing



// tvoje telo je tvoje
i na netu i u stvarnom svetu

// Čemu ovaj pojmovnik i kako ga koristiti?

Rodno zasnovano nasilje počinjeno posredstvom tehnologije (engl. *technology-facilitated gender-based violence*, skr. *TFGBV*) pojava je relativno novijeg datuma, koja je pre trideset godina bila gotovo nezamisliva. Kako su informaciono-komunikacione tehnologije postajale sve zastupljenije u našim svakodnevnim životima, do te mere da je sada već teško zamisliti najobičniji dan bez interneta, laptopa, pametnog telefona ili društvenih mreža, tako je i rodno zasnovano nasilje koje se vrši u digitalnom prostoru postajalo sve učestalije.

Podaci ukazuju da je veliki broj žena širom sveta doživeo neki oblik rodno zasnovanog nasilja počinjenog posredstvom tehnologije, kao i da su posebno ranjive devojčice, devojke i mlade žene – 58% njih je doživelo neki oblik rodno zasnovanog nasilja u digitalnom okruženju, u većini slučajeva to se dogodilo između njihove četrnaeste i šesnaeste godine života, a skoro polovina njih (47%) susrelo se i s pretnjama fizičkim i seksualnim nasiljem.¹ Istraživanja takođe pokazuju da je 45% žena koje su doživele nasilje u intimnom partnerskom odnosu bilo zlostavljano i posredstvom tehnologije, a za 48% njih se rodno zasnovano nasilje posredstvom tehnologije nastavilo i nakon završetka veze.²

Zbog svega navedenog, u aprilu 2022. godine Evropska unija započela je rad na stvaranju pravnog okvira regulacije rodno zasnovanog nasilja, tako da on u sebe uključuje i nasilje koje se vrši posredstvom tehnologije.³

Međutim, iako je rodno zasnovano nasilje koje se vrši posredstvom tehnologije sve učestalije, prepoznajući se kao pretnja i u međunarodnim pravnim aktima, i dalje ne postoji zajednički dogovor u vezi s njegovim definisanjem, kao ni definisanjem njegovih pojava oblika. Zbog toga se termini „uznemiravanje” i „zlostavljanje”, kao i termini „sajber”, „digitalno”, „onlajn” i „posredstvom tehnologije”, često upotrebljavaju kao sinonimi kada govorimo o ovom obliku nasilja. Takođe, ni broj pojava oblika ove vrste nasilja još nije konačan – s napretkom tehnologije, dolazi i do novih mogućnosti za njenu zloupotrebu u svrhu vršenja rodno zasnovanog nasilja.

U pojmovniku pred vama nalaze se, izdvojene, dve krovne definicije rodno zasnovanog nasilja počinjenog posredstvom tehnologije, koje su se u praksi pokazale kao najrelevantnije i najsveobuhvatnije, dok su različiti pojava oblici ove vrste nasilja izdvojeni na osnovu zastupljenosti na prostoru Zapadnog Balkana. Pojavni oblici nasilja grupisani su u četiri velike grupe, kako bi se olakšalo snalaženje čitateljki i čitatelja. Ova podela nije konačna niti nepromenljiva, jer se različiti oblici nasilja posredstvom tehnologije često prepliću i prethode jedni drugima. Svaki oblik je opisan, definisan i ilustriran primerom iz stvarnog života, u cilju njegovog prepoznavanja, ali i ukazivanja na opasnost koju rodno zasnovano nasilje posredstvom tehnologije predstavlja po živote devojčica, devojaka i žena, kao i rodno varijantnih osoba.

Prvu grupu čini **Sajber (ili digitalno) nasilje i rodno zasnovano onlajn uznemiravanje**, koje obuhvata različite oblike i vrste uznemiravanja i zlostavljanja u digitalnom prostoru, najčešće sprovedene posredstvom teksta. To su *umreženo uznemiravanje i uznemiravanje na različitim platformama, rodni i seksistički govor mržnje (uključujući i seks posramljivanje onlajn, trolovanje, trolovanje na osnovu roda, potpirivanje i trolovanje u cilju zastrašivanja), odmazda zbog podrške osobama koje su preživele nasilje i kleveta u onlajn prostoru.*

Druga grupa obuhvata **seksualno nasilje u digitalnom okruženju**, s posebnim naglaskom na neželjena seksualna iskustva posredovana tehnologijom. Ova grupa izdvojena je od prethodne zbog izuzetno naglašene rodne komponente i rastuće prevalence. U okviru nje su izdvojeni: *zlostavljanje posredstvom vizuelnog sadržaja (u koje spadaju podsuknjavanje i perverzijačko fotografisanje; pornografija bez saglasnosti i iznuda na seksualnoj osnovi; sintetički seksualni mediji, dipfejkovi i lažna (dipfejk) pornografija; seksting i zlostavljajući seksting; sajber egzibicionizam, neželjena pornografija i dikpik fotografije/neželjene fotografije penisa), snimanje i/ili emitovanje seksualnih napada i silovanja, grumovanje u onlajn prostoru, neželjena seksualna iskustva uživo omogućena tehnologijom i elektronski potpomognuta trgovina ljudima i vrbovanje.*

Treća grupa se sastoji od oblika nasilja čiji je cilj **ugrožavanje bezbednosti i privatnosti posredstvom tehnologije**. Nju čine *doksovanje, dednejmovanje i autovanje bez saglasnosti, lažno predstavljanje i ketfišing, ograničavanje ili kontrolisanje pomoću tehnologije, finansijsko zlostavljanje elektronskim putem, sajber proganjanje i opsesivno praćenje na internetu, napadi "u stvarnom životu", onlajn pretnje, bombardovanje na Guglu i Zumu, kao i napad uskraćivanjem pristupa i napad uskraćivanjem usluga.*

Četvrta grupa obuhvata **druge oblike nasilja u digitalnom okruženju** – one koji nisu obuhvaćeni prethodnim celinama, a koji mogu imati rodnu dimenziju, premda se ona ne podrazumeva onako kako se podrazumeva u prethodne tri grupe. Druga zajednička odlika ovih oblika nasilja jeste činjenica da je njihova učestalost na Zapadnom Balkanu niža u odnosu na prethodne grupe, što ne znači da se to u budućnosti neće promeniti. U njih spadaju *astroturfing, lažne optužbe za bogohuljenje, posthumno trolovanje i trolovanje na osnovu šoka i žalosti, svotovanje i trovanje heštega.*

Na kraju pojmovnika nalazi se i kratak rečnik **pojмова iz domena tehnologije**, u kome je objašnjeno četrnaest termina iz oblasti tehnologije u cilju lakšeg razumevanja gorenavedenih oblika nasilja.

Pojmovnik koji je pred vama nastao je na osnovu publikacije "Rodno-zasnovano nasilje posredstvom tehnologije - učiniti svaki prostor bezbednim", koji je Populacioni fond Ujedinjenih nacija objavio u decembru 2021. godine, sa nastojanjem da svi pojmovi budu definisani u skladu sa lokalnim kontekstom i potkrepljeni primerima koji su nama poznati i bliski. Pojmovnik je nastao u širokom konsultativnom procesu sa stručnim licima, mladim ljudima i opštom javnošću, koji su dali mnogo značajnih sugestija i predloga koje smo pokušali da uvrstimo u dokument. Svesni smo, međutim, da je ovo živ dokument koji će se tek razvijati i dorađivati i unapred se radujemo svim dodatnim komentarima i predlozima koji će nam stići.

U ime Populacionog fonda Ujedinjenih nacija (UNFPA) želimo da se zahvalimo svima koji su učestvovali u nastajanju i prilagođavanju Pojmovnika učešćem na fokus grupama ili slanjem predloga i sugestija. Posebnu zahvalnost dugujemo Hristini Cvetinčanin Knežević koja je vodila konsultativni proces i priredila ovaj Pojmovnik na srpskom jeziku.

// Krovne definicije rodno zasnovanog nasilja počinjenog posredstvom tehnologije

Ujedinjene nacije ⁴	Onlajn nasilje protiv žena i djevojčica posredovano informaciono-komunikacionom tehnologijom	Definicija onlajn nasilja protiv žena odnosi se na bilo koji čin RZN protiv žena koji se počinji, potpomogne ili čije se posljedice pogoršaju uz delimičnu ili potpunu upotrebu informaciono-komunikacione tehnologije (kao što su mobilni telefoni i pametni telefoni, internet, platforme društvenih mreža ili imejl), a koje je usmereno protiv žene samo zato što je žena ili nesrazmerno pogađa žene.
Evropski institut za rodnu ravnopravnost ⁵	Sajber nasilje protiv žena i djevojčica	<p>RZN počinjeno putem elektronske komunikacije i interneta. Iako sajber nasilje može da utiče i na žene i na muškarce, žene i djevojčice doživljavaju drugačije i traumatičnije oblike sajber nasilja.</p> <p>Postoje različiti oblici sajber nasilja protiv žena i djevojčica, uključujući, između ostalog, sajber proganjanje, pornografiju bez saglasnosti (odnosno „osvetničku pornografiju“, engl. <i>revenge porn</i>), rodno zasnovane uvrede (engl. <i>slurs</i>)¹, govor mržnje i uznemiravanje, „seks posramljivanje“ (engl. <i>slut-shaming</i>), neželjenu pornografiju, iznudu na seksualnoj osnovi (engl. <i>sextortion</i>), pretnje silovanjem i smrću, kao i elektronski pomognutu trgovinu ljudima. Sajber nasilje nije odvojeni fenomen od „pravog“ nasilja, jer često prati iste obrasce kao i oflajn nasilje.</p>

¹ Pod rodno zasnovanim uvredama podrazumeva se rodni i seksistički govor mržnje.



// Oblici rodno zasnovanog
nasilja počinjenog
posredstvom tehnologije

Sajber (ili digitalno) nasilje i rodno zasnovano onlajn uznemiravanje

Sajber (ili digitalno) nasilje (engl. *cyberbullying*) je krovni termin koji obuhvata različite oblike nasilja na internetu, odnosno, nasilja koje se sprovodi posredstvom tehnologije. Ono se definiše kao „svesno nanošenje i ponavljanje štete uz pomoć računara, mobilnih telefona ili drugih elektronskih uređaja“⁶, najčešće kroz korišćenje tekstualnog ili grafičkog sadržaja, kako bi se osoba zastrašila, negativno se uticalo na njeno samopouzdanje ili joj se narušio ugled.⁷ Iako se pod ovim terminom najčešće podrazumeva vršnjačko nasilje na internetu, pri kom se pojedinci ili grupa vršnjaka udružuju kako bi drugu osobu omalovažile i nanele štetu njenom ugledu, ličnosti i dostojanstvu, meta sajber nasilja mogu biti i odrasle osobe.^{8,9} Počinioci mogu biti poznanici, ali i nepoznate osobe.

Kada je sajber nasilje, najčešće počinjeno tekstualnim formama, usmereno ka nekoj osobi zbog njenog pola, roda, seksualnosti ili seksualne orijentacije, koristimo termin **rodno zasnovano onlajn uznemiravanje** (engl. *online [gender] harassment*). Rodno zasnovano onlajn uznemiravanje može imati različite oblike – osoba se može konstantno i bez njeine saglasnosti kontaktirati, može joj se pretiti, može se zastrašivati putem slanja neželjenih, neprijatnih, ponižavajućih ili uvredljivih slika ili komentara (rodni i seksistički govor mržnje), ili se o njoj širiti kleveta. Počinioci rodno zasnovanog onlajn uznemiravanja najčešće su pojedini muškarci ili grupe muškaraca (umreženo uznemiravanje), a ono se može vršiti kako na više platformi istovremeno tako i na jednoj platformi.¹⁰ Pod rodno zasnovanim onlajn uznemiravanjem podrazumevamo **umreženo**

uznemiravanje i uznemiravanje na različitim platformama, rodni i seksistički govor mržnje, u koji spadaju seks posramljivanje onlajn i trolovanje, trolovanje na osnovu roda, uključujući i potpirivanje i trolovanje u cilju zastrašivanja, odmazdu zbog podrške osobi koja je preživela nasilje i klevete u onlajn prostoru.

b) Umreženo uznemiravanje i uznemiravanje na različitim platformama

Umreženo uznemiravanje, često nazivano i **sajber mobing** (engl. *cyber mobbing*), sastoji se od organizovanih, koordinisanih i sistematskih napada grupe ljudi na određene pojedince, odnosno, pojedinke, ili ideje, kao što čine grupe koje napadaju feministkinje ili one koji se bore protiv rasizma.¹¹ Grupno uznemiravanje je vođeno psihologijom mase, koja je fokusirana na to da javno izloži, ponizi i kazni osobu koja je meta napada. U najvećem broju slučajeva, osoba je meta samo zato što deli mišljenje o političkim temama ili idejama s kojim se grupa napadača ne slaže.¹² Umreženo uznemiravanje se može vršiti na jednoj platformi, ali može da se odvija i na više platformi istovremeno – tada govorimo o **uznemiravanju na različitim platformama** (engl. *cross-platform harassment*), prilikom koga uznemirivači koriste prednost toga što većina platformi moderira isključivo sadržaj svog sajta.¹³

Česta meta umreženog uznemiravanja na jednoj ili više platformi jesu novinarki. Istraživanje koje je sproveo UNESCO pokazalo je da je 40% novinarki bilo meta rodno zasnovanog onlajn uznemiravanja koje je bilo umreženo. Na ovaj način su vršene kampanje protiv njih. Jedna od deset novinarki je nakon rodno zasnovanog onlajn uznemiravanja izostajala s posla, jedna od tri bila primorana da bude manje vidljiva u javnosti (koristile su pseudonime ili su njihove emisije sklonjene s programa), 4% je dalo otkaz, a 2% je u potpunosti odustalo od novinarske karijere.¹⁴

b) Rodni i seksistički govor mržnje

Rodni i seksistički govor mržnje (engl. [*Gendered or sexist*] *hate speech*) obuhvata bilo koju vrstu komunikacije, kroz govor, tekst ili neverbalno ponašanje, kojom se napada, ponižava, vređa i diskriminiše osoba na osnovu pola, roda, seksualne orijentacije ili rodnog identiteta. Rodni i seksistički govor mržnje u onlajn prostoru podupire sistemski seksizam,² a pritom dehumanizuje žene, devojčice i LGBTQIA+ osobe, te podstiče nasilje protiv njih.¹⁵ **U rodni i seksistički govor mržnje spadaju seks posramljivanje i trolovanje, posebno trolovanje na osnovu roda, uključujući i potpirivanje i trolovanje u cilju zastrašivanja.**

b) Seks posramljivanje onlajn

Seks posramljivanje onlajn (engl. *slut-shaming online*), neretko nazivano i **slatšejmovanjem**, jeste oblik rodno zasnovanog nasilja često usmerenog na tinejdžerke i LGBTQIA+ osobe, koje bivaju diskriminisane i ponižavane jer ne ispunjavaju društvene i rodne norme u vezi sa seksualnim ponašanjem, izgledom i seksualnošću. Seks posramljivanje onlajn se neretko preklapa sa sajber proganjanjem, deljenjem pornografije bez saglasnosti i umreženim uznemiravanjem, čime se negativni uticaj na osobe koje su meta ovakvog ponašanja pojačava.¹⁶

*Seks posramljivanje onlajn se najčešće ispoljava kroz vređanje, bilo da je reč o komentarima ili fotografijama, mimovima, video snimcima i animacijama, s ciljem da se osoba ponizi na osnovu roda, seksualnosti i seksualnog ponašanja. Pored osoba koje se percipiraju kao devijantne ili promoskuitetne jer njihovo ponašanje, izgled ili oblačenje nije u skladu s patrijarhalnim normama, mete seks posramljivanja u digitalnom okruženju takođe su i osobe koje su preživle seksualno nasilje, što se temelji na netačnom ubeđenju da su svojim ponašanjem izazvale nasilnika.*¹⁷

b) Trolovanje, trolovanje na osnovu roda, potpirivanje i trolovanje u cilju zastrašivanja

Trolovanje (engl. *trolling*) je oblik sajber zlostavljanja čiji je cilj da se druge osobe iznerviraju i/ili da se internet diskusija na određenu temu obesmisli i spreči konstruktivna i civilizovana razmena različitih mišljenja. Trolovanje se najčešće vrši tekstualnim putem, objavljivanjem ponižavajućih ili uvredljivih komentara. Trolovi (osobe koje troluju) uživaju u tome, a kada im se ukaže na opasne posledice njihovog ponašanja, poriču svoju odgovornost tvrdeći da je sve to šala, te da drugi „nemaju smisao za humor”. **Trolovanje na osnovu roda** (engl. *gender trolling*) za metu zlostavljanja ima devojčice, devojke i žene, i to samo zato što su žene. Trolovanje na osnovu roda uključuje upotrebu rodno obojenih uvreda, seksističkog i mizoginog jezika u porukama i komentarima, kreiranje nasilničkih i uvredljivih heštegova koji pozivaju na nasilje prema ženama, ali i pretnje smrću ili silovanjem.¹⁸ Najnasilniji oblik trolovanja na osnovu roda čini **potpirivanje** (engl. *flaming*), koje se sastoji od objavljivanja ili slanja uvredljivih poruka putem interneta s ciljem da se osoba uznemiri i uplaši. Ovakve poruke se postavljaju na forume i/ili druge onlajn grupe za razmenu informacija, ili se pak šalju putem imejla i/ili drugih alata za onlajn razmenu poruka. Poseban oblik trolovanja predstavlja **trolovanje u cilju zastrašivanja**, kada je cilj da se osoba zastraši time da će biti napadnuta mimo digitalnog konteksta, jer je trolovi uveravaju da zlostavljač zna kako da je pronađe.¹⁹ Mnogi trolovi su anonimni i koriste lažne naloge, a dešava se i da se udruže, kako bi sproveli umreženo uznemiravanje. Bez obzira na to o kom obliku trolovanja je reč, ono često prati ili prethodi drugim oblicima nasilja u digitalnom okruženju.

*Osim svog tekstualnog oblika, trolovanje na osnovu roda može biti i vizuelno, kada se šalju ili postavljaju fotografije, mimovi, animacije i video snimci čija je svrha nerviranje i provociranje devojčica, devojaka i žena, kao i podsticanje na nasilje prema njima.*²⁰

² Seksizam predstavlja uverenje da su muškarci superiorniji od žena, a na osnovu tog uverenja i diskriminaciju zasnovanu na rodu ili polu koja se smatra opravdanom. Kada ovo uverenje i diskriminacija postanu opšteizostupljeni (na primer, u institucijama ili u medijima), govorimo o sistemskom seksizmu.

b) Odmazda zbog podrške osobama koje su preživele nasilje

Ovaj oblik nasilja uključuje pretnje i uznemiravanje članova porodice, prijatelja, poslodavca ili zajednice koja osobi s iskustvom nasilja pruža podršku.²¹ Iako **odmazda zbog podrške osobama koje su preživele nasilje** (engl. *retaliations against supporters of survivors*) potiče iz oflajn sveta, u eri #MeToo pokreta, kada se sve više žena oseća osnaženo da progovori u onlajn prostoru o nasilju koje su preživele, a sve više osoba da im pruže podršku, digitalni oblik omazde zbog podrške osobama koje su preživele nasilje postaje sve zastupljeniji. U digitalnom svetu, na meti se, pored osoba iz šire i bliže okoline žrtava nasilja, nalaze i njoj nepoznate osobe koje su joj pružile podršku.

*Predsednica Komisije za žene Delhija Svati Malival je dobila pretnje silovanjem na svom Instagram nalogu nakon što je pisala ministru Anuragu Takuru zahtevajući uklanjanje reditelja Sajida Kana iz rijaliti emisije Bigg Boss. Malival je svoj zahtev poslala ministru kao čin podrške glumicama koje su Sajida Kana optužile za seksualno nasilje i uznemiravanje, o kome su i javno progovorile služeći se #MeToo heštegom.*²²

b) Kleveta u onlajn prostoru

Kleveta u onlajn prostoru (engl. *online defamation* ili *online libel*) odnosi se na objavljivanje i širenje izmenjenih ili lažnih informacija koje narušavaju ugled neke osobe putem interneta. Cilj klevete je ponižavanje, upućivanje pretnji, diskreditovanje, zastrašivanje ili kažnjavanje osobe, a najčešće se usmerava ka javnim ličnostima: na primer, na javne zvaničnike i zvaničnice, aktiviste i aktivistkinje, te novinare i novinarkе.²³

*Tokom 2021. godine, vlada Australije je najavila kriminalizaciju klevete u onlajn prostoru. Ovaj predlog zakona će primorati društvene mreže, poput Tvitera ili Fejsbuka, da otkriju identitet anonimnih naloga koji iznose klevete, što će oštećenima omogućiti da zatraže pravdu na sudu ukoliko te objave ne budu uklonjene.*²⁴

Seksualno nasilje u digitalnom okruženju

Seksualno nasilje u digitalnom okruženju obuhvata različite oblike seksualnog zlostavljanja koje se sprovodi posredstvom informaciono-komunikacionih tehnologija i/ili se vrši u digitalnom okruženju. Ono uključuje **zlostavljanje posredstvom vizuelnog sadržaja**, bez obzira na to da li je vizuelni materijal stvaran ili se do njega došlo manipulacijom kompjuterskim programima – u drugom slučaju, govorimo o **dipfejku**. U zlostavljanje posredstvom vizuelnog sadržaja spadaju **podsumknjavanje i perverznojačko fotografisanje; pornografija bez saglasnosti i seksualna iznuda; sintetički seksualni mediji, dipfejkovi i lažna (dipfejk) pornografija; seksting i zlostavljački seksting; sajber egzibicionizam, neželjena pornografija i dikpik fotografije / fotografije penisa**. Seksualno nasilje u digitalnom okruženju se, nažalost, često preliiva i preklapa sa seksualnim nasiljem u oflajn svetu, a kada se to desi, govorimo o **grumovanju u onlajn prostoru, neželjenim seksualnim iskustvima uživo omogućenim tehnologijom**, kao i o **elektronski potpomognutoj trgovini ljudima**. Seksualno nasilje u digitalnom okruženju može predstavljati i nastavak seksualnog nasilja u oflajn svetu – primer je praksa **snimanja i/ili emitovanja seksualnih napada i silovanja**.

b) Zlostavljanje posredstvom vizuelnog sadržaja

Zlostavljanje posredstvom vizuelnog sadržaja (engl. *image-based abuse, IBA*) je krovni pojam koji obuhvata različite oblike rodno zasnovanog seksualnog nasilja u digitalnom prostoru²⁵. **Zlostavljanje posredstvom vizuelnog sadržaja se temelji na pravljenju, slanju ili pretnjama slanjem fotografija ili video snimaka intimne ili seksualne prirode kako bi se osoba uznemirila,**

ucenila, pretilo joj se, uništio joj se ugled i reputacija, ili se predstavila kao seksualni objekt.

Ovo se čini bez saglasnosti osobe koja je na fotografijama ili video snimcima. Vizuelni sadržaj koji se koristi za zlostavljanje može biti i veštački napravljen, upotrebom dipfejk tehnologije. Zlostavljanje posredstvom vizuelnog sadržaja uključuje i slanje pornografskog i seksualnog sadržaja osobi bez njene saglasnosti. Posledice ovog oblika nasilja, sem psiholoških, mogu biti i društvene: poput gubitka posla ili selidbe u drugo mesto, gde žrtvu niko ne poznaje. U zlostavljanje posredstvom fotografije spadaju **podsumknjavanje i perverznojačko fotografisanje, pornografija bez saglasnosti i iznuda na seksualnoj osnovi**, kao i **sintetički seksualni mediji** poput **dipfejkova i lažne (dipfejk) pornografije**.

b) Podsumknjavanje i perverznojačko fotografisanje

Podsumknjavanje (engl. *upskirting*) i **perverznojačko fotografisanje** (engl. *creepshots*) obuhvataju snimanje devojčica, devojaka i žena na javnim mestima, a bez njihove dozvole. Ovo se najčešće dešava na javnim mestima, kao što su prodavnice, javni toaleti, javni saobraćaj, svlačionice, učionice ili ulice, ali i u privatnim stanovima devojčica, devojaka i žena. Podsumknjavanje predstavlja potajno pravljenje fotografija i video snimaka ispod suknje ili haljine,²⁶ dok perverznojačko fotografisanje obuhvata pravljenje seksualno sugestivnih fotografija i video snimaka neke ženske osobe, a da ona to ne primeti.²⁷

U Japanu je 2021. godine zabeležena „pandemija“ podsumknjavanja, kada je u prvih šest meseci 2021. godine uočen porast prijavi policiji od 30% u odnosu na isti period prethodne godine. Devojčice, devojke i žene bile su fotografisane najčešće u javnom prevozu, a, osim mobilnih telefona, nasilnici su koristili i sofisticiranu tehnologiju nalik na špijunsku opremu – kamere u olovkama, naočarima, drškama kišobrana i cipelama. Tokijski metro od 2019. godine ima po-

seban vagon za žene, baš zbog različitih vrsta seksualnog nasilja s kojima se žene u javnom prevozu susreću, uključujući i ovaj njegov digitalni oblik.²⁸

b) Pornografija bez saglasnosti i iznuda na seksualnoj osnovi

Pornografiju bez saglasnosti (engl. *non-consensual pornography*), koja se često naziva i **osvetničkom pornografijom** (engl. *revenge porn*), čini svako neovlašćeno snimanje (fotoaparatom ili kamerom) i/ili deljenje, kao i pretnje deljenjem, snimaka na kojima se osoba nalazi obnažena ili u situaciji sa seksualnom konotacijom, a sve u cilju da se osoba ponizi, osramoti ili uceni.²⁹ Kada je cilj ucena, možemo govoriti i o **iznudi na seksualnoj osnovi** (engl. *sextortion*), čiji je cilj da se od osobe iznudi novac ili se primora da uradi nešto što ne želi, poput seksualnog čina, pod pretnjom da će njene nage fotografije ili snimci sa seksualnom konotacijom biti objavljeni. Iznuda na seksualnoj osnovi u nekim državama, poput Ujedinjenog Kraljevstva, predstavlja i krivično delo. S napretkom tehnologije i softvera za modifikaciju video snimaka i fotografija, pornografija bez saglasnosti progresivno uključuje i lažnu pornografiju (dipfejk pornografiju), a obe se mogu koristiti za iznudu na seksualnoj osnovi.

Početkom 2021. godine na Balkanu su otkrivene Telegram grupe Javna soba, Ex Yu Balkanska soba i Nišlijke, koje su služile za razmenu pornografije bez saglasnosti. Ove grupe su brojale na desetine hiljada članova, a, pored razmene fotografija i video snimaka devojaka, razmenjivani su i njihovi lični podaci (doksovane su), poput imena i prezimena, brojeva telefona i imejl-ova, adrese ili linkova ka društvenim mrežama.³⁰

b) Sintetički seksualni mediji, dipfejkovi i lažna (dipfejk) pornografija

Sintetički seksualni mediji (engl. *synthetic sexual media*) služe za manipulaciju fotografija

i video sadržaja u cilju da se proizvede utisak da su određene osobe učestvovala u seksualnoj aktivnosti u kojoj, u stvarnosti, nisu učestvovala. Razlozi iz kojih se koriste sintetički seksualni mediji mogu biti različiti – od zabave, preko zarade, pa sve do ucene i uznemiravanja žena i uništavanja njihovog ugleda i reputacije. Sintetički seksualni mediji predstavljaju krovni pojam, a dipfejkovi su njihov najčešći oblik.³¹

Dipfejkovi (engl. *deepfakes*) su digitalni foto, video i audio sadržaji koji se naknadno menjaju ili se njima manipuliše uz pomoć specijalizovanih programa. Cilj dipfejka je da se stekne utisak da je neko rekao ili uradio nešto što zapravo nije. Dipfejk se može koristiti u političke svrhe, ali se češće koristi u obliku lažne pornografije. **Lažna (dipfejk) pornografija** (engl. *deepfake pornography*) nastaje bez pristanka osobe čiji se lik koristi u pornografskom materijalu, i predstavlja oblik pornografije bez saglasnosti.

U skoro svim slučajevima lažne (dipfejk) pornografije, mete su žene, među kojima se nalaze i javne ličnosti, poput glumice Kristen Bel, ali i nepoznate žene i devojke, s obzirom na to da je ova tehnologija finansijski sve dostupnija.³² Zbog toga je dipfejk pornografija u nekim zemljama, poput Hrvatske, kriminalizovana (Zloupotreba snimke spolno eksplicitnog sadržaja čl. 144a).

b) Seksting i zlostavljački seksting

Seksting (engl. *sexting*) je elektronska razmena nagih ili fotografija sa seksualnom konotacijom, kao i video snimaka seksa i seksualnog tekstualnog sadržaja uz saglasnost svih strana. Iako je seksting često predstavljen kao opasan, on sam po sebi to nije, sve dok postoji saglasnost i poštuje se privatnost svih osoba koje su uključene u njega. Od ovakvog sekstinga razlikuje se **zlostavljački seksting** (engl. *abusive sexting*), u kome pristanak osobe kojoj se sadržaj šalje izostaje. Ukoliko se osobe ne ponašaju odgovorno prema sadržaju koji je sekstingom razmenjen i ne poštuju privatnost osobe koja se nalazi na sadržaju, te ga prosle-

đuju trećim licima, reč je o pornografiji bez saglasnosti.

Iako i tinejdžeri i tinejdžerke sekstuju u istoj meri, verovatnoća da će dečaci dalje proslediti fotografije koje su im poslate jeste dva do tri puta veća.³³ Takođe, istraživanja pokazuju da je iskustvo zlostavljačkog sekstinga češće kod mlađih tinejdžera i tinejdžerki, te predadolescenta i predadolescentkinja,³⁴ kao i kod onih čija je seksualnost različita od heteroseksualne.³⁵

b) Sajber egzibicionizam, neželjena pornografija i dikpik fotografije / neželjene fotografije penisa

Sajber egzibicionizam (engl. *cyberflashing*) predstavlja oblik zlostavljanja posredstvom fotografija prilikom koga se nepoznatim osobama, bez njihovog pristanka, šalju seksualno eksplicitne fotografije i video snimci. **Neželjena pornografija** (engl. *unsolicited pornography*) predstavlja oblik sajber egzibicionizma u kom osoba šalje neželjenu fotografiju svojih genitalija ili seksualno eksplicitan materijal drugoj osobi bez njene saglasnosti.³⁶ **Neželjene fotografije penisa**, često nazivane i **dikpik fotografijama** (engl. *dick pics*), predstavljaju najčešći vid neželjene pornografije. Reč je o fotografijama na kojima je uslikan penis, najčešće u erekciji, a koje se šalju putem interneta. Sajber egzibicionizam, pored dikpikova, uključuje i druge oblike neželjene i pornografije bez saglasnosti, kao i fotografije, video snimke i GIF animacije sa scenama seksa, ali i silovanja.³⁷

Sajber egzibicionizam, dikpik fotografije i neželjena pornografija predstavljaju veliki problem, u meri da je Ujedinjeno Kraljevstvo trenutno u procesu usvajanja zakona kojima će ovo ponašanje biti kriminalizovano.³⁸ Kriminalizacija je predložena nakon što je istraživanje iz 2019. godine pokazalo da je 76% tinejdžerki uzrasta od dvanaest do osamnaest godina dobilo neželjenu fotografiju penisa.³⁹

b) Snimanje i/ili emitovanje seksualnih napada i silovanja

Seksualno nasilje u digitalnom okruženju može predstavljati i nastavak seksualnog nasilja u oflajn svetu – primer je praksa **snimanja i/ili emitovanja seksualnih napada i silovanja** (engl. *documenting or broadcasting sexual assault/rape videos*) na društvenim mrežama, putem poruka ili sajtova, koja predstavlja dodatni čin seksualnog nasilja protiv žrtve/preživele. Ovi snimci se ponekad koriste i kako bi se osobe koje su preživele seksualno nasilje ponizile ili ucenjivale, a takođe se prodaju i kao pornografija bez saglasnosti.

Kampanja #NotYourPorn je pokrenuta s ciljem podizanja svesti o manjkavosti regulatornih mehanizama na popularnim pornografskim sajtovima koji bi uklonili ili onemogućili postavljanje snimaka seksualnih napada i silovanja, pornografije bez pristanka, kao i dobrovoljno snimljenog materijala koji je ukraden od seksualnih radnika i radnica i objavljen bez njihove saglasnosti.

b) Grumovanje u onlajn prostoru

Grumovanje u onlajn prostoru (engl. *grooming online*) predstavlja predatorski oblik ponašanja čija je namera da se stupi u kontakt s decom i mladima putem društvenih mreža ili drugih digitalnih platformi, a sve u cilju seksualnog nasilja. Grumovanje funkcioniše tako što grumer (osoba koja grumuje) uspostavlja lažnu emotivnu vezu sa svojom metom i obmanjuje je u cilju vršenja seksualnog zlostavljanja, seksualnog iskorišćavanja (na primer, seksualne eksploatacije kroz primoravanje na prostituciju) ili trgovine decom. Prilikom grumovanja u onlajn prostoru, predatori se često i sami predstavljaju kao deca ili mladi, a ponekad, kada uspostave odnos, zahtevaju i susret uživo, što otvara mogućnost za seksualnu eksploataciju i seksualno i fizičko nasilje u oflajn prostoru.

U poslednje četiri godine zabeležen je porast od čak 84% slučajeva grumovanja u onlajn prostoru

*u Ujedinjenom Kraljevstvu. Deca i mladi su najčešće grumovani na društvenim mrežama i sajtovima za igranje igrice, a grumeri su od njih zahtevali da im pošalju seksualno eksplicitni materijal.*⁴⁰

b) Neželjena seksualna iskustva uživo omogućena tehnologijom

Do **neželjenih seksualnih iskustava uživo omogućenih tehnologijom** (engl. *technology-facilitated unwanted sexual experiences*) dolazi kada se informaciono-komunikacione tehnologije koriste kako bi se omogućilo seksualno uznemiravanje ili seksualno nasilje prilikom susreta u oflajn svetu. Tehnologije koje se upotrebljavaju za ovaj oblik nasilja najčešće su aplikacije, sajtovi i platforme za upoznavanje partnera (onlajn dejting), preko kojih se dogovara susret uživo, na kome i dolazi do seksualnog napada.⁴¹

*Istraživanje iz Ujedinjenog Kraljevstva ukazuje da se broj osoba koje su prijavile silovanje na prvom sastanku s osobom koju su upoznale onlajn uvećao šest puta u roku od pet godina, pri čemu su u 85% slučajeva žene te koje su prijavile silovanje u periodu između 2003. i 2015. godine. Najranjivije su bile mlade žene, starosti od dvadeset do dvadeset četiri godine, koje su imale dvostruko veću šansu da dožive neželjeno seksualno iskustvo posredovano tehnologijom u odnosu na starije žene.*⁴²

b) Elektronski potpomognuta trgovina ljudima i vrbovanje

Informaciono-komunikacione tehnologije se takođe koriste prilikom trgovine ženama i devojčicama, i tada govorimo o **elektronski potpomognutoj trgovini ljudima** (engl. *electronically facilitated trafficking*). Informaciono-komunikacione tehnologije mogu biti korišćene za **vrbovanje** (engl. *recruitment*). Trgovci ljudima veoma često upotrebljavaju internet za vrbovanje tako što objavljuju lažne oglase za posao ili studiranje, najčešće u inostranstvu, ili koriste lažne profile na aplikacijama i sajtovima za upozna-

vanje odnosno sajtovima „bračnih“ agencija.⁴³ Trgovci ljudima tehnologiju zloupotrebljavanju i u drugim fazama seksualne eksploatacije, kao i prilikom upućivanja pretnji u cilju prinude i kontrole trafikovanih žena i devojčica, kada je reč o iznudi na seksualnoj osnovi. Za elektronski potpomognutu trgovinu ljudima najčešće se koriste platforme društvenih mreža ili aplikacije i sajtovi za upoznavanje.^{44 45}

*Istraživanje organizacije Atina, udruženja građana za borbu protiv trgovine ljudima i svih oblika nasilja prema ženama, pokazalo je da je veliki broj žena i devojaka koje su bile trafikovane vrbovan posredstvom digitalnih medija, dok je 30% njih vrbovano kako bi se nad njima izvršio i neki drugi oblik nasilja, poput silovanja, razbojništva ili fizičkog nasilja. Više od polovine žrtava trgovine ljudima se susrelo i s objavljivanjem oglasa na internetu u cilju „reklamiranja“ njihove seksualne eksploatacije, a polovina je takođe preživela iznudu na seksualnoj osnovi, kada su ih trafikeri ucenjivali video materijalom.*⁴⁶

Ugrožavanje privatnosti i bezbednosti posredstvom tehnologije

Ugrožavanje privatnosti i bezbednosti posredstvom tehnologije obuhvata čitav niz radnji koje imaju za cilj da se osoba oseti nebezbedno, ugroženo i nepoželjno, ne samo u digitalnom okruženju već i u oflajn svetu. Upravo to čini jednu od najvažnijih odlika ove grupe ponašanja – nemogućnost da se napravi jasna razlika između onlajn i oflajn okruženja. Objavljivanje ličnih informacija o osobi bez njenog pristanka na internetu, **doksovanje, dednejmovanje ili autovanje bez saglasnosti**, za posledicu mogu

imati ugrožavanje bezbednosti te osobe u oflajn svetu; **lažno predstavljavanje i ketfišing** za cilj imaju ne samo sticanje finansijske koristi već, potencijalno, i seksualno nasilje ukoliko dođe do susreta uživo, a tehnologija se može koristiti i za **ograničavanje i kontrolisanje** određene osobe, najčešće intimnog partnera ili partnerke, kao i za **finansijsko zlostavljanje**. Kada je reč o **sajber proganjanju i opsesivnom praćenju na internetu**, oni se često nadovezuju ili prethode proganjanju u oflajn svetu, a **onlajn pretnje** se u većini slučajeva tiču života osobe kojoj se pretilo van interneta. Kada se zlostavljanje „prelije“ iz onlajn u oflajn svet, možemo govoriti o **napadima „u stvarnom životu“**. Takođe, u ovu vrstu nasilja spadaju i **bombardovanje na Guglu i Zumu**, kao i **napadi uskraćivanjem pristupa i usluga**.

b) Doksovanje, dednejmovanje i autovanje bez saglasnosti

Doksovanje (engl. *doxxing* ili *doxing*) predstavlja oblik digitalnog rodno zasnovanog uznemiravanja u okviru kojeg jedna osoba, dokser, prikuplja podatke o drugoj osobi, analizira ih i objavljuje, a sve to s namerom da tu drugu osobu prikaže u negativnom svetlu i naruši njen ugled i/ili bezbednost.⁴⁷ U slučaju doksovanja najčešće se objavljuju lične informacije – adresa stanovanja ili imejl adresa, broj telefona, kontakti poslodavaca ili članova porodice, odnosno fotografije dece ili škole koju deca pohađaju, a sve s ciljem da se obelodani/sazna tačna lokacija i sprovede fizičko nasilje.⁴⁸ Posebne oblike doksovanja predstavljaju autovanje bez saglasnosti i dednejmovanje, čije su mete pripadnici i pripadnice LGBTQIA+ i TIRV zajednice. Prilikom **autovanja bez saglasnosti** (engl. *non-consensual outing*) otkriva se seksualna orijentacija LGBTQIA+ osobe, a prilikom **dednejmovanja** (engl. *deadnaming*) ime dato po rođenju trans osobe, kako bi se željeni identitet trans osobe umanjio, poništio ili obezvređio. I u slučajevima autovanja bez saglasnosti i dednejmovanja doksovanje se vrši s idejom da se osobi nanese šteta, te da se ona izloži nasilju i diskriminaciji, kako u onlajn tako i u oflajn svetu.⁴⁹

Doksovanje često prati druge oblike rodno zasnovanog nasilja, a njemu su posebno izložene žene koje su vidljive u javnosti, poput novinarki. Novinarica i osnivačica neformalne grupe Novinarke protiv nasilja, Jovana Gligorijević, često je bila meta pretnji, rodnog i seksističkog govora mržnje, kao i trolovanja na osnovu roda, a 2019. godine, u komentaru na Jutjub videu, objavljeni su i njen matični broj (JMBG) i adresa stanovanja.⁵⁰

b) Lažno predstavljanje i ketfišing

Lažno predstavljanje (engl. *impersonation*) je proces krađe nečijeg već postojećeg identiteta radi pretnje ili zastrašivanja, kao i da bi se ta osoba diskreditovala ili narušio njen ugled.⁵¹ Poseban oblik lažnog predstavljanja čini **ketfišing** (engl. *catfishing*), prilikom koga dolazi do lažnog predstavljanja s ciljem prevare. Ketfišing se najčešće odvija tako što se žrtva zaljubi u počinioca te, kada razvije intimna osećanja i poveruje da su u vezi, počinitelj od nje traži novac ili poklone, kako bi stekao finansijsku korist. Počinitelj takođe može da traži i određene informacije i/ili intimne fotografije, kako bi žrtvu dalje ucenjivao. I kod lažnog predstavljanja i kod ketfišinga, u kreiranju lažnog identiteta, počinioci se često služe fotografijama drugih ljudi, te smišljaju detaljne lažne biografije i životna iskustva, kao i poslove i prijatelje.^{52 53}

*Lažno predstavljanje i ketfišing se najčešće odigravaju na sajtovima i aplikacijama za upoznavanje partnera, te većina ovih sajtova i aplikacija pokušava da razvije mehanizme provere identiteta ne bi li ovaj vid prevare sprečile. U ovim slučajevima, cilj ketfišinga ne mora biti nužno ostvarivanje finansijske koristi, bilo kroz poklone ili iznudu, već i seksualno nasilje kada dođe do susreta uživo, a tada govorimo o neželjenim seksualnim iskustvima uživo omogućenim tehnologijom. Jedan od najpoznatijih počinitelja lažnog predstavljanja i ketfišinga je Simon Leviev, o kome je snimljen dokumentarni film *Tinder Swindler*. Leviev je svoje žrtve prevario za milione dolara, a i dalje se nalazi u bekstvu.*⁵⁴

b) Ograničavanje ili kontrolisanje pomoću tehnologije

Nasilnici mogu koristiti tehnologiju da zlostavljaju ili kontrolišu, tako što osobu prate, nadziru ili ograničavaju kretanje, komunikaciju i aktivnosti te osobe. Ova ponašanja variraju od prinude osobe, najčešće intimne partnerke ili partnera, da preda lozinke u cilju sticanja pristupa njenim onlajn nalogima, pa sve do direktnog ograničavanja ili zabrane korišćenja tehnoloških uređaja. U partnerskim odnosima u kojima postoji zlostavljanje, **ograničavanje ili kontrolisanje pomoću tehnologije** (engl. *limiting or controlling use of technology*) može prethoditi drugim oblicima zlostavljanja.⁵⁵

*Problem s ovim oblikom rodno zasnovanog nasilja je u tome što se često romantizuje, tako što se davanje sopstvenih loznika i pristupa onlajn nalogima ili instaliranje aplikacija za praćenje predstavlja kao vid brige i dokaz ljubavi između partnera. Kako je tehnologija danas jedan od načina na koji stupamo u kontakt sa spoljnim svetom, ograničavanje ili kontrolisanje njene upotrebe od strane partnera jeste pokušaj izolacije, kontroisanja i uskraćivanja resursa da se iz nasilne veze izađe, što je česta tehnika koju nasilnici koriste.*⁵⁶

b) Finansijsko zlostavljanje elektronskim putem

Finansijsko zlostavljanje elektronskim putem (engl. *electronically enabled financial abuse*) čini produžetak odnosno preseljenje ekonomskog nasilja u digitalni prostor. Ono obuhvata različite načine upotrebe interneta i drugih oblika informaciono-komunikacionih tehnologija u cilju vršenja finansijskog pritiska na osobu. Finansijsko zlostavljanje elektronskim putem najčešće doživljavaju žene, a zlostavljači su pritom njihovi intimni partneri.

Finansijsko zlostavljanje elektronskim putem obuhvata uskraćivanje onlajn pristupa bankovnim računima, te krivotvorenje informacija kako bi se napravio negativan kreditni status ili ukrao

identitet.⁵⁷ Na ovaj način, zlostavljači imaju potpunu kontrolu nad svojim žrtvama jer im one moguće pristup novcu, kao i mogućnost da dignu kredit kako bi došle do novca koji im je potreban da napuste zlostavljače.⁵⁸

b) Sajber proganjanje i opsesivno praćenje na internetu

Sajber proganjanje (engl. *cyberstalking*) je oblik zlostavljanja prilikom koga počinitelj koristi tehnologiju kako bi pratio osobu i njegovo ponašanje na internetu. Ono ne mora uključivati direktne pretnje, već obuhvata sve one aktivnosti koje kod mete napada izazivaju osećaj straha, zabrinutosti, anksioznosti i bespomoćnosti. Sajber progonitelj će svojoj meti slati poruke, zvati je, ili joj slati glasovne poruke s ciljem da je drži u aktivnom stanju stalne uznemirenosti i straha za svoju bezbednost van interneta.⁵⁹ **Opsesivno praćenje na internetu** (engl. *cyber-obsessional pursuit*) odlikuje korišćenje tehnologije kako bi se osoba proganjala, a od sajber proganjanja se razlikuje utoliko što se od žrtve zahteva neki oblik intimne veze. Opsesivno praćenje na internetu karakteriše zahtevanje intimnosti kroz narušavanje fizičke i onlajn privatnosti, i ono obuhvata ponašanja poput onlajn i oflajn proganjanja, slanja neželjenih poklona, zahteva za praćenje/prijateljstvo na društvenim mrežama, kao i poruka poput imejllova, tekstualnih poruka ili poruka preko različitih mesindžer aplikacija.⁶⁰

Često možemo čuti da sajber proganjanje nije nešto strašno, jer osoba može ugasiti svoje naloge na internetu i „isključiti računar“. To, nažalost, nije tačno – sajber proganjanje deluje na žrtvu na isti način na koji to čini proganjanje u oflajn životu, a u određenom broju slučajeva prethodi ili je deo proganjanja osobe van interneta.⁶¹ Zbog toga je u nekim zemljama, poput Srbije, sajber proganjanje kriminalizovano (u okviru krivičnog dela proganjanja čl. 138a Krivičnog Zakonika).

b) Napadi „u stvarnom životu“

O **napadima „u stvarnom životu“** (engl. *in-real-life (IRL) attacks*) govorimo onda kada onlajn zlostavljanje pređe u nedigitalni kontekst, ili je sastavni deo već postojećeg proganjanja ili zlostavljanja u partnerskom odnosu.⁶²

*Napadima „u stvarnom životu“ su posebno izložene žene koje su vidljive u javnosti, poput novinarki. Novinarke Dafne Karuna Galicija i Gauri Lankeš ubijene su 2017. godine nakon što su bile izložene umreženom uznemiravanju u vidu pretnji silovanjem i smrću.*⁶³

b) Onlajn pretnje

Onlajn pretnja (engl. *online threats*) je „izjava o nameri da se nanese bol, povreda, šteta ili druga neprijateljska radnja“ osobi kojoj je upućena. Pored pretnji nasiljem u onlajn okruženju (pretnje uskraćivanjem pristupa, pretnje dipfejk pornografijom ili doksovanjem), pretnje se sve češće odnose na nasilje u oflajn svetu – tu spadaju pretnje smrću, kao i pretnje fizičkim i/ili seksualnim nasiljem.⁶⁴

*Žene koje su u digitalnom prostoru glasne kada je reč o ženskim i ljudskim pravima česta su meta pretnji. Prema podacima Nezavisnog udruženja novinara Srbije (NUNS), u Srbiji su tri četvrtine pretnji novinarkama pokušaji ugrožavanja reputacije, a preko polovine imaju oblike seksualnog uznemiravanja i ugrožavanja bezbednosti i života.*⁶⁵

b) Bombardovanje na Guglu i Zumu

Bombardovanje na Guglu (engl. *Google bombing*) uključuje ciljano prilagođavanje algoritma radi pozicioniranja sajtova na internetu koji sadrže zlonamerne i netačne informacije o nekoj osobi ili pojavi, tako da se upravo oni vide prvi ili među prvim kada se pretražuje zadati pojam ili osoba.⁶⁶ S druge strane, **bombardovanje na Zumu** (engl. *Zoom bombing*) odnosi se na nepozvani „upad“ u tuđ razgovor na

ovoj platformi, s ciljem širenja rasističkih, seksističkih, pornografskih, homofobnih ili antisemitskih sadržaja, kako bi se prisutni gledaoci uznemirili i šokirali. Bombardovanje na Zumu predstavlja oblik umreženog uznemiravanja.⁶⁷

*Jedan od primera bombardovanja na Guglu usmerenog protiv žena jeste događaj iz 2011. godine, kada su aktivisti – protivnici prava na prekid trudnoće uspjeli da prilagode Guglov algoritam tako da Vikipedijina stranica o abortusu izlazi kao prvi rezultat prilikom pretraživanja pojma ubistvo (engl. murder).*⁶⁸

b) Napad uskraćivanjem pristupa i napad uskraćivanjem usluga

Napad uskraćivanjem pristupa (engl. *denial of access*) predstavlja iskorišćavanje određenih opcija tehnologija ili platformi kako bi se nanela šteta osobi, tako što će joj se uskratiti pristup ličnom profilu na društvenim mrežama ili imejlu. Postoje dva osnovna oblika uskraćivanja pristupa. Prvi se sastoji od koordinisanog napada zlostavljača koji lažno i udruženo prijavljuju nalog osobe, kolektiva ili institucije zbog navodne zloupotrebe ili nekog drugog kršenja pravila, a sve kako bi blokirali ili ugasili taj nalog. Na ovaj način se najčešće uskraćuje pristup društvenim mrežama. Drugi oblik uskraćivanja pristupa se odnosi na masovno slanje velikog broja imejlova ili preplavlivanje sms porukama, čiji je cilj da se osoba, kolektiv ili institucija spreče da koriste platformu, na primer imejl, zbog bombardovanja velikom količinom neželjenog sadržaja.⁶⁹ Pored napada uskraćivanjem pristupa, postoji i **napad uskraćivanjem usluga** – DoS napad (engl. *denial of service*). Dok je cilj napada uskraćivanjem pristupa da se onemogući pristup određenoj platformi ili nalogu, cilj napada uskraćivanjem usluga je da se onemogući pristup računar, odnosno računarskoj mreži. Osim uskraćivanja pristupa računar ili mreži, napadi uskraćivanjem usluga mogu da kompromituju osetljive informacije koje su sačuvane na tim uređajima. Do distribuisanog uskraćivanja usluga – DDoS (engl. *Distributed Denial of*

service) dolazi kada napadač preuzme kontrolu nad računarima većeg broja korisnika kako bi napao računar drugog korisnika. Na taj način napadač navodi „otete“ računare da šalju velike količine zahteva određenoj internet stranici ili da šalju spem na ciljane imejl adrese. DDoS napadi funkcionišu tako što sistem preopterećete podacima koje napadač šalje s drugih računara.

*S napadom uskraćivanjem pristupa se često susreću feministkinje i aktivistkinje širom sveta, jer je reč o pokušaju ućutkivanja i oduzimanja glasa ženama. U Kini je 2021. godine ugašeno nekoliko feminističkih kanala na popularnim forumima Douban i Weibo. Oni su ugašeni nakon velikog broja prijava zbog „ekstremističkog i ideološkog sadržaja“, uprkos tome što njihove vlasnice nisu prekršile nijedno od pravila ponašanja na ovim mrežama.*⁷⁰

Drugi oblici nasilja u digitalnom okruženju

b) Astroturfing

Astroturfing (engl. *astroturfing*) je praksa objavljivanja i širenja informacija i sadržaja (čiji cilj može biti i maltretiranje i zlostavljanje) na internetu, a s namerom stvaranja utiska da je do toga došlo na prirodan, organski način, te da je reč o opšteprihvaćenom gledištu. Cilj astroturfinga je stvaranje utiska da određene ideje i sadržaji imaju podršku velikog broja građana i građanki iako je reč o obmani, odnosno o lažiranju. Astroturfing predstavlja pažljivo koordinisani čin iza koga stoje pojedinci, interesne grupe, političke stranke ili organizacije, i u kome često učestvuju brojni lažni nalozi, tzv. botovi.

Naziv „astroturfing“ potiče od poznate marke veštačke trave AstroTurf, pri čemu je primetna igra reči – za razliku od „grassroot“ inicijativa kakvom pokušava da se predstavi, astroturfing predstavlja veštački stvorene medijske i reklamne kampanje s ciljem manipulacije javnosti.

b) Lažne optužbe za bogohuljenje

Žene se suočavaju s onlajn pretnjama na globalnom nivou, ali su u posebnom riziku u konzervativnim religioznim zemljama, gde je bogohuljenje protivzakonito i gde su ubistva iz časti ozbiljna pretnja. U tom smislu, **lažna optužba za bogohuljenje** (engl. *false accusations of blasphemy*) može sama po sebi da postane čin nasilja.⁷¹

Novinarka i braniteljka ljudskih prava Marvi Sirmed iz Pakistana bila je privedena 2020. godine nakon što je lažno optužena za bogohuljenje na društvenoj mreži Twitter, a, osim tužbe, Sirmed se susrela i s brojnim pretnjama.⁷²

b) Posthumno trolovanje i trolovanje na osnovu šoka i žalosti

Posthumno trolovanje (engl. *RIP trolling*) je oblik sajber zlostavljanja koji se temelji na objavljivanju ružnih i uvredljivih komentara na memorijalnim stranicama za preminule osobe na društvenim mrežama, ili pak na ličnim profilima preminulih osoba.⁷³ **Trolovanje na osnovu šoka i žalosti** (engl. *shock and grief trolling*) za metu ima porodicu i prijatelje preminulih, koji se uznemiravaju pravljenjem mimova, sajtova i lažnih naloga na društvenim mrežama s imenom i likom preminulih osoba.⁷⁴

Dva najpoznatija slučaja posthumnog trolovanja i trolovanja na osnovu šoka i žalosti dogodili su se 2010. godine, kada je trenericu morskih životinja Dawn Brancheau ubio kit s kojim je izvodila tačku. Nakon njene smrti trolovi su preplavili društvene mreže podrugljivim i seksističkim mimovima, ali i sintetičkim seksualnim medijima s njenim likom. Gotovo istovremeno, tinejdžerka Chelsea King je nestala, te su trolovi odlučili da naprave niz memorijalnih RIP stranica posvećenih njoj, iako još nije bila pronađena. Nakon što je njeno telo pronađe-

no, napravljena je Fejsbuk stranica pod nazivom „Kladim se da ovaj krastavac može da ima više fanova od Chelsea King“ (engl. „I Bet This Pickle Can Get More Fans than Chelsea King“), na kojoj je objavljena satelitska fotografija njene kuće, tražena njena pornografija bez saglasnosti, ali i prećeno silovanjem ženskih članova porodice onih koji su u komentarima pokušavali da odbrane sećanje na Chelsea King.⁷⁵

b) Svotovanje

Svotovanje (engl. *swatting*, jer je svot [SWAT, *special weapons and tactics*] skraćena za interventnu jedinicu policije) predstavlja lažno prijavljivanje nasilja, ubistva, pretnji bombom ili taočkih situacija policiji, što za rezultat ima dolazak potpuno naoružane interventne jedinice na nečiju, najčešće kućnu, adresu. Svotovanje je retko, ali je izuzetno opasno, i jasan je primer na koji način onlajn uznemiravanje ima potencijal da nanese ozbiljnu štetu osobi, a u ovom slučaju i čitavoj njenoj porodici, u oflajn životu.⁷⁶

Iako je svotovanje često shvaćeno kao šala, naročito među gejmerima, ono ima ozbiljne posledice, koje se kreću od uništavanja imovine, preko psihičkog stresa, pa sve do ozbiljnih fizičkih povreda i smrtnih ishoda. Na sreću, svotovanje na Zapadnom Balkanu nije zastupljeno u istoj meri kao u Sjedinjenim Američkim Državama, odakle je i poteklo.

b) Trovanje heštega

Trovanje heštega (engl. *hashtag poisoning*) predstavlja kreiranje uvredljivog heštega, ili, češće, otimanje već postojećeg heštega, tako da se njegovo značenje i namera menjaju. Ovako „otrovan“, hešteg se zatim koristi kao poziv na okupljanje za masovni sajber napad (engl. *cybermob attack*) na pojedinca, ili pak u cilju uništavanja inicijalne, veoma često feminističke, kampanje.⁷⁷

Popularni feministički heštegovi #TakeBackTheTech i #ImagineAFeministInternet, koji su 2015. godine promovisali ideju interneta na kome će žene biti bezbedne od rodno zasnovanog nasilja, bili su preplavljeni koordinisanom poplavom rodnog i seksističkog govora mržnje u cilju uništavanja kampanja.⁷⁸

// Pojmovi iz domena
tehnologije

A

Algoritam

Algoritam je niz instrukcija koje govore računaru na koji način da reši problem, izvrši funkciju ili pretvori set podataka u korisne informacije. Algoritmi se koriste u svim oblastima informacione tehnologije. Na primer, bilo koji računarski program može se smatrati složenim algoritmom.⁷⁹

Aplikacija ili ep (engl. *app*)

Aplikacije su softverski programi, uglavnom za mobilne uređaje kao što su pametni telefoni i tableti, kod kojih se preuzimanje i instalacija obično odvijaju u istom koraku. Prilikom instalacije aplikacija nisu potrebne dodatne korisnikove radnje, a aplikacije se mogu ukloniti s uređaja, deinstalirati, bez uticaja na njegovo funkcionisanje.⁸⁰ Važno je naglasiti da prilikom instaliranja aplikacija na mobilne uređaje korisnik/ca pristaje na uslove korišćenja koji se često odnose na deljenje podataka i ličnih informacija s uređaja, ponekad uključujući i geolokaciju, ali i kontakte iz telefonskog imenika.

D

Digitalna platforma

Digitalne platforme su onlajn preduzeća koja omogućavaju interakcije i razmenu podataka, robe i usluga između proizvođača i potrošača, kao i zajednice koja je u interakciji s pomenu-
tom platformom. Digitalne platforme mogu biti platforme društvenih mreža (Facebook, Twitter i LinkedIn), platforme znanja (Yahoo!Answers i Google Scholar), platforme za razmenu medija (Spotify, YouTube i Netflix), ili platforme orijentisane na usluge (Airbnb, Amazon i Uber).⁸¹

Digitalne tehnologije

Digitalne tehnologije su elektronski alati, sistemi, uređaji i resursi koji generišu, pohranjuju ili obrađuju podatke. Oni obuhvataju infrastrukturu, uređaje, medije, onlajn servise i platforme koje koristimo za potrebe komunikacije, informisanja, dokumentovanja, umrežavanja i povezivanja.⁸²

Društvene mreže

Društvene mreže su kolektivan pojam za veb-sajtove i aplikacije koji su usmereni na komunikaciju putem interneta, komentare zajednice, interakciju, razmenu sadržaja i saradnju. Forumi, mikroblogovi, društvene mreže, sajtovi i/ili platforme za pravljenje zbirke članaka, slika ili postova i njihovo deljenje, kao i *wiki* sadržaji, neke su od različitih vrsta društvenih mreža koje omogućavaju brz elektronski prenos sadržaja korisnicima. Sadržaj obuhvata lične informacije, dokumente, video i audio sadržaj, te fotografije. Korisnici upotrebljavaju društvene mreže putem računara, tableta ili pametnih telefona, uz pomoć softvera na internetu ili aplikacija. Platforme društvenih mreža koje se najčešće koriste jesu *Facebook*, *YouTube*, *WhatsApp*, *Facebook Messenger*, *Instagram* i *TikTok*.⁸³

Dron

U tehnološkom kontekstu, dron je bespilotna letelica – leteći robot koji se može kontrolisati na daljinu ili leteti nezavisno uz pomoć planova leta koje kontroliše softver unet u njegov sistem, a koji radi zajedno sa senzorima i GPS-om na letelici. Dronovi se još nazivaju i „bespilotni vazduhoplovi“ ili „bespilotni vazduhoplovni sistemi“ (engl. UAV i UAS). Dronovi se danas koriste za širok spektar civilnih uloga, od potrage i spasavanja, preko nadzora, praćenja saobraćaja, vremenskih prilika i požara, do lične i poslovne fotografije uz pomoć dronova, kao i profesionalnog snimanja, poljoprivrede, pa čak i usluga dostave.⁸⁴

G

GPS i GPS praćenje

GPS (skr. globalni pozicioni sistem) predstavlja konstelaciju dvadeset četiri dobro postavljena satelita koji orbitiraju oko Zemlje i omogućavaju da se utvrdi geografska lokacija ljudi sa zemljišnim prijemnicima, odnosno GPS uređajima za praćenje. GPS može da utvrdi geografsku dužinu i širinu tla i brzinu i pravac kretanja meta, a tačnost lokacije je između deset i stotinu metara kod većine opreme. GPS oprema je sada integrisana u pametne telefone, tablete i GPS uređaje za navigaciju. GPS tehnologija u mobilnim telefonima, osim u cilju navigacije, često se koristi i za praćenje broja koraka preko specijalizovanih aplikacija za fitnes i zdravlje. GPS praćenje jeste nadzor lokacije pomoću GPS-a, kojim se prati lokacija nekog subjekta ili objekta na daljinu. Zagovarači privatnosti upozoravaju da ova tehnologija takođe može da omogućiti oglašivačima, državi, hakerima i sajber progoniteljima da prate korisnike uz pomoć njihovih mobilnih uređaja.⁸⁵

H

Hakovanje

Hakovanje predstavlja neovlašćen pristup informacijama i programima na elektronskim uređajima i njihovim mrežama – pametnim telefonima, računarima, računarskim sistemima i serverima. Hakovanje može biti zlonamerno i etičko. Zlonamerno hakovanje podrazumeva ilegalan ili nedozvoljen pristup sistemima čiji je cilj napadanje, nanošenje štete ili inkriminisanje druge osobe ili organizacije putem krađe ili menjanja podataka, pribavljanja ličnih informacija, narušavanja privatnosti ili inficiranja uređaja virusom.⁸⁶ U ovom slučaju, hakovanje predstavlja krivično delo, a haker sajber kriminalca. Etičko hakovanje se odnosi na hakova-

nje čiji je cilj otkrivanje bezbednosnih propusta u okviru računarskih sistema kako bi se zaštita sistema unapredila.

I

Informaciono-komunikacione tehnologije

Raznovrstan skup tehnoloških alata i resursa koji se koristi da se šalju, čuvaju, kreiraju, dele ili razmenjuju podaci. Ovi tehnološki alati i resursi uključuju računare, internet (sajtove, blogove i mejlove), tehnologije za direktan prenos (putem radija, televizije i interneta), tehnologije za snimljeni prenos (podkasti, audio i video prenosnici i uređaji za čuvanje podataka) i telefoniju (npr. fiksnu ili mobilnu, satelitsku i opremu za vizio/video konferencije).⁸⁷

M

Mim (engl. meme)

Mim ili mema je vizuelni format koji se sastoji od slike i prateće fraze. Osim formata slike, mim se može naći i u formatu kraćeg videa ili GIF-a, odnosno animacije. Po pravilu, mimovi se odnose na neki fenomen popularne kulture i napravljeni su s idejom da se masovno dele po društvenim mrežama.⁸⁸ Iako je mim najčešće šaljivog karaktera i za cilj ima da nasmeje i oraspoloži ljude, oni mogu biti i podrugljivi, uznemirujući i/ili se koristiti s idejom da se osoba zlostavlja.

O

Onlajn platforma

Onlajn platforma je digitalni servis koji omogućava interakcije između dva ili više različitih ali

međusobno zavisnih skupova korisnika (bilo firmi ili pojedinaca), koji su u interakciji preko servisa putem interneta. Pojam „onlajn platforma“ koristi se da opiše niz usluga dostupnih na internetu, uključujući onlajn prodavnice, pretraživače, društvene mreže, servise s kreativnim sadržajem, prodavnice aplikacija, servise za komunikaciju, sisteme za plaćanje, servise koji čine takozvanu „kolaborativnu“ odnosno „gig“ ekonomiju (frilensovanje), i mnoge druge.⁸⁹

T

Tehnološke kompanije⁹⁰

Tehnološke kompanije obuhvataju širok raspon organizacija, uključujući, između ostalog, sledeće:

- određene pružaoce internet usluga: subjekte koji omogućavaju krajnjim korisnicima da pristupe onlajn materijalima i pružaoce internet usluga, kao što su subjekti koji pružaju usluge pretraživanja interneta, uključujući, između ostalog, *Google*, *Safari* i *Firefox*;
- pružaoce usluga društvenih mreža: subjekte koji pružaju usluge koje povezuju dvoje krajnjih korisnika onlajn, uključujući, između ostalog, *Facebook*, *LinkedIn* i *Instagram*;
- pružaoce elektronskih usluga: subjekte koji omogućavaju krajnjim korisnicima da komuniciraju jedni s drugima (npr. *Outlook* i gejming čet službe, poput *Discord*-a);
- pružaoce usluga distribucije aplikacija: subjekte koji obezbeđuju pristup servisima aplikacija, uključujući, između ostalog, *Google* (putem *Google PlayStore*-a) i *Apple* (putem *iOS App Store*-a);
- pružaoce usluga hostinga: subjekte koji omogućavaju hosting sačuvanih materijala koji se obezbeđuje na servisima društvenih mreža, relevantnim elektronskim servisima ili određenim internet servisima, koji uključuju, između ostalog, *Apple* i *Microsoft*, svaki putem pružanja svojih usluga na kladu;
- kompanije za razvoj hardvera: subjekte koji kreiraju, razvijaju i/ili održavaju tehnološku opremu, fizičku imovinu i druge materijalne predmete;
- kompanije za razvoj softvera: subjekte koji kreiraju, osmišljavaju, razvijaju i održavaju

programme, aplikacije, okvire i druge softverske komponente.

Š

Špijunski softver (engl. *spyware*)

Špijunski softver je vrsta zloćudnog softvera koji se instalira na računar bez znanja krajnjeg korisnika. On okupira uređaj, krade osetljive informacije i podatke o korišćenju interneta i prenosi ga oglašivačima, kompanijama za podatke ili spoljnim korisnicima. Kada se instalira, prati aktivnost na internetu, prati podatke za logovanje i špijunira osetljive informacije.

Špijunski softver se takođe može koristiti da prati lokaciju neke osobe, kao što je slučaj sa softverom za proganjanje (engl. *stalkerware*). Ovaj softver često instaliraju u tajnosti na mobilnim telefonima supružnici, partneri, bivši partneri, pa čak i roditelji i članovi porodice. Ova vrsta špijunskog softvera može da prati fizičku lokaciju osobe, presretne njene imejlove i poruke, prisluškuje telefonske pozive i snima razgovore, a takođe i da pristupa ličnim podacima, kao što su fotografije i video snimci.⁹¹

V

Veštačka inteligencija

Razvoj veštačke inteligencije je oblast koja kombinuje računarsku nauku i velike količine podataka da bi se omogućilo rešavanje problema. Ona takođe obuhvata podoblasti mašinskog učenja i dubokog učenja. Razvoj i upotreba veštačke inteligencije nastoji da napravi ekspertske sisteme, koji sa svoje strane prave predviđanja ili klasifikacije na osnovu unesenih podataka, te uz pomoć računara i mašina oponaša sposobnosti rešavanja problema i odlučivanja koje poseduje ljudski um.⁹²



- 1 UN Women. Accelerating Efforts to Tackle Online and Technology Facilitated Violence Against Women and Girls (VAWG). Dostupno na: https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf
- 2 Laxton, C. 2014. Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking. Bristol, UK: Women's Aid Federation of England.
- 3 European Commission. Proposal for a directive of the European parliament and of the Council on combating violence against women and domestic violence. Strasbourg, 8.3.2022 COM(2022) 105 final 2022/0066 (COD). Dostupno na: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0105&from=EN>
- 4 United Nations Human Rights Council. Report by Special Rapporteur Dubravka Šimonović (18 June 2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. UN Doc A/HRC/38/47.
- 5 EIGE. 2017. Cyber violence against women and girls. Dostupno na: <https://eige.europa.eu/publications/cyberviolence-against-women-and-girls>
- 6 Cyberbullying Research Centre. What is cyberbullying? Dostupno na: <https://cyberbullying.org/what-is-cyberbullying>
- 7 Van Der Wilk, A. and M. Natter. 2018. Cyber violence and hate speech online against women. Study for the FEEM Committee.
- 8 Pen America, Online harassment field manual. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 9 Radoičić, A. 2020. Iza ekrana: analiza zlopotreba žrtava trgovine ljudima u digitalnom okruženju. Dostupno na: <http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zlopotreba%20%C5%B8rtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%B8nju.pdf>
- 10 VAW Learning Network. 2013. Technology-related Violence Against Women. Dostupno na: <http://www.vawlearningnetwork.ca/our-work/issuebased-newsletters/issue-4/index.html>
- 11 N. Henry and A. Powell, "Technology-facilitated sexual violence: a literature review of empirical research". *Trauma, Violence & Abuse*, vol. 19, No. 2, (2018), pp. 195–208. <https://doi.org/10.1177/1524838016650189>
- 12 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg-38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 13 GBV AoR Helpdesk. 2021. Learning Series on Technology-Facilitated Gender-Based Violence. Learning Brief 1: Understanding technology-facilitated GBV.
- 14 Pen America, Online harassment field manual. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 15 Pen America, Online harassment field manual. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 16 Posetti, J. et al. 2020. Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts. UNESCO. Dostupno na: <https://www.icfj.org/our-work/icfj-unesco-global-study-online-violence-against-women-journalists>
- 17 United Nations. 2019. United Nations Strategy and Plan of Action on Hate Speech. Dostupno na: <https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml>
- 18 Ibid.
- 19 Gordon, S., 2020. Slut-Shaming: The Scarlett Letter Of The 21st Century.
- 20 Mantilla, K., 2013. "Gendertrolling: Misogyny adapts to new media". *Feminist studies*, 39(2), pp.563-570.
- 21 Women's Media Centre. WMC Speech Project: Online Abuse 101. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 22 eSafety Commission Australia. Online abuse targeting women. Dostupno na: <https://www.esafety.gov.au/women/online-abuse-targeting-women>
- 23 Women's Media Centre. WMC Speech Project: Online Abuse 101. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 24 Kumar, R. 2022. DCW chief Swati Maliwal gets rape threats after she seeks 'MeToo' accused Sajid Khan's ouster from Bigg Boss. *India TV News*. Dostupno na: <https://www.indiatvnews.com/news/india/dcw-chief-swati-maliwal-gets-rape-threats-after-she-seeks-me-too-accused-sajid-khan-s-ouster-from-bigg-boss-16-filmmaker-2022-10-12-815679>
- 25 Douglas, D. "Doxing: a conceptual analysis", *Ethics Information Technology*, vol. 18,(2016), pp. 199–210.
- 26 Dunn, S. "Technology-facilitated gender-based violence: An overview." Centre for International Governance Innovation: Supporting a Safer Internet Paper 1 (2020).
- 27 Lagan, B. 2021. Australian law will force social media firms to unmask trolls. *The Times*. Dostupno na: <https://www.thetimes.co.uk/article/new-australian-law-will-force-social-media-firms-to-unmask-trolls-tqchmf6k9>
- 28 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 29 McGlynn, C. E. Rackley and R. Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse", *Feminist Legal Studies*, vol. 15, (2017), pp. 1–22.
- 30 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders. (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 31 Dictionary.com. Creepshot. Dostupno na: <https://www.dictionary.com/e/slang/creepshot/#:~:text=Creepshot%20typically%20refers%20to%20a,backside%2C%20legs%2C%20or%20cleavage.>
- 32 Ryall, J. 2021. Japan records surge in upskirt photography, perverts 'bored' amid pandemic to blame, experts say. *South China Morning Post*. Dostupno na: <https://www.scmp.com/week-asia/lifestyle-culture/article/3150610/coronavirus-boredom-moves-japanese-perverts-upskirt>
- 33 Cvetinčanin Knežević, Hristina. „Digitalno okruženje i rodno zasnovano nasilje – prilog proučavanju." *Antropologija* (2020).

- 30 Cvetinčanin Knežević, Hristina. 2021. „Someone's Daughter': Unpunished Revenge Porn's Terrifying Toll in The Balkans." *Balkan Insight*. Dostupno na: <https://balkaninsight.com/2021/10/18/someones-daughter-unpunished-revenge-porns-terrifying-toll-in-the-balkans/>
- 31 Dunn, S. "Technology-facilitated gender-based violence: An overview." Centre for International Governance Innovation: Supporting a Safer Internet Paper 1 (2020).
- 32 Selbie, T. and C. Williams. 2021. Deepfake pornography could become an 'epidemic', expert warns. *BBC*. Dostupno na: <https://www.bbc.com/news/uk-scotland-57254636>
- 33 APC. 2020. *How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it*. Dostupno na <https://www.apc.org/en/pubs/research/how-technology-being-used-perpetrate-violence-agai>
- 34 Rice, E., Gibbs, J., Winetrobe, H., Rhoades, H., Plant, A., Montoya, J., et al. 2014. Sexting and sexual behavior among middle school students. *Pediatrics* 134, e21–e28.
- 35 Van Oosten, J. M. F., Peter, J., and Vandenbosch, L. 2017. Adolescents' sexual media use and willingness to engage in casual sex: differential relations and underlying processes. *Hum. Commun. Res.* 43, 127–147.
- 36 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 37 Women's Media Centre. WMC Speech Project: Online Abuse 101. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 38 Huet, N. 2022. Cyberflashing: People who send unwanted 'dick pics' will face jail under UK's new online safety law. *EuroNews*. Dostupno na: <https://www.euronews.com/next/2022/03/14/cyberflashing-people-who-send-unwanted-dick-pics-will-face-jail-under-uk-s-new-online-safe>
- 39 Ringrose, J. 2020. 'Staying Safe Online' survey: what unwanted sexual images are being sent to teenagers on social media?. *London's Global University*. Dostupno na: <https://blogs.ucl.ac.uk/ioe/2020/06/19/staying-safe-online-survey-what-unwanted-sexual-images-are-being-sent-to-teenagers-on-social-media/>
- 40 National Society for the Prevention of Cruelty to Children. 2022. *Online grooming crimes have risen by more than 80% in four years*. Dostupno na: <https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/>
- 41 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 42 Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Dostupno na: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP4-Flynn_et_al-TFa_Stakeholder_Survey.pdf
- 43 APC. 2020. *How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it*. Dostupno na <https://www.apc.org/en/pubs/research/how-technology-being-used-perpetrate-violence-agai>
- 44 Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective, 2018.
- 45 Brittany, A. "On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking", *Polaris*, 2018.
- 46 Radoičić, A. 2020. Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju. Dostupno na: <http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf>
- 47 Radoičić, A. 2020. Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju. Dostupno na: <http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf>
- 48 Douglas, D., "Doxing: a conceptual analysis", *Ethics Information Technology*, vol. 18, (2016), pp. 199–210.
- 49 Women's Media Centre. WMC Speech Project: Online Abuse 101. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 50 Redakcija. ND. Sapštenje redakcije «Vremena» povodom pretnji Jovani Gligorijević. *Vreme*. Dostupno na: <https://www.vreme.com/projekat/sapstenje-redakcije-vremena-povodom-pretnji-jovani-gligorijevic/>
- 51 Van der Wilk, A. 2018. *Cyber violence and hate speech online against women*. Study for the FEEM Committee.
- 52 eSafety Commission Australia. *Catfishing*. Dostupno na: <https://www.esafety.gov.au/young-people/catfishing>
- 53 Radoičić, A. 2020. Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju. Dostupno na: <http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf>
- 54 Wikipedia. Simon Leviev. Dostupno na: https://en.wikipedia.org/wiki/Simon_Leviev
- 55 Levy, K and B. Schneier, "Privacy threats in intimate relationships", *Journal of Cybersecurity* (Oxford), vol. 6, No. 1, (2020), <https://doi.org/10.1093/cybsec/tyaa006>
- 56 Havard, T.E. and M. Lefevre. "Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control." *Journal of gender-based violence* 4, no. 2 (2020): 223–239.
- 57 Women's Media Centre. WMC Speech Project: Online Abuse 101. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 58 PenzeyMoog, E. and D. C. Slakoff. "As technology evolves, so does domestic violence: Modern-Day tech abuse and possible solutions." In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, pp. 643–662. Emerald Publishing Limited, 2021.

- 59 Radoičić, A. 2020. Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju. Dostupno na: <http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf>
- 60 Ibid.
- 61 Henry, N. and A. Powell, "Technology-facilitated sexual violence: a literature review of empirical research". *Trauma, Violence & Abuse*, vol. 19, No. 2, (2018), pp. 195–208. <https://doi.org/10.1177/1524838016650189>
VAW Learning Network. 2013. *Technology-related Violence Against Women*. Dostupno na: <http://www.vawlearningnetwork.ca/our-work/issuebased-newsletters/issue-4/index.html>
- 62 Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 63 Posetti, J., J. Harrison and S. Waisbord. 2020 Online Attacks on Women Journalists Leading to 'Real World' Violence, New Research Shows. *International Center for Journalists*. Dostupno na: <https://www.icfj.org/news/online-attacks-women-journalists-leading-real-world-violence-new-research-shows>
- 64 Pen America, *Online harassment field manual*. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 65 Lončar, S. 2021. Kako internetski napadaju novinarke. *Nezavisno udruženje novinara Srbije*. Dostupno na: <https://nuns.rs/kako-internetski-nasilnici-napadaju-novinarke/>
- 66 Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 67 Dunn, S. "Technology-facilitated gender-based violence: An overview." *Centre for International Governance Innovation: Supporting a Safer Internet Paper 1* (2020).
- 68 CBS News. 2011. New "Google Bomb" links murder to abortion. *CBS News*. Dostupno na: <https://www.cbsnews.com/news/new-google-bomb-links-murder-to-abortion/>
- 69 Pen America, *Online harassment field manual*. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 70 Yang, W. 2021. China feminists face clampdown, closure of online accounts. *Deutsche Welle*. Dostupno na: <https://www.dw.com/en/china-feminism-free-speech/a-57277438>
- 71 Ibid.
- 72 Amnesty International. 2020. Pakistan: Accusations of blasphemy continue to endanger lives. *Amnesty International*. Dostupno na: <https://www.amnesty.org/en/latest/news/2020/08/accusations-of-blasphemy-in-pakistan-continue-to-endanger-lives/>
- 73 Phillips, W. "LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online." *First Monday* (2011).
- 74 Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 75 Phillips, W. "LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online." *First Monday* (2011).
- 76 Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Dostupno na: <https://womensmediacenter.com/speech-project/online-abuse-101>
- 77 Pen America, *Online harassment field manual*. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
- 78 APC WRP. 2015. Take Action for #TakeBackTheTech and #ImagineAFeministInternet. *APC*. Dostupno na: <https://www.apc.org/en/pubs/take-action-takebackthetech-and-imagineafeministin>
- 79 The Conversation 2020. What is an algorithm? How computers know what to do with data. Dostupno na: <https://theconversation.com/what-is-an-algorithm-how-computers-know-what-to-do-with-data-146665>
- 80 Techopedia. 2012. App. Dostupno na: <https://www.techopedia.com/definition/28104/app>
- 81 BMC blogs. 2020. Digital Platforms: A Brief Introduction. Dostupno na: <https://www.bmc.com/blogs/digital-platforms/#>
- 82 GBV AoR Helpdesk. 2021. *Learning Series on Technology-Facilitated Gender-Based Violence*. Learning Brief 1: Understanding technology-facilitated GBV.
- 83 GBV AoR Helpdesk. 2021. *Learning Series on Technology-Facilitated Gender-Based Violence*. Learning Brief 3: Implications of technology-facilitated GBV and actions for humanitarian agencies, donors and online industries.
- 84 Drone (UAV). 2019. IoT Agenda. Dostupno na: <https://internetofthingsagenda.techtarget.com/definition/drone>
- 85 WhatIs.com. 2014. GPS tracking. Dostupno na: <https://whatis.techtarget.com/definition/GPS-tracking>
- 86 Pen America, *Online harassment field manual*. Dostupno na: <https://onlineharassmentfieldmanual.pen.org/>
VAW Learning Network. 2013. *Technology-related Violence Against Women*. Dostupno na: <http://www.vawlearningnetwork.ca/our-work/issuebased-newsletters/issue-4/index.html>
- 87 UNESCO Institute for Statistics. *Glossary: Information and communication technologies (ICT)*. Dostupno na: <http://uis.unesco.org/en/glossary>
- 88 Internet meme. 2022. Wikipedia. Dostupno na: https://en.wikipedia.org/wiki/Internet_meme
- 89 OECD. 2019. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Dostupno na: https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en
- 90 Online Safety Act 2021 (Cth). No. 76, 2021. (Austl.)
- 91 TechTarget. 2021. Spyware. Dostupno na: <https://searchsecurity.techtarget.com/definition/spyware>
- 92 IBM. 2020. Artificial Intelligence (AI). Dostupno na: <https://www.ibm.com/cloud/learn/what-is-artificial-intelligence>

// tvoje telo je tvoje
i na netu i u stvarnom svetu

b

