ПОИМНИК НА РОДОВО БАЗИРАНОТО НАСИЛСТВО ИЗВРШЕНО СО (ЗЛО)УПОТРЕБА НА ТЕХНОЛОГИЈАТА

20

Електронски потпомогната трговија со луѓе и врбување

Загрозување на приватноста и на безбедноста со (зло)употреба на технологија

21

Доксинг (злокументирање), мртвоименување (деднејминг) и аутирање без согласност

Лажно претставување и кетфишинг

22

Ограничување или контролирање со помош на технологија

Електронски потпомогната финансиска злоупотреба

Сајбердемнење и опсесивно следење на интернет

23

Напади „во вистинскиот живот“

Онлајн закани

24

Бомбардирање на Гугл и на Зум

Напад со оневозможување пристап и напад со одбивање услуга

25

Други облици на насилство во дигиталната средина

Астротурфирање

Лажни обвинувања за богохулење

Постхумно тролање и тролање врз основа на шок и тага

26

Свотинг

Труење хаштаг

27

Концепти од доменот на технологијата

// ТВОЕТО ТЕЛО Е ТВОЕ, И НА ИНТЕРНЕТ, И ВО ВИСТИНСКИОТ СВЕТ.

// ЗА ШТО Е НАМЕНЕТ И КАКО ДА СЕ КОРИСТИ ОВОЈ ПОИМНИК?

Родово базираното насилство изршено со (зло)употреба на технологијата (РБНИУТ, англ. Technology facilitated gender-based violence – TFGBV) е релативно нова појава, нешто што би било речиси незамисливо пред триесетина години. Со сè поголемата застапеност на информациските и комуникациските технологии во нашиот секојдневен живот, до степен до којшто сега е тешко да се замисли еден најобичен ден без интернет, лаптоп, паметен телефон или без социјалните мрежи, родовото насилство извршено во дигиталниот простор станува сè позачестено.

Податоците покажуваат дека многу жени ширум светот доживеале некаква форма на родово базирано насилство извршено со злоупотреба на технологијата, додека девојчињата, девојките и младите жени се особено подложни – 58 % од нив доживеале некаква форма на родово базирано насилство во дигиталното опкружување, а во повеќето случаи тоа им се случило на возраст меѓу четиринаесет и шеснаесет години, при што речиси половина од нив (47 %) наишле на закани со физичко и сексуално насилство[1]. Истражувањата исто така покажуваат дека 45 % од жените кои доживеале насилство од интимен партнер биле исто така злоставувани и со посредство на технологија, при што кај 48 % од нив родовото насилство со (зло)употреба на технологијата продолжило и по завршувањето на врската[2].

Поради горенаведените фактори, во април 2022 година, Европската Унија започна да работи врз создавање правна рамка за регулирање на родово базираното насилство, на таков начин што тоа би го опфатило и насилството што се извршува со (зло)употреба на технологијата[3].

Сепак, иако родовото насилство извршено со (зло)употреба на технологијата е сè почеста појава и се препознава како закана во меѓународните правни акти, сè уште не е постигната согласност во однос на неговото дефинирање, како ниту во однос на дефинирањето на начините на кои се манифестира тоа. Затоа термините „вознемирување“ и „злоупотреба“, како и термините „кибер/сајбер“, „дигитално“, „онлајн“ и „со (зло)употреба на технологија“ честопати се користат како синоними кога станува збор за овој облик на насилство. Понатаму, бројот на појавните облици на овој вид насилство сè уште не е конечен – со напредокот на технологијата, се отвораат нови можности за нејзина злоупотреба со цел вршење родово базирано насилство.

Во поимникот пред нас дадени се две чадор-дефиниции за родово базирано насилство извршено со (зло)употреба на технологијата, кои во праксата се покажале како најрелевантни и сеопфатни, додека различните форми на овој вид насилство се издвоени врз основа на нивната застапеност на Западен Балкан. Облиците во кои се појавува насилството се поделени во четири големи групи, со цел читателките и читателите да можат полесно да се снајдат. Оваа поделба не е ниту конечна, ниту пак непроменлива, бидејќи различните облици на насилство извршено со (зло)употреба технологијата често се испреплетуваат и си претходат едни на други. Секој облик е опишан, дефиниран и илустриран со пример од реалниот живот, со цел да се препознае, но и да се укаже на опасноста што родово базираното насилство извршено со (зло)употреба на технологијата ја претставува по животите на девојчињата, на девојките и на жените, како и по родово флуидните и небинарните лица.
Првата група ја сочинуваат дигиталното или **сајбер/кибернасилството** и **родово базираното онлајн вознемирување,** кое опфаќа различни форми и видови

вознемирување и злоупотреба во дигиталниот простор, а најчесто се извршува со употреба на текст. Станува збор за вмрежено вознемирување преку интернет и вознемирување на различните платформи, родово базиран и сексистички говор на омраза (меѓу другото и онлајн курвоклетство, тролање, родово базирано тролање, потпалување и тролање со цел заплашување), одмазда кон поддржувачите на лицата што преживеале насилство и клевета во онлајн просторот.

Втората група се состои од **сексуално насилство во дигиталната средина**, со посебен акцент врз несаканите сексуални искуства со (зло)употреба на технологијата. Оваа група се разликува од претходната поради исклучително нагласената родова компонента и растечката преваленца. Во рамките на таа група се издвојуваат: злоупотреба со визуелна содржина (која се состои од снимање под фустан и перверзно фотографирање; порнографија без согласност и сексуална изнуда; синтетички сексуални медиуми, дипфејкови и лажна (дипфејк) порнографија; секстинг и злоупотреба преку секстинг; сајберегзибиционизам, изложување на порнографија без согласност и куроslики, снимање и/или емитување сексуални напади и силувања, онлајн кротење (груминг), несакани сексуални искуства во живо и електронски потпомогната трговија со луѓе и врбување.

Третата група се состои од форми на насилство чија намена е да се **загрози безбедноста и приватноста со посредство на технологија**. Се состои од доксирање, мртвоименување (деднејмување) и аутирање без согласност, лажно претставување и кетфишинг (измамништво), ограничување или контрола со (зло)употреба на технологија, електронска финансиска злоупотреба, сајбердемнење и опсесивно следење на интернет, напади во „вистинскиот живот", онлајн закани, бомбардирање на Гугл (Google) и Зум (Zoom), како и напад преку оневозможување пристап и напад преку оневозможување услуга.

Четвртата група се состои од **останатите облици на насилство во дигиталното опкружување** – оние кои не се опфатени со претходните целини, а кои може да имаат родова димензија, иако таа не игра иста улога како во претходните три групи. Друга заедничка карактеристика на овие облици на насилство е фактот што нивната зачестеност на Западен Балкан е помала во споредба со онаа на претходните групи, што не значи дека тоа нема да се промени во иднина. Тука спаѓаат астротурфирањето, лажните обвинувања за богохулење, постхумното тролање и тролање врз основа на шок и жалење, свотингот и труењето/киднапирање хаштагови.

На крајот од поимникот даден е и краток речник на термини од областа на технологијата, во којшто се објаснети четиринаесет термини од **областа на технологијата** со цел да се олесни разбирањето на горенаведените облици на насилство.

Овој Поимник е изработен врз основа на публикацијата „Родово базирано насилство со посредство на технологија - секој простор да биде безбеден", објавен од Фондот за население на Обединетите нации - УНФПА во декември 2021 година, како обид се дефинираат сите концепти во согласност со локалниот контекст и поткрепени со примери кои ни се познати и блиски. Поимникот се изработи по пат на широк консултативен процес со експерти, млади и пошироката јавност, кои дадоа многу важни предлози и коментари коишто се обидовме да ги вклучиме во документот. Сепак, свесни сме дека ова е жив документ што ќе продолжи да се развива и доработува, и со нетрпение ги очекуваме сите дополнителни коментари и предлози што ќе ни бидат упатени. Во име на УНФПА, би сакале да им се заблагодариме на сите кои учествуваа во изработката и прилагодувањето на Поимникот преку учество во фокус групите или со испраќање предлози и сугестии. Посебна благодарност им должиме на Ана Василева, Ана Мартиноска и Сара Миленковска кои го водеа процесот на консултации и го приредија овој Поимник на македонски јазик.

// ПРЕДГОВОР КОН МАКЕДОНСКОТО ИЗДАНИЕ НА ПОИМНИКОТ

Од многуте нови видици, предности, но и опасности кои сме свесни дека ни ги отвори појавата и огромниот подем на мрежното поврзување, или интернетот, еден факт е сосема извесен – ниту постарите генерации како дигитални мигранти (лица родени пред експанзијата на интернетот, со аналогно детство, но дигитална младост и полнолетство), ниту дигиталните домородци (лицата родени во дигиталната ера) сè уште не се свесни за сите промени и предизвици што ги носи интернетот како депо на колективни информации и средство за меѓусебно поврзување, ниту, пак, за најдобрите начини за негова (само)регулација. Секако, едно е јасно – колку сме поинформирани за разновидните начини на коишто интернетот може да биде (зло)употребен како алатка за насилство, толку полесно ќе биде тоа да се спречи, соодветно да се реагира и да се санира.

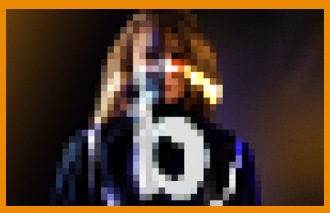
Првиот чекор во овој процес е соодветно именување на сите поими врзани за родово базираното насилство со злоупотреба на технологијата. Кога можеме да ги именуваме нештата, полесно ќе ги дефинираме и полесно ќе ги препознаваме. Токму затоа и се впуштивме во овој преведувачки и приспособувачки потфат, како обид да ги разјасниме, да ги приближиме и да ги локализираме главните поими поврзани со родово базираното насилство извршено со (зло)употреба на технологијата, да направиме мост помеѓу претставниците на помладите и на постарите генерации за полесно заемно разбирање, но и за да ја олесниме идентификацијата и преземањето соодветно дејство кон ваквите видови насилство, а секако и нивното воведување во кривичниот законик, во оние случаи во кои е применливо.

Во поимникот се дадени и, условно кажано, „похрабри“ преводни решенија за дел од поимите, затоа што сметавме дека се илустративни и дека на лицата кои не се толку активни корисници на социјалните мрежи ќе можат лесно да им ги доловат концептите за коишто станува збор.

Искрено се надеваме дека барем дел од поимите ќе фатат корен и дека овој Поимник ќе поттикне широка и континуирана дебата затоа што свеста за постоењето за негативните појави во дигиталниот свет и информираноста за тоа како може најделотворно да им се спротивставиме ќе бидат неопходни за заштита на сегашните деца и млади, како и на идните генерации. Генерацијата родители и образовен кадар (како и сите останати лица што работат со деца/млади) коишто по игра на случајот се наоѓаат на фронтот на овој предизвик мора да имаат солидни познавања за да може целисходно и безбедно да ги насочуваат своите штитеници и да им овозможат делотворни алатки и механизми за заштита и за соодветно постапување.

// ЧАДОР–ДЕФИНИЦИИ НА РОДОВО–БАЗИРАНОТО НАСИЛСТВО ИЗВРШЕНО СО ПОСРЕДСТВО НА ТЕХНОЛОГИЈА

Обединети нации[4]	**Онлајн насилство врз жените и девојчињата со посредство на информациска и комуникациска технологија**	Дефиницијата за онлајн насилство врз жените се однесува на секој чин на насилство врз жените што е извршен, олеснет или чии последици се влошени со делумна или со целосна употреба на информатичката и комуникациската технологија (како што се мобилните и паметните телефони, интернетот, платформите за социјално вмрежување или е-поштата), којшто е насочен против жените само затоа што се жени или којшто несразмерно ги погодува жените.
Европски институт за родова еднаквост[5]	**Дигитално (кибер/ сајбер) насилство врз жените и девојчињата**	Родово базирано насилство извршено со зло(употреба) на електронска комуникација и на интернет. Иако кибернасилството може да е насочено и против жените и против мажите, жените и девојчињата доживуваат поинакви и потрауматични форми на сајбермалтретирање. Постојат различни форми на дигитално насилство врз жените и девојчињата, вклучувајќи ги, меѓу другото, и сајбердемнењето, порнографијата без согласност (односно „одмаздничка порнографија“ – англ. revenge porn), родово базирани навреди (англ. slurs)[6], говор на омраза и вознемирување, курвоклетство (англ. slut-shaming), несакана порнографија, сексуална изнуда (сексторција), закани со силување и смрт, како и електронски потпомогната трговија со луѓе. Дигиталното (сајбер) насилство не е феномен издвоен од „вистинското“ насилство, бидејќи често ги следи истите обрасци како и насилството офлајн.



// ФОРМИ НА РОДОВО БАЗИРАНО НАСИЛСТВО ИЗВРШЕНИ СО (ЗЛО) УПОТРЕБА НА ТЕХНОЛОГИЈА

ДИГИТАЛНО (ИЛИ САЈБЕР/КИБЕР) НАСИЛСТВО И РОДОВО БАЗИРАНО ВОЗНЕМИРУВАЊЕ

Дигиталното (или сајбер/кибер) насилство (англ. сајбермалтретирање/cyberbullying) е чадор-термин што ги опфаќа различните форми на насилство на интернет, односно насилството што се врши со посредство на технологијата. Се дефинира како „свесно нанесување и повторување штета со помош на компјутери, мобилни телефони или други електронски уреди“[7], најчесто преку употреба на текстуална или графичка содржина, со цел да се заплаши некое лице, негативно да се влијае врз неговата самодоверба или да му се наруши угледот[8]. Иако овој термин најчесто се однесува на врсничкото насилство на интернет, во кое поединци или група врсници се здружуваат со цел да омаловажат друго лице или да им нанесат штета на неговиот оглед, личност и достоинство, цел на сајбернасилството може да бидат и полнолетни лица[9]. [10]Сторителите може да бидат познајници, но и непознати лица.

Кога дигиталното насилство, најчесто извршено во текстуални форми, е насочено кон некое лице поради неговиот пол, род, сексуалност или сексуална ориентација, го користиме терминот **родово базирано онлајн вознемирување** (англ. online gender harassment). Родово базираното онлајн вознемирување може да има различни облици – лицето може да мета на постојано контактирање без негова согласност, може да му се закануваат, може да го заплашуваат со испраќање несакани, непријатни, понижувачки или навредливи слики или коментари (родово базиран и сексистички говор на омраза), или да шират клевети за него. Извршителите на родово базираното онлајн вознемирување се обично поединечни мажи или групи мажи (**вмрежено** вознемирување), и тоа може да се врши како на повеќе платформи истовремено, така и на една платформа[11]. Под родово базирано онлајн вознемирување мислиме на вмрежено **вознемирување и вознемирување преку различни платформи, родово базиран и сексистички говор на омраза што го опфаќа и онлајн курвоклетството и тролањето, родово базираното тролање, вклучувајќи го и потпалувањето и тролањето со цел заплашување, одмазда на поддржувачи на лице што преживеало насилство и клевета во онлајн просторот.** Членот 190-а од Кривичниотзакониксокојсекриминализира сексуалното вознемирување неодамна беше дополнет со вознемирување преку „електронски средства за комуникација“ и наскоро ќе стапи во сила.

(b) Вмрежено вознемирување и вознемирување на различни платформи

Вмреженото вознемирување, често наречено и сајбер мобинг (англ. cyber mobbing), се состои од организирани, координирани и систематски напади од група луѓе врз одредени поединци, односно поединки или идеи, како што се групите кои ги напаѓаат феминистките или лицата што се борат против расизмот[12]. Групното вознемирување се води според психологијата на толпата, која е фокусирана врз јавно разоткривање, понижување и казнување на лицето кое е цел на нападот. Во повеќето случаи, лицето е на нишан само затоа што споделува некакво мислење за политички теми или идеи со кои не се согласува групата на напаѓачот[13] Вмреженото вознемирување може да се врши на една платформа, но може да се случи и на неколку платформи

истовремено – во таков случај зборуваме за **вознемирување на различни платформи**/ трансверзално вознемирување (англ. cross-platform harassment), при што вознемирувачите ја искористуваат предноста на тоа што повеќето платформи ја модерираат само содржината на својата веб-страница[14].

Често на нишан на онлајн вознемирувањето на една или повеќе платформи се новинарките. Истражувањето спроведено од УНЕСКО покажа дека 40 % од новинарките биле цел на вмрежено родово базирано вознемирување на интернет. На овој начин се вршат кампањи против нив. Една од десет новинарки отсуствувала од работа по родово базирано онлајн вознемирување, секоја трета била принудена да биде помалку видлива во јавноста (користеле псевдоними или нивните емисии биле отстранети од програмата), 4 % дале отказ, додека 2 % целосно се откажале од новинарската кариера[15].

Во локален контекст, дури 81,6 % од 103 анкетирани новинарки во земјава се соочиле со онлајн вознемирување, откриваат резултатите од анкетата спроведена од Платформата за истражувачко новинарство и анализи, ПИНА. Според новинарките, мотивот за вознемирувањето најчесто бил поради објава на новинарски текстови насочени кон други центри на моќ (56.6 %), во 43.4 % од случаите поради објава на сопствени новинарски текстови за општествени случувања кои биле критички кон властите, во 36.1 % поради објавени новинарски текстови за општествени случувања кои биле критички насочени кон некоја партија[16].

b Родово базиран и сексистички говор на омраза

Родово базираниот и сексистички говор на омраза (англ. gendered or sexist hate speech) опфаќа секаков вид комуникација, преку говор, текст или невербално однесување, што напаѓа, понижува, навредува и дискриминира некое лице врз основа на пол, род, сексуална ориентација или родов идентитет. Родово базираниот и сексистичкиот говор на омраза на интернет го поткрепува системскиот сексизам[17], а во исто време ги дехуманизира жените, девојчињата и ЛГБТКИ+ лицата и поттикнува насилство врз нив[18]. Родово базираниот и сексистичкиот говор на омраза, меѓу другото, се состојат и од **курвоклетство** и **тролање**, особено **родово базирано тролање**, вклучително и **потпалување** и **тролање со цел заплашување.**

b Курвоклетство или сексуално срамење на интернет

Курвоклетството или сексуалното посрамување на интернет (англ. slut-shaming online), честопати нарекувано и слатшејминг, е форма на родово базирано насилство често насочено кон тинејџерки и ЛГБТКИ+ лица, кои се дискриминирани и понижени бидејќи не ги исполнуваат социјалните и родовите норми во однос на сексуалното однесување, изглед и сексуалност. Онлајн сексуалното срамење често се преклопува и со сајбердемнење, споделување порнографија без согласност и вмрежено вознемирување, што го интензивира негативното влијание врз лицата кои се цел на ова однесување[19].

Курвоклетството на интернет најчесто се манифестира преку навреди, без разлика дали станува збор за коментари или фотографии, мемиња/мимови, видеоснимки и анимации, со цел да се понижи личноста врз основа на

пол, сексуалност и сексуално однесување. Покрај лицата кои се перципираат како девијантни или промискуитетни бидејќи нивното однесување, изглед или облекување не е во согласност со патријархалните норми, цел на сексуалното срамење во дигиталната средина се и лицата кои преживеале сексуално насилство, што е втемелено во погрешното убедување дека тие го испровоцирале насилникот со своето однесување[20].

b Тролање, родово базирано тролање, потпалување и тролање заради заплашување

Тролање (англ. trolling) е форма на дигитална злоупотреба чија цел е да ги изнервира останатите лица и/или да обесмисли некоја дискусија на интернет на одредена тема, како и да спречи конструктивна и цивилизирана размена на различни мислења. Тролањето најчесто се врши преку текст, со објавување понижувачки или навредливи коментари. Троловите (лицата кои тролаат) уживаат во тоа, а кога ќе им се се укаже на опасните последици од нивното однесување, тие одрекуваат каква било одговорност, инсистирајќи дека е тоа шега и дека другите „немаат смисла за хумор". **Родово базираното тролање** ги зема девојките, девојчињата и жените како цел на злоупотреба, и тоа само затоа што се жени. Родово базираното тролање подразбира употреба на родово базирани навреди, сексистички и мизогин (женомразечки) јазик во пораките и во коментарите, создавање насилни и навредливи хаштагови што повикуваат на насилство врз жените, но и закани со смрт или силување[21]. Најнасилната форма на родово тролање е **потпалување** (англ. flaming), која се состои од објавување или испраќање навредливи пораки преку интернет со цел некое лице да се вознемири и да се исплаши. Ваквите пораки се објавуваат на форуми и/или на други онлајн групи за размена на информации или се испраќаат преку е-пошта и/или други алатки за онлајн пораки. Посебен облик на тролање е **тролањето заради заплашување,** кога целта е да се предизвика страв кај лицето дека ќе биде нападнато надвор од дигиталниот контекст, бидејќи троловите го уверуваат дека насилникот знае како да го најде[22]. Многу од троловите се анонимни и користат лажни профили, а се случува и да се здружат за да вршат мрежно вознемирување. Без оглед на тоа за каква форма на тролање станува збор, тоа често следи или им претходи на другите форми на насилство во дигиталното опкружување.

Покрај текстуалната форма, родовото тролање може да биде и визуелно, кога се испраќаат или објавуваат фотографии, мемиња, анимации и видеоснимки со цел да се вознемират и да се испровоцираат девојчињата, девојките и жените, како и да се поттикне насилство врз нив[23].

b Одмазда/реперкусии против поддржувачи на лица кои преживеале насилство

Овој облик на насилство се состои од закани и вознемирување на членовите на семејството, на пријателите, на работодавците или на заедницата која дава поддршка на лице што доживеало насилство[24]. Иако **одмаздата поради поддршка на лицата што преживеале насилство** (англ. retaliations against supporters of survivors) потекнува од офлајн светот, во ерата на движењето #MeToo (како и во локалниот пандан #СегаКажувам), кога сè повеќе жени и девојки се чувствуваат оснажени да проговорат онлајн за насилството што го преживеале, а сè повеќе луѓе ги поддржуваат, дигиталниот облик на одмазда против поддржувачите на лицата што преживеале насилство станува сè поприсутен. Во дигиталниот свет, покрај

луѓето од поширокото и поблиското опкружување на жртвите на насилство, на нишан се и непознатите луѓе кои им дале поддршка.

Претседателката на Комисијата за жени во Делхи, Свати Маливал, добила закани за силување на својот профил на Инстаграм откако му пишала на министерот Анураг Такур барајќи да го отстрани режисерот Сајид Кан од реалното шоу „Бигг Бос". Маливал го испратила своето барање до министерот како акт на поддршка за актерките кои го обвиниле Сајид Кан за сексуално насилство и вознемирување, за што јавно проговориле користејќи го хаштагот #MeToo[25].
Во екот на најсилниот бран на движењето #СегаКажувам, голем број од лицата што изразија поддршка за жртвите исто така беа земени на нишан и напаѓани во онлајн просторот.

b Клевета во онлајн просторот

Клеветата во онлајн просторот (англ. online defamation или online libel) се однесува на објавување и ширење изменети или лажни информации преку интернет кои му наштетуваат на угледот на некое лице. Целта на клеветата е понижување, закана, дискредитација, заплашување или казнување на некоја личност, а најчесто е насочена кон јавни личности: на пример, јавни функционери, активисти и новинари[26].

Во текот на 2021 година, австралиската влада објави криминализација на клеветата во онлајн просторот. Ваквиот предлог-закон ќе ги принуди социјалните мрежи, како што се Твитер или Фејсбук, да го откријат идентитетот на анонимните клеветнички профили, овозможувајќи им на жртвите да бараат правда на суд доколку таквите објави не се отстранат[27].
*Новинарката **Мери Јордановска** беше брутално нападната и против неа беше употребен говор на омраза, што доби судска разврска*[28].

СЕКСУАЛНО НАСИЛСТВО ВО ДИГИТАЛНАТА СРЕДИНА

Сексуалното насилство во дигиталната средина опфаќа различни облици на сексуална злоупотреба што се одвива со (зло)употреба на информациските и комуникациските технологии и/или се врши во дигитална средина. Ја опфаќа **злоупотребата со посредство на визуелна содржина**, без разлика дали визуелниот материјал е реален или е добиен со манипулација преку компјутерски програми – во вториот случај станува збор за **дипфејк**. Вознемирувањето со посредство на визуелна содржина се состои од **снимање под фустан и манијачки фотки; порнографија без согласност и сексуална изнуда; синтетички сексуални медиуми, дипфејк и лажна (дипфејк) порнографија; секстинг и злоупотреба преку секстинг; сајберегзибиционизам и куроslики како дел од изложувањето на порнографија без согласност.** Сексуалното насилство од дигиталната средина, за жал, често се прелева и се преклопува со сексуалното насилство во офлајн светот, а кога ќе се случи тоа, зборуваме за кротење (груминг) во онлајн просторот, несакани сексуални искуства во живо овозможени преку технологијата, како и електронски потпомогната трговија со луѓе. Сексуалното насилство во дигиталната средина може да претставува продолжение на сексуалното насилство во офлајн светот – пример е практиката на **снимање и/или емитување сексуални напади и силувања.**

Загрижувачки пораст на родово базираното насилство во сајбер просторот врз жените и девојките покажуваат

најновите истражувања не само во светски рамки, туку и во Северна Македонија. Според истражувањето на Хелсиншкиот комитет (2021) во кое се опфатени 300 испитаници во три града, 78 % биле жртви на сајбернасилство. Во одредени ситуации ваквите случаи завршуваат со самоубиство, поради фактот дека жртвите на ова насилство, каде што без согласност се споделуваат слики, содржини и лични податоци, се чувствуваат немоќни да го спречат[29].

b Злоупотреба со посредство на визуелна содржина

Злоупотреба со посредство на визуелна содржина (англ. Image-based abuse, IBA) е чадор-термин којшто опфаќа различни облици на родово базирано насилство во дигиталниот простор[30]. *Злоупотребата со посредство на визуелна содржина се состои од фотографирање, испраќање или закана со испраќање фотографии или видеоснимки од интимна или сексуална природа со цел некое лице да се вознемири, да се уценува и да биде под закана, да му се уништи угледот и репутацијата или да се претстави како сексуален објект.*

Ова се врши без согласност на лицето што е на фотографиите или видеоснимките. Визуелната содржина што се користи за злоупотреба, исто така, може да биде вештачки креирана, со користење на технологијата за дипфејк. Злоупотребата со посредство на визуелна содржина го опфаќа и испраќањето порнографски и сексуални содржини на некое лице без негова согласност. Последиците од оваа форма на насилство, освен психолошки, можат да бидат и социјални, од типот на губење на работно место или преселба некаде каде што никој не ја познава жртвата. Злоупотребата со посредство на фотографија се состои од **снимање под фустан и манијачки фотки, порнографија без согласност и сексуална изнуда, како и синтетички сексуални медиуми,** како што се **дипфејкот** и **лажната (дипфејк) порнографија.**

b Снимање под фустан и манијачки фотки

Снимањето под фустан (англ. upskirting) и **манијачките фотки** (англ. creepshots) се состојат од снимање на девојчиња и жени на јавни места, без нивна дозвола. Тоа најчесто се случува на јавни места, како што се продавници, јавни тоалети, јавен превоз, соблекувални, училници или улици, но и во приватните станови на девојчињата, жените и девојките. Снимањето под фустан е тајно фотографирање и снимање под здолништето или фустанот[31], додека манијачките фотки се всушност правење сексуално сугестивни фотографии и видеоснимки од некоја жена без таа да забележи[32].

Во 2021 година во Јапонија е забележана „епидемија“ на манијачки фотки, кога во првите шест месеци таа година е забележан пораст на пријавите во полиција за 30 отсто во споредба со истиот период од претходната година. Девојчињата, девојките и жените најчесто се фотографирани во јавниот превоз, а насилниците, освен мобилни телефони, користеле и софистицирана технологија слична на шпионската опрема – камери во пенкала, очила, рачки од чадори и чевли. Од 2019 година, метрото во Токио има посебен вагон за жени, токму поради различните видови на сексуално насилство со кои тие се среќаваат во јавниот превоз, меѓу другото и со оваа негова дигитална форма[33].

b Порнографија без согласност и сексуална изнуда

Порнографија без согласност (англ. non-consensual pornography), која често се нарекува и одмаздничка порнографија (англ. revenge porn), е секое неовластено снимање (со фотоапарат или камера) и/или споделување, како и закани за споделување, на снимки во кои лицето е прикажано разголено или во ситуација со сексуална конотација, сè со цел да се понижи, да се посрамоти или да се уценува[34]. Кога целта е уцена, можеме да зборуваме и за **сексуална изнуда (сексторција)** (анг: sextortion), чија цел е да се изнудат пари од лице или да се принуди да направи нешто што не сака, како на пример сексуален чин, под закана дека разголените фотографии или видеа со сексуална конотација ќе бидат објавени. Во некои земји, како што е Обединетото Кралство, сексуалната изнуда претставува кривично дело. Со напредокот во технологијата и во софтверот за уредување видео и фотографии, порнографијата без согласност сè почесто се состои и од лажна порнографија (дипфејк порнографија), а и двете може да се искористат за сексуална изнуда.

На почетокот од 2021 година, на Балканот беа откриени групи на Телеграм – Јавна соба, Екс Ју Балканска соба и Нишлијке, кои служеа за размена на порнографија без согласност[35]. Овие групи броеја десетици илјади членови, а покрај фотографии и видеа од девојки, беа разменувани и нивните лични податоци (доксинг), како што се имиња и презимиња, телефонски броеви и е-адреси или линкови до профилите на социјалните мрежи[36].
Еден од поновите случаи во Северна Македонија, е оној со полицаец од Велес, кој со компромитирачки фотографии уценувал сограѓанка и изнудил секс, откако претходно сексуално ја вознемирувал[37].

b Синтетички сексуални медиуми, дипфејкови и лажна (дипфејк) порнографија

Синтетичките сексуални медиуми (англ. synthetic sexual media) се користат за манипулација со фотографии и со видео-содржини, со цел да се создаде впечаток дека одредени лица учествувале во сексуална активност во која реално не учествувале. Причините за користење синтетички сексуални медиуми можат да бидат различни – од забава, преку заработка, па сè до уценување и вознемирување на жените и уништување на нивниот имиџ и углед. Синтетичките сексуални медиуми се чадор-поим, додека дипфејковите се нивната најчеста форма[38]. Дипфејковите (англ. deepfakes) се дигитални фото, видео и аудиосодржини кои дополнително се менуваат или се манипулираат со помош на специјализирани програми. Целта на дипфејковите е да се создаде впечаток дека некој рекол нешто што не рекол или дека направил нешто што не направил. Дипфејк може да се користи за политички цели, но почесто се користи во форма на лажна порнографија. **Лажната (дипфејк) порнографија** (англ. deepfake pornography) се создава без согласност на лицето чијшто лик се користи во порнографскиот материјал и претставува облик на неконсензуална порнографија.

Речиси во сите случаи на лажната (дипфејк) порнографија, оние што се на нишан се жени, меѓу кои и јавните личности, како актерката Кристен Бел, но и непознати жени и девојки, со оглед на тоа што оваа технологија е сè повеќе финансиски достапна[39]. Поради ова, лажната порнографија е криминализирана во некои земји, како што е Хрватска (Злоупотреба на снимки од сексуално експлицитна содржина, член 144а).

b Секстѝнг и злоупотреба преку секстѝнг

Секстѝнг (англ. sexting) е електронска размена на разголени или фотографии со сексуална конотација, како и видеоснимки од сексуални односи и сексуална текстуална содржина, со согласност на сите вклучени страни. Иако секстѝнгот често се прикажува како опасен, тој не е опасен сам по себе, сè додека постои согласност и се почитува приватноста на сите вклучени. **Злоупотребата преку секстѝнг** (англ. abusive sexting) се разликува од секстѝнгот затоа што отсуствува согласност од лицето до кое се испраќа содржината. Доколку лицата не се однесуваат одговорно кон содржината што се разменува преку секстѝнг, не ја почитуваат приватноста на лицето претставено во содржината и ја проследуваат на трети лица, веќе станува збор за порнографија без согласност.

Иако и момчињата и девојчињата тинејџери имаат секс во еднаква мера, веројатноста момчињата да ги проследат фотографиите што им биле испратени е два до трипати поголема[40]. Покрај тоа, истражувањата покажуваат дека искуството со злоупотреба преку секстѝнг е почесто кај помладите тинејџери и предадолесцентите[41], како и кај оние чија сексуалност е различна од хетеросексуалната[42].

b Сајберегзибиционизам, изложување на порнографија без согласност и курослики

Сајберегзибиционизам (англ. cyberflashing) претставува облик на злоупотреба со посредство на визуелна содржина, при што едно лице испраќа непосакувана фотографија од своите гениталии до непознати лица, без нивна согласност. Сајберегзибиционизмот претставува дел од **изложувањето на порнографија без согласност** (англ. unsolicited pornography), што подразбира испраќање сексуално експлицитни фотографии и видеосодржини од секаков тип на друго лице без негова согласност[43]. **Несаканите фотографии од пенисот**, наречени курослики (англ. dick pics), се најчестиот облик на изложување на порнографија без согласност. Станува збор за фотографии од пенисот, вообичаено во ерекција, кои се испраќаат преку интернет. Сајберегзибиционизмот, покрај куросликите, може да опфаќа и други облици на изложување на порнографија без согласност, од типот на фотографии, видеа и ГИФ (англ. GIF) анимации со сцени на секс, но и на силувања[44].

Сајберегзибиционизмот, куросликите и несаканата порнографија се голем проблем, до толкав степен што Обединетото Кралство моментално е во процес на донесување закони кои ќе го криминализираат ваквото однесување[45]. Криминализацијата беше предложена откако едно истражување од 2019 година покажа дека 76 % од тинејџерките на возраст меѓу дванаесет и осумнаесет години добиле несакана фотографија од пенис[46].

b Снимање и/или емитување сексуални напади и силувања

Сексуалното насилство во дигиталната средина може да претставува и продолжение на сексуалното насилство во офлајн светот – пример е **практиката на снимање и/или емитување сексуален напад и силување** (англ. documenting or broadcasting sexual assault/rape videos) на социјалните мрежи, преку пораки или веб-локации, што претставува дополнителен акт на сексуално насилство врз жртвата. Овие снимки понекогаш се користат за понижување или за уценување на лицата што преживеале сексуално насилство, а исто така се продаваат и како порнографија без согласност.

Кампањата #NotYourPorn беше отпочната со цел да се подигне свеста за недостигот од регулаторни механизми на популарните порносајтови кои би го отстраниле или спречиле поставувањето видеа од сексуален напад и силување, порнографијата без согласност, како и доброволно снимениот материјал украден од сексуалните работнички и работници и објавен без нивна согласност.

b Кротење (груминг) во онлајн просторот

Кротењето во онлајн просторот (англ. online grooming) претставува предаторски облик на однесување со намера да се дојде во контакт со деца и со млади преку социјалните мрежи или други дигитални платформи, сè со цел сексуално насилство. Кротењето функционира на тој начин што кротителот (лицето што кроти) воспоставува лажна емоционална врска со лицето што му претставува цел и го намамува со цел да изврши сексуална злоупотреба, сексуална експлоатација (на пример, сексуална експлоатација преку присилна проституција) или трговија со деца. Во случаите на кротење во онлајн просторот, предаторите често и самите се претставуваат како деца или млади луѓе, а понекогаш кога ќе воспостават однос бараат средба во живо, што отвора можност за сексуална експлоатација и сексуално и физичко насилство во офлајн просторот.

Во последните четири години има зголемување од дури 84 % на случаите на кротење во онлајн просторот во Обединетото Кралство. Децата и младите најчесто стануваат цел на кротење на социјалните мрежи и на сајтовите за играње игри, а кротителите бараат од нив да им испраќаат сексуално експлицитни материјали[47].

b Несакани сексуални искуства во живо овозможени од технологијата

Несаканите сексуални искуства во живо овозможени од технологијата (англ. technology-facilitated unwanted sexual experiences) се јавуваат кога информациските и комуникациските технологии се користат за да се овозможи сексуално вознемирување или сексуално насилство за време на средбите во офлајн светот. Технологиите што се користат за овој облик на насилство се најчесто апликации, сајтови и платформи за средба со партнери (онлајн дејтинг), преку кои се договара состанок во живо, каде што доаѓа до сексуалниот напад[48].

Истражување од Обединетото Кралство укажува на тоа дека бројот на луѓе кои пријавиле силување на првиот состанок со лице што го запознале на интернет се зголемил за шестпати во рок од пет години, при што 85 % од случаите биле пријавени од жени помеѓу 2003 и 2015 година. Најранливи биле младите жени, на возраст од дваесет до дваесет и четири години, за кои постоела двојно поголема веројатност да доживеат несакано сексуално искуство со посредство од технологијата, во споредба со постарите жени[49]. Неодамна разоткриениот случај во којшто пет лица сексуално злоупотребувале малолетничка и изготвувале порнографски материјал е илустративен за начинот на којшто насилството лесно се прелева од онлај во офлајн просторот, или таканаречениот „вистински живот“, но и за начинот на којшто се преклопуваат различните форми на насилство – кротење, сексуална изнуда, електронски потпомогната трговија со деца и порнографија без согласност[50].

(b) Електронски потпомогната трговија со луѓе и врбување

Информатичките и комуникациските технологии се користат и при трговија со жени и девојки, и во тие случаи станува збор за **електронски потпомогната трговија со луѓе** (англ. electronically facilitated trafficking). Информациските и комуникациските технологии може да се користат за **врбување** (англ. recruitment). Трговците со луѓе многу често го користат интернетот за врбување преку објавување лажни огласи за работа или за студирање, обично во странство, или преку користење лажни профили на апликации и веб-страници за запознавање, т.е. сајтови на „брачни агенции“ [51].

Трговците со луѓе ја злоупотребуваат технологијата и во други фази од сексуалната експлоатација, како и при испраќање закани со цел принуда и контрола на тргуваните жени и девојки, кога станува збор за сексуална изнуда. За електронски потпомогнатата трговија со луѓе најчесто се користат платформите на социјалните мрежи или апликациите и сајтовите за запознавање[52 53].

Истражувањето на организацијата „Атина“, здружение на граѓани за борба против трговијата со луѓе и сите облици на насилство врз жените, покажа дека голем број жени и девојки кои биле жртви на трговија со луѓе биле врбувани преку дигитални медиуми, додека 30 % од нив биле врбувани со цел врз нив да се изврши и некој друг облик на насилство, како силување, грабеж или физичко насилство. Повеќе од половина од жртвите на трговија со луѓе се соочиле и со објавување огласи на интернет со цел да ја „рекламираат“ нивната сексуална експлоатација, а половина преживеале и сексуална изнуда, кога трговците со луѓе ги уценувале со видеоматеријал[54].

ЗАГРОЗУВАЊЕ НА ПРИВАТНОСТА И НА БЕЗБЕДНОСТА СО (ЗЛО)УПОТРЕБА НА ТЕХНОЛОГИЈА

Загрозувањето на приватноста и безбедноста преку технологијата опфаќа цела низа дејства кои се насочени кон тоа лицето да се чувствува небезбедно, загрозено и непосакувано, не само во дигиталната средина туку и во офлајн светот. Токму тоа претставува една од најважните својства на оваа група однесувања – неможноста да се направи јасна разлика помеѓу онлајн и офлајн средината. Објавувањето лични информации за лицето без нивна согласност на интернет, **доксирање, мртвоименување или аутирањето без согласност** може да доведе до загрозување на безбедноста на тоа лице во офлајн светот; **лажното претставување и кетфишингот** имаат за цел не само да добијат финансиски придобивки, туку и да се изврши потенцијално сексуално насилство доколку дојде до средба во живо, а технологијата може да се користи и за **ограничување и контрола** на одредена личност, најчесто интимен партнер, како и за **финансиска злоупотреба**. Кога станува збор за **сајбердемнењето и опсесивното следење на интернет**, тие често се надоврзуваат или му претходат на демнењето во офлајн светот, а **онлајн заканите** во повеќето случаи се однесуваат на животот на лицето кое е под закана надвор од интернетот. Кога злоупотребата „се прелева“ од онлајн во офлајн светот, можеме да зборуваме за **напади во „вистинскиот живот“.** Исто така, овој вид на насилство го опфаќа и **бомбардирањето на Гугл и на Зум, како и нападите со оневозможување на пристап и услуги.**

b Доксинг (злокументирање), мртвоименување (деднејминг) и аутирање без согласност

Доксинг/злокументирање (англ. doxxing или doxing) претставува форма на дигитално родово базирано вознемирување во кое едно лице, доксерот, собира податоци за друго лице, ги анализира и ги објавува, а сето тоа е со злобна намера да го прикаже тоа друго лице во негативно светло и да му наштети на угледот и/или на безбедноста[55]. Во случај на доксинг, најчесто се објавуваат лични податоци – адреса на живеење или е-пошта, телефонски број, контакти на работодавците или на членовите на семејството, т.е. фотографии од децата или училиштето кое го посетуваат децата, а сето тоа е со цел да се открие/дознае точната локација и да се изврши физичко насилство[56]. Посебни облици на доксирање се аутирањето без согласност и мртвоименувањето, при што на нишан се припадниците на ЛГБТКИА+ и ТИРФ (транссексуални, интерсексуални и родово-флуидни лица) заедниците. Во случаите на **аутирање/разоткривање без согласност** (англ. non-consensual outing) се открива сексуалната ориентација на ЛГБТКИА+ лице, а во случаите на **мртвоименување (deadnaming),** се разоткрива името дадено при раѓање на транс лице, со цел да се омаловажи, да се поништи или да се обезвредни посакуваниот идентитет на транс лице. Како во случаите на аутирање без согласност, така и во случаите на мртвоименување и доксирање, намерата е на одредено лице да му се нанесе штета и да се изложи на насилство и на дискриминација, како во онлајн така и во офлајн светот[57].

Доксирањето често оди рака под рака со другите облици на родово базирано насилство, а жените кои се видливи во јавноста, како новинарките, се особено подложни на него. Новинарката и основачка на неформалната група Новинарки против насилството Јована Глигоријевиќ често беше цел на закани, родово базиран и сексистички говор на омраза, како и родово базирано тролање, а во 2019 година, во коментар на видео на Јутјуб дури беа објавени нејзиниот матичен број (ЕМБГ) и адресата на живеење[58].

b Лажно претставување и кетфишинг

Лажното претставување (англ. impersonation) е процес на кражба на нечиј веќе постоечки идентитет со цел за закана или заплашување, како и со цел да се дискредитира тоа лице или да се наруши неговиот углед [59]. Посебен облик на лажно претставување е **кетфишингот/измамништвото** (сленг: преварантство) (англ. catfishing), што претставува лажно претставување со цел измама. Кетфишингот обично се јавува кога жртвата ќе се вљуби во сторителот, т.е. кога ќе развие интимни чувства и ќе поверува дека се во врска, по што сторителот од неа бара пари или подароци за да се стекне со финансиска корист. Сторителот може да побара и одредени информации и/или интимни фотографии, со цел дополнително да ја уценува жртвата. И при лажно претставување и при кетфишинг, во создавањето лажен идентитет сторителите често користат фотографии од други луѓе и доаѓаат до детални лажни биографии и животни искуства, како и работни места и пријатели[60 61].

Лажното претставување и кетфишингот најчесто се случуваат на сајтовите и на апликациите за запознавање, па така повеќето од овие сајтови и апликации се обидуваат да развијат механизми за проверка на идентитетот со цел да се спречи овој тип на измама. Во ваквите случаи, целта на кетфишингот не е нужно стекнување финансиска корист, без разлика дали е преку подароци или изнуда, туку може да биде и сексуално насилство штом ќе дојде до средба во живо, а тогаш станува збор за непосакувани сексуални искуства во живо потпомогнати од

технологијата. Еден од најпознатите извршители на лажно претставување и кетфишинг е Симон Левиев, за кого е снимен документарен филм „Измамникот од Тиндер“. Левиев ги измамил своите жртви за милионски суми и сè уште е во бегство[62].

b Ограничување или контролирање со помош на технологија

Насилниците можат да ја користат технологијата да злоупотребуваат или да контролираат, преку следење, надзор или ограничување на движењето, комуникацијата и активностите на едно лице. Овие однесувања се движат од принудување на лицето, најчесто интимна партнерка или партнер, да ги каже своите лозинки со цел да се добие пристап до неговите онлајн профили, па сè до директно ограничување или забрана за употреба на технолошките уреди. Во партнерските односи каде што има злоупотреба, **ограничувањето или контролирањето на пристапот/користењето на технологијата** (англ. limiting or controlling use of technology) може да претходи на други форми на злоупотреба[63].

Проблемот со овој облик на родово базирано насилство е тоа што често се романтизира, така што давањето на сопствените лозинки и пристапот до онлајн профилите или инсталирањето апликации за следење се претставува како форма на грижа и доказ за љубов меѓу партнерите. Со оглед на тоа што технологијата денес е еден од начините на кои стапуваме во контакт со надворешниот свет, ограничувањето или контролирањето на нејзината употреба од страна на партнерот е обид да се изолираат, да се контролираат и да секнат ресурсите за да се излезе од насилна врска, што е честа техника што ја користат насилниците[64].

b Електронски потпомогната финансиска злоупотреба

Електронски потпомогната финансиска злоупотреба (англ. electronically enabled financial abuse) претставува продолжение, односно поместување на економското насилство во дигиталниот простор. Се состои од различни начини на користење на интернетот и другите форми на информациски и комуникациски технологии со цел да се изврши финансиски притисок врз некоја личност. Електронски потпомогнатата финансиска злоупотреба најчесто ја трпат жените, а притоа сторителите се нивните интимни партнери.

Електронски потпомогнатата финансиска злоупотреба *се состои од недозволување онлајн пристап до банкарските сметки и фалсификување информации за создавање негативен кредитен статус или кражба на идентитет*[65]. *На овој начин, сторителите имаат целосна контрола врз своите жртви бидејќи им го оневозможуваат пристапот до пари, како и можноста да подигнат кредит за да дојдат до средствата што им се потребни за да ги напуштат насилниците*[66].

b Сајбердемнење и опсесивно манијачење (следење) на интернет

Сајбердемнењето (англ. cyberstalking) е форма на злоупотреба во која сторителот користи технологија за да демне некое лице и неговото однесување на интернет. Не мора да се состои од директни закани, туку ги опфаќа оние активности што предизвикуваат лицето што е цел на демнењето да чувствува страв, загриженост, анксиозност и беспомошност. Сајбердемначот на својата цел ѝ испраќа пораки, ѝ се јавува или ѝ испраќа гласовни пораки со цел да ја одржува во активна состојба на постојана вознемиреност и страв за својата безбедност надвор од интернетот[67]. **Опсесивното манијачење на интернет** (англ. cyber-obsessional pursuit) се

одликува со употреба на технологија со цел да се прогонува некоја личност и се разликува од сајбердемнењето поради тоа што од жртвата се бара некаков облик на интимна врска. Опсесивното манијачење на интернет се карактеризира со барање за интимност преку нарушување на физичката и на онлајн приватноста, а тоа се состои од однесување од типот на онлајн и офлајн демнење, испраќање непосакувани подароци, барање заследување/ пријателство на социјалните мрежи, како и пораки од типот на е-пошта, текстуални пораки и пораки преку различните апликации за разговор[68].

Често слушаме дека сајбердемнењето не е страшна работа, бидејќи лицето може да ги изгасне своите профили на интернет и да го „исклучи компјутерот". Ова, за жал, не е точно – сајбердемнењето влијае врз жртвата на истиот начин како и офлајн демнењето, а во некои случаи и претходи или е дел од офлајн демнењето[69]. Затоа во Република Северна Македонија, член 144-а од Кривичниот законик е дополнет за да вклучува и демнење „со користење на средства за јавно информирање или други средства за комуникација" и за делото е предвидена затворска казна. Во Србија, сајбердемнењето е криминализирано (во рамките на кривичното дело демнење, член 138а од Кривичниот законик).

b Напади „во вистинскиот живот"

За „напади во вистинскиот живот" (англ. in-real-life (IRL) attacks) станува збор кога злоупотребата на интернет преминува во недигитален контекст или е составен дел од веќе постојно демнење или злоупотреба во партнерски однос[70].

Жените кои се видливи во јавноста, како новинарките, се особено подложни на напади „во вистинскиот живот". Новинарите Дафне Каруна Галиција и Гаури Ланкеш беа убиени во 2017 година, откако беа изложени на вмрежено вознемирување во форма на закани со силување и смртни закани[71].
Три малолетни девојчиња од Република Северна Македонија во периодот од 2019 до 2020 година биле првин демнети на Фејсбук, а потоа станале жртви на демначот кој ги силувал повеќепати[72].

b Онлајн закани

Онлајн закана (англ. online threats) е „исказ за намера да се нанесе болка, повреда, штета или друго непријателско дејствие" на лицето на кое му е упатен исказот. Покрај заканите со насилство во онлајн опкружувањето (закани за недавање пристап, закани за дипфејк порнографија или доксирање), заканите сè почесто се поврзани со насилството во офлајн светот – тука спаѓаат заканите со смрт, како и заканите со физичко и/или сексуално насилство[73].

Жените кои се гласни во дигиталниот простор кога се во прашање женските и човековите права често се мета на закани. Според податоците на Независното здружение на новинари на Србија (НЗНС), во Србија три четвртини од заканите за новинарките се обиди да се загрози нивниот углед, а повеќе од половина содржат сексуално вознемирување и закани по безбедноста и животот[74].
Во локален контекст, над 29.7 % од новинарките кажале дека биле споделени нивни фотографии во одредени групи на социјалните мрежи, со цел нивна дискредитација. Со онлајн демнење се соочиле 22 % од новинарките, додека оркестрирани кампањи биле организирани против 18.7 %.

Според содржината на онлајн вознемирувањето, доминира говорот на омраза (69 %), а во околу половина од случаите бил демонстриран сексизам (51,7 %) и шовинизам (43,7 %). Нападите во

дигиталниот простор преоѓаат и во закани за физичко насилство (24,1 %) и закани по животот (19,5 %). Загрижувачки е и податокот што дури 36 % од испитаничките сметаат дека се соочиле и со организирани напади.

b Бомбардирање на Гугл и на Зум

Бомбардирањето на Гугл (англ. Google bombing) се состои од насочено приспособување на алгоритмот со цел да се позиционираат сајтови на интернет што содржат малициозни и неточни информации за некое лице или појава, така што тие да се видат први или меѓу првите кога се пребарува определен термин или лице[75]. Од друга страна, **бомбардирањето на Зум** се однесува на непоканет „упад" во туѓ разговор на на оваа платформа, со цел ширење расистичка, сексистичка, порнографска, хомофобична или антисемитска содржина, со цел да се вознемират и да се шокираат присутните гледачи. Бомбардирањето на Зум е форма на вмрежено вознемирување[76].

Еден пример за бомбардирање на Гугл насочено против жените е настанот од 2011 година кога активистите противници на правото за прекинување на бременоста успеаја да го приспособат алгоритмот на Гугл така што страницата на Википедија за абортус почна да се појавува како прв резултат при пребарувањето на поимот убиство (англ. murder) [77].

b Напад со оневозможување пристап и напад со одбивање услуга

Напад со оневозможување пристап (англ. denial of access) е користење одредени опции на технологијата или на платформите со цел да се нанесе штета на некое лице, со тоа што му се оневозможува пристап до неговиот личен профил на социјалните мрежи или е-пошта. Постојат две основни форми на одбивање пристап. Првиот се состои од координиран напад од страна на насилниците кои лажно и заеднички пријавуваат профил на некое лице, колектив или институција поради наводна злоупотреба или некое друго прекршување на правилата, сè со цел да го блокираат или да го затворат тој профил. На овој начин најчесто се оневозможува пристап до социјалните мрежи. Другата форма на недавање пристап се однесува на масовно испраќање голем број електронски пораки или преплавување со смс-пораки, чија цел е да се спречи лицето, колективот или институцијата да користи одредена платформа, на пример е-пошта, поради бомбардирање со голема количина непосакувана содржина[78]. Покрај нападите со оневозможување пристап, постои и **напад на оневозможување на услугата** – DoS напад (англ. Denial of service). Додека целта на нападот со оневозможување пристап е да се оневозможи пристапот до одредена платформа или профил, целта на нападот со оневозможување услуга е да се оневозможи пристапот до компјутер, односно компјутерска мрежа. Покрај оневозможувањето пристап до компјутер или мрежа, нападите со оневозможување на услугата можат да ги компромитираат осетливите информации складирани на тие уреди. До Дистрибуирано оневозможување услуги – DDoS (Distributed Denial of Service) доаѓа кога напаѓачот ја презема контролата врз компјутерите на повеќе корисници со цел да нападне компјутер на друг корисник. На овој начин, напаѓачот им дава налог на „киднапираните" компјутери да испраќаат големи количини барања до одредена интернет-страница или да испраќаат спам до насочени адреси на е-пошта. ДДоС (англ. DdoS) нападите работат со преоптоварување на системот со податоци испратени од напаѓачот од други компјутери.

Феминистките и активистите ширум светот често се соочуваат со напади на оневозможување пристап, бидејќи тоа е

обид да се замолчи и да се одземе гласот на жените. Во Кина, во 2021 година, беа затворени неколку феминистички канали на популарните форуми Дубан и Веибо. Тие згаснаа по големиот број пријави поради „екстремистичка и идеолошка содржина“, и покрај тоа што нивните сопственички немаа прекршено ниту едно од правилата за однесување на овие мрежи[79].

ДРУГИ ОБЛИЦИ НА НАСИЛСТВО ВО ДИГИТАЛНАТА СРЕДИНА

Астротурфирање

Астротурфирање (англ. astroturfing) е практика на објавување и ширење информации и содржини (чија цел може да биде вознемирување и злоупотреба) на интернет, со намера да се создаде впечаток дека тоа се случило на природен, органски начин и дека станува збор за општоприфатена гледна точка. Целта на астротурфирањето е да се создаде впечаток дека одредени идеи и содржини имаат поддршка од голем број граѓани, иако се работи за измама, односно за фалсификување. Астротурфирањето е внимателно координиран чин зад којшто стојат поединци, групи на интерес, политички партии или организации, во кои често учествуваат многубројни лажни профили, т.н. ботови. Еден пример за тоа се антиродовите движења кои имаат за цел патријархалниот поредок да го прикажат како природен, без притоа да ги откријат организациите, финансиските поддржувачи и групите на интерес што стојат зад движењето.

Името „астротурфинг“ доаѓа од познатиот бренд на вештачка трева ‘астротурф’ (англ. AstroTurf), при што е забележлива играта со зборови – за разлика од „грасрут“ – самоникната иницијатива, имиџот што астротурфингот се стреми да го прикаже, всушност, е вештачки креирана медиумска и рекламна кампања со цел да се манипулира со јавноста.

Лажни обвинувања за богохулење

Жените се соочуваат со онлајн закани на глобално ниво, но се изложени на посебен ризик во конзервативните религиозни земји, каде што богохулењето е нелегално, а убиствата поради чест се сериозна закана. Во оваа смисла, **лажните обвинениј за богохулење** можат самите по себе да станат чин на насилство[80].

Новинарката и бранителка на човековите права Марви Сирмед од Пакистан беше приведена во 2020 година, откако беше лажно обвинета за богохулење на социјалната мрежа Твитер, а покрај со тужбата, Сирмед се соочи и со бројни закани[81].

Постхумно тролање и тролање врз основа на шок и тага

Постхумното тролање (англ. RIP trolling) е форма на сајберзлоупотреба која се заснова врз објавување грди и навредливи коментари на меморијалните страници за починати лица на социјалните мрежи или на личните профили на починати лица[82]. **Тролање врз основа на шок и тага** (англ. shock and grief trolling) ги таргетира семејството и пријателите на починатиот, кои се малтретирани со создавање мемиња, веб-страници и лажни сметки на социјалните мрежи со името и сликата на починатиот[83].

Двата најпознати случаи на постхумно тролање и тролање врз основа на шок и тага се

случија во 2010 година, кога обучувачката на морски животни Даун Браншо ја усмрти китот со кој таа изведуваше точка. По нејзината смрт, троловите ги преплавија социјалните мрежи со исмејувачки и сексистички мемиња (мимови), како и со синтетички сексуални содржини со нејзиниот лик. Речиси во исто време, исчезна тинејџерката Челзи Кинг, а троловите решија да создадат серија од меморијални 'RIP' страници посветени на неа, иако таа сè уште не беше пронајдена. Откако беше пронајдено нејзиното тело, беше креирана страница на Фејсбук под името „Се обложувам дека оваа кисела краставичка може да добие повеќе фанови од Челзи Кинг" (I Bet This Pickle Can Get More Fans than Chelsea King), на која беше објавена сателитска фотографија од нејзината куќа, се бараше нејзината порнографија без согласност, но беа упатени и закани со силување до женските членови на семејството на оние кои се обиделе да го одбранат споменот на Челзи Кинг во коментарите[84].

Свотинг

Свотинг (англ. swatting, бидејќи СВОТ [SWAT, special weapons and tactics] е кратенка за интервентната единица на полицијата) е лажно пријавување насилство, убиство, закани со бомба или заложнички ситуации во полицијата, што резултира со пристигнување на целосно вооружени интервентни единици на нечија, обично домашна адреса. Свотингот е редок, но исклучително опасен и е јасен пример за тоа како онлајн вознемирувањето има потенцијал да предизвика сериозна штета на некое лице, а во овој случај и на целото негово семејство, во офлајн животот[85].

Иако свотингот често се сфаќа како шега, особено меѓу гејмерите, тој има сериозни последици, кои се движат од уништување на имотот, психолошки стрес, па дури и сериозни физички повреди и смрт. За среќа, свотингот не е застапен на Западен Балкан во иста мера како во САД, од каде што потекнува.

Труење хаштаг

Труење хаштаг (англ. hashtag poisoning) претставува создавање навредлив хаштаг или, почесто, киднапирање веќе постоен хаштаг така што неговото значење и намера се менуваат. Така „отруениот" хаштаг потоа се користи како собирен повик за масовен сајбернапад (англ. cyber-mob attack) врз поединец, или, пак, со цел да се уништи зачетокот на некоја, многу често феминистичка, кампања[86].

Популарните феминистички хаштагови #TakeBackTheTech и #ImagineAFeministInternet, кои во 2015 година ја промовираа идејата за интернет каде што жените ќе бидат безбедни од родово базирано насилство, беа преплавени од координирана поплава на родово базиран и сексистички говор на омраза, чија цел беше уништување на кампањите[87].

Слични полууспешни обиди имаше и со хаштаговите #СегаКажувам и #КадеНеОдам, кои беа преплавени со тривијални содржини со цел да се попречи нивната цел за подигнување на свеста околу сеприсутноста на родово базираното вознемирување.

// КОНЦЕПТИ ОД ДОМЕНОТ НА ТЕХНОЛОГИЈАТА

А

Алгоритам

Алгоритам е серија од инструкции кои му кажуваат на компјутерот како да реши проблем, да изврши функција или да конвертира збир на податоци во корисни информации. Алгоритмите се користат во сите области на информатичката технологија. На пример, секоја компјутерска програма може да се смета за сложен алгоритам[88].

Апликација или ап (англ. application)

Апликациите се софтверски програми, најчесто за мобилни уреди како паметни телефони и таблети, каде што преземањето и инсталирањето обично се одвиваат во истиот чекор. При инсталирањето апликации не се потребни дополнителни кориснички дејства, а апликациите може да се отстранат од уредот, т.е. да се деинсталираат без да се влијае врз неговото функционирање[89]. Важно е да се нагласи дека при инсталирањето апликации на мобилните уреди, корисникот се согласува со условите за користење кои често се однесуваат на споделување податоци и лични информации од уредот, понекогаш вклучувајќи геолокација, но и контакти од телефонскиот именик.

В

Вештачка интелигенција

Развојот на вештачката интелигенција е поле кое комбинира компјутерски науки и големи количини податоци за да овозможи решавање проблеми. Ги вклучува и подобластите на машинско учење и длабоко учење. Развојот и употребата на вештачката интелигенција настојува да создаде експертски системи, кои, пак, прават предвидувања или класификации врз основа на внесените податоци и со помош на компјутери и машини ги имитираат способностите за решавање проблеми и одлучување на човечкиот ум[90].

Д

Дигитална платформа

Дигиталните платформи се онлајн компании кои овозможуваат интеракција и размена на податоци, стоки и услуги помеѓу производителите и потрошувачите, како и во рамките на заедницата која е во интеракција со гореспоменатата платформа. Дигиталните платформи може да бидат платформи за социјално вмрежување (Facebook, Twitter и LinkedIn), платформи за знаење (Yahoo!Answers и Google Scholar), платформи за споделување медиуми (Spotify, YouTube и Netflix) или платформи ориентирани кон услуги (Airbnb, Amazon и Uber) [91].

Дигитални технологии

Дигиталните технологии се електронски алатки, системи, уреди и ресурси кои генерираат, складираат или обработуваат податоци. Тие ја опфаќаат инфраструктурата, уредите, медиумите, онлајн услугите и платформите што ги користиме заради комуникација, информации, документација, вмрежување и поврзување[92].

Социјална мрежа

Социјалните мрежи се колективен термин за веб-локации и апликации што се фокусираат врз онлајн комуникација,

коментари на заедницата, интеракција, споделување содржина и соработка. Форуми, микроблогови, социјални мрежи, сајтови и/или платформи за креирање збирки од написи, слики или објави и нивно споделување, како и вики-содржини се само некои од различните типови на социјални мрежи кои овозможуваат брз електронски пренос на содржината до корисниците. Содржината се состои од лични информации, документи, видео и аудиосодржина и фотографии. Корисниците ги користат социјалните мрежи преку компјутери, таблети или паметни телефони, со помош на софтвер на интернет или апликации. Најчесто користените платформи за социјално вмрежување се Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram и TikTok[93].

Дрон

Во технолошки контекст, дронот е беспилотно летало – летечки робот што може да се контролира од далечина или да лета самостојно со помош на планови за летање контролирани од софтвер внесен во неговиот систем, којшто работи заедно со сензори и со GPS-системот на леталото. Дроновите се нарекуваат и „беспилотни воздухоплови“ или „беспилотни воздухопловни системи“ (англ. UAV и UAS). Денес, беспилотните летала се користат за широк спектар од цивилни улоги, од пребарување и спасување, до надзор, сообраќај, временска прогноза и следење пожари, до фотографирање лични и деловни беспилотни летала, како и професионална фотографија, земјоделство, па дури и услуги за испорака[94].

И

Информациски и комуникациски технологии

Разновидна низа од технолошки алатки и ресурси што се користат за испраќање, складирање, креирање, споделување или размена на податоци. Овие технолошки алатки и ресурси вклучуваат компјутери, интернет (веб-страници, блогови и е-пошта), технологии за директен пренос (преку радио, телевизија и интернет), технологии за снимен пренос (поткасти, аудио и видеопредаватели и уреди за складирање податоци) и телефонија (на пр. фиксна или мобилна, сателитска и видео/видеоконференциска опрема) [95].

М

Меме (мим) (англ. meme)

Мим или меме е визуелен формат што се состои од слика и придружна фраза. Покрај форматот на сликата, мемето може да се најде и во формат на пократко видео или ГИФ/GIF, т.е. анимација. По правило, мемињата се однесуваат на некој феномен од популарната култура и се создаваат со идеја да бидат широко споделени на социјалните мрежи[96]. Иако мемињата најчесто имаат хумористичен карактер, исто така можат да исмејуваат, да вознемируваат и/или да се користат со намера да се злоупотребува некое лице.

О

Онлајн платформа

Онлајн платформа е дигитална услуга која овозможува интеракција помеѓу две или повеќе различни, но меѓусебно зависни множества на корисници (без разлика дали се компании или поединци), кои комуницираат преку услугата преку интернет. Терминот 'онлајн платформа' се користи за опишување низа услуги достапни на интернет, вклучително онлајн продавници, пребарувачи, социјални мрежи, услуги за креативна содржина, продавници за апликации, комуникациски услуги, платежни системи, услугите што прават т.н. „колаборативна" или економија на „тезги" (хонорарна работа) и многу други[97].

Т

Технолошки компании [98]

Технолошките компании опфаќаат широк спектар од организации, вклучувајќи но не ограничувајќи се на следново:

- одредени даватели на интернет-услуги: субјекти кои им овозможуваат на крајните корисници пристап до онлајн материјали и даватели на интернет-услуги, како што се субјекти кои обезбедуваат услуги за прелистување на интернет, вклучувајќи но не ограничувајќи се на Google, Safari и Firefox;
- даватели на услуги за социјална мрежа: субјекти кои обезбедуваат услуги што поврзуваат двајца крајни корисници онлајн, вклучувајќи но не ограничувајќи се на Facebook, LinkedIn и Instagram;
- даватели на електронски услуги: субјекти кои им овозможуваат на крајните корисници да комуницираат едни со други (на пр. Outlook и услуги за разговор за игри, како што е Discord);
- даватели на услуги за дистрибуција на апликации: субјекти кои обезбедуваат пристап до апликативни услуги, вклучувајќи но не ограничувајќи се на Google (преку Google PlayStore) и Apple (преку IOS App Store);
- даватели на услуги за хостирање: субјекти кои го олеснуваат хостирањето на зачуваните материјали обезбеденипреку услугите на социјалните мрежи, релевантните електронски услуги или одредени интернет-услуги, кои ги вклучуваат, меѓу другото, Apple и Microsoft, секој преку обезбедување на своите облак-услуги;
- компании за развој на хардвер: субјекти кои создаваат, развиваат и/или одржуваат технолошка опрема, физички средства и други материјални предмети;
- Компании за развој на софтвер: субјекти кои создаваат, дизајнираат, развиваат и одржуваат програми, апликации, рамки и други софтверски компоненти.

Х

Хакирање

Хакирањето претставува неовластен пристап до информации и до програми на електронските уреди и нивните мрежи – паметнителефони,компјутери,компјутерски системи и сервери. Хакирањето може да биде злонамерно и етичко. Злонамерно хакирање значи нелегален или неовластен пристап до системи што има за цел да нападне, да повреди или да инкриминира друго лице или организација преку кражба или промена на податоци, добивање лични информации, нарушување на приватноста или инфицирање на уредот со вирус[99]. Во овој случај, хакирањето е кривично дело, а хакерот е киберкриминалец. Етичкото хакирање се однесува на хакирање чијашто цел е откривање безбедносни пропусти во компјутерските системи за да се подобри заштитата на системот.

Џ

Џипиес/GPS и Џипиес/GPS следење

Џипиес/GPS (кратенка за Глобален систем за позиционирање) е констелација од дваесет и четири добро поставени сателити кои орбитираат околу Земјата и овозможуваат да се одреди географската локација на луѓето со земјени приемници, т.е. со џипиес-уреди за следење. Џипиес-системот може да ја одреди географската должина и ширина на локацијата и брзината и насоката на движење на целите, а точноста на локацијата е помеѓу десет и сто метри за повеќето уреди. Џипиес-опремата сега е интегрирана во паметните телефони, во таблетите и во уредите за навигација. Џипиес-технологијата во мобилните телефони, освен за навигација, често се користи и за следење на бројот на чекори преку специјализирани апликации за фитнес и здравје. Следењето со 'Џипиес' е следење на локацијата со помош на 'Џипиес', што ја следи локацијата на субјектот или објектот на далечина. Поборниците за приватност предвидуваат дека оваа технологија може да им овозможи на огласувачите, на државата, на хакерите и на сајбер-демначите да ги следат корисниците со помош на нивните мобилни уреди.[100]

Ш

Шпионски софтвер (англ. Spyware)

Spyware е вид малициозен софтвер што се инсталира на компјутер без знаење на крајниот корисник. Го киднапира уредот, краде осетливи информации и податоци за користење на интернет и ги пренесува на огласувачи, на компании за податоци или до надворешни корисници. Откако ќе се инсталира, ја следи активноста на интернет, ги следи информациите за најавување и шпионира чувствителни информации.

Шпионскиот софтвер може да се користи и за следење на локацијата на некоја личност, како што е случајот со софтверот за демнење (англ. stalkerware). Овој софтвер честопати е тајно инсталиран на мобилни телефони од сопружниците, партнер(к)ите, поранешни партнер(к)и, па дури и од родителите и од членовите на семејството. Овој тип на шпионски софтвер може да ја следи физичката локација на едно лице, да ја пресретнува неговата е-пошта и пораки, да прислушува телефонски повици и да снима разговори, а исто така да пристапува до лични информации, како што се фотографии и видеа[101].

1. UN Women. Accelerating Efforts to Tackle Online and Technology Facilitated Violence Against Women and Girls (VAWG). Достапно на: 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. Europian 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). Достапно на: 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.* Достапно на: https://eige.europa.eu/publications/cyberviolence-against-women-and-girls

6. Родово базираните навреди претставуваат родово базиран и сексистички говор на омраза.

7. Cyberbullying Research Centre. *What is cyberbullying?* Достапно на: https://cyberbullying.org/what-is-cyberbullying

8. Van Der Wilk, A. and M. Natter. 2018. *Cyber violence and hate speech online against women.* Study for the FEEM Committee.

9. Pen America, *Online harassment field manual.* Достапно на: https://onlineharassmentfieldmanual.pen.org/

10. Radoičić, A. 2020. *Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju.* Достапно на: http://www.atina.org.rs/sites/default/files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf

11. VAW Learning Network. 2013. *Technology-related Violence Against Women.* Достапно на: http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html
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
Flynn, A., Powell, A., and Hindes, S. 2021. *Technology-facilitated abuse: a survey of support services stakeholders* (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg-38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_Survey.pdf

12. GBV AoR Helpdesk. 2021. *Learning Series on Technology-Facilitated Gender-Based Violence*. Learning Brief 1: Understanding technology-facilitated GBV.

13. Pen America, *Online harassment field manual.* Достапно на: https://onlineharassmentfieldmanual.pen.org/

14. Pen America, *Online harassment field manual.* Достапно на: https://onlineharassmentfieldmanual.pen.org/

15. Posetti, J. et all. 2020. *Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts.* UNESCO. Достапно на: https://www.icfj.org/our-work/icfj-unesco-global-study-online-violence-against-women-journalists

16. Извор: *ПИНА: Над 81 % од 103 анкетирани новинарки се соочиле со онлајн вознемирување*

17. Сексизам е верувањето дека мажите се супериорни во однос на жените и, врз основа на тоа верување, дискриминацијата врз основа на полот или родот се смета за оправдана. Во случаите кога ваквите верувања и дискриминација се широко распространети (на пример, во институциите или во медиумите), станува збор за системски сексизам.

18. United Nations. 2019. *United Nations Strategy and Plan of Action on Hate Speech.* Достапно на: https://www.un.org/en/genocideprevention/hate- speech-strategy.shtml

19. *Ibid.*

20. Gordon, S., 2020. *Slut-Shaming: The Scarlett Letter Of The 21St Century*.

21. Mantilla, K., 2013. "Gendertrolling: Misogyny adapts to new media". *Feminist studies*, 39(2), pp.563-570.

22. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

23. eSafety Commission Australia. *Online abuse targeting women*. Достапно на: https://www.esafety.gov.au/women/online-abuse-targeting-women

24. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

25. 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*. Достапно на: 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

26. Douglas. D. "Doxing: a conceptual analysis", *Ethics Information Technology*, vol. 18,(2016), pp. 199–210.
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.* Достапно на: https://www.thetimes.co.uk/article/new- australian-law-will-force-social-media-firms-to-unmask-trolls-tqchmf6k9

28. Извор: *Мери Јордановска, новинарка – „Говорот на омраза постојано се користи за да се дискредитираат новинарите и нивната работа" – Portret digital*

29. Извор: *https://mhc.org.mk/wp-content/uploads/2021/12/izvestaj-mk.pdf*

30. Flynn, A., Powell, A., and Hindes, S. 2021. *Technology-facilitated abuse: a survey of support services stakeholders* (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4- Flynn_et_al-TFa_Stakeholder_Survey.pdf
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.

31. Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders. (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_ Survey.pdf

32. Dictionary.com. Creepshot. Достапно на: https://www.dictionary.com/e/slang/creepshot/#:~:text=Creepshot%20typically%20refers%20to%20a,backside%2C%20legs%2C%20or%20cleavage.

33. Ryall, J. 2021. Japan records surge in upskirt photography, perverts 'bored' amid pandemic to blame, experts say. *South China Morning Post.* Достапно на: https://www.scmp.com/week-asia/lifestyle-culture/article/3150610/coronavirus-boredom-moves-japanese-perverts-upskirt

34. Cvetinčanin Knežević, Hristina. „Digitalno okruženje i rodno zasnovano nasilje – prilog proučavanju." *Antropologija (2020).*

35. Извор: *Во Северна Македонија, групата „Јавна соба" на „Телеграм" има повеќе од 6.500 членови и се споделени околу 10.000 фотографии и видеа.*

36. Cvetinčanin Knežević, Hristina. 2021. „'Someone's Daughter': Unpunished Revenge Porn's Terrifying Toll in The Balkans." *Balkan Insight.* Достапно на: https://balkaninsight.com/2021/10/18/someones-daughter-unpunished-revenge-porns-terrifying-toll-in-the-balkans/

37. Извор: *Полицаец од Велес уценувал сограѓанка и ја принудил на секс*

38. Dunn, S. "Technology-facilitated gender-based violence: An overview." Centre for International Governance Innovation: Supporting a Safer Internet Paper 1 (2020).

39. Selbie, T. and C. Williams. 2021. Deepfake pornography could become an 'epidemic', expert warns. *BBC*. Достапно на: https://www.bbc.com/news/uk-scotland-57254636

40. APC. 2020. *How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it.* Достапно на https://www.apc.org/en/pubs/research/ how-technology-being-used-perpetrate-violence-agai

41. 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.

42. 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.

43. Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_ Survey.pdf

44. Women's Media Centre. *WMC Speech Project: Online Abuse 101.* Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

45. Huet, N. 2022. Cyberflashing: People who send unwanted 'dick pics' will face jail under UK's new online safety law. *EuroNews.* Достапно на: https:// www.euronews.com/next/2022/03/14/cyberflashing-people-who-send-unwanted-dick-pics-will-face-jail-under-uk-s-new-online-safe

46. Ringrose, J. 2020. 'Staying Safe Online' survey: what unwanted sexual images are being sent to teenagers on social media?. *London's Global University.* Достапно на: 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/

47. National Society for the Prevention of Cruelty to Children. 2022. *Online grooming crimes have risen by more than 80% in four years.* Достапно на: https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/

48. Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_ Survey.pdf

49. Flynn, A., Powell, A., and Hindes, S. 2021. Technology-facilitated abuse: a survey of support services stakeholders (Research report, 02/2021). ANROWS. Достапно на: https://20ian81kynqg38bl3l3eh8bf-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/4AP.4-Flynn_et_al-TFa_Stakeholder_ Survey.pdf

50. Извор: *Пет лица сексуално злоупотребувале малолетничка во Велес и изготвувале порнографски материјал – Слободен печат*

51. APC. 2020. *How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it.* Достапно на https://www.apc.org/en/pubs/research/ how-technology-being-used-perpetrate-violence-agai

52. 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.

53. Brittany, A. "On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking", *Polaris,* 2018.

54. Radoičić, A. 2020. *Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju.* Достапно на: http://www.atina.org.rs/sites/default/ files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf

55. Radoičić, A. 2020. Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju. Достапно на: http://www.atina.org.rs/sites/default/ files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf

56. Douglas, D., "Doxing: a conceptual analysis", *Ethics Information Technology,* vol. 18, (2016), pp. 199–210.

57. Women's Media Centre. *WMC Speech Project: Online Abuse 101.* Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

58. Redakcija. ND. Sapštenje redakcije «Vremena» povodom pretnji Jovani Gligorijević. *Vreme*. Достапно на: https://www.vreme.com/projekat/sapstenje-redakcije-vremena-povodom-pretnji-jovani-gligorijevic/

59. Van der Wilk, A. 2018. *Cyber violence and hate speech online against women.* Study for the FEEM Committee. 52 eSafety Commission Australia. Catfishing. Достапно на: https://www.esafety.gov.au/young-people/catfishing

60. eSafety Commission Australia. Catfishing. Достапно на: https://www.esafety.gov.au/young-people/catfishing

61. Radoičić, A. 2020. *Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju.* Достапно на: http://www.atina.org.rs/sites/default/ files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf

62. Wikipedia. *Simon Leviev*. Достапно на: https://en.wikipedia.org/wiki/Simon_Leviev

63. 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

64. 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.

65. Women's Media Centre. *WMC Speech Project: Online Abuse 101.* Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

66. 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.

67. Radoičić, A. 2020. *Iza ekrana: analiza zloupotreba žrtava trgovine ljudima u digitalnom okruženju.* Достапно на: http://www.atina.org.rs/sites/default/ files/Iza%20ekrana%20Analiza%20zloupotreba%20%C5%BErtava%20trgovine%20ljudima%20u%20digitalnom%20okru%C5%BEenju.pdf

68. *Ibid.*

69.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*. Достапно на: http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

70. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

71. 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*. Достапно на: https://www.icfj.org/news/online-attacks-women-journalists-leading-real-world-violence-new-research-shows

72. Извор: *ДЕМНЕЛ И УЦЕНУВАЛ НА ФЕЈСБУК, А ПОТОА СИЛУВАЛ ТРИ ДЕВОЈЧИЊА, ДЕМНЕЊЕТО ПРВПАТ ВЛЕГУВА ВО ДВА*

73. Pen America, Online harassment field manual. Достапно на: https://onlineharassmentfieldmanual.pen.org/

74. Lončar, S. 2021. Kako internetski nasilnici napadaju novinarke. *Nezavisno udruženje novinara Srbije.* Достапно на: https://nuns.rs/kako-internetski- nasilnici-napadaju-novinarke/

75. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101

76. Dunn, S. "Technology-facilitated gender-based violence: An overview." *Centre for International Governance Innovation: Supporting a Safer Internet* Paper 1 (2020).

77. CBS News. 2011. New "Google Bomb" links murder to abortion. *CBS News.* Достапно на: https://www.cbsnews.com/news/new-google-bomb-links-murder-to-abortion/

78. Pen America, Online harassment field manual. Достапно на: https://onlineharassmentfieldmanual.pen.org/

79. Yang, W. 2021. China feminists face clampdown, closure of online accounts. *Deutsche Welle*. Достапно на: https://www.dw.com/en/china-feminism-free-speech/a-57277438

80. *Ibid.*

81. Amnesty International. 2020. Pakistan: Accusations of blasphemy continue to endanger lives. *Amnesty International*. Достапно на: https://www. amnesty.org/en/latest/news/2020/08/accusations-of-blasphemy-in-pakistan-continue-to-endanger-lives/

82. Phillips, W. "LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online." *First Monday* (2011).

83. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. **Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101**

84. Phillips, W. "LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online." *First Monday* **(2011).**

85. Women's Media Centre. *WMC Speech Project: Online Abuse 101*. **Достапно на: https://womensmediacenter.com/speech-project/online-abuse-101**

86. Pen America, *Online harassment field manual.* **Достапно на: https://onlineharassmentfieldmanual.pen.org/**

87. APC WRP. 2015. Take Action for #TakeBackTheTech and #ImagineAFeministInternet. *APC*. **Достапно на: https://www.apc.org/en/pubs/take-action-takebackthetech-and-imagineafeministin**

88. The Conversation 2020. *What is an algorithm? How computers know what to do with data.* **Достапно на: https://theconversation.com/what-is-an- algorithm-how-computers-know-what-to-do-with-data-146665**

89. Techopedia. 2012. *App.* **Достапно на: https://www.techopedia.com/definition/28104/app**

90. IBM. 2020. *Artificial Intelligence (AI)*. **Достапно на: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence**

91. BMC blogs. 2020. *Digital Platforms: A Brief Introduction.* **Достапно на: https://www.bmc.com/blogs/digital-platforms/#**

92. GBV AoR Helpdesk. 2021. *Learning Series on Technology-Facilitated Gender-Based Violence.* **Learning Brief 1: Understanding technology-facilitated GBV.**

93. 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.

94. Drone (UAV). 2019. IoT Agenda. Достапно на: https://internetofthingsagenda.techtarget.com/definition/drone

95. UNESCO Institute for Statistics. *Glossary: Information and communication technologies* **(ICT). Достапно на: http://uis.unesco.org/en/glossary**

96. Internet meme. 2022. Wikipedia. Достапно на: https://en.wikipedia.org/wiki/Internet_meme

97. OECD. 2019. An Introduction to Online Platforms and Their Role in the Digital Transformation. Достапно на: https://www.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en

98. Online Safety Act 2021 (Cth). No. 76, 2021. (Austl.)

99. Pen America, Online harassment field manual. Достапно на: https://onlineharassmentfieldmanual.pen.org/

VAW Learning Network. 2013. Technology-related Violence Against Women. Достапно на: http://www.vawlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

100. WhatIs.com. 2014. GPS tracking. Достапно на: https://whatis.techtarget.com/definition/GPS-tracking

101. TechTarget. 2021. *Spyware*. **Достапно на: https://searchsecurity.techtarget.com/definition/spyware.**

// ТВОЕТО ТЕЛО Е ТВОЕ,
И НА ИНТЕРНЕТ, И ВО ВИСТИНСКИОТ СВЕТ.