Univerza v Mariboru

Fakulteta za varnostne vede

Neža Flac

KIBERNETSKO NASILJE NAD ŽENSKAMI V SLOVENIJI

Magistrsko delo

Ljubljana, junij 2022

Univerza v Mariboru

Fakulteta za varnostne vede

KIBERNETSKO NASILJE NAD ŽENSKAMI V SLOVENIJI

Magistrsko delo

Študentka: Neža Flac

Študijski program: magistrski študijski program Varstvoslovje

Mentor: Prof. dr. Gorazd Meško

Lektorica: Larisa Trdina Bernik, univ. dipl. slovenistka in sociologinja

ZAHVALA

Najprej bi se rada zahvalila svojemu mentorju prof. dr. Gorazdu Mešku, za vse usmeritve in napotke pri pisanju magistrskega dela. Zahvaljujem se tudi za hitro odzivnost in prijazen odnos.

Rada bi se zahvalila tudi mojim staršem, za vso podporo in pomoč v času pisanja naloge. Zahvalila bi se jim tudi za vso finančno pomoč pri uresničitvi mojih ciljev.

Zahvala gre tudi mojemu fantu, ki mi je vse čas stal ob strani in prijateljem, med katerimi bi se še posebej rada zahvalila Nadji in Ladu za vse nasvete in pomoč.

Iskrena hvala tudi vsem sodelavkam za izkazano podporo in pomoč pri usklajevanju službe in šolanja. Zahvalila pa bi se rada tudi vsem ženskam, ki so bile pripravljene sodelovati pri intervjujih, saj brez njih magistrska naloga ne bi bila takšna, kot je.

Posebna zahvala pa gre tudi prijateljici Larisi, ki si je vzela čas za lektoriranje moje magistrske naloge.

Še enkrat iskrena hvala vsem za izkazano podporo in pomoč.

KIBERNETSKO NASILJE NAD ŽENSKAMI V SLOVENIJI

Ključne besede: kibernetsko nasilje, storilci, žrtve, kibernetski prostor in ženske

UDK: 343.615:316.356.2(497.4)

Povzetek

Spletno nasilje je nova oblika nasilja, ki v zadnjih letih narašča. Danes je to vse pogostejša dejavnost, ki prizadene različne skupine ljudi, med katerimi pa so najbolj izpostavljene osebe ženskega spola, ki so tudi najpogosteje žrtve. Spletno nasilje se nad njimi izvaja vsakodnevno in lahko za seboj pusti hude posledice, ki se s spletnega okolja lahko prenesejo tudi v realni svet. Prav zaradi takšnih razlogov je zelo pomembna pomoč žrtvam in nudenje zaščite. S tem, ko se žrtve počutijo varno, lahko tudi spregovorijo o svojih izkušnjah in s tem pomagajo in opogumijo druge osebe, da se izpovejo.

Ženske so žrtve različnih spletnih dejanj, med katerimi so zelo pogosta kazniva dejanja, ki vsebujejo neprimerno spolno vsebino. Velikokrat so prisiljene tudi izvrševati določene dejavnosti, saj jim v primeru upora sledijo grožnje in izsiljevanje.
Največkrat pa spletno nasilje izvajajo moški, ki si lastijo občutek moči in nadvlade nad ženskami. Pogosto menijo, da so glavni in da je kibernetski prostor namenjen le njim. Velikokrat želijo ženske izriniti in jih osramotiti. Največkrat pa moškim predstavljajo problem ženske, ki so bolj izobražene in bolj uspešne od njih. Moški storilci se pogosto skrivajo za lažnimi profili, preko katerih izvajajo nasilje. To je zanje nekakšna prednost, ampak se velikokrat ne zavedajo, da se tudi lažne profile da odkriti.
Zelo pomembno je tudi, da se žrtvam pomaga na različne načine, za kar skrbijo različne organizacije in osebe. Pomoč pa jim nudijo na različne načine, ki žrtvam olajšajo določene situacije.

Velik pomen pred tem, da postanemo žrtve spletnega nasilja, pa imajo tudi najrazličnejši preventivni ukrepi, s katerimi že sami veliko storimo za našo varnost.

Pomembno za zaščito pa je tudi, da o dejavnostih, ki jih izvajamo na spletu dobro premislimo in se prepričamo, da je stvar, ki jo želimo izvesti primerna in si to želimo. Važno pa je tudi, da si vzamemo čas in o stvareh dobro premislimo in da podatke delimo le z osebami, katerim zaupamo, ostalim pa omejimo ali preprečimo dostop do njih.

CYBERVIOLENCE AGAINST WOMEN IN SLOVENIA

Keywords: cyber violence, attackers, victims, cyberspace and women

UDC: 343.615:316.356.2(497.4)

Abstract

Cyber violence is a new form of a violence that occurs in cyber space and grows quickly every day. Today this is a very common activity, that hurts a lot of different groups of people, but the victims who suffer the most are women. Cyber violence against them is occurring every day and it can leave consequences on them, which can be very tough and hurtful and the consequences can also be seen in real world. Because of that it is necessarily to help those victims and give them all the protection they need. With these types of help, we can make them feel safer and protected.

Women are victims of different cyber-attacks, but the most common attacks are connected with unappropriated sexual content. In many cases they are forced to perform different activities, because if they do not obey them, they will be punished and blackmailed.

The most common cyber attackers are men, who own a feeling of a power. In a lot of cases they think they can overpower women. Usually they have a mind, that they are the most important and are main characters in cyberspace. In a lot of cases they want to embarrass women. Usually the problem for men is higher educated and more successful women, who are threat to them. They want to evict them from cyberspace. Men often create fake social media profiles, from where they perform different attacks. Fake profiles give them a special power and advantage, but sometimes it is not all good things. Even fake profiles can lead police to discover the real persons behind all this.

It is very important that different organisations and people help victims and protect them. The help can be provided in many ways and they can make victims feel better.

The big meaning have preventive measures, which can help us not to become victims of cyber violence. We can do a lot by ourselves to protect our safety. It is very important that we think twice before we post something online or preform some actions. It is also important that we protect our information and data and not trust everyone.

KAZALO VSEBINE

1 UVOD

Danes živimo v času, ko je kriminaliteta prisotna na skoraj vsakem koraku. Zadnja leta je bilo mogoče opaziti upad tradicionalnih oblik kriminalitete in zmanjšanje števila njenih žrtev. Statistični podatki policije za Slovenijo kažejo, da so leta 2011 policisti zabeležili približno 77 000 kaznivih dejanj klasične kriminalitete, leta 2020 pa približno 46 000, kar je 31 000 kaznivih dejanj manj (Urbas, 2021).

Kasnejše raziskave so pokazale, da temu ni povsem tako in, da se je kriminal prestavil le v novo okolje – kibernetski prostor, kjer ljudje vsakodnevno preživimo veliko časa (Leukfeldt in Weijer, 2017). Tudi različne študije so potekale na temo iskanja podobnosti in razlik med tradicionalno in kibernetsko kriminaliteto. Glavno vprašanje pa je, če se pojavljajo novi storilci kibernetskega kriminala, ali če so stari storilci samo zamenjali svoje okolje (Leukfeldt idr., 2022).

Največkrat so za primerjanje tradicionalne in kibernetske kriminalitete analizirali njihove storilce. Za storilce klasične kriminalitete je značilno, da so to pogosteje moški, ki imajo nižji ekonomsko-statusni položaj, so manj inteligentni, bolj maščevalni, nepotrpežljivi in da so v nekaterih primerih to osebe, ki nimajo urejenega življenja in so zaradi tega bolj izpostavljene tveganjem, da postanejo kriminalci. Na drugi strani pa so storilci spletnega nasilja, ki so najpogosteje izobraženi moški iz premožnih družin. Seveda se pojavljajo tudi odstopanja in lahko tudi zelo inteligentne osebe storijo zločine tradicionalne oblike in tudi manj inteligentne osebe lahko izvedejo preproste kibernetske napade (Leukfeldt idr., 2022).

Na izvedbo nasilja naj bi vplivalo tudi pet lastnosti, te pa so odprtost, vestnost, ekstravertiranost, sprejemljivost in nevroticizem. Prav teh pet lastnosti naj bi bilo ključnih pri definiranju osebnosti ljudi in njihovih značilnosti, vsak posameznik pa vsebuje različno stopnjo teh lastnosti, ki ga oblikujejo (Cherry, 2021).

Poleg osebnostnih značilnosti na obliko kriminalitete vpliva tudi okolje, kjer se osebe vsakodnevno nahajajo in krog ljudi, s katerimi se družijo. Za osebe, ki se družijo s prestopniki ali drugimi sumljivimi osebami obstaja velika verjetnost, da tudi sami nekega dne postanejo deviantni (Leukfeldt in Weijer, 2017).

Danes ima že skoraj vsak posameznik mobilno napravo in zna uporabljati internet. Raba takšnih naprav mnogim uporabnikom predstavlja način življenja, saj so se skoraj vse glavne dejavnosti prenesle na splet. Mobilne naprave se nenehno povezujejo v kibernetski prostor, kjer poteka komunikacija med računalniškimi omrežji. Uporabniki internet in kibernetski prostor lahko uporabljajo za delo, nakupovanje, bančništvo, iskanje informacij, šolanje in zabavo (Choudhury in Malik, 2019).

Prav s prenosom teh aktivnosti na spletna okolja, je raba interneta v zadnjih letih močno narasla, kar potrjujejo tudi podatki, pridobljeni s pomočjo različnih raziskav. Podatki za leto 2021 kažejo, da je v Sloveniji takrat internet redno uporabljalo 89 % ljudi. Največjo uporabo interneta so zasledili pri osebah starih med 16 in 24 let, najmanjšo uporabo pa pri osebah med 65 in 74 let. Največkrat osebe do interneta dostopajo preko pametnih telefonov (Mlakar, 2021).

Kljub velikim prednostim, ki jih je internet prinesel ljudem, pa je mogoče zaznati tudi kar nekaj njegovih slabosti (Choudhury in Malik, 2019). Ena izmed glavnih in tudi nevarnejših slabosti je zagotovo prenos kriminalitete v kibernetski prostor. Danes se kibernetska kriminaliteta vsakodnevno povečuje, saj ima kibernetski prostor vsak dan več uporabnikov (Bernik in Meško, 2011).

Ta se je predvsem povišala v času epidemije Covid-19, ko se je večina opravil prenesla na spletna okolja. Najpogostejši napadi, ki so jih v Sloveniji zaznale organizacije, ki se ukvarjajo s kibernetsko varnostjo so bili phishing napadi, izsiljevanja, grožnje in okužba

naprav s škodljivimi virusi (»Covid-19 je okrepil trend rasti kibernetskih napadov«, 2020).

Kibernetsko kriminaliteto strokovnjaki delijo na tri večja področja, kar jim omogoča lažjo klasifikacijo posameznih kaznivih dejanj v določeno skupino. V prvo skupino uvrščajo napade, kjer se računalniki storilcev kaznivih dejanj uporabljajo za ciljne napade, kar pomeni, da s pomočjo lastnih računalnikov napadejo računalnike žrtev. V drugo skupino uvrščajo računalnike, ki se uporabljajo kot orodje za izvajanje napadov. V tretjo skupino pa se uvršča raba računalnikov kot dodatno opremo, s katero se lahko izvaja škodovanje uporabnikom (Sukhai, 2004).

Kibernetsko kriminaliteto uvrščamo med novejše oblike kriminalitete in zaradi tega mnogo uporabnikov ne ve, da jim takšna oblika kriminalitete lahko škodi in ima zanje hude posledice (Žakelj, 2013). Veliko uporabnikov interneta ima mišljenje, da so zaščiteni pred kibernetskimi napadi in da se kaj takšnega njim ne more pripetiti in zaradi takšnega mišljenja premalo pozornosti namenijo zaščiti (Alshalan, 2006).

Na internetu je mogoče zaslediti tudi veliko spletnega nasilja nad ženskami, ki so pogosteje žrtve spletnega nasilja kakor moški, kar kaže na to, da se tudi na spletnem okolju velikokrat pojavlja neenakost med spoloma (Klun in Meško, 2017; Petek, 2019a). Ženske že same po sebi veljajo za nežnejše in s tem izkazujejo tudi večji strah pred kriminaliteto, na kar pa imajo vpliv viktimizacija, socializacija in spomin (Klun in Meško, 2017).

Najpogostejši napadi, ki se dogajajo ženskam na spletu so različna nadlegovanja, flaming, prevare, grozilna in izsiljevalna pisma, e-mačizem, seksistični komentarji, spolna nadlegovanja in sexting (Petek, 2019a; Sedej in Završnik, 2011). Največkrat pa se spletno nasilje nad ženskami izvaja preko različnih socialnih omrežij (Facebook, YouTube, Twitter in e-pošta). Spletno nasilje lahko na žrtvah pusti zelo hude posledice, ki jih zaznamujejo celo življenje. Posledice, ki jih pusti za seboj so lahko finančne,

psihološke, socialne in fizične, pogosto pa se pojavljajo tudi težave z zdravjem (West, 2014).

Storilci se odločajo za izvajanje spletnega nasilja iz razloga, da to lahko počnejo v udobju svojega doma. Storilci se pri izvajanju spletnega kriminala počutijo varno, udobno in zaščiteno (Brodnik, 2015). Izvajanje spletnega kriminala je v večini primerov zelo enostavno (West, 2014).

Za žrtve spletnega kriminala je zelo pomembno, da spregovorijo o svojih izkušnjah in si poiščejo ustrezno pomoč. Žrtve se v primerih spletnega nasilja lahko obrnejo na policijo ali na druge organizacije, ki jim bodo pomagale v takšnih primerih (Bulatović, 2017).

Policija in druge organizacije za pomoč žrtvam spletnega nasilja uporabljajo za kaznovanje storilcev spletnega nasilja različne zakone in konvencije. Najpomembnejša je konvencija o kibernetskem kriminalu, ki policiji in drugim organizacijam nudi vpogled v različne vrste kibernetskih kaznivih dejanj in kako kaznovati storilce za izvršeno določeno kaznivo dejanje (»Konvencija o kibernetski kriminaliteti«, 2004).

Za prihodnost pa je zelo pomembno, da žrtve spregovorijo o svojih izkušnjah in na ta način opozorijo uporabnike na to, da tudi sami lahko hitro postanejo žrtve kibernetskega kriminala. Potrebno je uporabnike tudi ozavestiti in poučiti o tem, kako nevaren je lahko kibernetski kriminal. Uporabnikom je potrebno predstaviti tudi preventivne ukrepe, ki jim pomagajo pri zaščiti, da postanejo žrtve spletnih storilcev in spletnih napadov (Bernik in Meško, 2011).

1.1 Namen in cilji magistrske naloge

Glavni namen magistrske naloge je ugotoviti, kdo so največkrat žrtve spletnega nasilja in kdo so največkrat njegovi povzročitelji. Cilj, ki smo si ga zastavili je tudi, da

ugotovimo, kateri so najpogostejši spletni napadi na ženske in kaj ima na to vpliv. Zanima nas tudi to, (če) kakšni odločilni dejavniki vplivajo na vrsto nasilja. S pisanjem naloge in prebiranjem literature želimo tudi izvedeti, če spletno nasilje na žrtvah pusti hude posledice, ali se takšne oblike nasilja preprosto pozabijo. Želimo izvedeti tudi, če se lahko nasilje prenaša iz spletnega okolja v fizični svet in obratno. Kot cilj naloge je tudi pridobiti podatke o tem, če se v Sloveniji dogajajo in pojavljajo enake oblike spletnega nasilja kot drugje po svetu. Zanima nas tudi, kakšen vpliv ima zakonodaja na reševanje primerov spletnega nasilja in na sankcioniranje storilcev. Radi pa bi izvedeli tudi, če se na spletu pojavljajo novi storilci, ki prej niso izvrševali kaznivih dejanj, ali pa če so stari storilci samo zamenjali svoje okolje delovanja.

1.2 Hipoteze magistrske naloge

Pred pisanjem magistrske naloge smo določili pet hipotez, ki jih želimo preveriti s pomočjo literature in intervjujev.

Hipoteza 1: Kibernetska kriminaliteta je v zadnjih letih postala ena izmed najbolj razširjenih oblik kriminalitete in se z vsakim dnem bolj razvija in narašča.

Hipoteza 2: Posledice kibernetskega nasilja so vidne tudi v realnem svetu zunaj kibernetskega prostora.

Hipoteza 3: Najpogostejši izvajalci spletnega nasilja nad ženskami so moški.

Hipoteza 4: Zaradi anonimnosti na spletu je kibernetsko nasilje lažje izvedljivo in storilce je težje odkriti.

Hipoteza 5: Storilci kibernetskega kriminala so bolj pogumni in se počutijo varneje pri izvajanju spletnega nasilja, saj so mnenja, da na spletu lahko počnejo kar si želijo brez omejitev.

1.3 Uporabljene metode pri zaključnem delu

Pisanje magistrskega dela smo razdelili na dva dela. V prvem delu smo izbrali deskriptivno metodo pisanja naloge, kar pomeni, da smo iskali in prebrali ustrezno literaturo, katere glavne ugotovitve in značilnosti smo kasneje zapisali. Pri tej metodi smo uporabili različne vire v slovenskem in tujem jeziku. S pomočjo te metode smo tudi izpisali potrebno vsebino, ki nam je koristila za potrjevanje ali zavračanje hipotez.

Za drugi, eksperimentalni del magistrske naloge smo si izbrali intervju, ki je kvalitativna metoda raziskovanja. Intervju smo si izbrali zaradi najbolj osebnega pristopa, saj na takšen način največ izvemo o sami žrtvi in njenih izkušnjah. S pomočjo intervjujev smo dobili še informacije iz prve roke, ki so nam kasneje pomagale pri hipotezah. Z intervjuji smo dobili tudi v pogled v človeško raznolikost in videli, kako različno ženske prenašajo spletno nasilje. Ta metoda nam je bila v veliko pomoč, s katero smo izvedeli veliko novega in tudi to, kakšno težo v resnici nosi spletno nasilje. Najbolj pa nas je zanimala povezava med žrtvami, storilci in posledicami spletnega nasilja.

2 KIBERNETSKO NASILJE

Kibernetska kriminaliteta je novejša vrsta kriminalitete, za katero so značilna kazniva dejanja, ki se izvajajo v kibernetskem prostoru, kar predstavlja virtualni svet, ki med seboj povezuje vse računalnike in omrežja v enoten prostor (Završnik, 2015). Zanjo je značilno tudi to, da se zelo hitro širi in da se vsakodnevno pojavljajo nove oblike kaznivih dejanj, zaradi katerih jo zagotovo uvrščamo med najbolj nevarne in škodljive oblike kriminalitete v današnjem času. Danes je veliko dela usmerjenega v smer, da se nadgradi varnostne ukrepe za njeno omejitev (Dimc in Dobovšek, 2012).

Kibernetska kriminaliteta nima točno določene ene definicije, ampak zajema več dejavnikov, ki se delijo v skupine, v vsaki pa so zajeta različna kazniva dejanja, ki nakazujejo na kibernetsko kriminaliteto. V prvo skupino uvrščamo kazniva dejanja zoper dostopnost, celovitost in zaupnost podatkov uporabnikov. Sem sodijo kazniva dejanja kjer gre za protipravne dostope do naprav in uporabniških podatkov, motenje naprav ter različna protipravna prestrezanja. V drugo skupino uvrščamo kazniva dejanja, kjer je potrebna uporaba računalnika za njihovo izvršitev. Kot primer kaznivega dejanja v tej skupini so različne računalniške goljufije. Naslednja, tretja skupina vsebuje kazniva dejanja, ki so povezana z vsebino različnih podatkov in informacij. Sem sodijo največkrat vsebine, ki so povezane s pornografijo. V zadnji, četrti skupini pa so kazniva dejanja, kjer se kršijo različne vrste pravic (Završnik, 2015).

V kibernetsko kriminaliteto pa uvrščamo tudi spletno nasilje, ki se dogaja v kibernetskem prostoru. Kibernetski prostor je sestavljen iz različnih virtualno-omrežnih komponent, ki nam omogočajo uporabo in iskanje po svetovnem spletu (Cyberspace, n. d.). Prav zaradi nasilja preko interneta se uporablja izraz spletno nasilje (Završnik, 2013). Nasilje se lahko preko spleta pojavlja v različnih oblikah, tudi storilci in žrtve so lahko vsi uporabniki interneta ne glede na njihovo starost, spol ali druge značilnosti (Center za varnejši internet, n. d. a).

V zadnjih nekaj letih lahko zasledimo veliko porast različnih socialnih omrežij. Ljudje socialna omrežja uporabljamo za različne namene, največkrat jih uporabljamo za medsebojno komunikacijo, kjer si izmenjujmo različne podatke in nasvete. Določene socialne platforme nam omogočajo iskanje in urejanje informacij, ki nas zanimajo (Densley in Peterson, 2017). Obstajajo različni blogi in druge spletne strani, kjer lahko vsak najde informacije o temi, ki nas zanima, lahko pa tudi sami napišemo določen prispevek o temi, na katero se spoznamo. Veliko oseb uporablja socialna omrežja za zabavo in poslušanje glasbe ali gledanje video vsebin. Določeni uporabniki socialna omrežja uporabljajo tudi za delo. Preko socialnih omrežij se povežejo z različnimi podjetji, preko katerih promovirajo njihove izdelke in na takšen način dosežejo ljudi, da kupijo določen izdelek, sami pa za takšno promocijo dobijo določeno plačilo (Bhasin, 2018). Najpogostejša socialna omrežja, ki pa jih ljudje uporabljamo pa so Facebook, YouTube, WhatsApp, Facebook Messenger, Instagram, TikTok, Snapchat in druge (Karl, 2021).

Različne študije so pokazale, da se preko socialnih omrežij odvija največ spletnega nasilja, seveda pa se spletno nasilje lahko odvija tudi preko SMS ali MMS sporočil, preko iger, klepetalnic in forumov (Center za varnejši internet, n. d. a; Matijašič, 2021). Spletno nasilje lahko definiramo kot štiri vrste kaznivih dejanj med katere sodijo zavajanja in kraja podatkov, pornografija, nasilje in druge kibernetske kršitve. Uporabniki socialnih omrežij so tudi različni člani tolp, preprodajalci drog ali drugi skrajneži, ki preko socialnih omrežij iščejo nove člane, ki bi se jim pridružili pri njihovem delu. Preko socialnih omrežij tudi rekrutirajo in učijo na novo pridobljene člane za opravljanje nalog, ki jih od njih zahtevajo vodje. Največkrat pa ti skrajneži pridobijo člane s pomočjo različnih laži in prevar, ter s praznimi obljubami o boljšem življenju (Densley in Peterson, 2017).

Preko socialnih omrežij je mogoče zaslediti veliko različnih vrst nasilja, med katerimi se pojavljajo čisto nove oblike odklonskega vedenja, ki jih je mogoče zaslediti le na spletu (Densley in Peterson, 2017). Najpogostejša kazniva dejanja, ki pa se pojavljajo na

spletu pa so širjenje laži o nekom, pošiljanje sporočil z neprimerno vsebino (največkrat gre pri tem za sporočila s spolno vsebino), pošiljanje neprimernih video vsebin, pisanje žaljivih in neprimernih komentarjev, različne grožnje, izsiljevanja, vdori v profile na socialnih omrežjih in ustvarjanje lažnih profilov (Novaković, 2019).

Spletno nasilje je še posebej nevarno, saj lahko že najmanjši komentar, ki na videz ne deluje nevarno, v žrtvi povzroči neprijetno počutje. Vsa dejanja spletnega nasilja pustijo za seboj resne posledice, ki se lahko prenesejo iz virtualnega v realni svet (Bohinec, 2021; Center za varnejši internet, n. d. a). Mnogokrat žrtve ne znajo ali si ne upajo priznati, da so bile žrtve spletnega nasilja in da jih takšna dejanja spravljajo v neprijeten položaj. Pri žrtvah spletnega nasilja se lahko pojavi depresija, tesnoba, želja po samopoškodovanju, ki pa včasih pripelje žrtve tudi do samomora (Center za varnejši internet, n. d. a; Matijašič, 2021). Tudi priče spletnega nasilja lahko ukrepajo in prijavijo žaljive in neprimerne komentarje ali objave. Če pa gre za zelo resno nasilje je o tem potrebno obvestiti policijo ali druge organizacije za pomoč žrtvam spletnega nasilja (Center za varnejši internet, n. d. a).

2.1 Predstavitev osnovnih pojmov in njihova definicija

Prva definicija, ki si jo bomo pogledali je **mobilna naprava,** za katero je značilno, da je to prenosna naprava, ki ima prilagojen operacijski sistem (Android, iOS in Windows) (Center za varnejši internet, n. d. b). V skupino mobilnih naprav, bi lahko uvrstili tudi vse naprave, ki se brezžično povezujejo v internet (Center za varnejši internet, n. d. b).

Poleg teh značilnosti za vse mobilne naprave velja tudi dolga moč baterij, tipkovnica za vnašanje podatkov, večina mobilnih naprav ima možnost zaslona na dotik, omogočena je uporaba različnih aplikacij in prenos podatkov z interneta, majhnost in lahkotnost, da uporabniki lahko kjer koli in kadarkoli uporabljamo takšne naprave in uporaba virtualnih pomočnikov, ki olajšajo nekatere dejavnosti uporabnikom. Med

najpogostejše mobilne naprave sodijo prenosni računalniki, pametni telefoni in tablični računalniki (Viswanathan, 2022).

Internet je ogromen mrežni sistem, ki med seboj povezuje računalnike in druge naprave po celem svetu. Internet za svoje delovanje uporablja protokol TCP/IP, ki omogoča prenos podatkov iz različnih medijev. Preko interneta si ljudje izmenjujemo informacije in lahko komuniciramo med seboj s pomočjo internetne povezave. Internet se prvič pojavi v Ameriki okoli leta 1970, ampak se je njegova uporaba začela šele okoli leta 1990 , danes pa internet uporablja že polovica celega sveta (Dennis, 2022).

Internet sestavljajo tri glavne skupine, ki so površinski internet, ki ga lahko uporablja vsak in tudi dostop do njega ni zahteven. Druga stopnja je *deep web*, kjer se nahajajo informacije, do katerih ne more dostopati čisto vsak. Do določenih podatkov v globokem spletu lahko dostopajo samo osebe, ki imajo za to dovoljenje (zdravniki, astronavti in kibernetski kriminalci). Do globokega spleta se lahko dostopa le preko posebnih operacijskih sistemov imenovanih *The Onion Router* ali *Tor* (Schober, 2015). Tretja skupina pa je *dark web*, na katerem se skrivajo temne stvari interneta in tam je mogoče najti zelo zanimive informacije, med katerimi je tudi veliko ilegalnih in bizarnih stvari (Torres, 2021).

Socialno omrežje sestavljajo internetni kanali, ki uporabnikom omogočajo medsebojno komunikacijo in izmenjavo informacij v realnem ali asinhronem času. Socialna omrežja temeljijo na določenih algoritmih, ki spremljajo vedenje ljudi na podlagi katerih se sama socialna omrežja nenehno spreminjajo in nadgrajujejo (Carr, 2015).

Danes ima že skoraj vsak uporabnik interneta vsaj en profil na socialnih omrežjih, ki ga pogosto uporablja. Med najpogostejša socialna omrežja, ki jih uporabljamo sodijo Facebook, Twitter, Snapchat, TikTok, Instagram in še mnoga druga (Karl, 2021).

Seksizem je izraz, ki se uporablja za mišljenje ljudi, ki zapostavljajo pripadnike določenega spola, najpogosteje gre za zapostavljanje žensk in za poveličevanje moških (Seksizem, 2014). Seksizem pogosto vodi v diskriminacijo in posledica tega je tudi nemožnost uspeha zaničevanega spola v določenih dejavnostih v družbi (Novaković, 2019).

Mizoginija ali ženskosovražnost je oblika seksizma, kjer je poudarjen sovražni odnos do žensk. Ta oblika seksizma pogosto vsebuje še dodatne elemente, ki spodbujajo močno sovraštvo in nenaklonjenost do žensk (Novaković, 2019).

Viktimizacijo lahko definiramo kot posebno obliko diskriminacije (Kraskova, 2017). Gre za izpostavljanje žrtve še dodatnim nevšečnostim (Viktimizacija, 2014). Beseda viktimizacija izvira iz glagola *victimize*, ki pomeni, da nekdo postane žrtev, izkusi trpljenje ali da postane žrtev različnih nevšečnosti (Kanduč, 2003).

2.2 Kibernetski prostor

Kibernetski prostor ali *cyberspace* je virtualni prostor, v katerem potekata komunikacija in delo med uporabniki (Dimc in Dobovšek, 2012). Gre za prostor, kjer so med seboj povezane mobilne in druge naprave, ki podpirajo internet (Bussell, 2013). Leta 1982 je pisatelj William Gibson prvi uporabil izraz kibernetski prostor v svojem delu Nevromant, predpona »*kiber*« pa izvira iz Grškega jezika in označuje besedo krmar (Bussell, 2013; Pajtler, 2002).

Za določitev kibernetskega prostora ne obstaja enotna definicija. V Sloveniji uporabljamo za definiranje kibernetskega prostora dva dokumenta, v katerih je zajeta struktura kibernetskega prostora in sicer sta to Zakon o informacijski varnosti in Strategija kibernetske varnosti (Štrucl, 2020).

Kibernetski prostor sestavljajo fizični, logični in socialni sloj. V fizični sloj uvrščamo omrežne komponente in naprave, ter geografske točke (države in kraje), v logičnem

sloju se nahajajo logične omrežne komponente in v zadnjem, socialnem sloju lahko najdemo ljudi in virtualne osebe. Vse te tri skupine skupaj tvorijo celoto, kjer so vse te komponente med seboj povezane. Kibernetski prostor pripada skupini, ki se imenuje informacijsko okolje, katerega tvorijo tudi socialna omrežja (Štrucl, 2020).

Izraz kibernetski prostor se je uporabljal že na samem začetku, ko so se začeli razvijati telefoni, saj je že takrat potekala komunikacija med prostori, ki se jih fizično ni dalo videti. Telefonska komunikacija je bila nekakšen predhodnik interneta in kibernetskega prostora, kot ga poznamo danes. Glavna sprememba kibernetskega prostora se vidi v tem, da je narasla njegova velikost, povečalo se je število uporabnikov, saj v današnjih časih že skoraj vsi uporabljamo internet. Število uporabnikov interneta je iz leta 2000 močno naraslo in je konec leta 2010 predstavljalo kar dve milijardi uporabnikov po celem svetu. Danes ljudje uporabljamo kibernetski prostor in internet predvsem za igranje iger, iskanje informacij, uporabo različnih aplikacij in za iskanje prijateljev ali ljubezni (Dimc in Dobovšek, 2012).

Kibernetski prostor uporabnikom prinaša veliko prednosti in tudi kar nekaj slabosti, katerih posledice lahko opazimo tudi v realnem, fizičnem svetu (Dimc in Dobovšek, 2012). Pozitivne stvari in prednosti, ki nam jih prinaša in omogoča kibernetski prostor so novi prijatelji, potovanja, lažje iskanje in pridobivanje informacij, enostavnejša komunikacija z ljudmi z drugega konca sveta, različna socialna omrežja in pa zabava, ki jo omogoča in ponuja internet (Dimc in Dobovšek, 2012; Vapulus, 2018).

Glavna slabost, ki se je pojavila s širitvijo in razvojem kibernetskega prostora je razvoj kibernetske kriminalitete in pojavljanje kibernetskega nasilja. Pojavljajo se nove, nepoznane oblike kaznivih dejanj, ki povzročijo veliko škodo pri uporabnikih. Gre za odklonska vedenja, kjer je ogrožena varnost uporabnikov in njihovih naprav, za različne viruse, ki lahko napadejo napravo in s tem nepooblaščeno pridejo do podatkov in za različna nadlegovanja in zasledovanja uporabnikov (Dimc in Dobovšek, 2012; Vapulus, 2018).

2.3 Oblike spletnega nasilja

Kibernetski kriminal se je danes zelo razširil in se vsakodnevno pojavljajo različne oblike spletnih napadov in odklonskih vedenj. Takšna odklonska vedenja so lahko zelo nevarna za uporabnika in pa tudi za njegove naprave. Poznamo več različnih oblik kibernetskih odklonskih vedenj, med katerimi so pogostejša:

Blackmail in extortion (Izsiljevanje) je zelo pogosta oblika spletnega nasilja. Velikokrat gre za primere, kjer izsiljevalci žrtve izsiljujejo za gole fotografije ali druge intimne posnetke. Poleg izsiljevanja s spolno vsebino, gre tudi za izsiljevanje z informacijami. Storilci velikokrat grozijo, da bodo informacije neke osebe posredovali javnosti, družini, prijateljem ali drugim osebam (Johnson, n. d.).

Cyberstalking (spletno zalezovanje) je zelo resna težava, saj lahko spletno zalezovanje postane tudi fizično in za seboj pusti hude posledice. Pri tem gre za ponavljajoča se spletna sporočila z grozilno ali nadlegovalno vsebino, katerih namen je prestrašiti žrtev. Pri tej obliki nadlegovanja se storilci lahko spravijo tudi na žrtvine prijatelje in družino (Bohinec, 2021; Johnson, n. d.).

Doxing je dejanje, kjer storilec razkriva osebne podatke oseb, brez da bi te dovolile objavo teh podatkov. Gre za to, da storilci poznajo določene podatke oseb, ki jih objavijo brez soglasja (Center za varnejši internet, n. d. a)

Flaming je oblika spletnega nasilja, za katerega je značilna izmenjava sovražnih misli ali besedil med dvema ali več uporabniki informacijsko-komunikacijske tehnologije. Flaming se pogosto pojavlja v spletnih klepetalnicah in forumih, ki dajejo zaščito uporabnikom za bolj nasilno vedenje (Žakelj, 2013).

Fotografiranje in snemanje ter objavljanje teh posnetkov brez dovoljenja (oseb, ki so na posnetkih) je oblika spletnega nasilja, kjer storilci brez dovoljenja snemajo določne

osebe in to objavljajo na internet brez njihovega dovoljenja (Center za varnejši internet, n. d. a).

Happy slaping predstavljajo posnetki pretepov ali drugih vrst nasilja. V teh primerih očividci snemajo pretepe/nasilje, ki se dogaja in to objavljajo na različnih spletnih portalih. V takšnih primerih žrtev zelo trpi in velikokrat izpade kot tarča posmeha. Žalostno je, da se očividci ne postavijo na žrtvino stran in ji ne pomagajo, temveč jo snemajo in se ji posmehujejo (Žakelj, 2013).

Izključevanje iz skupin pomeni, da skupina izključi posameznika iz neke skupine ali pogovora, včasih pa določenim uporabnikom celo preprečijo vstop v skupino preko različnih spletnih kanalov (Center za varnejši internet, n. d. a).

Kraja gesel je, ko storilci pridobijo nepooblaščen dostop do gesel. Kasneje lahko ta gesla uporabijo in posledično vdrejo v tuj profil in si pridobijo podatke tujih oseb (Center za varnejši internet, n. d. a).

Lažni profili se ustvarjajo z namenom, da se določene osebe izdajajo za nekoga drugega, kot pa so v resnici. Preko lažnih profilov lahko objavljajo različne vsebine, ki se nekaterim ne zdijo neprimerne, lahko pa tudi objavljajo neprimerne komentarje in širijo sovražni govor (Novaković, 2019).

Obrekovanje ima enak pomen kot v fizičnem svetu, le da se tukaj laži in lažne govorice širijo po spletu in socialnih omrežjih. Lahko gre tudi za to, da se lažne govorice širijo v realnem svetu, nato pa se prenesejo še na spletno okolje (Novaković, 2019).

Online harassment (spletno nadlegovanje) je spletna diskriminacija ali nadlegovanje določene osebe ali celo določene skupine. Velikokrat se osebe nadleguje zaradi njihovega spola, različnih ovir/napak, spolne usmerjenosti, vere ali zaradi rasne

pripadnosti. Spletno nadlegovanje se lahko odvija preko SMS sporočil, socialnih omrežij, e-pošte, ali drugih spletnih platform (Johnson, n. d. ; Žakelj, 2013).

Phishing ali po slovensko ribarjenje je oblika kibernetskega napada, za katerega je značilno lažno predstavljanje oseb. Največkrat se phishing napadi izvajajo tako, da storilec pošlje elektronsko pošto žrtvi, ki vsebuje povezavo do spletne strani, kjer se zahtevajo podatki od oseb in jih na takšen način pretentajo in ukradejo podatke. Deluje tako, da hekerji ustvarijo klon originalne spletne strani in lažno povezavo pošiljajo ljudem v upanju, da odprejo povezavo. Obstaja tudi več vrst napadov, kot so *email phishing*, ki so namenjeni širši populaciji, *spear phishing*, ki je usmerjeno na točno določeno osebo, *whaling*, kjer so napadi usmerjeni na točno določeno eno osebo, ki je največkrat vodja, direktor ali lastnik neke ustanove ali organizacije in *vishing*, kar so phishing napadi izvedeni preko telefona ali SMS sporočila (Al-Nemrat idr., 2014; Fruhlinger, 2020).

Poosebljanje je oblika, kjer se storilec pretvarja, da je žrtev in s tem uporablja njena gesla in socialna omrežja, preko katerih kasneje objavlja neprimerne fotografije ali zapise. S tem, ko storilec pridobi dostop do žrtvinega profila lahko tega tudi spreminja in upravlja kot svojega (Žakelj, 2013).

Predelava fotografij pomeni uporabo programov za spreminjanje slik, kjer lahko storilci spreminjajo ali preoblikujejo žrtvine fotografije, lahko pa tudi njihove obraze ali druge dele telesa izrežejo in jih nato prilepijo na neko drugo fotografijo (Center za varnejši internet, n. d. a).

Seksting je oblika spletnega nasilja, ki se je pojavila v zadnjih desetih letih in pomeni objavljanje oz. širjenje fotografij ali drugih vsebin povezanih s spolnostjo. Takšne fotografije se pošiljajo preko mobilnih naprav ali preko družbenih omrežij. Za seksting je značilno to, da takšne vsebine ne pošiljajo osebe, ki so na posnetkih, ampak to pošilja nekdo drug (Žakelj, 2013).

Socialni inženiring je manipulativna tehnika, ki izkorišča napake ljudi za pridobitev osebnih podatkov. Gre za to, da storilci vzpostavijo stik z žrtvijo in pridobijo njihovo zaupanje, ki ga na koncu izkoristijo in pridobijo svojo korist. Velikokrat gre za to, da storilci žrtvam predajo okužene USB ključke, ki onemogočijo delovanje računalnika. To storijo tako, da se žrtvi zlažejo, da ključki vsebujejo pomembne informacije zanje (Kaspersky, 2022; Kogovšek, 2021).

Sovražne skupine so skupine, ki so ustanovljene z namenom širjenja sovraštva med drugimi preko spleta. Takšne skupine želijo privabiti člane le zato, da se njihova ideja o sovraštvu razširi kolikor se to le da (Center za varnejši internet, n. d. a).

Spletni grooming je navezovanje stikov odraslih oseb z otroki. Glavni namen takšnega vedenja je ta, da otroke spolno zlorabijo na različne načine (Center za varnejši internet, n. d. a).

Trolanje se pojavi v primerih objavljanja žaljivih in sovražnih sporočil na spletu. Glavni namen takšnega odklonskega vedenja je provokacija ali pridobivanja pozornosti (Center za varnejši internet, n. d. a).

Vdor v račune ali profile je zelo nevarna stvar, kjer storilci z nepooblaščenim dostopom vdrejo v določen sistem ali profil in na takšen način lahko (na daljavo) upravljajo z informacijami na žrtvenem računalnik (Center za varnejši internet, n. d. a).

Zloraba zaupanja in prevara pomeni, da storilec izrabi zaupanje neke osebe in objavi zaupne in tajne informacije o njem. Velikokrat so ti podatki javni, žrtev pa to še dodatno prizadene, saj je zaupala določeni osebi njemu zelo pomembne informacije in ni želela, da bi prišle v javnost, hkrati pa je namen objave teh podatkov tudi osramotitev žrtve (Žakelj, 2013).

Zaradi pretirane uporabe interneta so se razvile tudi nove oblike spletnega nasilja in škodovanja, ki so psihološke narave in vplivajo na zdravje. Za takšne oblike spletnega nasilja je lahko kriva kar sama žrtev in ni potrebno, da je v takšne oblike vključen storilec (Starcevic in Aboujaoude, 2015).

Ena izmed novih oblik psihičnih motenj je **kiberhondrija**, kjer gre za to, da osebe neprestano iščejo nasvete povezane z njihovim zdravjem, ne glede na to ali so zdravi ali ne. Zaradi takšnega pretiranega branja nasvetov o zdravju osebe velikokrat mislijo, da imajo neko bolezen, ker so to prebrali na internetu. S tem se še dodatno krepi njihova tesnoba in strah pred novimi boleznimi (Starcevic in Aboujaoude, 2015).

Naslednja oblika je **kibernetski samomor**, kjer osebe pretirano iščejo informacije, kako storiti samomor in kateri so najučinkovitejši načini za to. Osebe, ki se podvržene takim mislim lahko pridejo na spletne strani, ki so posebej zasnovane na način, da osebam dajejo nasvete, kako storiti samomor. S tem se poveča obupanost žrtev in lahko zaradi takšnih spletnih strani na koncu izvedejo samomor (Starcevic in Aboujaoude, 2015).

Starcevic in Aboujaoude (2015) opozarjata tudi na problematiko **kibernetske spolnosti**, kjer gre predvsem za to, da bi osebe prejele spolno zadovoljstvo. Takšna vsebina je lahko tudi negativna in ima ilegalne posledice, če so v posnetke s spolnostjo vključeni otroci. Gledanje vsebine s spolnostjo na internetu lahko privede do zasvojenosti in zdravstvenih težav.

2.4 Kdo so največkrat žrtve spletnega nasilja

Različne raziskave so pokazale, da so največkrat žrtve spletnega nasilja ženske. Največkrat so žrtve različnih oblik odklonskega vedenja. Manjvredna vloga žensk izhaja že iz zgodovinske predstave njihove vloge (Densley in Peterson, 2017).

Za spletno nasilje nad ženskami je značilno to, da je njegov glavni namen ponižati ženske in si pridobiti moč in nadvlado nad njimi, ženske pa se v takšnih primerih počutijo ogroženo in nemočno (West, 2014). Spletno nasilje nad ženskami in dekleti ima tudi svoje ime in se imenuje *Cyber VAWG*, ki označuje povečanje nasilja na internetu nad ženskami, sestavljeno je iz treh delov: žrtve so vedno ženske, nadlegovanje je usmerjeno v točno določeno osebo in ženske se počutijo nemočno in se jim grozi z raznimi oblikami spletnega nasilja (Citron, 2009; Faith in Fraser, 2018).

Eden izmed glavnih razlogov, zakaj so ženske večkrat žrtve spletnega nasilja je zagotovo neenakost med spoloma. Moški so že skozi zgodovino predstavljeni kot močni, dominantni in pogumni, ženske pa so predstavljene kot nežnejši in milejši spol (West, 2014). Neenakost močno podpirajo različni stereotipi in predsodki (Krebelj, 2021; Plesničar, 2012).

Stereotipi so prepričanja, ki jih sami ozavestimo, od nas pa zahtevajo določeno razmišljanje in vedenje. Pogosto se do oseb, ki so drugačne od nas obnašamo drugače in imamo drugačen pogled nanje, kar nekateri ljudje izrabijo za svojo korist in se iz takšnih oseb norčujejo ali jih zlorabljajo in nadlegujejo. Zelo pogosta oblika so spolni stereotipi, ki zahtevajo določeno obnašanje od določenega spola. Tukaj se močno ločuje ženska in moška vloga, saj je ženska vloga povezana s kuho in skrbjo za otroke, moški pa lahko počnejo najrazličnejše dejavnosti in opravila (Krebelj, 2021; Plesničar, 2012).

Poleg stereotipov pa se pojavljajo tudi različni predsodki, ki so neupravičeni, neargumentirani in nepreverjeni pogledi ljudi oziroma gre za napačne predstave o ljudeh ali skupinah. Za predsodke je značilno to, da jih običajno spremljajo močna, sovražna čustva. Eden izmed glavnih stereotipov je ta, da so ženske za nekatere ljudi manj vredne kakor moški in, da morajo imeti ženske manj pravic kakor moški (Krebelj, 2021). Spletno nasilje nad ženskami temelji na rasizmu, homofobiji, seksizmu in mizoginiji (Dunn idr., 2017).

Seksizem in mizoginija sta na internetu velikokrat prisotna pri igranju spletnih iger, kjer se moški spravljajo nad ženske igralke in jim grozijo ali jim pišejo neprimerne in žaljive komentarje. Poleg spletnih iger pa najdemo žaljive komentarje tudi na drugih socialnih platformah (Krebelj, 2021).

Na spletu velja tudi hierarhična ureditev, kjer so ženske velikokrat predstavljene kot manjvredne in se zaradi tega pogosto soočajo s kaznivimi dejanji, ki so povezani s spolnostjo. Velikokrat so žrtve žaljivih komentarjev, ki temeljijo na stereotipih o spolnosti (Citron, 2009). Pogosto se srečujejo tudi z grožnjami, ukinjanjem njihovih spletnih strani, vdiranjem v račune, lažnim predstavljanjem, nadzorom in sledenjem, nadlegovanjem, novačenjem v nasilne situacije, škodljivo distribucijo intimnih fotografij in sporočil ter lahko so tudi žrtve spletnega nasilja preko aplikacij za zmenke (Densley in Peterson, 2017; Faith in Fraser, 2018). Tudi preko interneta imajo manj svobode govora in dostikrat se njihovo mnenje uporabi za manj verodostojno, včasih pa se ga celo prezre in ignorira (Citron, 2009).

Pogosto so napadene v klepetalnicah in na drugih platformah, že iz tega razloga, ker so ženske in nekateri še vedno mislijo, da so manjvredne in nimajo pravice do izražanja lastnega mnenja (West, 2014). Velikokrat se ženske tudi izključuje iz raznih dejavnosti na spletu, saj naj ne bi bile tako dobre in pomembne, kot so to moški (Citron, 2009).

Velikokrat ženske na spletu ustvarjajo tudi lažne profile na spletnih straneh, kjer se izdajajo, da so moški, da se sliši njihovo mnenje in da zaradi tega niso zasmehovane ali žrtve neprimernih komentarjev (Citron, 2009). Med bolj ogrožene predstavnice žensk pa sodijo ženske političarke, novinarke, izobražene ženske in ženske, ki zagovarjajo pravice žensk, saj so vsakodnevno žrtve spletnega nasilja, največkrat pa sovražnega govora in različnih zlorab (Van der Wilk, 2018).

Spletno nasilje nad ženskami rani celo populacijo žensk, in ne samo posameznic. V veliko primerih ženske ne upajo prijaviti spletnega nasilja, ker se bojijo, kaj se bo z njimi zgodilo, če ga prijavijo (Citron, 2009). V primerih nasilja se pogosto raje umaknejo in ne izrazijo svojega mnenja (West, 2014).

Policija velikokrat ne jemlje resno spletnega kriminala in morajo ženske velikokrat ukrepati kar same, da se kaj spremeni, za kar pa je potrebno veliko poguma in moči. Ženskam pravijo tudi, da če jim zloraba ni všeč, naj se umaknejo z interneta. Sporočilo nekaterih ljudi je, da kibernetsko nasilje ni resna skrb in da je na ženskah, da ignorirajo in se zaščitijo pred spletnimi zlorabami. Najbolj zahrbten odziv je, ko člani skupnosti krivijo dekleta in ženske za nasilje, ki se jim dogaja in se postavijo na stran storilcev kibernetskega nasilja (Citron, 2009).

Zaradi takšnih težav lahko ženske izgubijo veliko in si težko opomorejo in se vrnejo nazaj v vsakdanje življenje, kot so ga živele pred napadi. Spletno nasilje za seboj pusti socialne, psihološke, fizične in ekonomske posledice (West, 2014). Izmed teh so najpogostejše psihološke posledice, ki se pojavljalo kot tesnoba ali samopoškodovanje. Zelo pogosto se pri žrtvah pojavlja insomnija (nespečnost), napadi panike, nepojasnjen strah pred različnimi stvarmi (nenehno se bojijo, da se jim bo pripetilo nekaj slabega), občutek ponižanja, stres in drugi pojavi, ki na koncu lahko vodijo tudi do posttravmatske stresne motnje in v nekaterih primerih tudi do poskusov samomora ali samomora (Matijašič, 2021; West, 2014).

Ekonomski problem predstavljajo službe žrtve, saj jih veliko izgubi delo zaradi različnih predelanih fotografij ali drugih stvari, ki se o njih objavljajo (West, 2014). Večina komentarjev in objav ostane na internetu, tudi če se jih izbriše ali, če si žrtev izbriše profil (Citron, 2009). V nekaterih primerih žrtve izgubijo delo zaradi takšnih dejanj in si težko najdejo novo delo, saj jih delodajalci zaradi takšnih “napak” ne želijo zaposliti. Prav zaradi takšnih vzrokov ženske zelo težko tudi napredujejo na delovnem mestu in posledično težje uresničijo svoje cilje (West, 2014).

Fizični znaki spletnega nadlegovanja se kažejo na način, da so žrtve zasledovane in lahko tudi ranjene zaradi določenih aktivnosti, ki se dogajajo na spletu. Znani so primeri, kjer so moški zasledovali ženske in jim grozili ali jih ranili, če niso storile, kar so zahtevali od njih. Včasih se v fizičnem svetu pojavijo napadi na žrtve z orožjem ali drugimi ostrimi in nevarnimi pripomoči, dostikrat pride tudi do posilstva (West, 2014).

Socialne posledice pogosto ne prizadenejo le žrtve, ampak velikokrat še celo njeno družino, prijatelje, sorodnike in sodelavce. Takšne ženske izločijo iz družbe, njihove starše/partnerje zaradi tega lahko tudi odpustijo in nadlegujejo. Spletno nasilje in grožnje so zelo resna stvar in velikokrat se žrtve izolirajo in ostanejo same, saj jih prijatelji pogosto zapustijo. Prav zaradi teh vzrokov pa ženske velikokrat naredijo tisto, kar jim naročijo storilci (West, 2014).

3 ZAKONODAJA

Pri preiskavi kaznivih dejanj so mobilne naprave danes zelo pomembne, saj predstavljajo nekakšen DNK oseb, ki je v pomoč preiskovalcem. Mobilna naprava vsebuje podatke o osebah, lokaciji, kjer se osebe nahajajo, njihovih dejavnostih in opravilih. S pomočjo takšnih naprav lahko vidimo vsakdan uporabnikov. Pri vsem tem pa moramo biti zelo pozorni in se spraševati o verodostojnosti podatkov in če je res prišlo do kaznivega dejanja. Pri pregledovanju naprav, moramo biti še posebej pozorni na to, da se osebni podatki ali fotografije ne zamenjajo za kaznivo dejanje (Dimc in Dobovšek, 2012).

Zelo pomembno vlogo pri preiskovanju mobilnih naprav in preučevanju njenih podatkov imajo digitalni forenziki, ki z različnimi postopki analizirajo podatke iz naprav. Digitalna forenzika pa se v večini ukvarja z zavarovanjem, zaznavanjem, analiziranjem in predstavljanjem dokazov v elektronski obliki. Forenziki morajo tudi dobro poznati različno zakonodajo, ki jim pomaga pri delu, da vse opravljajo v okviru, ki ga določa zakonodaja (Dimc in Dobovšek, 2012). Za njihovo delo je značilno to, da se vsako kaznivo dejanje razlikuje od drugega. Za iskanje dokazov morajo forenziki vedno narediti kopijo podatkov, katero lahko spremenijo ali obdelajo (Bernik in Ilievski, 2013).

Zakonodaja je pomembna, saj nam pomaga pri obravnavi kaznivih dejanj, ki so povezana s kibernetiko. Zaradi vsakodnevne rasti spletnega nasilja in kibernetske kriminalitete Evropska Unija pogosto išče nove zakone in ukrepe, s katerimi bi se zmanjšalo spletno nasilje in kaznovalo storilce (Svet Evropske Unije, 2022). V nekaterih primerih je zelo težko določiti pravni okvir za določena kazniva dejanja v kibernetskem prostoru, saj je to neomejen prostor, ki presega meje držav in to predstavlja še dodaten izziv pravosodju (Dimc in Dobovšek, 2012).

Eden izmed dokumentov, ki ga uporabljamo članice Evropske Unije je Direktiva EU o napadih na informacijske sisteme (»Direktiva EU o napadih na informacijske sisteme«,

2013). Direktiva opredeljuje kazniva dejanja, opisuje kazni za storilce kaznivih dejanj in navaja ukrepe za boljše sodelovanje pristojnih organov in policije pri reševanju takšnih kaznivih dejanj. Pri tem za hujša kazniva dejanja, ki presegajo meje države navaja tudi pomoč Eurojusta in Europola (»Direktiva EU o napadih na informacijske sisteme«, 2013).

Svet Evropske Unije je 22. Marca 2021 sprejel dokument Strategija EU za kibernetsko varnost, kjer so opisani ukrepi, kako narediti Evropsko Unijo močnejšo in bolj odporno na kibernetske napade. V tem dokumentu si prizadevajo tudi za enakopravne možnosti vseh državljanov, da bi lahko uporabljali varne in zanesljive naprave, ki bi bile zaščitene pred kibernetskimi grožnjami. Svet EU je poudaril tudi, da je to korak k ustvarjanju bolj varne Evrope. V dokumentu gre tudi za boljši in natančnejši opis kaznovanja in sankcioniranja storilcev (Svet Evropske Unije, 2022).

V slovenski zakonodaji lahko opazimo, da imamo dobro zasnovane definicije, ki opisujejo kibernetsko kriminaliteto in s tem povezana kazniva dejanja (Markelj in Zgaga, 2018). Pomembnejši zakoni, ki se uporabljajo za reševanje spletnega nasilja v Sloveniji so Zakon o kazenskem postopku, Zakon o nalogah in pooblastilih policije in Zakon o preprečevanju nasilja v družini (Obran, 2014). Najpomembnejša sta dva pravna zapisa in sicer Kazenski zakonik in Konvencija o kibernetski kriminaliteti. Prvi je zakon in bolj splošno opisuje kaznivo dejanje in sankcioniranje storilcev (»Kazenski zakonik (KZ-1-UPB2)«, 2012). Druga pa je konvencija, kjer so zapisana in opisana najpogostejša kazniva dejanja (Šepec, 2018).

Pri vsem tem je potrebno upoštevati tudi druge zakone, ki temeljijo na spoštovanju človekovih pravic. V Sloveniji se za reševanje primerov spletnega nasilja, kjer so žrtve ženske ali otroci uporablja tudi Istanbulska konvencija, ki temelji na preprečevanju nasilja in daje več pravic ženskam (Kastelic, 2020).

Pomembno vlogo ima tudi Zakon o kazenskem postopku (ZKP-J), še posebej 219. a člen in 223. a člen. Ta zakon opisuje zaseg elektronske naprave, zavarovanje podatkov na napravi in opravljanja preiskav elektronskih naprav. Pri vsem tem je zelo pomembno, da se napravo najprej pregleda in naredi kopijo podatkov, ki se kasneje uporablja za preiskavo. Za sam začetek preiskave morajo biti izpolnjeni strogi pogoji glede tega, ali je preiskava smiselna in opravičena (Završnik, 2015).

Glavno vlogo ima v Sloveniji sodišče, ki s pomočjo zakonske ureditve rešuje primere spletnega nasilja. Ženske, ki so žrtve spletnega nasilja imajo v Sloveniji nekaj privilegijev, ki jim vsaj malo olajšajo doživljanje med kazenskim in predkazenskim postopkom. Žrtve imajo ves čas sojenja lahko ob sebi osebo, ki ji zaupajo in jim ta oseba nudi podporo in pomoč. Žrtvam je omogočeno tudi to, da v času sojenja ne pridejo v stik s storilcem, razen, če je to za nadaljevanje preiskave nujno potrebno. Žrtve lahko opravijo zaslišanje tudi preko video konferenc od doma ali v varnih sobah, ki so opremljene podobno kot domače okolje. V takšnih primerih video klic sliši samo sodnik ali sodnica, ostale osebe udeležene pri tem postopku pa so izolirane. Na koncu sojenja se poda sodba, v kateri je razvidno, ali je nekdo storil kaznivo dejanje, ali ne (Novaković, 2019).

3.1 Istanbulska konvencija

Konvencija Sveta Evrope o preprečevanju in boju proti nasilju nad ženskami in nasilju v družini ali bolj znana pod imenom Istanbulska ali Carigrajska konvencija, je dokument, ki se zavzema za pravice in enakopravnost žensk, hkrati pa vsebuje zapise, ki se navezujejo na družinsko nasilje in kako ravnati v tem primeru (»Konvencija Sveta Evrope o preprečevanju in boju proti nasilju nad ženskami in nasilju v družini«, 2011). Konvencijo je sprejel Svet Evrope v Istanbulu, sedmega aprila leta 2011 (»Zakon o ratifikaciji konvencije Sveta Evrope o preprečevanju nasilja nad ženskami in nasilja v družini ter o boju proti njima (MKPNZNDG)«, 2011).

Konvencijo sestavlja dvanajst poglavij, ki vsebujejo člene, ki podrobneje opisujejo določeno poglavje (»Konvencija Sveta Evrope o preprečevanju in boju proti nasilju nad ženskami in nasilju v družini«, 2011). Na začetku dokumenta najdemo preambulo, na koncu pa še kot dodatek pravice in imunitete, ki pripadajo določeni osebi. Poglavja pa opisujejo namen same konvencije in razlago osnovnih pojmov, politiko dokumenta in zbiranje podatkov, preprečevanje nasilja in drugi ukrepi, zaščito in podporo, materialno pravo, preiskave, procese, pregone storilcev in zaščitne ukrepe za žrtve nasilja, migracije in dodeljevanje azila, mednarodno sodelovanje, kdo spremlja žrtve in jim nudi pomoč, razmerje do drugih mednarodnih instrumentov, spremembe in končne določbe konvencije (»MKPNZNDG«, 2011).

Konvencija je najmočnejši in tudi najobsežnejši ukrep, ki se bori za pravice žensk in navaja ukrepe za boj proti družinskemu nasilju (Kastelic, 2020). Predstavlja tudi dokument, v katerem so zapisani minimalni zahtevki in enotna obravnava žrtev nasilja (Mayer, 2020). Konvencija ima štiri glavna načela, ki predstavljajo zaščito, preprečevanje, podporo žrtvam in pregon s strani policije in drugih uradnih oseb (Kastelic, 2020).

Poleg nasilja v družini in pravic žensk, pa opisuje tudi, da nihče ne sme biti diskriminiran, da se ljudi ne sme ločevati glede na raso in versko pripadnost in tudi ne glede na spol. Konvencija daje pravice vsem ljudem in opisuje enakopravnost med ljudmi in, da si vsi zaslužijo enake pravice (Kastelic, 2020; Mayer, 2020).

Prvotno je konvencijo sprejelo in podpisalo petinštirideset držav in tudi članice Evropske unije. Kasneje je nekaj držav izstopilo iz tega dogovora, saj niso želeli sprejeti nekaterih ukrepov, med katerimi so tudi istospolne poroke (Kastelic, 2020). Slovenija je konvencijo sprejela leta 2015, zanjo je pa značilno tudi to, da velja v mirovnem in vojnem stanju (Mayer, 2020).

3.2 Konvencija o kibernetski kriminaliteti

Konvencija o kibernetski kriminaliteti je dokument, ki opisuje vse glavne kibernetske napade in rešitve, kako ukrepati v primeru določenega kaznivega dejanja. Konvencija je bila sprejeta v Budimpešti 23. novembra 2001, sprejel in potrdil pa jo je Svet Evrope. Do leta 2004 so jo v Evropi uporabljale in potrdile že skoraj vse članice, konvencija pa se je razširila tudi izven Evrope in jo uporabljajo tudi v Ameriki, Kanadi, Avstraliji in na Japonskem (Šepec, 2018).

Na samem začetku je dokument veljal za zelo napredenega in modernega, in je imel natančno opisane in razložene vse oblike kaznivih dejanj. Z naraščanjem in širjenjem kibernetske kriminalitete pa je bilo kar nekaj stvari takšnih, ki niso bile zapisane v sami konvenciji in je bilo to potrebno spremeniti. Kmalu so opazili, da sta pri spletnem nasilju zelo prisotna ksenofobija in rasizem, kar je bilo potrebno dodati k samemu dokumentu. V ta namen je Svet Evrope leta 2003 izdal nov, dodaten dokument imenovan Dodatni protokol, ki so ga dodali k sami konvenciji. V tem Dodatnem protokolu so zapisani in dodani primeri kaznivih spletnih dejanj, ki temeljijo na rasizmu in ksenofobiji. Konvencija o kibernetski kriminaliteti in Dodatni protokol h konvenciji temeljita tudi na spoštovanju človekovih pravic (Šepec, 2018).

Konvencija o kibernetski kriminaliteti je sestavljena iz preambule in štirih poglavij. V preambuli so opisani pravni okviri konvencije, opisano je pa tudi to, da konvencija temelji na spoštovanju človekovih pravic in da se povezuje z nekaterimi evropskimi dokumenti (Rupnik, 2003).

V prvem poglavju konvencije so predstavljeni in razloženi izrazi, ki se navezujejo na kibernetsko kriminaliteto. Tukaj so opisani tudi osnovni pojmi, ki se največkrat povezujejo s kibernetsko kriminaliteto (Rupnik, 2003).

V drugem poglavju lahko najdemo ukrepe, ki se navezujejo na kazensko materialno in procesno pravo in navezovanje na sodno pristojnost. V tem poglavju so enotno opredeljena kazniva dejanja in določena nacionalna pooblastila in postopki preiskovanja kaznivih dejanj (Dimc in Dobovšek, 2012). V kazenskem materialnem pravu so zajeta kazniva dejanja, ki se nanašajo na predmet dejanja in na način napada. V tem sklopu je pet skupin, pod katerim so različni členi, ki definirajo določeno kaznivo dejanj (Rupnik, 2003).

Prva skupina so napadi, ki kršijo zaupnost, celovitost in dostopnost računalniških sistemov in podatkov. Členi v tem poglavju pa so naslednji: protipraven dostop, protipravno prestrezanje, motenje podatkov, motenje sistemov in zloraba naprav členov, ki definirajo posamezni napad (»Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih (MKKKDP)«, 2004). V drugi skupini najdemo kazniva dejanja, ki so povezana z računalniki, sem pa sodita računalniško ponarejanje in računalniške goljufije. Tretja skupina opredeljuje kazniva dejanja, ki so povezana z vsebino, sem sodijo primeri povezani z otroško pornografijo, v četrto skupino sodijo napadi, ki so povezani s kršitvijo sodne in avtorske pravice in v peti skupini pa sta definirani odgovornost storilcev in njihova sankcija. Členi tega poglavja so poskus in pomoč ali napeljevanje, odgovornost pravnih oseb in opis sankcij (»MKKKDP, 2004«).

V kazensko procesnem delu so opisani ukrepi, ki se navezujejo na to, kako zavarovati in shraniti podatke in informacije v računalniških sistemih, da se ne izgubijo, do začetka preiskave (Rupnik, 2003). Procesni del sestavlja pet naslovov. Najprej najdemo splošne določbe, nato sledi naslov, kako takoj zavarovati računalniške podatke, odredba za pripravo, preiskovanje in zaseg shranjenih računalniških podatkov in zbiranje računalniških podatkov v dejanskem času. V tem poglavju imamo poleg teh naslovov opisano še sodno pristojnost, kjer so opisani ukrepi kaj se stori s storilcem (»MKKKDP, 2004«).

V tretjem delu konvencije je opisano mednarodno sodelovanje, ki presega državne meje. V tem delu je opisana predaja storilcev državi, katere prebivalec je storilec, opisana je pomoč članic v primeru bolj zapletenih kaznivih dejanj, opisuje tudi izmenjavo informacij med državami, brez posebnih dodatnih zaprosil in omejitvi uporabe določenih ukrepov in v četrtem delu so zapisane končne določbe, ki se navezujejo na podpisovanje konvencije, njeno veljavnost in druge zahteve (Rupnik, 2003).

3.3 Kazenski zakonik

Kazenski zakonik je zakon, v katerem je opisano kaznovanje polnoletnih storilcev za storjeno kaznivo dejanje. V zakonu je tudi opisano, da se kaznuje samo osebe, ki so storile kaznivo dejanje. Za osebe, ki se bile neprištevne v času kaznivega dejanja se kaznovanje opravi drugače, glede na zapis v zakonu (»KZ-1-UPB2«, 2012).

Kazenski zakonik se v Sloveniji ne uporablja samo za kaznovanje storilce kaznivih dejanj klasične kriminalitete, ampak se uporablja tudi za kaznovanje storilcev kibernetske kriminalitete. Kazenski zakonik pomaga pravosodju pri prepoznavi kaznivega dejanja in kaznovanju storilca (»KZ-1-UPB2«, 2012).

V njem kibernetski napadi niso posebej obravnavani, ampak je takšne napade potrebno uvrstiti v določeno skupino. Kazenski zakonik obravnava tri večje skupine, pri prvi gre za kazniva dejanja, pri katerih je cilj napada informacijski sistem in napad na informacijski sistem, pri drugi skupini je cilj zloraba informacijskega sistema, v tretjo skupino pa uvrščamo kazniva dejanja, ki se povezujejo z izdelovanjem in pridobivanjem orožja in pripomočkov, namenjenih za kaznivo dejanje (»KZ-1-UPB2«, 2012; Markelj in Zgaga, 2018).

Napad na informacijski sistem je kaznivo dejanje, kjer nekdo nepooblaščeno vstopi ali vdre v informacijski sistem. Takšna oseba lahko prestreže zaupne in pomembne

informacije posameznika. Storilca takšnega kaznivega dejanja se kaznuje z zaporno kaznijo do dveh let. V to skupino napadov sodijo tudi osebe, ki potem te podatke neupravičeno uporabijo, jih spremenijo, objavijo ali pa lastniku teh podatkov onemogočijo dostop do njih ali jih ovirajo pri dostopanju do njih. Pri takšnih kaznivih dejanjih, storilcu sledi zaporna kazen do treh let. V primeru, da gre pri teh kaznivih dejanjih še za uporabo različnih nevarnih pripomočkov in so pri tem ranjeni trije ali več informacijskih sistemov, se storilcu dodeli zaporna kazen od treh mesecev do štirih let . Če je pri samem dejanju povzročeno veliko škode se storilca kaznuje z zaporno kaznijo od treh mesecev pa do petih let (»KZ-1-UPB2«, 2012).

Definicije, ki zajemajo in opisujejo napade na informacijske sisteme so v osnovi dobro zasnovane in v veliki meri zavzemajo bistvo teh napadov in kaznovanja storilcev. V nekaterih primerih so še vedno vidne pomanjkljivosti, ki bi jih bilo potrebno popraviti (Markelj in Zgaga, 2018).

Zlorabo informacijskega sistema opisuje 237. člen kazenskega zakonika. Sem sodijo kazniva dejanja, ki so povezana z gospodarskim poslovanjem (Markelj in Zgaga, 2018). Gre za kazniva dejanja, kjer oseba pri gospodarskem poslovanju nepooblaščeno vstopa do določenih podatkov in jih nato spremeni, preslika ali jih drugače uporabi in pri tem pridobi gospodarsko korist ali drugemu udeležencu poslovanja povzroči premoženjsko škodo. Lahko pa storilec tudi omeji ali prepreči dostop do teh podatkov. V primeru takšnih kaznivih dejanj, se storilca kaznuje z zaporno kaznijo do treh let (»KZ-1-UPB2«, 2012).

Člen številka 306 opisuje kazniva dejanja v povezavi z izdelovanjem in pridobivanjem orožja in pripomočkov, namenjenih za kaznivo dejanje (»KZ-1-UPB2«, 2012). Sem sodijo osebe, ki posredujejo, prodajajo, uživajo, izvažajo ali dajejo drugim osebam v uporabo pripomočke ali druge naprave, s katerimi lahko nekdo vdre v informacijski sistem ali omeji njegov dostop (Markelj in Zgaga, 2018).

Najpogostejša kazniva dejanja, ki jih opredeljuje kazenski zakonik pa so zalezovanje (134. člen), zloraba osebnih podatkov (143. člen), izsiljevanje (213. člen) in neupravičeno slikovno snemanje (138. člen). Posamezni členi opisujejo njihovo razlago in način sankcioniranja (»KZ-1-UPB2«, 2012; Novaković, 2019).

4 POMOČ ŽRTVAM

Žrtve spletnega nasilja so zelo velikokrat še bolj ranjene in obupane kot žrtve klasičnega nasilja. Za žrtve spletnega nasilja je značilno to, da se jim spletno nasilje dogaja večkrat in ne samo enkrat, ter, da se takšnemu nasilju zelo težko izognejo in ga prekinejo (Novaković, 2019).

Zato je še bolj pomembno, da imajo žrtve ob sebi osebe, ki jim lahko zaupajo in računajo na njihovo pomoč v primeru spletnega nasilja. V prvi vrsti se žrtve lahko na pomoč obrnejo na svojo družino in prijatelje, ki tudi kazniva dejanja in odklonsko vedenje storilcev prijavijo policiji ali drugim ustanovam, če žrtev sama tega ne more storiti (West, 2014).

Kljub temu, da se internet uporablja za povzročanje spletnega nasilja, se uporablja tudi za boj proti njemu (Magnet in Mason, 2012). V nekaterih primerih ženske javno spregovorijo o svojih izkušnjah in o tem, da so bile žrtve spletnega nasilja. Svoje mnenje delijo preko socialnih omrežij ali preko drugih platform. Takšna dejanja od žensk zahtevajo veliko poguma in moči. Na takšen način se med seboj poveže več žensk z enakimi izkušnjami in si med seboj pomagajo ter delijo nasvete (West, 2014). Skupine teh žensk ustanavljajo tudi različne programe za pomoč žrtvam (Magnet in Mason, 2012). Borijo pa se tudi za izboljšanje politike na spletu in za pravice ženskih uporabnic (Faith in Fraser, 2018).

Magnet in Mason (2012) pravita, da internet prinaša prednosti tudi v primerih, da žrtve lažje in hitreje dostopajo do informacij za pomoč v primeru nasilja. Na spletnih straneh najdejo tudi ukrepe in korake, kako se bolje zaščititi na internetu in kako varneje uporabljati aplikacije.

Proti nasilju na spletu se borijo tudi socialna omrežja, spletne strani in druge nadzorne tehnologije. Zanje je značilno, da imajo opisano politiko delovanja, v kateri so zapisane

tudi kršitve, ki so neprimerne za objavo (Magnet in Mason, 2012). Na socialnih omrežjih vidimo tudi možnost, da neprimerno in žaljivo vsebino skrijemo, ali prijavimo, kar vodi v blokiranje računa storilca za nekaj časa. Vsa socialna omrežja bi morala biti odgovorna za ustvarjanje varnega okolja za ženske, ki jih uporabljajo. Omogočati bi morali tudi varne spletne prostore, kjer bi bile ženske enakopravne moškim (Dunn idr., 2017). Naloga socialnih omrežij bi morala biti tudi ta, da se že samodejno odstranijo neprimerne vsebine, brez prijave. Ženske se vedno lahko obrnejo tudi na policijo ali na druge organizacije, ki jim pomagajo pri reševanju spletnega nasilja. (Novaković, 2019).

Ena izmed pomembnejših stvari, ki osebe do neke mere obvarujejo pred kibernetskimi napadi so tudi najrazličnejši preventivni ukrepi (Bratuša in Verdonik, 2005). V prvi vrsti so zagotovo zelo pomembna močna in unikatna gesla, katere pozna samo njihov uporabnik. Takšna gesla morajo biti dolga in vsebovati nabor različnih znakov. Priporočljiva je tudi uporaba programov, ki upravljajo z gesli. Takšni programi pomagajo osebam sestaviti unikatna gesla in z njimi tudi upravljajo in jih varujejo (*Ključni nasveti za varnost vaših računov*, n. d.).

Nadvse priporočljiva je tudi večstopenjska avtentikacija, ki vsebuje različne načine dostopa do informacij. Primer je uporaba biometričnega vzorca in vpis izbranega gesla. Na takšen način povečamo našo varnost in s tem poskrbimo za to, da storilci težje vdrejo v naš profil (*Ključni nasveti za varnost vaših računov*, n. d.).

Za večjo varnost pripomorejo tudi različni programi, ki šifrirajo in zavarujejo naše podatke pred drugimi osebami. Veliko mobilnih naprav ima že vgrajeno to funkcijo, da samodejno šifrira in zaklene podatke, da oseba brez dovoljenja ne more priti do njih (Verdonik in Bratuša, 2005).

Za varnost naprav pa je potrebno tudi njihovo posodabljanje in nadgrajevanje, saj se s tem pojavijo novi ukrepi, ki skrbijo za varnost oseb in naprav (Leaf, 2019). Pomemben del preventivne zaščite sta požarni zid in antivirusni programi, ki uporabnike

opozarjata pred nevarnostmi in blokirata neznane in sumljive dejavnosti (Verdonik in Bratuša, 2005). Za boljšo varnost in zaščito je potrebno tudi ustvarjanje kopij, ki jih shranjujejo na druge nosilce. Z ustvarjanjem kopij imamo vedno na voljo še en dokument, ki ga lahko spreminjamo v primeru izgube ali izbrisa originalnih podatkov (Leaf, 2019).

Pri vsem tem pa ne smemo pozabiti na fizično zaščito naprav, ki je tudi zelo pomembna za našo varnost. Pri tem je bistveno to, da do določenih pomembnih informacij omejimo dostop oseb in da do njih lahko dostopajo le pooblaščene osebe. Pri fizični zaščiti sami tudi določimo kdo bo lahko uporabljal naše naprave in kdo ne (Leaf, 2019; Verdonik in Bratuša, 2005).

Pri varovanju informacij in podatkov je pomembno upoštevanje modela CIA, ki ga sestavljajo zaupnost, ki pomeni to, komu lahko zaupamo naše informacije, celovitost, kar pomeni, da so nam naši podatki vedno na voljo v celoti in dostopnost, ki nam omogoča dostop do podatkov kjer koli in kadar koli (Verdonik in Bratuša, 2005).

4.1 Zavezniki

Eden izmed glavnih zaveznikov je policija, ki ima zelo pomembno vlogo pri reševanju spletnega nasilja. Njena primarna naloga je zaščititi žrtev spletnega nasilja in ji ponuditi vso potrebno podporo, pomoč in zaščito (Novaković, 2019). V naslednjem koraku policija želi najti in identificirati storilca kaznivega dejanja in ga ustrezno kaznovati, glede na vrsto kaznivega dejanja. Policija mora na spletno nasilje odreagirati takoj, brez dolgoročnega čakanja in odlašanja (Policija, n. d. a).

V primeru, da postanemo žrtev spletnega nasilja je najprej potrebno poklicati policijo na številko 113, v pogovoru policistom povemo kje se nahajamo, naše osebne podatke in kaj se je zgodilo. Če smo sami preveč ogroženi to lahko namesto nas stori kakšna druga oseba, ki ji zaupamo (Obran, 2014).

Ko je žrtev na varnem, policija opravi z njo razgovor v katerem žrtev opiše svojo izkušnjo in žrtev katerega kibernetskega kaznivega dejanja je bila. Takšni razgovori potekajo v točno določenem prostoru, kjer je žrtev zavarovana. V primeru, ko je žrtev ženska, lahko pogovor z njo opravi policistka in jim s tem olajša pripovedovanje. Za policiste in policistke, ki opravljajo razgovore z žrtvami je nujno, da imajo znanje o tem področju in da imajo razvito čustveno inteligenco in empatijo, da žrtev razumejo in ji pomagajo. Žrtvam ponudijo tudi vso potrebno pomoč. Ponudijo jim tudi osebe, ki jim lahko zaupajo, da jim stojijo ob strani in jim pomagajo v težkih trenutkih. Ponudijo pa jim tudi strokovno pomoč in v hujših primerih tudi prostore, ki so varnostno nadzorovani in zaščiteni, kjer lahko živijo brez strahu pred storilci kaznivih dejanj (Novaković, 2019).

Policisti imajo na voljo kar nekaj ukrepov, s katerimi pomagajo žrtvam. Eden izmed takšnih ukrepov je prepoved približevanja. Policisti jo lahko izrečejo na samem mestu dogodka, velja pa oseminštirideset ur in v obsegu dvesto metrov. Kraj, kjer ukrep velja se nanaša na vse kraje, kjer se oseba giblje. Kasneje lahko odločbo o prepovedi približevanja podaljša preiskovalni sodnik na deset dni, na predlog žrtve pa preiskovalni sodnik lahko odločbo podaljša še za šestdeset dni. Pri podaljšanjih, morajo biti podani pisni razlogi za to (Obran, 2014).

Policisti v Sloveniji uporabljajo predvsem mešane pristope za reševanje kibernetskih napadov, kar pomeni, da kombinirajo klasične načine reševanja kaznivih dejanj z računalniškimi metodami (Bernik in Ilievski, 2013).

Slovenska policija je ustanovila tudi svoj Center za računalniško preiskovanje, ki se deli na štiri regije, v njem pa so zaposleni kriminalisti, ki imajo dobro znanje informatike in računalništva. Ti kriminalisti skrbijo tudi za nadgradnjo in posodabljanje računalniške opreme in programov (Bernik in Ilievski, 2013).

V času preiskave morajo policisti zbirati in shranjevati dokazno gradivo, ki ga pridobijo v času preiskave, saj so dokazi pomembni za zaključitev predkazenskega postopka in za izročilo podatkov sodišču. Policisti lahko pri svojem delu uporabijo različne ukrepe za pridobitev dokazov. Storilcem lahko zasežejo mobilno napravo, za katero menijo ali sumijo, da je bila uporabljena pri storitvi kaznivega dejanja. Policisti lahko opravljajo tudi hišne in osebne preiskave, če sumijo na to, da se tam nahaja storilčevo orodje za povzročitev kaznivega dejanja. Osumljenca lahko zaslišijo in mu omejijo gibanje, ali ga pridržijo za največ oseminštirideset ur (Novaković, 2019).

V primerih, ko sumijo, da bi lahko šlo za bolj hudo in nevarno kaznivo dejanje, vložijo kazensko ovadbo proti storilcu, lahko pa storilca tudi pripeljejo pred preiskovalnega sodnika ali sodnico, ki se naprej odloča o tem, kaj storiti s storilcem in kakšno sankcijo mu določiti (Novaković, 2019).

V nekaterih primerih policija ni takoj odzivna in ne zna pristopiti k reševanju spletnega nasilja, saj za nekatere vrste nasilja ne vedo, kako se lotiti reševanja in pomoči žrtvam, zato je potrebno, da se policiste usposablja in uči o posledicah spletnega nasilja (West, 2014).

Pri kompleksnejših primerih spletnega nasilja, lahko policija za pomoč zaprosi tudi organe pregona iz drugih držav, da jim pomagajo pri iskanju storilca in reševanju primerov kibernetske kriminalitete. Najpogosteje se obrnejo na pomoč Europola in različnih centrov za socialno delo, ter drugih organizacij, ki skrbijo za kibernetsko varnost. Velikokrat pa policija sodeluje tudi z drugimi organizacijami, ki se borijo proti kibernetskemu nasilju, saj so takšne organizacije bolj usposobljene za določene vrste kaznivih dejanj, ker se z njimi srečujejo vsakodnevno (Bernik in Ilievski, 2013).

Zelo pomembno je, da policija zbrane digitalne podatke dobro zaščititi in jih shrani na varno, da do njih ne more dostopati nobena oseba z nepooblaščenim dostopom (Novaković, 2019). Dokaze zbirajo s pomočjo dokazovanja, odkrivanja, preiskovanja in

preprečevanja kaznivih dejanj storjenih v kibernetskem prostoru, s pomočjo elektronskih naprav (Bernik in Ilievski, 2013).

Policija ima na svoji spletni strani objavljene različne preventivne ukrepe, ki pomagajo, da ne postanemo žrtve spletnega nasilja. Ukrepi se navezujejo na nastavitev zasebnosti do te mere, da smo najbolj zaščiteni in težje postanemo tarča napadalcev. Policija poudarja, da preko interneta ne smemo zaupati neznancem in da ne smemo privoliti njihovim željam ali ukazom. Nikoli ne smemo preko spletna pošiljati golih fotografij, saj te lahko za vedno ostanejo na internetu (Policija, n. d. a). Neznancem ali osebam, ki jim ne zaupamo ne smemo posredovati osebnih podatkov. Policija opozarja tudi na to, da se ne smemo v živo dobivati z osebami, ki jih poznamo samo preko interneta, saj gre v veliko primerih za osebe, ki se pretvarjajo, da so nekdo drug kot so v resnici. Pazljivi pa moramo biti tudi pri odpiranju sumljivih spletnih povezav (Policija, n. d. b).

Pri preventivnih ukrepih lahko najdemo tudi nasvete, kaj storiti, če postanemo žrtev spletnega nasilja in na koga se obrniti. Opisani so tudi postopki, kako poteka prijava storilca in katera ustanova lahko najbolje pomaga pri pomoči spletnega nasilja (Policija, n. d. a).

4.2 Društva in organizacije za pomoč žrtvam

Pomoč žrtvam spletnega nasilja nudijo tudi različna podjetja in organizacije, ki so specializirana na področju kibernetske varnosti in nudijo žrtvam ustrezno pomoč in nasvete, kako se zavarovati pred spletnim nasiljem (Petek, 2019b).

Ženske, ki so bile žrtve spletnega nasilja, se lahko za pomoč obrnejo na različne organizacije. Ena izmed bolj znanih organizacij je društvo SOS, ali SOS telefon, kamor lahko žrtve pokličejo, če se znajdejo v stiski. Telefonska številka, na katero lahko žrtve pokličejo je 080 -11 -55. Pogovori potekajo anonimno in strokovnjaki jim pomagajo z različnimi nasveti. Telefonska linija je na voljo 24 ur na dan in žrtev lahko pokliče

kadarkoli (Društvo SOS, n. d). Poleg telefona ima društvo SOS tudi zatočišča, kamor se lahko žrtve umaknejo in s strokovno pomočjo začnejo novo življenje. Potekajo tudi srečanja v podpornih skupinah, kjer so združene žrtve podobnih primerov nasilja in s tem žrtve ugotovijo, da niso edine, ki so doživele spletno nasilje. Ženske se lahko obrnejo na osebno pomoč, kjer potekajo pogovori ena na ena s terapevtom ali psihologom. V primerih, ko strokovnjaki ugotovijo, da gre lahko za večji problem in so žrtve bolj ogrožene, takrat pa lahko vključijo tudi policijo, ki jim pomaga pri zavarovanju žrtve (Društvo SOS, n. d.).

Naslednja organizacija je Tom, ki ima prav tako svojo telefonsko linijo (telefon: 116 111), kamor lahko pokličejo žrtve spletnega nasilja. Na spletni strani Tom so objavljeni različni prispevki, ki opisujejo negativni vplive socialnih omrežij na posameznike, nudijo ukrepe za preventivno zaščito pred spletnim nasiljem in kaj storiti v primeru, če postanemo žrtev spletnega nasilja (Tom, n. d.).

Zelo pomembno je tudi Društvo za nenasilno komunikacijo, ki nudi nasvete za žrtve spletnega ali drugega nasilja. V Društvu za nenasilno komunikacijo nudijo pravno pomoč, pogovor in različna svetovanja. Na njihovi spletni strani najdemo tudi korake, kako ukrepati, če postanemo žrtev nasilja. Vsi nasveti, ki jih nudijo pa so brezplačni in vedno pomagajo žrtvam, kolikor je to v njihovi moči (Društvo za nenasilno komunikacijo, n. d.).

Pomoč nudijo tudi Centri za socialno delo, ki žrtvam nudijo prostovoljno pomoč v obliki zaupnih pogovorov. Socialni delavci žrtvam pomagajo pri iskanju varnega zavetja. S pomočjo socialnih delavcev se opravi ocena ogroženosti in varnostni načrt, ki sta v pomoč žrtvam in preiskovalnim organom za zaščito žrtve in kaznovanje storilcev. Ocena ogroženosti pa je pomembna tudi za brezplačno pravno pomoč žrtvam (Obran, 2014).

Takšna ocena ogroženosti vsebuje podatke o tem, kdo je povzročitelj nasilja, psihično in fizično stanje žrtev, njihovo prepričanje in podporo različnih socialnih ustanov, ki tvorijo medsebojno povezavo (Horvat idr., 2014). Poleg centrov za socialno delo pomaga pri ugotavljanju posledic na žrtvah tudi zdravniška pomoč, ki jim nudi zdravstvene preglede in pomoč (Horvat idr., 2014).

Naslednja organizacija je SI-CERT, ki je nacionalni odzivni center za kibernetsko varnost. SI-CERT ponuja svetovanje osebam, ki so bile žrtve različnih spletnih vdorov, prevar, računalniških okužb ali drugih incidentov. Organizacija izdaja opozorila o grožnjah in drugih kibernetskih nevarnostih na nacionalni ravni. Organizirajo pa tudi različne mednarodne programe ozaveščanja. V Sloveniji je zelo znan program ozaveščanja Varni na internetu, kjer so predstavljeni preventivni ukrepi za zaščito (SI-CERT, n. d.). SI-CERT je članica svetovnih odzivnih in varnostnih centrov, ki se zavzemajo za kibernetsko varnost (SI-CERT, n. d.).

Safe.si je program z nasveti o spletni varnosti. Organizacija ponuja veliko nasvetov, kako se zaščititi na internetu, na katere stvari moramo biti še posebej pazljivi in kakšna je politika obnašanja na internetu. Najdemo lahko tudi različne delavnice in predavanja na temo kibernetske varnosti. Žrtve se lahko na organizacijo obrnejo, če potrebujejo nasvete ali kakršno koli drugo obliko pomoči (Center za varnejši internet, n. d. c).

V Sloveniji je tudi nekaj drugih podjetij, ki nudijo varnost in pomoč v primerih kibernetskih nadlegovanj. Najbolj znana pa so zagotovo Sistemator, Hic Salta, ACROS, D-NET, Virtua, Palsit in druga (Bernik in Ilievski, 2013).

5 IZVAJALCI SPLETNEGA NASILJA

Storilci so lahko različnih starosti in spola. Velikokrat izberejo žrtve, ki se jim zdijo ranljivejše, naivnejše, neprevidne, osamljene in bolj zaupljive. Storilci škodujejo izbranim žrtvam zaradi finančne in osebne koristi, maščevanja, zabave ali pa želijo samo povzročiti škodo (Policija, n. d. c).

Med storilce spletnega nasilja spadajo tako moški kot ženske, vendar obstajajo razlike med njimi v načinu nasilja in nadlegovanja. Moški najpogosteje uporabljajo seksistične izjave, nagovarjajo žrtve, da dobijo, kar si želijo, uporabljajo žaljivke, zmerjajo druge osebe, nadlegujejo uporabnike, pošiljajo neprimerna sporočila, nagovarjajo ženske/moške k spolnosti, na drugi strani pa ženske pogosteje ustrahujejo in sramotijo osebe in so krute do njih, uporabljajo manipulacijo, žaljivke, govorijo o zasebnih stvareh prijateljev, izvajajo spletne goljufije in širijo neresnične govorice, velikokrat pa tudi nadlegujejo žrtve zaradi pridobivanja moške pozornosti (Favela, 2010; Petek, 2019a).

S pomočjo opravljenih raziskav so ugotovili, da so izvajalci kibernetskega kriminala najpogosteje, mladi, beli, heteroseksualni moški, ki imajo višji statusni in ekonomski položaj in, da redkeje prihajajo iz etničnih manjšin. Zanje je značilno tudi to, da so bolj inteligentni in imajo dobro razvite sposobnosti za reševanje problemov ter imajo višjo stopnjo izobrazbe (Leukfeldt idr., 2022; Van der Wilk, 2018).

Žrtve svoje storilce v nekaterih primerih poznajo, saj so največkrat storilci bivši ali trenutni partnerji, sodelavci ali prijatelji (Horvat idr., 2014; Van der Wilk, 2018). Še vedno pa so pogostejši napadi, ko storilci niso znani in si ustvarijo lažne profile z lažnimi informacijami in tako naprej delujejo in povzročajo škodo. Najprej se vse začne precej nedolžno, kasneje pa se to vse stopnjuje. Največkrat so žrtve samske, starejše in osamljene ženske, kar storilci izkoristijo in se pretvarjajo, da se zanimajo zanje in da so jim všeč. Ženske pogosto zaradi “lepih” besed verjamejo storilcem in so pripravljene

narediti vse zanje, kar vključuje finančno izkoriščanje žrtev, različna nadlegovanja, izsiljevanja in grožnje (Policija, n. d. c).

Moški se nad ženske najpogosteje spravljajo zaradi neenakosti med spoloma in ne želijo, da bi bile ženske enakovredne moškim na internetu. Moški velikokrat nadlegujejo in ustrahujejo ženske, da si pridobijo moč in nadzor nad njimi. Pogosto se spravljajo nad ženske tudi zato, ker so bili oni žrtve nasilja in ne prenesejo tega občutka in želijo, da se nekdo počuti slabo zaradi njih (West, 2014). Pogosto vršijo nasilje tudi partnerji ženski, ki so ljubosumni in želijo imeti popoln nadzor nad njo. Da bi to dosegli nadzirajo njihova socialna omrežja in druge dejavnosti, ki jih počnejo na spletu. Dunn idr. (2017) pravijo tudi, da včasih moški zahtevajo tudi vsa gesla in podatke od žensk, da dostopajo do njihovih profilov.

Moški zelo pogosto napadajo ženske igralke spletnih iger, saj v njih prevladuje prepričanje, da one tega ne bi smele početi. Še večje sovraštvo se v njih vzbudi, če so ženske igralke uspešnejše od moški. Moški storilci velikokrat objavljajo seksualne, predelane fotografije žensk, da jih osramotijo ali spravijo v zadrego. Velikokrat objavijo tudi zasebne fotografije deklet, brez njihove privolitve (Dunn idr., 2017).

Različni raziskovalci so opredelili tri skupine storilcev in kaznivih dejanj, ki jih počnejo: Prva skupina so storilci, ki se ne zavedajo, da delajo nekaj narobe. Druga skupina so storilci, ki izvajajo različne oblike nasilja na spletu in tretja skupina, kamor uvrščajo storilce, ki so že bili žrtve spletnega nasilja in se želijo maščevati in tudi sami postanejo storilci in povzročitelji kaznivih dejanj (Petek, 2019a).

Strokovnjaki so s pomočjo raziskav ugotovili, da med žrtvami kibernetskega nasilja in storilci kibernetskega nasilja obstajajo določene povezave (Feijóo idr., 2021). Ugotovili so, da sta obe skupini veliki uporabnici kibernetskega prostora in tam preživijo veliko svojega časa. Večkrat so žrtve osebe, ki preživijo veliko časa na internetu, kot tiste, ki tam preživijo manj časa (Feijóo idr., 2021).

5.1 Prednosti izvajalcev spletnega nasilja

Ena izmed glavnih prednosti, ki jih prinaša spletno nasilje za izvajalce je kibernetski prostor, ker je za storilce to prostor, kjer je vse enostavno. Za izvajanje spletnega nasilja osebe ne potrebujejo posebnega znanja in drugih veščin. Storilcem je na voljo veliko brezplačnih spletnih programov, ki so enostavni za uporabo. S pomočjo takšnih programov storilci lahko na enostaven način predelajo fotografije žrtev ali njihove komentarje v neprimerno vsebino in jih tako objavljajo na internetnih platformah pod žrtvinem imenom (West, 2014). Velika prednost kibernetskega prostorja je tudi njegova neomejenost, saj ni omejen na meje države in lahko storilec iz drugega konca sveta izvaja kazniva dejanja in spletno nasilje (Bernik in Meško, 2011). Izvajalci spletnega nasilja lahko nasilje izvršujejo preko javnih ali zasebnih platform, največkrat pa ga izvršujejo preko socialnih omrežij (Van der Wilk, 2018).

Za nekatere storilce je prednost zasebnost. Velikokrat osebe, ki so povzročitelji spletnega nasilja ne objavljajo veliko na socialnih omrežjih, da imajo žrtve čim manj podatkov o njih in jih težje obtožijo. S tem, ko ne delijo osebnih podatkov, je oteženo ugotavljanje, če to realni ali lažni profil (Van der Wilk, 2018).

Velika prednost spletnih storilcev je tudi anonimnost, saj storilci lahko izvajajo spletno nasilje pod izmišljenim uporabniškim imenom in jim to nudi zaščito pred identifikacijo (West, 2014). Zaradi anonimnosti so storilci bolj samozavestni in imajo več moči pri izvedbi kaznivih dejanj (Žakelj, 2013). Velikokrat zaradi tega ne poznajo nobenih omejitev in posežejo po različnih metodah za povzročanje neprijetnosti na spletu (Petek, 2019a). Hkrati jim anonimnost nudi tudi zaščito in (lažen) občutek varnosti. Prav zaradi anonimnosti storilcev je kibernetsko nadlegovanje unikaten pojav (Žakelj, 2013).

Bernik in Ilievski (2013) opozarjata na to, da storilci izkoriščajo pri svojem škodovanju tudi odvisnost ljudi od interneta. Takšna odvisnost uporabnikov interneta je zanje

prednost, saj s tem lažje najdejo žrtve, ki jim bodo škodili. S tem ko osebe preživijo več časa na spletu, večja je verjetnost, da postanejo žrtve.

5.2 Slabosti izvajalcev spletnega nasilja

Največkrat so prednosti storilcev kaznivih dejanj tudi njihove pomanjkljivosti in slabosti. Prva slabost storilcev je zagotovo anonimnost, ki v njih zbudi občutek moč in samozavesti, kar jih v nekaterih primerih lahko zavede. Zaradi pretirane samozavesti in ideje o zaščiti, si osebe upajo veliko več in izvršujejo različna kazniva dejanja, ki jih ne bi nikoli storili, če bi bila njihova identiteta znana (Žakelj, 2013). V takšne namene tudi ustvarjajo lažne profile preko katerih izvršujejo nasilje. Kljub anonimnosti in lažnim imenom lahko policija slej ko prej izsledi storilca kaznivih dejanj in ga poveže z resnično osebo (West, 2014). Največkrat storilce najdejo po IP naslovih, kjer je razvidna lokacija storilca (Čaleta in Powers, 2020; Leukfeldt idr., 2022).

Naslednja slabost, ki jim lahko škoduje pa je ne zavedanje o tem, kaj počnejo. Velikokrat se storilci ne zavedajo, da delajo nekaj škodljivega in kaznivega. S tem, ko objavljajo sovražne komentarje ali drugo neprimerno vsebino, pogosto mislijo, da imajo pravico do svobode govora in da zaradi tega lahko napišejo in objavijo, kar želijo (Policija, n. d. a; Policija, n. d. c). Tudi, ko objavijo fotografijo neke osebe, brez njihovega dovoljenja je to kaznivo in v žrtvi lahko povzroči negativne občutke, vendar se storilcu ne zdi to nič spornega, saj je mnenja, da gre za šalo in nikomur ni storil nič hudega (West, 2014). Pogosto ne vedo, da se spletni kriminal kaznuje tako kot, če bi storili določeno kaznivo dejanje v realnem svetu. V nekaterih primerih pa so kazni tudi zelo visoke (Policija, n. d. a; Policija, n. d. c).

Težava samih storilcev je tudi v njihovi sproščenosti in ponavljanju kaznivih dejanj. Na samem začetku so storilci bolj previdni in pazljivi pri tem, kaj delajo. Pazijo na svojo zaščito in neprepoznavnost. S tem, ko pa izvršujejo več kaznivih dejanj pa jim to postane že vsakdanja navada in so zaradi tega tudi manj pazljivi in površni. Rezultat

tega pa je, da prihaja do napak, ki jih opazijo osebe in lahko obvestijo policijo, ki jih nato ustrezno kaznuje (Policija, n. d. a; Policija, n. d. c).

S tem ko napadalci grozijo in izsiljujejo več žrtev, lahko pride do njihove združitve in skupaj odkrijejo storilca, glede na podobnost groženj in ga na podlagi tega lažje identificirajo (West, 2014). Velikokrat pa se storilci ne zavedajo tudi tega, da se situacija lahko hitro obrne in, da tudi sami lahko zelo hitro postanejo žrtve kibernetskega kriminala (Leukfeldt idr., 2022).

6 PREDSTAVITEV INTERVJUJEV

Za eksperimentalni del magistrske naloge smo si izbrali kvalitativno metodo raziskovanja. Izbrali smo intervju, s pomočjo katerega je najlažje vzpostaviti stik z žrtvami spletnega nasilja in ker skozi pogovor lahko začutimo in opazimo različna čustva in občutke, ki jih ima v sebi sogovornik.

Za intervjuvanje smo si izbrali dvanajst žrtev spletnega nasilja. Za izvedbo pogovorov smo izbrali ženske, saj so prav one glavni proučevani subjekt in so nas zanimale njihove izkušnje v povezavi s spletnim nasiljem. Izbrali smo ženske različnih starosti, ker nas je zanimalo, če obstaja kakšna razlika v spletnem nasilju med starejšimi in mlajšimi osebami. Najmlajša oseba, s katero smo izvedli intervju je bila stara osemnajst let, najstarejša pa štiriinpetdeset let.

Nekaj oseb, s katerimi smo opravili intervju in so bile žrtve spletnega nasilja, smo osebno poznali že od prej in smo tudi vedeli za njihove izkušnje s spletnim nasiljem. Nekaj izmed intervjuvank je bilo tudi znank drugih oseb, ki so nam nato dali kontakt teh žensk, ki smo jih nato povprašali za sodelovanje v intervjuju. Nekaj žrtev pa je bilo izbranih naključno preko različnih socialnih omrežij. Naključnim intervjuvankam smo najprej poslali zasebno sporočilo, v katerem smo jih povprašali o tem, če so bile že kdaj žrtve spletnega nasilja. V primerih, da so že bile žrtve smo jih vprašali, če bi bile pripravljene sodelovati v intervjuju. S tistimi, ki so želele sodelovati smo nato izvedli intervju.

Intervjuje smo začeli izvajati v začetku meseca aprila in jih izvajali približno en mesec. Pogovori so potekali predvsem v Gorenjski in Osrednjeslovenski regiji. Vse intervjuje smo izvedli v živo, izbiro lokacije smo prepustili žrtvam, saj smo jim želeli zagotoviti najbolj ustrezen prostor, kjer bi se dobro in varno počutile. Vsi intervjuji so bili opravljeni pod pogoji, ki zagotavljajo varnost in zaščito sogovornic. Žrtvam smo zagotovili tudi to, da bodo njihovi podatki ostali anonimni in da ne bodo nikjer

objavljeni. Pred samo izvedbo intervjujev smo dobili tudi soglasje žrtev, da se strinjajo, da z njimi opravimo pogovor.

Sam intervju je sestavljalo dvanajst vprašanj, ki so se med seboj razlikovala. Nekatera vprašanja so bila bolj zaprtega, druga pa bolj odprtega tipa. V samem vprašalniku smo uporabili več vprašanj odprtega tipa, da so imele žrtve možnost podrobnega pripovedovanja in opisovanja svojih zgodb in izkušenj. Vprašanja so se nanašala na njihove izkušnje s spletnim nasiljem in kako se ali so se soočale s takšnimi oblikami odklonskega vedenja in, če je to na njih pustilo kakšne posledice.

Z intervjuji smo želeli tudi preveriti ugotovitve iz literature. Najbolj nas je zanimalo to, kdo so največkrat storilci spletnega nasilja, in če jih žrtve poznajo, njihove izkušnje s spletnim nasiljem in če so takšna dejanja na njih pustila kakšne posledice.

6.1 Glavne značilnosti

Intervjuje sestavlja dvanajst vprašanj, na katere so žrtve odgovorile. V tem delu bomo predstavili vprašanja intervjuja in odgovore žrtev spletnega nasilja.

1. Ali ste bili že kdaj žrtev spletnega nasilja?

Vse intervjuvanke so odgovorile, da so bile že žrtve spletnega nasilja.

2. Žrtev katerega spletnega kaznivega dejanja ste bili (npr. nadlegovanje, izsiljevanje, phishing)?

Ženske, s katerimi smo opravili intervju so bile največkrat žrtve vdorov v profile na socialnih omrežjih, žrtve poskusa vdora v mobilno napravo, veliko jih je bilo tudi žrtev izsiljevanja, groženj in nadlegovanja. Med bolj pogoste odgovore lahko štejemo tudi ustrahovanje, širjenje lažnih govoric, spreminjanje in predelovanj ter objava fotografij žrtev brez njenega dovoljenja. Bilo je tudi nekaj primerov, kjer so ženske izsiljevali z

golimi fotografijami ali pa so jim storilci pošiljali gole fotografije brez njihovega dovoljenja.
Med manj pogoste oblike odklonskega vedenja smo uvrstili phishing napade in prejemanje neprimernih sporočil z namigovanjem na prostitucijo. Bilo je le nekaj žrtev, ki se jim je zgodilo takšno nasilje.

Med najbolj pozitivne oblike spletnega nasilja lahko štejemo poskuse vdorov v mobilno napravo in na socialna omrežja, saj je šlo le za poskus in do dejanskega vdora ni prišlo. Med bolj pozitivne in manj nevarne oblike spletnega nasilja lahko uvrstimo tudi pošiljanje in prejemanje golih fotografij ter prejemanje sporočil s spolno vsebino, saj žrtev na takšna sporočila ni bila prisiljena odgovoriti in jih je lahko izbrisala.

Med bolj negativnimi oblikami pa je zagotovo širjenje lažnih govoric, vdori v naprave, grožnje in nadlegovanje oseb, saj je v teh primerih prišlo do objave ali kraje osebnih podatkov žrtev. Pri takšnih primerih so se žrtve tudi prestrašile in jih je bilo strah, če se bo dogajanje preneslo v fizični svet.

Med najbolj negativne primere pa bi lahko uvrstili phishing napade ter spreminjanje in objavo fotografij. Te vrste napadov se nam zdijo najbolj nevarne, saj zaradi phishing napadov lahko osebe izgubijo vse podatke, ki jih hranijo na mobilni napravi in so posledice lahko zelo velike. Predelava in objava fotografij žrtev brez njenega dovoljenja pa je nevarna, saj lahko takšne fotografije končajo na neprimernih spletnih straneh in se žrtve tega ne zavedajo. Takšne fotografije na internetu ostanejo ves čas in se jih zelo težko izbriše in zaradi tega lahko žrtve celo življenje nosijo posledice.

3. Kdo je izvrševal spletno nasilje nad vami in, če mogoče veste, zakaj je bilo temu tako?

Pri tem vprašanju so bili najpogostejši odgovori povezani s tem, da so bili storilci neznane osebe in jih žrtve niso poznale. To je bilo predvsem v primerih vdorov v

spletne profile. Pri vdoru v mobilno napravo se je na žrtvinem telefonu izpisala lokacija, kjer so ji poskušali vdreti v telefon. V primeru phishing napadov pa sta žrtvi povedali, da sta bili le eni izmed mnogih žrtev in, da je bilo takšno dejanje verjetno naključno. Tudi v primeru prošnje za prostitucijo je bil storilec neznana oseba, saj je sporočila pošiljal preko lažnih profilov kot vrinjeno pošto.

Primer neznanega storilca je opisala tudi gospa, ki je nek moški obtožil, da v službi gleda pornografske video vsebine. V tem primeru je bil storilec neznan moški, ki je zahteval nakazilo denarja na bančni račun ali pa bi informacije posredoval naprej do lastnikov podjetja.

V nekaj primerih pa so ženske poznale osebe, ki so nad njimi izvrševale nasilje. Največkrat je šlo za primere, ko so se nekdanji partnerji ženskam želeli maščevati. Pri tem je šlo za to, da so želeli objaviti intimne fotografije nekdanjih partnerk. Imeli smo tudi primer, ko je nek moški izsiljeval dekle s tem, da naj mu pošlje gole fotografije.

V nekem primeru je bil storilec poznana oseba, saj ga je ženska prej spoznala preko aplikacije za zmenke. Poznala je tudi razlog, zakaj ji je storilec grozil in ta razlog je bil razočaranje, saj se ženska ni želela dobiti z njim na drugem zmenku.

Zelo zanimiv primer pa je bil, ko je ženska spoznala moškega v nočnem klubu in jo je kasneje dodal za prijateljico na Facebooku in ji je kar na enkrat začel pošiljati gole fotografije brez njenega dovoljenja.

Zelo zanimiv je bil primer, ko je žrtev omenila, da poza storilce, ki so ji vdrli v Facebook račun. Posebnost tega primera je ta, da so takšno nadlegovanje storila dekleta, ki jih je poznala, njihov namen pa je bil, da bi jo osramotila.

4. Kje se je nad vami izvajalo spletno nasilje? Preko socialnih omrežij, ali kako drugače?

Največ primerov spletnega nasilja se je dogajalo preko socialnih omrežij, med katerimi so bili najpogostejši odgovori Facebook, Instagram in Snapchat. Nekaj primerov se je zgodilo tudi preko elektronske pošte (Gmail) in aplikacije Tinder, ki je namenjena spoznavanju novih ljudi in zmenkom. Nekaj pa je bilo tudi primerov, kjer se je nasilje izvajalo preko SMS in MMS sporočil.

5. Ste bili mogoče večkrat žrtev spletnega nasilja, ali se vam je to zgodilo le enkrat in se je potem nasilje končalo?

Najbolj pogost odgovor intervjuvank je bila ta, da so bile le enkrat žrtve spletnega nasilja. Nekatere pa so bile žrtve tudi dvakrat ali večkrat, kjer so bile večkrat žrtve enakih oblik spletnega nasilja in je bil tudi storilec vedno ista oseba. Nekatere pa so bile žrtve večkrat in sicer so se jim zgodili različni primeri kaznivih dejanj in so bili tudi storilci velikokrat druge osebe. V nekaterih izmed teh primerov so bili storilci znane in neznane osebe.

6. Ali ste komu povedali za spletno nasilje, ki se vam je dogajalo? Ste se mogoče obrnili tudi na kakšno organizacijo za pomoč žrtvam spletnega nasilja, ali vam je pomagala tudi kakšna uradna oseba?

Najpogosteje so sogovornice odgovorile, da so za primere nasilja povedale vsaj eni osebi. To so najpogosteje osebe, ki jim zelo zaupajo. Največkrat so takšne osebe partnerji žensk, prijatelji, sodelavci in družina. Bilo je tudi nekaj primerov, kjer so se ženske obrnile na uradne osebe ali na centre za pomoč. Ena izmed njih se je poleg družine obrnila še na Društvo za nenasilno komunikacijo, ki ji je ponudilo pomoč. Žrtvi v primeru phishinga je pomagal računalničar, ki ji je nekatere podatke lahko obnovil.

Ena izmed žrtev je svojo izkušnjo prijavila policiji, saj je nasilje prišilo tako daleč, da se je bala za svoje življenje. V tem primeru je policija storilcu odredila tudi pripoved

približevanja. Le na takšen način se je lahko izognila moškemu, ki jo je zasledoval in ji grozil.
Vse ženske, ki so sodelovale v intervjuju so povedale, da bi se v primeru nadaljevanja nasilja obrnile na policijo. Nanje bi se obrnile tudi v primeru, če bi njihovo življenje postalo ogroženo in bi se bale za svojo varnost.

7. Ali je takšno nasilje na vas pustilo hude posledice in če se z njimi soočate še danes?

Pri tem vprašanju so se pokazale razlike med samimi oblikami odklonskega vedenja in kako je žrtev to sprejela. Eden izmed bolj pozitivnih primerov je ta, ko je ženska dobivala prošnje za spolne odnose. Povedala je, da na srečo takšno dejanje na njej ni pustilo hudih posledic, ni pa se počutila prijetno. Omenila je tudi, da se ji je takšna ponudba zdela skoraj nemogoča, saj ni verjela, da se to danes še dogaja in, da lahko tudi sama postane žrtev tega.

Med bolj negativne primere bi lahko uvrstili odgovor ženske, ki je bila žrtev kraje podatkov. Ta gospa je priznala, da danes postane zelo nervozna, če prejme elektronsko pošto neznanega pošiljatelja. Omenila je tudi, da na banko sedaj hodi samo osebno in da ne opravlja več nobenih storitev preko spletne banke.

Ena intervjuvanka je povedala, da se boji biti sama in da vedno opazuje okolico, kje se kdo nahaja. Izogibati se je začela tudi bolj sumljivih oseb. Eno izmed intervjuvank pa je strah, da ne bi moški prišel k njej v službo in ji tam začel groziti. Ta dva primera bi zagotovo lahko uvrstili med bolj negativne odgovore.

Nekatere izmed žrtev nadlegovanja so postale bolj nezaupljive do socialnih omrežij in se bojijo, da bi kdo pridobil njihove osebne podatke ali ukradel njihove fotografije. Nekatere so postale bolj pazljive in pazijo, koga sprejmejo v krog prijateljev na

socialnih omrežjih. Nekatere se ob občutkih pritiska s strani socialnih omrežij z njih preprosto umaknejo za nekaj dni.
Nekaj žensk pa je povedalo, da niso imele nobenih posledic in da se danes z njimi ne soočajo.

8. Zanima me, če se je nasilje, ki ste ga doživeli preko spleta preneslo tudi v vaše vsakdanje življenje?

V tem delu sta najbolj zanimiva dva negativna odgovora žrtve. V prvem primeru se je nasilje nad žrtvijo najprej preneslo iz fizičnega v virtualni svet, kasneje pa nazaj v fizični svet. Bivši partner je žensko zasledoval in jo čakal pred hišo, ter ji grozil, da bo ubil njo in njeno družino. Žrtev je bila pri tem zelo prestrašena in se je obrnila na pomoč policije. V tem primeru ji je nekdanji partner tudi grozil s tem, da bo objavil na socialnih omrežjih njene gole fotografije. Na njen profil je pisal neprimerne in nesprejemljive komentarje o njej.

V drugem primeru pa je moški zasledoval žensko in jo čakal v garaži pred blokom. Sledil ji je tudi na delovno mesto in jo tam kdaj čakal. Žrtev je bila takrat zelo prestrašena in ni upala sama hoditi do avtomobila. Imela je občutek, da jo v določenih trenutkih nekdo opazuje in nadzira.

Kljub nekaterim izjemam je bil najpogostejši in najbolj pozitiven odgovor intervjuvank ta, spletno nasilje na njihovem življenju ni pustilo vidnih posledic. Takšne osebe nimajo nobenega večjega strahu pred tem, da bi se nasilje nad njimi pojavilo v realnem svetu.

9. Ali vam je spletno nasilje, ki ste ga doživeli spremenilo življenje in zaradi tega določenih aktivnosti izogibate/ vas je strah/ste bolj previdni?

Vse intervjuvanke so podale odgovor, da jim je izkušnja s spletnim nasiljem spremenila življenje. Vse so omejile svojo aktivnost na socialnih omrežjih, postale so tudi

previdnejše, kaj objavljajo in kaj komentirajo. Ena izmed njih je povedala, da sproti briše pogovore na socialnih omrežjih, saj se boji, da bi ji ponovno vdrli v profil in objavili pogovore. Žrtve tudi ne obiskujejo več tako pogosto aplikacij za zmenke in se ne videvajo več z vsakim, ki jim pošlje sporočilo. Osebe večkrat premislijo preden kaj objavijo in uporabljajo samo preverjene spletne strani, ki so vredne zaupanja.

10. Je kdaj spletno nasilje prišlo tako daleč, da ste si želeli škodovati?

Pri tem vprašanju je bil največkrat podan odgovor ne. V večini primerih je bil odgovor pozitiven in so ženske pritrdile, da nikoli ni nasilje prišlo tako daleč, da bi si želele škodovati.

Neprijetni občutki so se pojavili le pri eni osebi, ki je bila zelo obupana in nervozna, ter ni vedela, kaj naj stori. Včasih je bila zelo izmučena ter zaskrbljena in ni več videla smisla v življenju. Na trenutke so se v njej pojavljale misli o samo poškodovanju, ampak so ji prijatelji in družina pravočasno pomagali.

11. Ste pred spletnim nasiljem uporabljali preventivne ukrepe za zaščito pred takimi dejanji?

Vse intervjuvanke so priznale, da pred spletnimi napadi niso uporabljale veliko preventivnih ukrepov, saj jih niso poznale in niso vedele, kaj jim lahko pomaga. Edini preventivni ukrep, ki so ga uporabljale so bila različna gesla, ki niso bila najbolj enostavna. Večina izmed njih pa je bila mnenja, da se kaj takega njim ne more pripetiti.

12. Ali ste danes še kdaj žrtve spletnega nasilja, ali se je za vas to končalo?

Vse ženske so odgovorile, da se je trenutno zanje spletno nasilje končalo in da imajo mir. Nekatere izmed njih pa se zavedajo, da se lahko stanje hitro spremeni in, da morajo biti vedno pripravljene, če se kaj takšnega zopet pojavi.

6.2 Odgovori na hipoteze

S pomočjo prebrane literature in intervjujev pa lahko sedaj tudi pogledamo naše hipoteze, ki smo si jih zastavili pred pisanjem naše magistrske naloge. Z zbranimi informacijami jih bomo poskušali potrditi ali zavrniti.

Hipoteza 1: Kibernetska kriminaliteta je v zadnjih letih postala ena izmed najbolj razširjenih oblik kriminalitete in se z vsakim dnem bolj razvija in narašča.

To hipotezo lahko potrdimo, saj smo s pomočjo literature ugotovili, da je število kaznivih dejanj, ki se dogajajo na spletu močno naraslo (Bernik in Meško, 2011). Tudi statistični podatki nakazujejo na to, da se je kriminaliteta preselila v novo okolje imenovano kibernetski prostor (Dimc in Dobovšek, 2012). Temu pa je tako predvsem zaradi prenosa vsakdanjih aktivnosti na splet. Zadnja leta se veliko dejavnosti odvija v kibernetskem prostoru, ki ga ljudje vsakodnevno uporabljamo (Choudhury in Malik, 2019).

Tudi s pomočjo intervjujev potrdimo hipotezo, da je spletno nasilje pogost pojav. Ugotovili smo, da se je v nekaterih primerih nasilje iz fizičnega sveta pri žrtvah preneslo na spletna okolja. Nekatere intervjuvanke so bile večkrat žrtve spletnega nasilja, kar nakazuje na pogostost in razširjenost spletnega nasilja. Tudi raznolikost napadov nakazuje na njihov razvoj in spreminjanje. Takšne oblike napadov so vsak dan bolj razvite in nevarne, storilci pa bolj izpopolnjeni.

Hipoteza 2: Posledice kibernetskega nasilja so vidne tudi v realnem svetu zunaj kibernetskega prostora.

To hipotezo lahko potrdimo, saj smo ugotovili, da se velikokrat občutki žrtev spletnega nasilja prenesejo tudi v njihovo vsakodnevno življenje. Videli smo, da lahko spletno nasilje za seboj potegne kar nekaj stvari, ki so vidne v fizičnem svetu. Največkrat za

seboj pusti psihološke, socialne, finančne in fizične posledice na osebah (West, 2014). Hkrati se vsa sodna in druga pomoč žrtvi odvija v realnem svetu (Obran, 2014).

Tudi z raziskovalno pomočjo smo prišli do tega, da so se primeri odklonskega vedenja storilcev in oblike spletnega nasilja nekaterih žrtev prenesla v realni svet. Takšen primer je zasledovanje ženske pred blokom in sledenje do delovnega mesta, ter primer, kjer je storilec izvrševal fizično nasilje nad žrtvijo in jo ustrahoval na krajih, kjer se je oseba nahajala. S pomočjo teh dveh primerov vidimo, da lahko spletno nasilje za seboj pusti resne posledice v realnem svetu.

Hipoteza 3: Najpogostejši izvajalci spletnega nasilja nad ženskami moški.

Tudi to hipotezo lahko potrdimo. Ugotovili smo, da so največkrat storilci spletnega nasilja moški, ki želijo prikazati svojo moč in nadvlado nad ženskami (Van der Wilk, 2018). Največkrat so storilci beli, heteroseksualni mlajši moški, ki imajo višji statusni položaj. Pogosto ženske uporabnice zatirajo in jim dajo občutek, da so manj vredne in, da internet ni prostor zanje. Moški velikokrat mislijo, da so glavni in lahko počnejo, kar jim paše (West, 2014).

Izvedba intervjujev je potrdila to hipotezo. Skoraj vsaka ženska, s katero smo opravili intervju je povedala, da so ji v primerih spletnega nasilja nagajali moški. Ti moški so bili lahko znane ali neznane osebe. Z intervjuji smo ugotovili, da so bili največkrat znani moški storilci v nekakšni povezavi z žrtvami. Največkrat so bili to njihovi nekdanji partnerji ali drugi znanci, s katerimi so imele nekakšno romantično vez. Neznani moški pa so bili naključni in jih ženske niso poznale.

Hipoteza 4: Kibernetsko nasilje je lažje izvedljivo in storilce je težje odkriti, zaradi anonimnosti na spletu.

Tudi ta hipoteza je resnična in jo lahko potrdimo. Storilci so v večini primerov spletnega nasilja anonimni in s tem izkazujejo svojo moč in pogum (West, 2014). Z anonimnostjo si pridobijo tudi več poguma, hkrati pa se njihove omejitve in vest počasi izgubljata (Žakelj, 2013). Z ustvarjanjem lažnih profilov si dovolijo in upajo veliko in ne poznajo nobenega sramu pri tem kar delajo (West, 2014). Velikokrat pa zaradi tega tudi izgubijo občutek o tem, kaj je prav in kaj narobe.

Preko intervjujev smo ugotovili to, da si osebe preko lažnih profilov dovolijo zelo veliko. Najboljši pokazatelj za potrditev te hipoteze je primer, ko so eni izmed žensk pošiljali ponudbe za spolne odnose v zameno pa bi ji kupili stvari ali ji dali denar. Vse to je pisala neznana oseba preko lažnega profila na socialnem omrežju, ki ga je kasneje zbrisala in ga ni bilo več mogoče najti.

Hipoteza 5: Storilci kibernetskega kriminala so bolj pogumni in se počutijo varneje pri izvajanju spletnega nasilja, saj so mnenja, da na spletu lahko počnejo kar si želijo brez omejitev.

Vsi storilci si preko spleta dovolijo veliko več, saj žrtve v resnici ne poznajo in je mogoče v realnem svetu tudi nikoli ne bodo srečali (West, 2014). Storilci lahko presegajo nacionalne meje in izvajajo kazniva dejanja z drugega konca sveta (Bernik in Meško, 2011). S tem, ko jih nihče ne pozna si tudi veliko dovolijo in ne pomislijo na posledice, ki jih lahko doletijo.

Tudi pri intervjujih se je to izkazalo za resnično stvar. V večini primerov, ko je bil storilec neznan, je bilo njihovo odklonsko vedenje hujše in kompleksnejše. Storilci so si upali več in so ženske spraševali za nenavadne stvari in jim grozili. V primerih, ko pa so bili storilci znani, kazniva dejanja niso segala v neke ekstremne primere. Pri neznanih osebah prevladuje mišljenje, da jih nikoli nihče ne more odkriti in jih kaznovati. S pomočjo teh ugotovitev lahko tudi zadnjo, peto hipotezo potrdimo.

7 RAZPRAVA

S pomočjo prebrane literature in intervjujev smo ugotovili, da je kibernetski kriminal nova oblika kriminalitete, ki se hitro širi po celem svetu, pri tem pa presega nacionalne meje.
Pridobljeni raziskovalni podatki so potrdili tudi to, da so največkrat žrtve ženskega spola in, da so storilci v večini primerov moški.

Zelo zanimivo se nam je zdelo, da kibernetsko nasilje izvajajo zelo izobražene ali pa zelo ne izobražene osebe, vse pa je odvisno od vrste kaznivega dejanja. Zanimivo je, da je razpon med oblikami kibernetskega nasilja kar velik in lahko skoraj vsaka oseba izvaja spletno nasilje, če si to želi.

Ugotovili smo, da je pri obravnavi spletnega nasilja zelo pomembna tudi zakonodaja, saj nam pomaga pri pomoči žrtvam in sankcioniranju storilcev. Presenetilo nas je predvsem to, da v Sloveniji obstaja kar nekaj organizacij in drugih ustanov, ki pomagajo žrtvam v primerih spletnega nasilja.

S pomočjo literature in intervjujev smo ugotovili, da žrtve res malokrat prijavijo spletno nasilje policiji ali prosijo za pomoč. Po navadi spletno nasilje prijavijo policiji šele takrat, ko je njegova stopnja že zelo visoka in pusti za seboj hude posledice. Za pomoč žrtve največkrat prosijo v primerih, ko izgubijo svoje podatke na napravah.

Zelo pomembna stvar, ki smo jo spoznali skozi branje literature je, da se uporabljajo preventivni, zaščitni ukrepi, ki nam pomagajo, da se že sami zaščitimo in s tem težje postanemo tarče nepridipravov. Pri izvedbi intervjujev nas je presenetilo, da veliko žensk pred napadi ni poznalo drugih preventivnih ukrepov, kakor dolga in zahtevna gesla. Preventivni ukrepi so pomembni tudi zaradi tega, ker nas v primeru groženj opozorijo in zavarujejo.

Veliko presenečenje pa je bilo, ko smo ugotovili, da lahko spletno nasilje za seboj pusti hude posledice, ki imajo vpliv na zdravje oseb. Zdravje pa ni edina stvar, na katero vpliva spletno nasilje, ampak lahko za seboj pusti tudi ekonomske in socialne posledice. Ugotovili smo, da so se nekatere osebe začele izogibati določenih dejavnosti ali so postale zelo previdne pri tem, kaj počnejo.

Negativno nas je presenetilo, da se v nekaterih primerih žrtvam ne pomaga in da se prav njih krivi za nastanek spletnega nasilja. Pogosto žrtvam tudi priporočajo, da se umaknejo iz interneta, če jim nasilje ni všeč. Določeni ljudje pa jim vzamejo pravico do opravljanja različnih dejavnosti v kibernetskem prostoru.

Večje odstopanje med prebrano literaturo in izvedbo intervjujev smo našli le pri najpogostejših oblikah spletnega nasilja. V literaturi je bilo v večini primerov navedeno, da so ženske največkrat žrtve sextinga, nadlegovanja in groženj, v intervjujih pa se je pokazalo, da so bile spraševane žrtve največkrat deležne vdorov v profile na socialnih omrežjih in vdore v mobilne naprave.

8 ZAKLJUČEK

Z izvedbo intervjujev in prebiranjem literature smo lahko potrdili vseh pet hipotez, ki smo si jih zastavili. Ugotovili smo, da je kibernetska kriminaliteta v zadnjih letih res narasla in da je pogostejša kakor klasična kriminaliteta. Videli smo, da se njene posledice lahko prenesejo tudi v realni svet in da so najpogostejši storilci spletnega nasilja prav moški, ki imajo veliko poguma in samozavesti, da izvršujejo spletno nasilje, saj v njih najpogosteje prevladuje mišljenje, da so zaščiteni in da jih policija ne more kaznovati.

Prva stvar, ki se nam zdi zelo pomembna in bi lahko zmanjšala število žrtev je uporaba različnih preventivnih ukrepov, ki nekatere vrste napadov in nasilja lahko popolnoma preprečijo, ali pa nas vsaj opozorijo na nevarnosti. Pomembno je, da pri uporabi interneta in aplikacij ne nasedamo vsem ljudem, ki nekaj prijaznega napišejo. V primerih, ko dobimo sporočilo neznane osebe to pogledamo in premislimo ali nam je v tem sporočilu kaj sumljivega ali ne. Paziti bi morali, da ne vpisujemo osebnih podatkov, gesel in telefonskih številk na nepreverjene strani, saj je to velikokrat pokazatelj, da gre za lažno stran.

Priporočljivo bi bilo, da bi ljudi poskušali čim bolj seznaniti s pastmi na spletu in jim pokazati, na kaj morajo biti še posebej pozorni. Na to temo bi lahko potekale različne delavnice ali oddaje, ki bi predstavile resnost takšnih dejanj. Takšne dejavnosti bi se lahko izvajale v šolah in na delovnih mestih.

Pomembno se nam zdi, da žrtve spregovorijo o svojih izkušnjah in da se jim pomaga ter opomni na to, da niso same v boju proti nasilju. Priporočljivo bi bilo, da se policiste in druge osebe pouči o tem s pomočjo raznih izobraževanj. Poudariti je potrebno, da je kibernetsko nasilje lahko enako ali bolj nevarno kot klasični kriminal.

Pri pisanju magistrske naloge pa se je pojavilo tudi nekaj manjših težav, ki so bile v večini povezane s pridobivanjem virov. Na največ ovir smo naleteli, ko smo iskali vire o primerjavi klasične in kibernetske kriminalitete. Skoraj vsa literatura, ki je obravnavala omenjeno tematiko, se je v večini ozirala bolj na to, kdo so storilci obeh vrst kriminalitete in kakšne so razlike in podobnosti med njimi. Težje pa je bilo zaslediti, katerih vrst kaznivih dejanj je več. Manj literature smo našli tudi pri opisovanju prednosti in slabosti izvajalcev spletnega nasilja.

Pri nadgradnji magistrskega dela bi se mogoče osredotočili tudi na bolj podrobno obravnavo oblik spletnega nasilja in kaznovanja storilcev. Obiskali bi javno sodbo, kjer bi potekalo sojenje proti povzročitelju spletnega nasilja in bi si zapisali glavne točke obravnave in na takšen način prišli do tega, kako vse skupaj poteka in kako zahteven proces je to. Izbrali bi tudi različne države in jih primerjali s Slovenijo, na takšen način pa bi prišli do podobnosti in razlik med posameznimi državami. S tem bi ugotovili, katere stvari potekajo podobno in katere drugače.

Za nadgradnjo pa bi izvedli še intervjuje s strokovnjaki s področja kibernetske varnosti, da bi dobili še drug pogled na to tematiko in bi nam oni mogoče znali še kaj svetovati in pomagati. Na takšen način bi lahko med seboj primerjali izkušnje žrtev in mnenja strokovnjakov, ki bi nam pomagala pri določitvi širše slike o tej tematiki. S tem bi spoznali, kako resen problem je v resnici kibernetsko nasilje. S pomočjo strokovnjakov bi lahko izvedli različne delavnice na temo spletnega nasilja, kjer bi ljudem predstavili resnost teh primerov, kako se z njimi spoprijeti in kako se pred njimi najbolje obvarovati.

VIRI IN LITERATURA

Al-Nemrat, A., Hosseinian-Far, A. in Jahankhani, H. (2014). Chapter 12- cybercrime classification and characteristics. V B. Akhgar, A. Staniforth in F. Bosco (ur.), *Cyber crime and cyber terrorism investigator's handbook* (str. 149–164). Syngress. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey* [Doktorska disertacija]. Mississippi State University. https://scholarsjunction.msstate.edu/cgi/viewcontent.cgi?article=2243&context=td

Bernik, I. in Ilievski, A. (2013). Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje. *Varstvoslovje, 15*(3), 317–337. https://www.fvv.um.si/rV/arhiv/2013-3/02_CombatingCybercrimeInSlovenia_2013_3.pdf

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminaliteto, 62*(3), 242–252. https://www.policija.si/images/stories/Publikacije/RKK/PDF/2011/03/RKK2011-03_Bernik_Mesko_KibernetskeGroznje.pdf

Bhasin, H. (6. 11. 2018). *What are the uses of social media?.* Marketing91. https://www.marketing91.com/what-are-the-uses-of-social-media/

Bohinec, A. (10. 3. 2021). *Ali smo na spletu varni?.* Zdaj. https://zdaj.net/solski-otrok/ali-smo-na-spletu-varni/

Brodnik, A. (ur.). (2015). *Informatika 1: E-učbenik za informatiko v gimnaziji.* Založba Univerze na Primorskem. https://lusy.fri.uni-lj.si/ucbenik/book/1901/index.html

Bulatović, K. (4. 8. 2017). Spletno nasilje: ključno je, da žrtev o nadlegovanju ne molči. *Delo.* https://old.delo.si/novice/slovenija/spletno-nasilje-kljucno-je-da-zrtev-o-nadlegovanju-ne-molci.html

Bussell, J. (12. 3. 2013). Cyberspace. V *Encyclopedia Britannica*. https://www.britannica.com/topic/cyberspace

Carr, C. T. (2015). Social media: Defining, developing and divining. *Atlantic journal of communication*. https://asset-pdf.scinapse.io/prod/2138156863/2138156863.pdf

Center za varnejši internet. (n. d. a). *Spletno nasilje*. Safe.si. https://safe.si/nasveti/spletno-in-mobilno-trpincenje/spletno-nasilje

Center za varnejši internet. (n. d. b). *Mobilna naprava.* Safe.si. https://safe.si/pojmi/mobilna-naprava

Center za varnejši internet. (n. d. c). *Točka osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje*. Safe.si. https://safe.si/

Cherry, K. (20. 2. 2021). *The big five personality traits.* Very well mind. https://www.verywellmind.com/the-big-five-personality-dimensions-2795422

Choudhury, S. In Malik, J. K. (2019). Cyber space- evolution and growth. *East African Scholars Journal of Education, Humanities and Literature, 2*(3), 170–190. https://www.easpublisher.com/media/articles/EASJEHL_23_170-190_c.pdf

Citron, K. D. (2009). Law's expressive value in combating cyber gender harassment. *Michigan Law Review, 108*(3). https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1300&context=mlr

Covid-19 je okrepil trend rasti kibernetskih napadov. (23. 10. 2020). *Delo.* https://www.delo.si/novice/slovenija/covid-19-je-okrepil-trend-rasti-kibernetskih-napadov/

Cyberspace. (n. d.). V *Techopedia.* https://www.techopedia.com/definition/2493/cyberspace

Čaleta, D. in Powers, J. F. (2020). *Cyber terrorism and extremism as threat to critical infrastructure protection.* Ministry of Defense Republic of Slovenia, Joint Special Operations University from Tampa, USA and Institute for Corporative Security Studies.

Dennis, M. A. (2022). Internet. V *Encyclopedia Britannica*. https://www.britannica.com/technology/Internet

Densley, J. in Peterson, J. K. (2017). C*yber violence: What do we know and where do we go from here*?. College of Liberal Arts All Faculty Scholarship. https://digitalcommons.hamline.edu/cgi/viewcontent.cgi?article=1004&context=cla_faculty

Dimc, M. in Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi.* Fakulteta za varnostne vede.

Direktiva EU o napadih na informacijske sisteme. (14. 8. 2013). *Uradni list EU,* (L 218/8). https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32013L0040&from=EN

Društvo SOS. (n. d.). *Potrebujete pomoč?.* Pridobljeno na https://drustvo-sos.si/oblike-pomoci/

Društvo za nenasilno komunikacijo. (n. d.). *Nasilje nad ženskami.* https://drustvo-dnk.si/o-nasilju/nasilje-nad-zenskami.html

Dunn, S., Lalonde, J.S. in Bailey, J. (2017). Terms of silence*. Berghahn journals, 10*(2). https://www.berghahnjournals.com/view/journals/girlhood-studies/10/2/ghs100207.xml

Faith, B. In Fraser, E. (17. 10. 2018). What works to prevent cyber violence against women and girls?. *VAWG Helpdesk Research Report*, 212. https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/14764/vawg-helpdesk-report-212-what-works-cybervawg.pdf?sequence=1)

Favela, L. O. (2010). Female cyberbullying: Causes and prevention. *Inquiries Journal Strategies*, *2*(11). http://www.inquiriesjournal.com/articles/322/female-cyberbullying-causes-and-prevention-strategies

Feijóo, S., Foody, M., O'Higgins Norman, J., Pichel, R. in Rial, A. (2021). Cyberbullies, the cyberbullied, and problematic internet use: Some reasonable similarities. *Psicothema, 33*(2), 198–205. http://www.psicothema.com/pdf/4664.pdf

Fruhlinger, J. (4. 9. 2020). *What is phishing? How this cyber attack works and how to prevent it.* CSO. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Horvat, D., Plaz, M. in Veselič, Š. (2014). *Priročnik za delo z ženskami in otroki z izkušnjo nasilja.* Društvo SOS telefon za ženske in otroke – žrtve nasilje. https://drustvo-sos.si/wp-content/uploads/2019/08/prirocnik-za-deloz-zenskami-in-otroki-z-izkusnjo-nasilja.pdf

Johnson, O. (n. d.). *Forms of cyber violence.* Liberty Lane. https://www.libertylane.ca/forms-of-cyber-violence.html

Kanduč, Z. (2003). Žrtve in viktimizacije v viktimološki in družbenokritični perspektivi. *Revija za kriminalistiko in kriminologijo, 54*(1), 23–40. https://www.policija.si/images/stories/Publikacije/RKK/PDF/2003/01/RKK2003-01_ZoranKanduc_ZrtveInViktimizacije.pdf

Karl. (13. 8. 2021). *The 15 Biggest social media stes and apps [2022].* Dreamgrow. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

Kaspersky. (2020). *What is social engineering?.* https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kastelic, Ž. (3. 9. 2020). *Kaj je Istanbulska konvencija?.* Študent. https://www.student.si/izpostavljeno/druzba/kaj-je-istanbulska-konvencija/?cn-reloaded=1

Kazenski zakonik (KZ-1-UPB2). (2012, 2015, 2016, 2017, 2020, 2021). *Uradni list RS*, (50/12, 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21). http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050

Ključni nasveti za varnost vaših računov. (n. d.). Varni na internetu. https://www.varninainternetu.si/kljucni-nasveti-za-varnost-vasih-racunov/

Klun, M. in Meško, G. (2017). Pregled študij o strahu pred kriminaliteto pri ženskah. *Varstvoslovje, 19*(1), 5–20. https://www.fvv.um.si/rV/arhiv/2017-1/01_Klun_Mesko_rV_2017_1.pdf

Kogovšek, A. (13. 9. 2021). *Kakšne so pasti socialnega inženiringa in kako se lahko zavarujete pred njim?.* Opticyber3. https://opticyber3.com/kaksne-so-pasti-socialnega-inzeniringa-in-kako-se-lahko-zavarujete-pred-njim-2/

Konvencija o kibernetski kriminaliteti. (2004). *Uradni list RS,* (17/04). http://www.svetevrope.si/sl/dokumenti_in_publikacije/konvencije/185/index.html

Konvencija Sveta Evrope o preprečevanju in boju proti nasilju nad ženskami in nasilju v družini. (7. 4. 2011). *Council of Europe,* (210). https://rm.coe.int/1680462542

Kraskova, Z. G. (24. 2. 2017). *Kolumna bralke: Viktimizacija ali povračilni ukrepi.* Delo. https://old.delo.si/mnenja/gostujoce-pero/viktimizacija-ali-povracilni-ukrepi.html

Krebelj, P. (16. 11. 2021). *Spletno nasilje se lahko zgodi tudi tebi! # Odklikni.* SŠTS Šiška. http://odklikni.enakostspolov.si/

Leaf. (2019). *10 ways to prevent cyber attacks.* https://leaf-it.com/10-ways-prevent-cyber-attacks/

Leukfeldt, E. in Weijer, S. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Leukfeldt, E., Schiks, J. in Weijer, S. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers and Human Behavior*, (126). https://doi.org/10.1016/j.chb.2021.106985

Magnet, S. in Mason, C. L. (2012). Surveillance studies and violence against women. *Surveillance & Society*, *10*(2), 106–118. https://doi.org/10.24908/ss.v10i2.4094

Markelj, B. in Zgaga, S. (2018). Kibernetska varnost in kibernetska kriminaliteta uporabnikov mobilnih naprav v Sloveniji. *Revija za kriminalistiko in kriminologijo, 69*(1), 15–29. https://www.policija.si/images/stories/Publikacije/RKK/PDF/2018/01/RKK2018-01_BlazMarkelj_KibernetskaVarnostInKriminaliteta.pdf

Matijašič, B. (21. 11. 2021). O*zaveščevalna kampanija #Odklikni: Ustavimo spletno nasilje nad ženskami in dekleti!.* Osnovna šola Ljudski vrt Ptuj. https://www.os-ljudskivrtptuj.si/ozavescevalna-kampanja-odklikni-ustavimo-spletno-nasilje-nad-zenskami-in-dekleti/

Mayer, T. (7. 9. 2020*). Istanbulska konvencija je najmočnejši ukrep proti nasilju nad ženskami in v družini: O pozivu Poljske k novi definiciji družine, poroke in otroka, odzivu Slovenije in pomenu istanbulske konvencije.* MMC RTV Slovenija. https://radioprvi.rtvslo.si/2020/09/istanbulska-konvencija-je-najmocnejsi-ukrep-proti-nasilju-nad-zenskami-in-v-druzini/

Mlakar, T. (7. 10. 2021). *Soočanje z dvomljivimi informacijami na novičarskih spletnih straneh ali družbenih medijih.* Statistični urad RS. https://www.stat.si/StatWeb/News/Index/9704

Novaković, T. (ur.). (2019). *Odklikni!: Ustavimo spletno nasilje nad ženskami in dekleti.* Fakulteta za družbene vede, Center za družboslovno informatiko.

Obran, N. (2014). *Nasilje nad ženskami – prav(n)e poti v varno življenje žensk in otok.* Društvo za nenasilno komunikacijo.

Pajtler, A. (2002). Kibernetski prostor. *Fakulteta za družbene vede, Univerza v Ljubljani*. http://uploadi.www.ris.org/editor/1132058378Kibernetski_prostor.pdf

Petek, A. (ur.). (2019a). *Odklikni! : ustavimo spletno nasilje nad ženskami in dekleti: Priročnik za strokovnjakinje in strokovnjake, ki delajo z mladimi.* Fakulteta za družbene vede, Univerza v Ljubljani. https://www.gov.si/assets/ministrstva/MDDSZ/Enake-moznosti/OdklikniPrirocnikMladina.pdf

Petek, A. (ur.). (2019b). *Odklikni! : ustavimo spletno nasilje nad ženskami in dekleti: Priročnik za strokovnjakinje in strokovnjake, ki delajo z mladimi.* Fakulteta za družbene vede, Univerza v Ljubljani. http://odklikni.enakostspolov.si/ozavescanje-in-pomoc/

Plesničar, M. M. (ur.). (2012). *Nežnejši spol? Ženske, nasilje in kazenskopravni sistem.* Inštitut za kriminologijo pri Pravni fakulteti.

Policija. (n. d. a). *Ne postanite tarča spletnega izsiljevanja z golimi posnetki ali fotografijami!.* https://www.policija.si/index.php/sl/preventiva-/kriminaliteta/78867-izsiljevanje-preko-spleta-in-druabnih-omreij

Policija. (n. d. b). *Starši in otroci, zavarujte se pred zlorabami na internetu.* https://www.policija.si/index.php/sl/preventiva-/kriminaliteta/6020-stari-in-otroci-zavarujte-se-pred-zlorabami-na-internetu-policija-svetuje

Policija. (n. d. c). *Varni na internetu.* https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu/varni-na-internetu

Rupnik, A. (2003). *Konvencija o kibernetski kriminaliteti: »Budimpeštanska konvencija«.* http://uploadi.www.ris.org/editor/1132054990Kiber_kriminaliteta.pdf

Schober, S. (27. 1. 2015). *Deep dark web of the internet iceberg.* Scottschober. https://scottschober.com/deep-dark-web-of-the-internet-iceberg/

Sedej, A. in Završnik, A. (2012). Spletno in mobilno nadlegovanje v Sloveniji. *Revija za kriminalistiko in kriminologijo, 63*(4), 263–280. https://www.policija.si/images/stories/Publikacije/RKK/PDF/2012/04/RKK2012-04_Zavrsnik_Sedej_SpletnoInMobilnoNadlegovanje.pdf

Seksizem. (2014). V *Slovar slovenskega knjižnega jezika* (2. dopolnjena in deloma prenovljena izd.). https://fran.si/iskanje?View=1&Query=seksizem

SI-CERT. (n. d.). *O centru SI-CERT.* Pridobljeno na https://www.cert.si/o-nas/

Starcevic, V. in Aboujaoude, E. (2015). Cyberchondria, cyberbullying, cybersuicide, cybersex: "new" psychopathologies for the 21st century?. *World Psychiatry, 14*(1), 97–100. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4329904/

Sukhai, N. B. (2004). Hacking and cybercrime. V InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development (str. 128–132). https://doi.org/10.1145/1059524.1059553

Svet Evropske Unije. (4. 1. 2022). *Kibernetska varnost: Kako se EU spoprijema s kibernetskimi grožnjami.* https://www.consilium.europa.eu/sl/policies/cybersecurity/

Šepec, M. (2018). *Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza.* Univerzitetna založba Univerze v Mariboru.

Štrucl, D. (oktober 2020). Terminološka zmeda pri zagotavljanju varnosti v kibernetskem prostoru. *Sodobni vojaški izzivi, 22*(4), 31–47. doi:10.33179/BSV.99.SVI.11.CMC.22.4.2

Tom. (n. d.). *Teme.* https://www.e-tom.si/category/teme/

Torres, S. R. (21. 7. 2021). *'Deep web' and 'dark web', the opposite side of the tip of the Internet iceberg.* Impactotic. https://impactotic.co/en/deep-web-and-dark-web-the-opposite-side-of-the-tip-of-the-internet-iceberg/

Ubas, V. (2021). Kriminaliteta v Sloveniji v letu 2020. *Revija za kriminalistiko in kriminologijo, 72*(3), 193–218. https://www.policija.si/images/stories/Publikacije/RKK/PDF/2021/03/RKK2021-03_VojkoUrbas_Kriminaliteta2020.pdf

Van der Wilk, A. (2018). *Cyber violence and hate speech online against women.* Policy Department for Citizens' Rights and Constitutional Affairs. https://dspace.ceid.org.tr/xmlui/bitstream/handle/1/889/QA0218994ENN.en.pdf?sequence=1&isAllowed=y

Vapulus. (25. 12. 2018). *Cyberspace advantages and disadvantages.* https://www.vapulus.com/en/cyberspace-advantages-and-disadvantages/

Verdonik, I. in Bratuša, T. (2005). *Hekerski vdori in zaščita*. Pasadena.

Viktimizacija. (2014). V *Slovar slovenskega knjižnega jezika* (2. dopolnjena in deloma prenovljena izd.). https://fran.si/iskanje?View=1&Query=viktimizacija

Viswanathan, P. (2022). *Kaj je mobilna naprava?* Eyewated. https://sl.eyewated.com/kaj-je-mobilna-naprava/

West, J. (2014). *Cyber-violence against women*. Battered Women's Support Services. https://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf

Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih (MKKKDP). (2004). *Uradni list RS,* (001-22-120/04). https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-

0068/#2.%C2%A0%C4%8Dlen%C2%A0%E2%80%93%C2%A0Protipravni%C2%A0dostop

Zakon o ratifikaciji Konvencije Sveta Evrope o preprečevanju nasilja nad ženskami in nasilja v družini ter o boju proti njima (MKPNZND). (2011). *Uradni list RS,* (542-08/11-2/17). https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2015-02-0001?sop=2015-02-0001

Završnik, A. (2013). Kibernetsko nadlegovanje: Pojem, metode in pojavnost po svetu in v Sloveniji. V M. Ambrož, K. Filipčič in A. Završnik (ur.), *Zbornik za Alenko Šelih: kazensko pravo, kriminologija, človekove pravice* (str. 427–448). Inštitut za kriminologijo pri Pravni fakulteti; Pravna fakulteta; Slovenska akademija znanosti in umetnosti. http://nenasilje.inst-krim.si/images/docs/kibernetsko-nadlegovanje-pojem-metode.pdf

Završnik, A. (2015). *Kibernetska kriminaliteta*. Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

Žakelj, T. (2013). Nasilje med mladimi v kibernetskem prostoru: neraziskanost pojava v Sloveniji. *Družboslovne razprave, 29*(74), 107–123. https://www.dlib.si/details/URN:NBN:SI:doc-LTZ0VHHP

PRILOGA A: PRIMER VPRAŠALNIKA

1.) Ali ste bili že kdaj žrtev spletnega nasilja?

2.) Žrtev katerega spletnega kaznivega dejanja ste bili (npr. nadlegovanje, izsiljevanje, phishing)?

3.) Kdo je izvrševal spletno nasilje nad vami in, če mogoče veste, zakaj je bilo temu tako?

4.) Kje se je nad vami izvajalo spletno nasilje? Preko socialnih omrežij, ali kako drugače?

5.) Ste bili mogoče večkrat žrtev spletnega nasilja, ali se vam je to zgodilo le enkrat in se je potem nasilje končalo?

6.) Ali ste komu povedali za spletno nasilje, ki se vam je dogajalo? Ste se mogoče obrnili tudi na kakšno organizacijo za pomoč žrtvam spletnega nasilja, ali vam je pomagala tudi kakšna uradna oseba?

7.) Ali je takšno nasilje na vas pustilo hude posledice in če se z njimi soočate še danes?

8.) Zanima me, če se je nasilje, ki ste ga doživeli preko spleta preneslo tudi v vaše vsakdanje življenje?

9.) Ali vam je spletno nasilje, ki ste ga doživeli spremenilo življenje in se zaradi tega določenih aktivnosti izogibate/ vas je strah/ste bolj previdni?

10.) Je kdaj spletno nasilje prišlo tako daleč, da ste si želeli škodovati?

11.) Ste pred spletnim nasiljem uporabljali preventivne ukrepe za zaščito pred takimi dejanji?

12.) Ali ste danes še kdaj žrtve spletnega nasilja, ali se je za vas to končalo?

PRILOGA B: PRIMER INTERVJUJA

1.) Ali ste bili že kdaj žrtev spletnega nasilja?

Da, bila sem že žrtev spletnega nasilja.

2.) Žrtev katerega spletnega kaznivega dejanja ste bili (nadlegovanje, izsiljevanje, phishing)

Bila sem žrtev prejemanja različnih groženj in tudi izsiljevali so me, ko sem bila v službi. Grozili pa so mi preko službenega maila.

3.) Kdo je izvrševal spletno nasilje nad vami in, če mogoče veste, zakaj je bilo temu tako?

Nasilje nad mano je izvajal nek moški, ki ga osebno ne poznam. Na službeni mail mi je pisal različne grožnje in želel je, da mu na račun nakažemo denar, ali pa bi informacije posredoval lastnikom podjetja. Obtožil pa nas je, da na delovnem mestu gledamo pornografijo (kar seveda ni bilo res).

4.) Kje se je nad vami izvajalo spletno nasilje? Preko socialnih omrežij, ali kako drugače?

Nasilje se j izvajalo samo preko službenega maila.

5.) Ste bili mogoče večkrat žrtev spletnega nasilja, ali se vam je to zgodilo le enkrat in se je potem nasilje končalo?

Bila sem žrtev samo te vrste nasilja, vendar mi je ta moški pisal dvakrat in mi grozil.

6.) Ali ste komu povedali za spletno nasilje, ki se vam je dogajalo? Ste se mogoče obrnili tudi na kakšno organizacijo za pomoč žrtvam spletnega nasilja, ali vam je pomagala tudi kakšna uradna oseba?

To sem povedala svojemu možu doma, sodelavki in šefu. Ne, nasilja nismo nikomur prijavili, smo se pa odločili, da bomo primer posredovali policiji, če se bo nadlegovanje še kdaj ponovilo.

7.) Ali je takšno nasilje na vas pustilo hude posledice in če se z njimi soočate še danes?

Mogoče je na meni pustilo nekaj posledic. Največkrat me je strah, da bi moški prišel k meni v službo in me tam začel nadlegovati in mi groziti.

8.) Zanima me, če se je nasilje, ki ste ga doživeli preko spleta preneslo tudi v vaše vsakdanje življenje?

Na srečo ne.

9.) Ali vam je spletno nasilje, ki ste ga doživeli spremenilo življenje in se zaradi tega določenih aktivnosti izogibate/ vas je strah/ste bolj previdni?

Za enkrat je skoraj vse ostalo enako, razen tega, da sem bolj previdna in ne zaupam vsaki osebi, ki jo spoznam. V službi pa sem tudi bolj pozorna na osebe, ki vstopajo v prostor.

10.) Je kdaj spletno nasilje prišlo tako daleč, da ste si želeli škodovati?

Na srečo ne.

11.) Ste pred spletnim nasiljem uporabljali preventivne ukrepe za zaščito pred takimi dejanji?

Ne, saj jih nisem poznala in sem odpirala vse elektronske pošte, saj sem mislila, da so sporočila strank. Danes pa sporočil sumljivih oseb ne odpiram, če se pa znajdem v dilemi pa sporočilo posredujem šefu

12.) Ali ste danes še kdaj žrtve spletnega nasilja, ali se je za vas to končalo?

Ne, trenutno se je nasilje končalo in se ne pojavlja več.

Univerza v Mariboru

Fakulteta za varnostne vede

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE ZAKLJUČNEGA DELA

Ime in priimek študent-a/-ke: NEŽA FLAC

Študijski program:
MAGISTRSKI PROGRAM VARSTVOSLOVJE

Naslov zaključnega dela:
SPLETNO NASILJE NAD ŽENSKAMI V SLOVENIJI.

Mentor: PROF. DR. GORAZD MEŠKO

Somentor: /

Podpisan-i/-a študent/-ka NEŽA FLAC

- izjavljam, da je zaključno delo rezultat mojega samostojnega dela, ki sem ga izdelal/-a ob pomoči mentor-ja/-ice oz. somentor-ja/-ice;
- izjavljam, da sem pridobil/-a vsa potrebna soglasja za uporabo podatkov in avtorskih del v zaključnem delu in jih v zaključnem delu jasno in ustrezno označil/-a;
- na Univerzo v Mariboru neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico ponuditi zaključno delo javnosti na svetovnem spletu preko DKUM; sem seznanjen/-a, da bodo dela deponirana/objavljena v DKUM dostopna široki javnosti pod pogoji licence Creative Commons BY-NC-ND, kar vključuje tudi avtomatizirano indeksiranje preko spleta in obdelavo besedil za potrebe tekstovnega in podatkovnega rudarjenja in ekstrakcije znanja iz vsebin; uporabnikom se dovoli reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo;
- dovoljujem objavo svojih osebnih podatkov, ki so navedeni v zaključnem delu in tej izjavi, skupaj z objavo zaključnega dela;
- izjavljam, da je tiskana oblika zaključnega dela istovetna elektronski obliki zaključnega dela, ki sem jo oddal/-a za objavo v DKUM.

Uveljavljam permisivnejšo obliko licence Creative Commons: CC BY NC ND (navedite obliko)

Kraj in datum: VOGLJE, 2.6.2022

Podpis študent-a/-ke:

Flac