კიბერდანაშაულისა და კიბერუსაფრთხოების ინციდენტების გენდერული ზემოქმედება

ნაზიბროლა ნასყიდაშვილი

რედაქტორი: ელენე ცაცუა

აბსტრაქტი

ტექნოლოგიების განვითარებასთან ერთად იზრდება ძალადობისა და დანაშაულის მასშტაბები. პრეზენტაციაში განხილულია კიბერდანაშაულისა და კიბერუსაფრთხოების ინციდენტები, კონკრეტულად კი ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV - Technology-Facilitated Gender-Based Violence). ქალები, რომლებიც ეწევიან კონკრეტულ საქმიანობას ან მიეკუთვნებიან გარკვეულ ჯგუფებს, ხშირად ხდებიან ფსიქოლოგიური წნეხის მსხვერპლი პირები კიბერშევიწროებისა და თვალთვალის მედეგად, რასაც შემდგომში მოჰყვება შფოთვა, ფსიქოლოგიური ტრავმა, იზოლაცია, შიში და უნდობლობა. ყოველივე ზემოთქმული დიდ გავლენას ახდენს მსხვერპლი ქალების სოციალურ ცხოვრებაზე, რაც ნათლად აისახება მათ მიერ პოლიტიკურ და სოციალურ სფეროში ჩართულობის შემცირებაზე, დასაქმების შესაძლებლობების შეზღუდვასა და განათლების ნაკლებ ხელმისაწვდომობაზე. პრეზენტაციაში გამოკვეთილად არის აღნიშნული კიბერშევიწროების დიფერენცირებული ზემოქმედება და შემოთავაზებულია რეკომენდაციები თუ როგორ ავირიდოთ ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა TFGBV, როგორ ვუპასუხოთ და გავუმკლავდეთ მსგავსი შემთხვევებით გამოწვეული კიბერდანაშაულის შედეგებს. მნიშვნელოვანია, მოვახდინოთ ადამიანებში, განსაკუთრებით ქალებში, ცნობიერების ამაღლება, რათა უზრუნველვყოთ მათთვის უსაფრთხო ციფრული გარემო.

შესავალი

დღევანდელ ციფრულ ეპოქაში ტექნოლოგიები ყოველდღიური ცხოვრების განუყოფელ ნაწილად იქცა, რომელიც უამრავ ახალ შესაძლებლობას გვთავაზობს. თუმცა, ის ასევე გახდა სივრცე, სადაც მოძალადე ადამიანებს მარტივად შეუძლიათ იძალადონ ქალებზე გენდერული ნიშნის საფუძველზე.

ქალები და გოგონები, განსაკუთრებით ისინი, რომლებიც უმცირესობაში არიან მათი რასის, ასაკის, ეთნიკური წარმომავლობის, სექსუალური ორიენტაციის, იდენტობის, შეზღუდული შესაძლებლობების, რელიგიისა და მიგრანტის სტატუსის გამო, არიან კიბერთავდასხმების მაღალი რისკის ქვეშ. მსოფლიოში ქალების მესამედზე მეტი გამხდარა ონლაინ ძალადობის მსხვერპლი და ეს მაჩვენებელი თითქმის 50%-მდე იზრდება ახალგაზრდა გოგონების შემთხვევაში.

საერთაშორისო ორგანიზაციებმა როგორიცაა Amnesty International, რომელიც ახორციელებს კამპანიას ადამიანის უფლებების დასაცავად მთელ მსოფლიოში, და Element AI, ხელოვნური ინტელექტის კომპანიამ, გამოიყენეს მონაცემთა მეცნიერებისა და მანქანათმცოდნეობის მოწინავე ტექნიკები, რათა გაეანალიზებინათ ძალადობის მასშტაბები, რომლებსაც ქალები აწყდებიან სოციალურ ქსელებში, მაგალითად Twitter-ზე (დღევანდელ X-ზე). Element AI-მ დაადგინა, რომ 1.1 მილიონი შეურაცხმყოფელი ან პრობლემური ტვიტერ შეტყობინება გაიგზავნა კვლევაში მონაწილე ქალებთან ერთი წლის განმავლობაში - ან საშუალოდ თითო ყოველ ოცდაათ წამში (Amnesty International, 2018).

ეს სტატისტიკა არის სულ მცირე ერთი მტკიცებულება იმისა, რომ ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV) რეალური პრობლემა გახდა.

ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV)

ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV) არის ძალადობის აქტი, რომელიც განხორციელებულია ერთი ან მეტი პირის მიერ, და ნაწილობრივ ან მთლიანად გაძლიერებულია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ან ციფრული მედიის გამოყენებით ადამიანის დაზიანების მიზნით მათი გენდერის საფუძველზე.

ტექნოლოგიებით წახალისებული გენდერის ნიშნით ძალადობა (TFGBV) მოიცავს როგორც კიბერდანაშაულის, ასევე კიბერუსაფრთხოების საკითხებს, რომელიც გულისხმობს კრიმინალური ქმედებების ციფრული საშუალებებით განხორციელებას, რაც თავისთავად საფრთხეს უქმნის ინდივიდების, განსაკუთრებით ქალებისა და გოგონების უსაფრთხოებასა და დაცულობას. ის ხაზს უსვამს ურთიერთკავშირს გენდერული ნიშნით ძალადობასა და ციფრულ ტექნოლოგიებს შორის.

TFGBV-ის გავრცელებული ფორმები

ონლაინ შევიწროება

ონლაინ შევიწროება გულისხმობს ტექნოლოგიის რეგულარულად გამოყენებას სხვა პირთან დასაკავშირებლად, გასაღიზიანებლად, მუქარისთვის ან დასაშინებლად. იგულისხმება მუდმივი ხასიათის ქცევა და არა ცალკეული, კონკრეტული ქმედებები. მოძალადე შეიძლება იყოს როგორც ინდივიდი, ასევე ინდივიდთა ჯგუფი (ცნობილია როგორც: მობინგი), ისინი როგორც წესი, არიან მამაკაცები, რომლებიც მიზნად ისახავენ ქალებისა და უმცირესობების შევიწროებას.

კიბერსტალკინგი (კიბერადევნება, კიბერთვალთვალი)

კიბერსტალკინგი გულისხმობს ტექნოლოგიის გამოყენებით ვინმეს საქმიანობისა და ქცევის თვალყურის დევნებასა და მონიტორინგს რეალურ დროში ან ისტორიულად. ის ხშირად განიხილება, როგორც ფიზიკური თვალთვალის გაგრძელება, რომელიც მოიცავს მუქარასა და ძალადობაზე დაფუძნებულ არასასურველ, განმეორებად, აგრესიულ ქმედებებს. აკვიატებული დევნისა და თვალთვალის ეს მძიმე ფორმა შეიძლება მოტივირებული იყოს ურთიერთობის დროს პარტნიორის კონტროლის ან დესტრუქციის მიზნით, რაც იწვევს მსხვერპლში შიშის მძაფრ გრძნობას (ჰენრი და პაუელი, 2016).

დოქსინგი

დოქსინგი გულისხმობს პერსონალური ინფორმაციის დაუკითხავად გამჟღავნებას, მათ შორის ისეთი პირადი და სენსიტიური ინფორმაციის საჯაროდ გავრცელებას, როგორიცაა სახლის მისამართები, ელექტრონული ფოსტის მისამართები, ტელეფონის ნომრები და ბავშვების ფოტოები. ონლაინ შევიწროების ეს ფორმა იშვიათად ხორციელდება ცალკეულად და ხშირად თან ახლავს შევიწროების სხვა ფორმებს, როგორიცაა IBA. არსებობს სამი სახის დოქსინგი: პირველი - დეანონიმიზაცია (ადამიანის ვინაობის გამჟღავნება), მეორე - მიზანში ამოღება გენდერული ნიშნით (პერსონალური ინფორმაციის გამჟღავნება, რომელიც საშუალებას აძლევს უცხო პირებს დაადგინონ სამიზნე პირის ფიზიკური ადგილსამყოფელი) და ამ გზით სერიოზული საფრთხე შეუქმნას ქალების

უსაფრთხოებას; მესამე - დელეგიტიმაცია, რომელიც მიზნად ისახავს შელახოს დაზარალებულის რეპუტაცია.

ჰაკეროზა

ჰაკეროზა გულისხმობს ტექნოლოგიის გამოყენებით სისტემებსა და რესურსებზე უკანონო ან არაავტორიზებული წვდომის მოპოვებას, რაც საშუალებას აძლევს მათ მიიღონ წვდომა პერსონალურ ინფორმაციაზე, შეცვალონ ის თავის სურვილისამებრ, ცილი დასწამონ და შეურაცხყოფა მიაყენონ მსხვერპლს. ასევე, შესაძლებელია ჰაკერებმა მსხვერპლის პერსონალური კომპიუტერი ან ტელეფონი დაშანტაჟების მიზნით გატეხონ; მსგავსი ქცევები გამიზნულია ადამიანების ონლაინ მანიპულაციისთვის ელექტრონული ფოსტისა და სოციალური მედიის პირადი ანგარიშების გასაკონტროლებლად; ამას ემატება მსხვერპლის საბანკო ანგარიშებში ფარულად შეღწევა ფინანსური ზიანის მიყენების მიზნით.

რეკრუტირება

ტექნოლოგიები შესაძლოა გამოყენებულ იქნას მსხვერპლზე ფიზიკური ან სექსუალური ძალადობის გასაადვილებლად. შესაძლებლობის შემთხვევაში მოძალადეები და ტრეფიკერები ავრცელებენ თაღლითურ პოსტებს და რეკლამებს გაცნობის საიტებზე, „ქორწინების სააგენტოებში" ან სატელეფონო დასაქმების სააგენტოებშიც პოტენციურ მსხვერპლთან დასაკავშირებლად. ისინი ხშირად იყენებენ Spyware ან GPS სათვალთვალო მონიტორინგის, კონტროლისა და ადგილმდებარეობის დასადგენად, მათი დაშინებისა ან ფიზიკური შეურაცხყოფის მიყენების მიზნით. ძალადობის ეს ფორმა შესაძლოა ქალების, ახალგაზრდებისა და ბავშვების ტრეფიკინგის საფუძველიც გახდეს.

ცილისწამება

ცილისწამება გულისხმობს ყალბი ინფორმაციის საჯაროდ გავრცელებას პიროვნების რეპუტაციის შელახვის, მსხვერპლის დამცირების, მუქარის, დაშინების ან დასჯის მიზნით. ქალის სექსუალობის მხრივ მკაცრი გენდერული ნორმების გათვალისწინებით, ცილისმწამებლური განცხადებები მათი პირადი ცხოვრების შესახებ შეიძლება განსაკუთრებით საზიანო იყოს. ქალებისა და გოგონების მიმართ ცილისმწამებლური თავდასხმების უმეტესობა ფოკუსირებულია მათ გენდერზე.

TFGBV-ის ზემოქმედება

მიუხედავად იმისა, რომ TFGBV ხშირად აღიქმება როგორც ნაკლებად სერიოზული პრობლემა ფიზიკურ ძალადობასთან შედარებით, მისი შედეგები შეიძლება საკმაოდ მძიმედ აისახოს ქალებისა და გოგონების ჯანმრთელობასა და სიცოცხლეზე. TFGBV-ის საჯარო, გავრცელებული, განმეორებადი და მუდმივი ხასიათის შემთხვევაში, როგორც ონლაინ, ისე ფიზიკური სახის ძალადობის უწყვეტობა, მსხვერპლში იწვევს შიშისა და დაუცველობის განცდას. ამ ფაქტს აუარესებს კონკრეტული, საჭირო ბერკეტების არარსებობა და რომ ტექნოლოგიების გზით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV) არ არის სერიოზულ საშიშროებად აღქმული, ის არ არის „რეალური" საფრთხე მოქალაქისთვის. ხშირად ისე ხდება, რომ TFGBV იწვევს ფიზიკურ ძალადობას ან პირიქით.

ძალადობას გადარჩენილი ადამიანები ხშირად აღნიშნავენ, რომ ისინი იმყოფებიან მძიმე ემოციური და ფსიქოლოგიური სტრესის ქვეშ, ახასიათებთ შფოთვა, დეპრესია, PTSD და, მძიმე შემთხვევაში, სუიციდური აზრები ან სუიციდის მცდელობები არის მათი მდგომარეობის თანმდევი. კვლევამ, რომელიც ჩაატარა ორგანიზაციამ Amnesty International რვა მაღალი შემოსავლების მქონე ქვეყანაში, დაადგინა, რომ ქალთა 54%-ს, რომლებსაც გამოუცდიათ გენდერული ნიშნით ძალადობა TFGBV, განიცდიდნენ პანიკურ

შეტევებს, შფოთვას ან სტრესს. ანალოგიურად, სამხრეთ ინდოეთში ჩატარებულმა კვლევამ აჩვენა, რომ ქალების 28% განიცდიდა შფოთვას ან დეპრესიას, ხოლო 6% ცდილობდა თვითდაზიანებას. ახალგაზრდა ქალებსა და გოგონებს შორის 42%-მა დააფიქსირა ფსიქიკური ან ემოციური სტრესი და დაბალი თვითშეფასება, რომელიც გამოწვეული იყო ონლაინ სივრცეში მათზე ძალადობით. 31 ქვეყანაში ჩატარებული Plan International-ის კვლევის მიხედვით. IBSA-ს გადარჩენილები ხშირად განიცდიან ფსიქიკურ აშლილობას, რომელიც ძალიან ჰგავს სექსუალური ძალადობის შემდგომ დაფიქსირებული მსხვერპლის ფსიქოლოგიურ მდგომარეობას (Plan International, n.d).

ქალები, რომლებსაც გამოუცდიათ გენდერული კუთხით ონლაინ ძალადობა (TFGBV), ხშირად ცდილობენ შეამცირონ აქტივობები ონლაინ, ზღუდავენ თავიანთ საქმიანობასა და აწესებენ თვითცენზურას. ეს დუმილის ეფექტი შემაშფოთებელი და დამაზიანებელია ქალებისთვის, რომელთა პროფესიული ცხოვრება დამოკიდებულია ონლაინ აქტიურობაზე, როგორიცაა ჟურნალისტიკისა და პოლიტიკის სფეროები. TFGBV-ის ფსიქოლოგიური ზემოქმედება ასევე გავლენას ახდენს საზოგადოებაში ქალთა პოლიტიკურ და სოციალურ ჩართულობაზე, დასაქმების შესაძლებლობებზე, განათლებისა და ინფორმაციის ხელმისაწვდომობაზე. აქვე უნდა აღინიშნოს, რომ გლობალურად, TFGBV-ს დაქვემდებარებული ახალგაზრდა ქალებისა და გოგონების 18%-ს პრობლემები ჰქონდა სკოლაშიც.

ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობასთან დაკავშირებული აქტუალური გამოწვევები

სამართლებრივი და მარეგულირებელი ხარვეზები

მოქმედი კანონები ხშირად ადეკვატურად არ განიხილავს ტექნოლოგიების გენდერის ნიშნით ონლაინ ძალადობას, რაც ჩვეულებისამებრ უნდა ჯდებოდეს არსებული გენდერზე დაფუძნებული ძალადობის ჩარჩოებში. ბევრ იურისდიქციას აქვს ზოგადი, გენდერულად უმოქმედო კანონები ონლაინ უსაფრთხოების შესახებ, რომლებიც ეფექტურად ვერ ახერხებენ ციფრული ზიანის თავიდან აცილებას ან დამნაშავეების პასუხისმგებლობაში მიცემას (UNICEF East Asia & Pacific & Pacific, 2021). ამ ხარვეზს ემატება კანონის არათანმიმდევრული განხორციელება და აღსრულება სამართალდამცავი და სასამართლო სისტემების მიკერძოებულობიდან გამომდინარე.

პლატფორმის პასუხისმგებლობა და ანგარიშვალდებულება

კერძო ტექნოლოგიური კომპანიები, მათ შორის სოციალური მედიის პლატფორმები და ინტერნეტ სერვისის პროვაიდერები, ხშირად ეჩეხებიან გამოწვევებს TFGBV-ზე ეფექტური რეაგირებისა და შემცირების კუთხით. საკითხები მოიცავს კონტენტის ზომიერების არათანმიმდევრულ პრაქტიკას, ალგორითმული გადაწყვეტილების მიღებისას მიკერძოებასა და ზოგიერთი პლატფორმის მოგებაზე ორიენტირებულ პოლიტიკას, რომლებისთვისაც მომხმარებელი არ არის პრიორიტეტი. საჭიროა უფრო მკაფიო რეგულაციები და ზომები ამ კომპანიების მხრიდან ტექნოლოგიებით გამოწვეული გენდერული ძალადობის პრევენციისა და მოგვარებისათვის.

კულტურული და სოციალური ნორმები

ტექნოლოგიებით გამოწვეული გენდერის ნიშნით ძალადობა (TFGBV) ხშირად მყარდება კულტურული და სოციალური ნორმებით, და ხშირად, დაბალი ცნობიერების გამო, ხდება ონლაინ შევიწროების პრობლემის, თვალთვალის, ინტიმური სურათების გაზიარებისა და ქალთა მიმართ ციფრული ძალადობის სხვა ფორმების ნაკლებ სერიოზულად აღქმა.

მსგავსი რწმენა-შეხედულებების და დამოკიდებულებების შეცვლა შესაძლებელია საგანმანათლებლო პროგრამებისა და მოქალაქეების ცნობიერების ასამაღლებელი კამპანიის განხორციელების გზით, რომელიც თავისთავად მოიაზრებს გენდერული თანასწორობისა და ადამიანების მიერ ონლაინ ურთიერთობების დროს მათ შორის პატივისცემის წახალისებასა და ხელშეწყობას.

რეკომენდაციები

- გამოიყენეთ ძლიერი პაროლები და არასოდეს გააზიაროთ ისინი.
  - დააყენეთ რთული პაროლები და შეცვალეთ ისინი რეგულარულად.
- დაიცავით თქვენი პირადი ინფორმაცია.
  - ფრთხილად იყავით პირადი დეტალების გამჟღავნებისას.
  - თავი შეიკავეთ სახიფათო აპლიკაციების დაყენებისგან და თქვენი ადგილსამყოფელის გაზიარებისგან.
- არ შეხვიდეთ საეჭვო ბმულებზე.
  - არასოდეს შეხვიდეთ ბმულზე, რომელიც გამოიყურება საეჭვოდ, სანამ დაადასტურებთ მის ნამდვილობას.
- არ დატოვოთ თქვენი ვებკამერა ჩართულ მდგომარეობაში.
  - გათიშეთ ვებკამერა, თუ მას არ იყენებთ.
- დაბლოკეთ არასასურველი კონტაქტები.
  - არ დაუდასტუროთ მეგობრობის თხოვნა უცხო ადამიანებს
  - მარტივად დაბლოკეთ ყველა მომხმარებელი ვისთანაც არაკომფორტულად გრძნობთ თავს
- დარწმუნდით, რომ ყველა ოპერაციული უსაფრთხოების სისტემა განახლებულია
  - მუდმივად განაახლეთ თქვენი ონლაინ უსაფრთხოების პროგრამული უზრუნველყოფა
  - რეგულარულად ჩაატარეთ ანტივირუსული სკანირება

დასკვნა

ტექნოლოგიების ხელშემწყობი გენდერული ნიშნით ძალადობის ფონზე, აუცილებელია ერთიანი სამოქმედო გეგმის ჩამოყალიბება. პოლიტიკოსებმა, ტექნოლოგიურმა კომპანიებმა და სამოქალაქო საზოგადოებამ ერთად უნდა ვიმუშაოთ ამ პრობლემების გადასაჭრელად. ჩვენ შეგვიძლია შევქმნათ ციფრული სამყარო, რომელიც იქნება ყველასათვის უსაფრთხო და ინკლუზიური. როგორც ნობელის პრემიის ლაურეატმა, მალალა იუსაფზაიმ, თქვა, ,,ჩვენ ყველანი წარმატებას ვერ მივაღწევთ, მაშინ როდესაც საზოგადოების ნახევარს უკან გვექაჩებიან". ამიტომ, მნიშვნელოვანია ძალისხმევა არ დავიშუროთ და ვეცადოთ, რომ ციფრულ ეპოქაში არც ერთი ჩვენგანი არ ჩამორჩეს და არ დაიჩაგროს.

ლიტერატურა

1. Communications. (2013, April). Issue 4: Technology-related violence against women. Learning Network - Western University.

https://gbvlearningnetwork.ca/our-work/issuebased_newsletters/issue-4/index.html

2. Douglas. (2016). "Doxing: A Conceptual Analysis", Ethics Information Technology, Vol. 18", pp. 199–210.
3. Gawn, A. (2023, March 17). What has cyber security got to do with Gender Equality and Social Inclusion?. What has cyber security got to do with gender equality and social inclusion? | Social Development Direct. https://www.sddirect.org.uk/blog-article/what-has-cyber-security-got-do-gender-equality-and-social-inclusion#_edn3
4. GBV AoR Helpdesk. (2023, February 8). Learning brief on technology facilitated gender-based violence - GBV AOR helpdesk 2021: Gender-based violence area of responsibility. Learning Brief on Technology Facilitated Gender-Based Violence - GBV AoR Helpdesk 2021 | Gender-Based Violence Area of Responsibility. https://gbvaor.net/node/1798
5. Gurumurthy, A., Vasudevan, A., & Chami, N. (2019, August 1). Born Digital, born free? A socio-legal study on young women's experiences of Cyberviolence in South India. IT for Change. https://itforchange.net/born-digital-born-free-a-socio-legal-study-on-young-womens-experiences-of-cyberviolence-south-india
6. Levy, K. L., Dell, N., McCoy , D., & Ristenpart, T. (2018, May 21). How domestic abusers use smartphones to spy on their partners. Vox. https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google
7. MacAllister. (2017). The doxing dilemma: seeking a remedy for the malicious publication of personal information.
8. Plan International. (n.d.). State of the world's girls 2020: Free to be online? Plan International. https://plan-international.org/publications/free-to-be-online/
9. Rose, C., & Goverde, R. (2021, August 26). India: Girls in India facing greater online risk of child marriage and trafficking during pandemic. Save the Children International. https://www.savethechildren.net/news/india-girls-india-facing-greater-online-risk-child-marriage-and-trafficking-during-pandemic
10. Solinge, D. van. (2019, June 12). Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address. Humanitarian Law & Policy Blog. https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/
11. UNFPA. (2021, December). Making all spaces safe - united nations population fund. https://www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making All Spaces Safe.pdf