კიბერდანაშაული, როგორც დანაშაულის გამოვლინების უნივერსალური ფორმა

გიორგი ამაშუკელი
საქ. ადვოკატთა ასოციაციის წევრი, კავკასიის საერთაშორისო უნივერსიტეტის დოქტორანტი

I. შესავალი

სოციალურ ურთიერთობათა სფეროში, იშვიათ გამონაკლისად შეიძლება ჩაითვალოს საყოველთაო კონსენსუსი კიბერუსაფრთხოების პრიორიტეტულობის თაობაზე. საოცარია, მაგრამ ფაქტია, რომ აზრთა თანხვედრას ხელი ვერ შეუშალა სახელმწიფოთა შორის არსებულმა პოლიტიკურმა, სოციალურმა, სამართლებრივმა, სამხედრო თუ სხა სახის აზრთა სხვადასხვაობამ. უფრო მეტიც, კიბერუსაფრთხოება მსოფლიო თანამეგობრობის მიერ აყვანილია ეროვნული უსაფრთხოების რანგში და მას ეთმობა განსაკუთრებული ყურადღება. მაგრამ დიამეტრალურად განსხვავებული მოცემულობაა უსაფრთხოების უზრუნველყოფის მეთოდებსა და კონცეპტუალურ ხედვაში, რაც უპირველეს ყოვლისა, მჟღავნდება მის სამართლებრივ სეგმენტში. სწორედ სამართლებრივი მხარე განიცდის პოლიტიკური ხასიათის ზემოქმედებას და წარმოშობს აზრთა სხვადასხვაობას. ამ მიმართულებით, ერთიანი ძალისხმევის გარეშე, კიბერუსაფრთხოება ყოველთვის მოწყვლადი და საფრთხის შემცველი იქნება.

დიდი ხანია დავას არ იწვევს თავად კიბერდანაშაულის ტრანსნაციონალური ბუნება და კრიტიკულად დიდი სოციალური საფრთხე, რის გამოც მიღებულია მთელი რიგი საერთაშორისო ხასიათის შეთანხმებები თუ სარეკომენდაციო რჩევები; გამოქვეყნებულია სამეცნიერო ნაშრომები და სტატიათა მთელი წყება, არ წყდება მსჯელობა კანონმდებლობის სრულყოფისა და საკანონმდებლო ჰარმონიზაციის თაობაზე, თუმცა, დღემდე არ არსებობს არც კიბერდანაშაულის პრევენციის მწყობრი საკანონმდებლო ბაზა და არც კიბერდანაშაულის, როგორც სამართლებრივი კატეგორიის, სრულყოფილი განმარტება.

საკითხი იმდენად კომპლექსური და მრავალგანზომილებიანია, რომ მისი არა თუ ანალიზი, არამედ ზოგადი მიმოხილვაც კი შორს წაგვიყვანდა, მით უმეტეს, რომ სტატიის ფორმატში ეს შეუძლებელია. ამიტომ ჩვენ შემოვიფარგლებით საკითხის მხოლოდ რამდენიმე ასპექტის ზოგადი განხილვით. კერძოდ, როდესაც საუბარია კიბერდანაშაულზე, გასარკვევია თავად მისი რაობის საკითხი. კერძოდ, კიბერდანაშაული წარმოადგენს დამოუკიდებელ სისხლისსამართლებრივ კონსტრუქციას თუ დანაშაულის შემადგენლობის ობიექტური მხარის ელემენტს, რომლის ფუნქცია მხოლოდ ქმედების განხორციელების საშუალებით ამოიწურება.

მართლაც, როდესაც არ გვაქვს კიბერდანაშაულის სრულყოფილი განსაზღვრება არც დოქტრინასა და არც საკანონმდებლო დონეზე, არაეფექტიანია მისი პრევენციაც. გარდა ამისა, ეს იწვევს მრავალ გაურკვევლობას საკანონმდებლო ტექნიკის თვალსაზრისით და ხელსაყრელ ნიადაგს ქმნის არაერთგვაროვანი სასამართლო პრაქტიკის ჩამოსაყალიბებლად.

ჩვენი მიზანია გამოვკვეთოთ პრობლემის მნიშვნელობა და მიუთითოთ მისი გადაჭრის გზებზე, რაც ხელს შეუწყობს ეროვნულ სისხლისსამართლებრივ კანონმდებლობაში ქაოტუ-

რად მიმობნეული სამართლებრივი კონსტრუქციების ერთიან, მოწესრიგებულ სისტემაში მოქცევის პროცესს.

II. კიბერდანაშაულის დეფინიცია

ეროვნული სისხლისსამართლებრივი კანონმდებლობა კიბერდანაშაულის დეფინიციას არ გვთავაზობს და შემოიფარგლება მხოლოდ კომპიუტერული სისტემის წინააღმდეგ მიმართული დანაშაულის შემადგენლობებით. ასეთი მდგომარეობა განპირობებულია ობიექტური მიზეზებით, რაც უკავშირდება ამ ფენომენის უნივერსალურ ხასიათს. მართლაც, შეუძლებელია ამ დანაშაულის ამომწურავი ნიშან-თვისებების ფიქსაცია და, მით უმეტეს, მისი საკანონმდებლო განმარტება. მიუხედავად ამისა, არსებობს საერთაშორისო დონეზე აღიარებული, ზოგადი ხასიათის განმარტებები, რომლების მიუთითებენ ამ ანტისოციალური მოვლენის ძირითად ნიშან-თვისებებზე. მაგალითად, ევროპის საბჭოს კონვენცია განასხვავებს კიბერდანაშაულის ხუთ კატეგორიას: 1. დანაშაული მიმართული კომპიუტერული სისტემისა და მონაცემების წინააღმდეგ; 2. მართლსაწინააღმდეგო ქმედება, შესაბამისი ტექნოლოგიური საშუალებების გამოყენებით; 3.სამართალდარღვევა, რომელიც უკავშირდება მონაცემთა ბაზას ან კონტენტს; 4. საავტორო და სხვა უფლებების დარღვევასთან დაკავშირებული ქმედება და 5. კიბერტერორიზმი და სხვა, ძალმომრეობით ქმედებებთან დაკავშირებული.

რა თქმა უნდა, არსებობს ევროპის საბჭოს ისევე, როგორც სხვა საერთაშორისო ორგანიზაციების მრავალი დეფინიცია, არაფერს ვამბობთ ცალკეულ მეცნიერთა მოსაზრებებზე. ყველა მათგანის მცდელობა მიმართულია კიბერდანაშაულის ძირითად ნიშან-თვისებათა განსაზღვრისკენ, მაგრამ მთავარი მაინც ისაა, რომ ამ ნიშან-თვისებათა განსაზღვრა უკავშირდება დანაშაულის შემადგენლობის ობიექტური მხარის ისეთ ელემენტებს, როგორიცაა დანაშაულის საგანი ან დანაშაულის განხორციელების საშუალება.

ტერმინი კიბერდანაშაული ხშირად იხმარება ინტერნეტდანაშაულთან ერთად და ისინი, ფაქტობრივად, წარმოადგენენ სინონიმებს. თუმცა, კიბერდანაშაული გაცილებით ფართო ცნებაა, ვიდრე კომპიუტერული დანაშაული. ეროვნულ კანონმდებლობაში ისევე, როგორც დოქტრინაში, უპირატესობა ენიჭება „ინტერნეტდანაშაულს“, რაც იმით უნდა იყოს გამოწვეული, რომ ამ საკითხის კვლევა, ძირითადად მიმდინარეობს სისხლისსამართლებრივ და პროცესუალურ ჭრილში.

მიუხედავად ამ ტერმინთა შინაარსობრივი და არსობრივი მსგავსებისა, განსხვავება არსებობს მათ ტერმინოლოგიურ საწყისებშიც. „Cybercrime“ მის ინგლისურენოვან ვარიანტში გაცილებით ფართო მნიშვნელობისაა, ვიდრე ინტერნეტდანაშაული (computer crime) და უფრო შეესაბამება ისეთ სფეციფიკურ მოვლენას, როგორიცაა საინფორმაციო სივრცეში ჩადენილი დანაშაული. ამას ადასტურებს ოქსფორდის განმარტებითი ლექსიკონი, რომელიც წინდებულ ,,Cyber''-ს მიაკუთვნებს რთულ სიტყვათა ისეთ კომპონენტს, რომელიც გულისხმობს მონაცემთა ბაზის, სისტემების, ნებისმიერი საინფორმაციო ტექნოლოგიების, ინტერნეტის ქსელებისა თუ ელექტრონული სისტემების ნებისმიერ ტექნოლოგიურ სფეროს.[1] ანალოგიური განმარტებაა მოცემული კემბრიჯის ლექსიკონში, რომლის მიხედვითაც „Cyber“ თავის თავში გულისხმობს კომპიუტერთა ქსელს, ინტერნეტს, საინფორმაციო სივრცეს. ამის საილუსტრაციოდ ლექსიკონში მოყვანილია მაგალითი „კიბერდანაშაული“ (Cybercrime).[2] ამდენად, შეიძლება ითქვას, რომ ტერმინი „კიბერდანაშაული“ (Cybercrime) გულისხმობს როგორც კომპიუტერის, ისე ნებისმიერი, გლობალური, საინფორმაციო ტექნოლოგიური საშუალების გამოყენებას. ამასთან, კომპიუტერული დანაშაული გულისხმობს მხოლოდ ისეთ სოციალურად საშიშ ქმედებას, რომელიც მიმართულია კომპიუტერული სისტემების წინააღმდეგ.

---

1 Oxford English Dictionary, URL:http://www.askoxford.com.

2 Cambridge Advanced Learner s Dictionary, URL:http://dictionary.cambridge.org.

ერთი შეხედვით, შეიძლება ვიფიქროთ, რომ სახეზეა მხოლოდ ტერმინოლოგიური წინააღმდეგობა მოვლენათა შინაარსობრივ ასპექტში, მაგრამ სასამართლო პრაქტიკის ანალიზი გვიჩვენებს, რომ ეს ხარვეზი სერიოზულ სიძნელეს წარმოშობს დანაშაულის კვალიფიკაციის დროს, დასაბამს უდებს მახინჯ სასამართლო პრაქტიკას და აფუძნებს ორმაგ სტანდარტებს. თუ იმასაც მივიღებთ მხედველობაში, რომ სისხლისსამართლებრივი პრაქტიკა, რომელიც, თავისი ბუნებით, ყოველთვის ტენდენციურია ქმედებათა შეფასებისას, უნდა ვივარაუდოთ, რომ პრობლემის აქტუალობა ნაკარნახევია პრაქტიკული მოსაზრებებითაც.

II. კიბერდანაშაულის მასშტაბი

საყოველთაოდ ცნობილი ფაქტია, რომ კიბერდანაშაულის შედეგად მიყენებული ზიანი მსოფლიო მასშტაბით გაცილებით უფრო დიდია, ვიდრე კაცობრიობის არსებობის განმავლობაში ერთად აღებული ყველა დანაშაულით გამოწვეული ზარალი. სტატისტიკური მონაცემების შეჯერებისას ზარალის საშუალო მაჩვენებლები ათობით ტრილიონ ამერიკულ დოლარს უტოლდება. თუ იმასაც მივიღებთ მხედველობაში, რომ ეს მონაცემები არასრულია, უნდა ვივარაუდოთ, რომ სიტუაცია კიდევ უფრო მძიმეა, ვიდრე წარმოგვიდგენია. მაგრამ, კიბერდანაშაულის მოქმედების სფერო მხოლოდ მატერიალური ზიანით არ შემოიფარგლება. იგი არა მარტო მონაწილეობს ადამიანთა ცხოვრების ყველა სფეროში, არამედ აქტიურად კარნახობს თავის დღის წესრიგს. ისიც გასაგებია, რომ ტექნიკური პროგრესის გარეშე თანამედროვე ყოფაცხოვრება წარმოუდგენელია, მაგრამ მისი რეგულირების გარეშე, მსოფლიო მასშტაბის კატასტროფა გარდაუვალია. აქ კი თავს იჩენს დამცავი მექანიზმების საჭიროება, რომელთა შორისაც მნიშვნელოვანი როლი ეკისრება სისხლისსამართლებრივ მხარეს.

როგორც უკვე აღინიშნა, კიბერდანაშაულის მონაცემთა უმრავლესობა სტატისტიკის ფარგლებს გარეთ რჩება, ხოლო ოფიციალურ სტატისტიკაში ხვდება რეალურად განხორციელებულ დანაშაულთა მხოლოდ 20%. კვლევებით დადგენილია, რომ კიბერდანაშაულის ლატენტობის ხარისხი რუსეთის ფედერაციაში შეადგენს 90%, ამერიკის შეერთებულ შტატებში 80%, დიდი ბრიტანეთში 85%, ხოლო გერმანიის ფედერაციულ რესპუბლიკაში 75% პროცენტს.[3]

აღნიშნულ საკითხზე ჩატარებულ კვლევათა მონაცემებს შორის ცდომილება, სამწუხაროდ, უმნიშვნელოა და აქედან გამომდინარე, სახეზე გვაქვს საგანგაშო მდგომარეობა.

საკითხის დრამატულობას ამძაფრებს ისეთი ფენომენის წარმოშობა, როგორიც ხელოვნური ინტელექტია. პროფესორ ზ. გაბისონიას აზრით, დღევანდელი რეალობა აჩვენებს, რომ ხელოვნური ინტელექტის სამართლებრივი მოწესრიგება და მისი გარკვეულ რეჟიმში მოქცევა, თანამედროვე იურისტების ახალ გამოწვევად იქცა.[4]

ამ ფონზე, საკითხის რეგულირება, სისხლისსამართლებრივი მექანიზმების გარეშე შეუძლებელია, ხოლო უმნიშვნელო დაყოვნებას კი შეიძლება გამოუსწორებელი შედეგები მოჰყვეს, რადგანაც ხელოვნურ ინტელექტი იძლევა თვისებრივად ახალი, სოციალურად საშიში ქმედებების წარმოშობის ნოყიერ ნიადაგს, რომლის თავიდან აცილება განსხვავებულ მიდგომებს მოითხოვს.

როგორც რეალობამ გვიჩვენა, ინტერნეტისა და საკომუნიკაციო ქსელების გლობალიზაციამ განაპირობა ისეთი სიტუაციის შექმნა, როდესაც შესაძლებელია სამართალდამრღვევი იმყოფებოდეს ერთ კონტინენტზე, ხოლო დანაშაულის ჩადენის ადგილი აღმოჩნდეს მეორე; ამასთან, დანაშაულებრივი შედეგი დადგეს მესამე კონტინენტზე.

სტრუქტურულად კიბერდანაშაული შესაძლებელია განსხვავებული იყოს ამა თუ იმ ქვეყნის სპეციფიკის გათვალისწინებით. ამის მიზეზი, როგორც წესი განპირობებულია თავად

[3] *Kabay*, Studies and surveys of Computer Crime-Northfield, 2001, 2.

[4] *გაბისონია*, ხელოვნური ინტელექტის არსი და მისი სამართლებრივი რეგულირების საჭიროება, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი 7/2021, 43.

ქვეყნის ეკონომიკური თუ კულტურული განვითარების დონითა და სხვა ფაქტორებით. მაგალითად, ამერიკის შეერთებულ შტატებში კიბერდანაშაულის 44% მოდის ელექტრონული ანგარიშებიდან ფულადი თანხების ქურდობაში, 16% პროგრამული უსაფრთხოების სისტემათა დაზიანებაზე, 12% ინფორმაციის ფალსიფიკაცია, 10% სხვისი ანგარიშის გამოყენებით, საყოფაცხოვრებო მომსახურების გამოყენებაზე.[5]

მსოფლიო გამოცდილება გვიჩვენებს, რომ ბოლო პერიოდში შეინიშნება ერთგვარი სპეციალიზაცია ანუ დანაშაულისადმი მეთოდოლოგიური მიდგომა, რაც ბუნებრივია. ჰაკერთა უმრავლესობა მიეკუთვნება მაღალი ინტელექტუალური დონის ადამიანებს, რომელთვისაც არ არსებობს დროისა და მანძილის პრობლემა. ამიტომ, არავითარ ეჭვს არ იწვევს პრევენციულ ღონისძიებათა უპირატესობა, რადგანაც ჩადენილი დანაშაულის გამოძიება და, მით უმეტეს, დამნაშავის გამოაშკარავება დაკავშირებულია სერიოზულ სიძნელეებთან, უმეტეს შემთხვევაში კი შეუძლებელია.

გაერთიანებული ერების ორგანიზაციის რეკომენდაციების თანახმად, კიბერდანაშაულის პრევენციის საქმეში ძირითადი ყურადღება უნდა გამახვილდეს პრობლემის ტექნოლოგიურ, ორგანიზაციულ და სამართლებრივ ასპექტებზე. როგორც აღმოჩნდა, საკითხის სამართლებრივმა მხარემ მიიქცია დიდი ყურადღება მსოფლიო თანამეგობრობის მხრიდან, მისი პოლიტიკური შემადგენელის გამო. ამ გარემოებამ კი მნიშვნელოვნად შეაფერხა კანონმდებლობის როგორც ჰარმონიზაციის, ისე კრიმინალიზაციის პროცესი. მიუხედავად ამისა, არსებობს პრობლემა და კაცობრიობას სხვა არჩევანი არ აქვს, გარდა იმისა, რომ თავი გაართვას 21-ე საუკუნის გამოწვევას. ამ კუთხით, რა თქმა უნდა, ჩვენი მიზანია ეროვნული კანონმდებლობის სრულყოფა და განვითარება.

III. კიბერდანაშაულის შემადგენლობის სამართლებრივი დახასიათება

დებულება იმის შესახებ, რომ კიბერდანაშაული დანაშაულის გამოვლინების უნივერსალური ფორმაა, საჭიროებს ანალიზსა და მეცნიერულ დასაბუთებას. საქმე ის გახლავთ, რომ ტერმინი „კიბერდანაშაული“ მისი იურიდიული გაგებით, შეიძლება არსებობდეს მხოლოდ კონკრეტული ქმედების განხორციელების კვალობაზე, მას შემდეგ, რაც სასამართლოს მიერ მოხდება მისი დანაშაულად კვალიფიკაცია. მანამდე, სანამ ეს არ მომხდარა, კანონმდებელი, ფიქციის გამოყენებით ქმნის რა ცალკეულ სისხლისსამართლებრივ კონსტრუქციებს, საკუთარ შეფასებას აძლევს ამა თუ იმ სოციალურად საშიშ ქმედებას და ასახავს კანონში, მაგრამ ეს ჯერ კიდევ არ არის დანაშაული მისი სამართლებრივი გაგებით. როგორც აღვნიშნეთ, იგი ამ სტატუსს მიიღებს მაშინ, როდესაც განხორციელდება კონკრეტული ქმედება და მიეცემა შეფასება სასამართლოს მიერ, როგორც დანაშაულისა. ამას ადასტურებს პროფესორ გურამ ნაჭყებიას მიერ განვითარებული დასაბუთებული დებულება, რომ დანაშაულის იურიდიული ცნება სისხლის სამართლის კანონის პრაქტიკული ამოქმედების გარეშე შეუძლებელია, მაშინ, როდესაც კრიმინალიზაციის ობიექტი სისხლის სამართლის კანონამდე არსებობს და კანონმდებლის საქმიანობის ობიექტს წარმოადგენს. დანაშაულის იურიდიული ცნების დაყვანა კრიმინალიზაციის ობიექტზე, ესაა დანაშაულის წმინდა სოციოლოგიურად გაგების პროცესი. კრიმინალიზაციის ობიექტი - ესაა კანონმდებლის საქმიანობის ობიექტი, მაშინ, როდესაც ქმედების დანაშაულად სასამართლო კვალიფიკაციის ობიექტია დანაშაულის შემადგენლობის შესაბამისი, მართლსაწინააღმდეგო და ბრალეული ქმედება.[6]

როგორც ვხედავთ, აქ საუბარია დანაშაულის სამ ნიშანზე: დანაშაულის შემადგენლობაზე, მართლწინააღმდეგობასა და ბრალზე. რადგანაც დანაშაული მისი იურიდიული გაგებით

[5] *Селико*, *Прохорова*, отмычка для компьютер-пресс-2002, N3, 38.

[6] *ნაჭყებია*, სისხლისსამართლებრივი ურთიერთობა და დანაშაულის ცნება, 2002, 13.

სასამართლოს უფლებამოსილებას განეკუთვნება, მაშინ კრიმინალიზაციის ობიექტში უნდა ვიგულისხმოთ დანაშაულის შემადგენლობა, როგორც დანაშაულის პირველადი ნიშანი. სწორედ დანაშაულებრივ შემადგენლობათა შექმნა-კონსტრუირება წარმოადგენს კანონშემოქმედებითი საქმიანობის ძირითად მიმართულებას, რომელიც რთული და კომპლექსური პროცესია და დაკავშირებულია მრავალ პრობლემასთან. ამჯერად, ჩვენი ინტერესის საგანს წარმოადგენს კონკრეტულად კიბერდანაშაულის შემადგენლობის ცნება, სტრუქტურა და სახეები ეროვნულ სისხლისსამართლებრივ კანონმდებლობასთან მიმართებაში, რომელიც საშუალებას მოგვცემს მკაფიოდ განვსაზღვროთ მისი ადგილი, დანიშნულება და სისხლისსამართლებრივი ფუნქცია სოციალური კონტროლის სფეროში. საკითხს გააჩნია დიდი მნიშვნელობა სამართალგამოყენებითი კუთხით, რაზედაც მეტყველებს არაერთგვაროვანი სასამართლო პრაქტიკა.

აღინიშნა და კვლავ გავიმეორებთ, რომ კიბერდანაშაულის საკანონმდებლო განმარტება არ არსებობს და სისხლის სამართლის კოდექსი იძლევა მხოლოდ ცალკეულ დანაშაულებრივ შემადგენლობებს. აღნიშნული შემადგენლობები შედის საქართველოს სისხლის სამართლის კოდექსის XXXV თავში (კიბერდანაშაული) და შედგება ხუთი საკანონმდებლო კონსტრუქციისგან. ესენია: 284-ე მუხლი (კომპიუტერულ სისტემაში უკანონო შეღწევა), 258-ე მუხლი (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება), 286-ე მუხლი (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა), 286^1-ე მუხლი (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით), 286^2-ე მუხლი (ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა).

წარმოდგენილი შემადგენლობების კრიმინალიზაციის პროცესს წინ უსწრებდა კიბერსივრცეში წარმოშობილ, სოციალურად საშიშ ქმედებათა მრავალსახეობა და ევროპის საბჭოს რეკომენდაციები. გასაგებია ისიც, რომ გარკვეულ ქმედებათა კრიმინალიზაცია ნაკარნახევია პრაქტიკული მოსაზრებებითა და ამ სფეროში შექმნილი უმძიმესი ვითარებით. მაგრამ, უაღრესად პრობლემატურად გვეჩვენება საკითხი ცალკეულ შემადგენლობათა სტრუქტურისა და მისი ადგილით სისხლისსამართლებრივ სისტემაში.

ჩვენს მოსაზრებას ადასტურებს სისხლის სამართლის კოდექსის სხვადასხვა კარში თუ თავებში ასახული დანაშაულის შემადგენლობები, რომლებიც ხორციელდება კიბერტექნოლოგიების გამოყენებით. ამასთან, ზოგიერთი მათგანი, თავისი სამართლებრივი ბუნებით, კიბერდანაშაულის შემადგენლობებს მიეკუთვნება. მაგალითად, სისხლის სამართლის კოდექსის VII კარი, რომელიც ეძღვნება ადამიანის წინააღმდეგ მიმართულ დანაშაულს, XIII თავის (დანაშაული ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ) 158-ე მუხლის პირველივე ნაწილში ჩამოყალიბებულია კერძო კომუნიკაციის საიდუმლოების დარღვევის მარტივი შემადგენლობა: „კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით ან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონო შენახვა.“

ალბათ ეჭვი არავის ეპარება არსებული დანაშაულებრივი ქმედების კრიმინალიზაციის მართებულობაში, ისევ როგორც სისხლის სამართლის კოდექსის 158-ე მუხლის საჭიროებაში, რომელიც მსგავსი შინაარსის დანაშაულებრივი შემადგენლობაა.

გარდა ამისა, სისხლის სამართლის კოდექსის XXXVIII თავი, რომელიც ეთმობა ტერორიზმს, 323-ე მუხლის 1-ლ ნაწილში მოცემულია ტერორიზმის განმარტება, როგორც აფეთქება, ცეცხლის წაკიდება, ადამიანზე თავდასხმა და სხვა ქმედება, ჩადენილი ტერორისტული მიზნით. ამავე თავის 324^1 მუხლში ვხვდებით სპეციალურ შემადგენლობას, კიბერტერორიზმს - ტერორისტულ საქმიანობას, რომლის დროსაც

გამოიყენება კომპიუტერული ტექნოლოგიები ან კომპიუტერული მონაცემები.

იგივე შეიძლება ითქვას 324-ე მუხლზე (ტექნოლოგიური ტერორიზმი), რომელიც თავისი შინაარსითა და განხორციელების მექანიზმით შეიძლება მივაკუთვნოთ კიბერდანაშაულთა კატეგორიას.

მაგრამ საკითხის პრობლემატურობა სწორედ იმაში მდგომარეობს, რომ არსებულ სისხლისსამართლებრივ უმართლობათა დიდი უმრავლესობა შეიძლება ჩადენილ იქნას კიბერტექნოლოგიების ან გამოყენებით ან საშუალებთ. ამ შემთხვევაში, თუ პრაქტიკულად განხორციელებული ქმედება არ თავსდება მხოლოდ ერთი შემადგენლობის ფარგლებში, ქმედება კვალიფიცირდება ორი ან სამი სხვადასხვა შემადგენლობის მიხედვით, ანუ დანაშაულთა ერთობლიობით. გამოდის, რომ ერთი და იგივე ქმედებისთვის, პირი სისხლისსამართლის პასუხისგებაში ეძლევა სხვადასხვა შემადგენლობის მიხედვით. ჩვენ, რა თქმა უნდა, მხედველობაში არ გვაქვს ისეთი შემთხვევები, როდესაც ცალკეული ქმედება სცილდება კონკრეტული დანაშაულებრივი შემადგენლობის ფარგლებს და რეალურად ქმნის დანაშაულთა ერთობლიობას. ამ მხრივ, სასამართლო პრაქტიკა აშკარად არაერთგვაროვანი და წინააღმდეგობრივიცაა, რომლის მიზეზიც უშუალოდ უკავშირდება დანაშაულის საკანონმდებლო კვალიფიკაციის ანუ კრიმინალიზაციის პროცესს.

მართლაც, იმ ვითარებაში, როდესაც კიბერსივრცე და მის წიაღში წარმოშობილი ტექნოლოგიები უშუალოდ მონაწილეობენ სოციალური ცხოვრების თითქმის ყველა სფეროში, რა თქმა უნდა, შესაბამის ზეგავლენასაც ახდენენ ადამიანთა ქცევაზე და ხელს უწყობენ გარკვეული ტიპის, ანტისოციალურ ქმედებათა ფორმირებას ან უკვე არსებულის განხორციელების გაადვილებას. ამიტომ, კანონმდებელი ცდილობს რა ადეკვატურად უპასუხოს შექმნილ ვითარებას, ახდენს ცალკეულ ქმედებათა კრიმინალიზაციას. მაგრამ, როგორც რეალობა გვიჩვენებს, ეს პროცესი არ ატარებს სისტემურ ხასიათს და, სავარაუდოდ, გათვლილია დროის მოკლე პერიოდის მოთხოვნათა გადასაწყვეტად. ამით აიხსნება სისხლის სამართლის კანონმდებლობაში ასახული კიბერდანაშაულის ხასიათის შემადგენლობები. დიდ ანალიზს არ საჭიროებს იმის დადგენა, რომ კიბერტექნოლოგიები თავისი ბუნებით, დამახასიათებელია რა ყველა შემადგენლობისთვის დანაშაულის შემადგენლობის ობიექტური მხარის ელემენტებს განეკუთვნება. ამითაა განპირობებული კანონმდებლის მიერ ცალკეულ შემთხვევებში სპეციალური შემადგენლობების შექმნა. მაგრამ პრობლემა იმაშია, რომ სპეციალური მუხლების, ანუ შემადგენლობების შექმნის აუცილებლობა ყოველდღიურად იზრდება, რაც კიბერსივრცის განსაკუთრებული ფენომენითაა განპირობებული. მსგავსი ტენდენცია კი უახლოვეს პერსპექტივაში შექმნის სერიოზულ სიძნელეებს საკანონმდებლო ტექნიკის თვალსაზრისით და ჩვენ მივიღებთ მრავალტომიან სისხლის სამართლის კოდექსს. ეს კი, თავის მხრივ, გაართულებს სამართალგამოყენებით საქმიანობას, არაფერს ვამბობთ კვალიფიკაციის პრობლემებზე.

ამრიგად, დღის წესრიგში უკვე დგას საკითხის დაუყოვნებლივ მოგვარების აუცილებლობა და, ვიდრე ეს არ მომხდარა, მიზანშეწონილად მიგვაჩნია ისეთი სამართლებრივი ნორმის შემუშავება და სისხლის სამართლის კოდექსში ასახვა, რომლითაც გათვალისწინებულ იქნება ყველა შესაძლო სისხლისსამართლებრივი უმართლობის განხორციელების შესაძლებლობა კიბერტექნოლოგიების გამოყენებით, როგორს მაკვალიფიცირებელი გარემოებისა. ეს, უპირველეს ყოვლისა, მოგვცემს საშუალებას სისტემურად იქნას მოწესრიგებული კიბერდანაშაულის ადგილი კოდექსში და, მეორე მხრივ, თავიდან აგვაცილებს ქმედების კვალიფიკაციასთან დაკავშირებულ პრობლემებს. თუ შევთანხმდებით საკითხის მოგვარების მართებულობაზე ზოგადად, მისი დეტალური კონსტრუირება არ იქნება დაკავშირებული რაიმე სახის სირთულეებთან, რადგანაც კიბერტექნოლოგიების როლი, როგორც ვთქვით, შემოიფარგლება მხოლოდ დანაშაულის განხორციელების ხერხითა და საშუალებით და, ჯერჯერობით, არ ქმნის დამოუკიდებელ შემადგენლობათა ტიპურ სიმრავლეს. ისიც გასათვალისწინებელია, რომ უახლოვეს მომავალში კიბერსივრცე შემოგვთავა-

ზებს ისეთ სიახლეს, რომელიც უთანაზომოდ გაზრდის კვლევის დიაპაზონს სამართლებრივ და მათ შორის სისხლისსამართლებრივ სფეროში. საკითხი ეხება ხელოვნური ინტელექტის შექმნა-განვითარებას, რომლის ფენომენი იმანენტურად შეიცავს სოციალურად საშიშ ქმედებათა წარმოშობის განუსაზღვრელ, რეალურ შესაძლებლობას. ამაზე მეტყველებს პროფესორ ზ. გაბისონიას სამეცნიერო სტატია, რომელიც ეძღვნება ხელოვნური ინტელექტის არსსა და მისი სამართლებრივი რეგულირების საჭიროებას. მართალია, იგი ეხება ხელოვნური ინტელექტის პროგრამის ან რობოტისთვის სამართლებრივი სტატუსის მინიჭების შესაძლებლობას და მსჯელობა მიმდინარეობს სამოქალაქოსამართლებრივ ჭრილში, მაგრამ წარმოდგენილ ფაქტობრივ რეალიებში ნათლად იკვეთება სოციალური ურთიერთობის ისეთი სპეციფიკური სახე, რომელიც დღემდე უცნობი იყო კაცობრიობისთვის და რომელიც მრავალ სისხლისსამართლებრივ პრობლემას დააყენებს.[7]

კიბერდანაშაულის შემადგენლობის სამართლებრივი დახასიათებისას, გვერდს ვერ აუვლით საკითხს მისი გაუფრთხილებლობით ჩადენის შესაძლებლობის შესახებ. მსგავს ფორმას ეროვნული სისხლისსამართლებრივი კანონმდებლობა არ იცნობს, მაშინ როდესაც მთელი რიგი ქვეყნების მიერ იგი გათვალისწინებულია და ეფექტიანად ასრულებს სისხლისსამართლებრივ ფუნქციებს. რა თქმა უნდა, კიბერდანაშაული, თავისი ბუნებით, შეუძლებელია არ გულისხმობდეს გაუფრთხილებლობას. მაშინ როდესაც სატრანსპორტო, საამშენებლო თუ სხვა სფეროში ჩადენილ დანაშაულთა უმრავლესობა გაუფრთხილებლობით ხდება, მით უმეტეს იგი დამახასიათებელია კიბერსივრცისთვის, რომელიც ყველა ამ დანაშაულის ობიექტურ მხარეს განეკუთვნება. სწორედ კიბერტექნოლოგიების გაუფრთხილებლობითი გამოყენების შედეგია ჩერნობილის ატომურ ელექტროსადგურზე მომხდარი ავარია, ისე როგორც კრუიზული გემის, ,,კონკორდიას'' დაღუპვა. მსგავსი მაგალითები უამრავია და, შეიძლება ითქვას, რომ იგი დამახასიათებელი, სისტემური და სოციალურად საშიშია სოციალური ცხოვრებისთვის. ამიტომ, კანონმდებლობაში არსებული ხარვეზი დაუყოვნებლივ მოწესრიგებას საჭიროებს.

IV. დასკვნა

დასკვნის სახით შეიძლება ითქვას, რომ კიბერსივრცე და მის წიაღში აღმოცენებული სოციალურად საშიში ქმედება, კიბერდანაშაულის შემადგენლობების სახით, არსებული მოცემულობით, სხვა არაფერია, თუ არა დანაშაულის განხორციელების, თვისებრივად სრულიად ახალი ტექნოლოგიური ხერხი და საშუალება. ამიტომ, გარდა იშვიათი გამონაკლისებისა, მიზანშეწონილია მისი ცალკეულ დანაშაულებრივ შემადგენლობებში ასახვა, როგორც მაკვალიფიცირებელი ნიშნისა, ან სისხლის სამართლის შესაბამის თავში აღნიშვნა იმისა, რომ ინტერნეტის და, ზოგადად, კიბერტექნოლოგიების გამოყენება წარმოადგენს დამამძიმებელ გარემოებას. საკანონმდებლო ტექნიკის თვალსაზრისით, ეს გაცილებით მისაღები და მოსახერხებელია, ვიდრე ამ ნიშნით ცალკეულ შემადგენლობათა შექმნა. წინააღმდეგ შემთხვევაში, სახეზე გვექნება განუსაზღვრელი ოდენობის შემადგენლობები, რომელთაც სისხლის სამართლის კოდექსი ვერ დაიტევს. გარდა იმისა, რომ იგი მოუხერხებელი იქნება ტექნიკური თვალსაზრისით, შექმნის სირთულეებს სამართლებრივი კუთხითაც, ქმედების დანაშაულად კვალიფიკაციისას. ამას ადასტურებს არაერთგვაროვანი სასამართლო და საგამოძიებო პრაქტიკა.

ამიტომ, კიბერტექნოლოგიების როლი დანაშაულის შემადგენლობებში შემოიფარგლება თავად შემადგენლობების ობიექტური მხარის ელემენტების ნაირსახეობით და უმეტეს შემთხვევაში, არ საჭიროებს ამ ნიშნით დამოუკიდებელი შემადგენლობის შექმნას.

დავას არ უნდა იწვევდეს კიბერდანაშაულის ჩადენის შესაძლებლობა გაუფრთხილებლობით, რაც ეროვნული სისხლისსამართლებრივი კანონმდებლობის ხარვეზია და საჭიროა აღნიშნული შემადგენლობის დაუყოვნებლივი კრი-

[7] *გაბისონია*, ხელოვნური ინტელექტის არსი და მისი სამართლებრივი რეგულირების საჭიროება, შედარებითი სამართლის ქართულ-გერმანული ჟურნალი 7/2021, 34-43.

მინალიზაცია. ამ პროცესის საჭიროება განსაკუთრებული სიმწვავით წარმოჩინდა პანდემიის დროს, როდესაც ბუნებრივად გამოიკვეთა ტექნოლოგიებთან სავალდებულო მიდგომის ვალდებულება და სხვა უამრავი საკითხი. მართლაც, როდესაც საუბარია კიბერსივრცის უნივერსალობასა და კიბერტექნოლოგიების გამოყენების განუსაზღვრელ პოტენციალზე, არ უნდა დაგვავიწყდეს საკითხი იმასთან დაკავშირებით, რომ მაღალტექნოლოგიების გამოყენება გულისხმოს მათდამი პასუხისმგებლურ დამოკიდებულებას და გარკვეული დოზით, მასთან დაკავშირებული ქმედებების კრიმინალიზაციის აუცილებლობას.