განაცხადი

„როგორც წარდგენილი [ნაშრომის ტიპი] ნაშრომის ავტორი, ვაცხადებ, რომ ნაშრომი წარმოადგენს ჩემს ორიგინალურ ნამუშევარს და არ შეიცავს სხვა ავტორებისადმი აქამდე გამოქვეყნებულ, გამოსაქვეყნებლად მიღებულ ან/და დასაცავად წარგენილ მასალებს, რომლებიც ნაშრომში არ არის მოხსენიებული ან ციტირებული სათანადო წესების შესაბამისად"

ნიმუში

[თარიღი]

სარჩევი

ანოტაცია.....iv
შესავალი.....6
1. თავი I. კიბერდანაშაულის ცნება, სახეები და სამართლებრივი ბაზა.....12
1.1. კიბერდანაშაულის დეფინიცია და დოქტრინალური მიდგომები.....12
1.2. კიბერდანაშაულის სახეები და კლასიფიკაცია.....18
1.3. საერთაშორისო და ეროვნული სამართლებრივი ჩარჩო.....25
2. თავი II. კიბერდანაშაულის კვალიფიკაციის დოქტრინალური პრობლემები.....33
2.1. ობიექტური და სუბიექტური შემადგენლობის თავისებურებები.....33
2.2. დანაშაულის დროისა და ადგილის განსაზღვრის პრობლემა.....39
2.3. კიბერდანაშაულის გამიჯვნა სხვა მონათესავე დანაშაულებისგან.....46
3. თავი III. კიბერდანაშაულის კვალიფიკაციის პრაქტიკული გამოწვევები საქართველოსა და საერთაშორისო პრაქტიკაში.....52
3.1. საქართველოს სასამართლო პრაქტიკის ანალიზი.....52
3.2. ევროპული სასამართლოსა და უცხო ქვეყნების პრაქტიკა.....58
3.3. მტკიცებულებითი სტანდარტები და გამოძიების სირთულეები.....63
დასკვნა.....73

ანოტაცია

სამაგისტრო ნაშრომში განხილულია კიბერდანაშაულის კვალიფიკაციის დოქტრინალური და პრაქტიკული პრობლემები თანამედროვე ქართულ სისხლის სამართალში. თემის აქტუალობას კიბერდანაშაულის მზარდი მასშტაბი და ამ სფეროში არსებული სამართლებრივი გაურკვევლობა განაპირობებს. ნაშრომის მიზანია კიბერდანაშაულის მარეგულირებელი კანონმდებლობისა და სასამართლო პრაქტიკის ანალიზი, პრობლემების იდენტიფიცირება და მათი გადაჭრის გზების ძიება. კვლევისას გამოყენებულია დოქტრინალური, შედარებით-სამართლებრივი და სისტემური ანალიზის მეთოდები, რომელთა საშუალებითაც შესწავლილია საერთაშორისო და ეროვნული კანონმდებლობა, ასევე სასამართლო პრაქტიკა.

კვლევამ ცხადყო, რომ კიბერდანაშაულის კვალიფიკაციის მთავარი გამოწვევებია: ტერმინის ერთიანი დეფინიციის არარსებობა, სისხლის სამართლის კოდექსში კიბერშემადგენლობების უსისტემო და ფრაგმენტული განლაგება და ტრადიციული დანაშაულებისგან გამიჯვნის სირთულე, რაც ხშირად ნორმათა კონკურენციასა და ქმედების დანაშაულთა ერთობლიობით კვალიფიკაციას იწვევს. ამ პრობლემების გადასაჭრელად ნაშრომში წარმოდგენილია რეკომენდაციები. მათ შორის უმთავრესია, რომ კიბერტექნოლოგიების გამოყენება დამოუკიდებელი დანაშაულების ნაცვლად ტრადიციული დანაშაულების მაკვალიფიცირებელ გარემოებად ჩაითვალოს. ამასთან, შემოთავაზებულია კოდექსის სტრუქტურული სისტემატიზაცია, ახალი ქმედებების (მაგალითად, კიბერგადაკიდების) კრიმინალიზაცია, სამართალდამცველთა კვალიფიკაციის ამაღლება და საერთაშორისო თანამშრომლობის გაღრმავება.

Annotation

The master's thesis discusses the doctrinal and practical problems of cybercrime qualification in modern Georgian criminal law. The relevance of the topic is determined by the growing scale of cybercrime and the legal uncertainty in this area. The aim of the work is to analyze the legislation and judicial practice regulating cybercrime, identify problems and search for ways to solve them. The research used doctrinal, comparative legal and systematic analysis methods, through which international and national legislation, as well as judicial practice, were studied.

The research revealed that the main challenges of cybercrime qualification are: the absence of a unified definition of the term, the unsystematic and fragmentary arrangement of cybercrime components in the Criminal Code, and the difficulty of distinguishing it from traditional crimes, which often leads to competition of norms and qualification of actions as a set of crimes. The paper presents recommendations to address these problems. The most important of these is to consider the use of cyber technologies as a qualifying circumstance for traditional crimes instead of independent crimes. In addition, structural systematization of the Code, criminalization of new actions (for example, cyberstalking), improvement of law enforcement qualifications, and deepening international cooperation are proposed.

შესავალი

ტექნოლოგიურმა რევოლუციამ და საზოგადოების ტოტალურმა კომპიუტერიზაციამ ჩვენი ცხოვრების ყველა სფერო რადიკალურად გარდაქმნა, თუმცა ამ პროცესს თან ახლავს ახალი, გლობალური გამოწვევები, რომელთა შორის ერთ-ერთი ყველაზე მწვავე კიბერდანაშაულია. იგი დღეს „ციფრულ ეპიდემიად“ იქცა, რომელიც მთელ კაცობრიობას სინქრონულად და კოორდინირებულად მოქმედებას აიძულებს.[1] კიბერსივრცე ერთგვარ ბრძოლის ველად გადაიქცა, სადაც დანაშაულებრივი ხელყოფა ნებისმიერი კანონით დაცული სიკეთის წინააღმდეგაა შესაძლებელი. ამ ფენომენის მასშტაბი და მისგან მომდინარე ზიანი იმდენად დიდია, რომ მისი აქტუალობა უდავოა. მაგალითად, კვლევებით დგინდება, რომ კიბერდანაშაულით გამოწვეული ზიანი ევროპაში ყოველწლიურად დაახლოებით 750 მილიონ ევროს შეადგენს, ხოლო ამერიკის შეერთებულ შტატებში ერთ მილიარდ დოლარს აღწევს.[2] უფრო მეტიც, კიბერდანაშაულიდან მიღებულმა შემოსავლებმა დიდი ხანია გადააჭარბა ნებისმიერი სხვა, მათ შორის ნარკოდანაშაულის, შემოსავლებს.[3] ეს სტატისტიკაც კი არასრულია, რადგან დანაშაულთა დიდი ნაწილი ლატენტური რჩება. ერთი შეფასებით, ჩადენილი დანაშაულების მხოლოდ 5% ხვდება სამართალდამცავი ორგანოების ხედვის არეში.[4]

კიბერდანაშაულის მზარდი საფრთხე იმითაც მძაფრდება, რომ მისი ჩადენა სულ უფრო მარტივდება. დღეს კიბერდამნაშავეს აღარ სჭირდება რთული ტექნიკური უნარ-ჩვევები, რადგან ინტერნეტში ხელმისაწვდომია მზა ინსტრუმენტები და სერვისებიც კი („კიბერდანაშაული როგორც სერვისი“), რაც დამნაშავეთა წრეს აფართოებს.[5] გაეროს მონაცემებით, კიბერდანაშაულებრივი ქმედებების 80%-ზე მეტს ორგანიზებული ჯგუფები ახორციელებენ, რომლებიც ქმნიან მავნე პროგრამებს, აინფიცირებენ კომპიუტერებს, ქმნიან ბოტნეტებს, იპარავენ პერსონალურ და ფინანსურ მონაცემებს და შემდეგ ყიდიან.[6] ვიქტიმიზაციის კვლევებიც ადასტურებს, რომ კიბერდანაშაულის მსხვერპლად

---

1 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 21-26.

2 იქვე., გვ. 21-26.

3 იქვე., გვ. 21-26.

4 Cernomoreț, S. and Nastas, A. Comparative Analysis of Cybercrime in the Criminal Law System. 2020, pp. 22-24.

5 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, pp. 19-21.

6 იქვე.

გახდომის რისკი გაცილებით მაღალია, ვიდრე ტრადიციული დანაშაულებისა. 21 ქვეყნის მონაცემებით, ონლაინ საკრედიტო ბარათის თაღლითობის, იდენტობის ქურდობის ან ფიშინგის მსხვერპლი ონლაინ მოსახლეობის 1%-დან 17%-მდე ხდება, მაშინ როდესაც იმავე ქვეყნებში ყაჩაღობის ან ქურდობის მაჩვენებელი 5%-ს არ აღემატება.[7]

კიბერდანაშაული მხოლოდ ინდივიდუალურ პირთა საკუთრების ხელყოფის პრობლემა აღარ არის და ის სულ უფრო ხშირად გამოიყენება როგორც გეოპოლიტიკური იარაღი სახელმწიფოებს შორის. 2007 წელს ესტონეთზე განხორციელებული მასშტაბური კიბერშეტევა, რომელიც რუსეთთან იყო დაკავშირებული, ერთ-ერთ პირველ პრეცედენტად იქცა, როდესაც სუვერენული სახელმწიფოს სტრატეგიული ინფრასტრუქტურა (სამთავრობო ვებგვერდები, ფინანსური ორგანიზაციები, მედიასაშუალებები) მიზანმიმართული შეტევის ობიექტი გახდა.[8] საქართველოსთვის ეს საფრთხე განსაკუთრებით მწვავედ 2008 წლის აგვისტოს ომის დროს გამოვლინდა, როდესაც რუსეთის ფედერაციის მიერ სამხედრო აგრესიის წინ განხორციელებული კიბერშეტევების შედეგად მწყობრიდან გამოვიდა სამთავრობო და სამხედრო დანიშნულების მრავალი დაწესებულება. ამ ფაქტმა ნათლად დაგვანახა სამომავლო ომების წარმოების რეალური სახე და მთლიანად შეცვალა მისი ბუნება.[9] 2008 წლის კიბერშეტევამ საქართველოს აჩვენა, რომ ქვეყნის ეროვნული უსაფრთხოების მიღწევა კიბერსივრცის უსაფრთხოების უზრუნველყოფის გარეშე შეუძლებელია და საზღვაო, საჰაერო თუ სახმელეთო სივრცეების დაცვის პარალელურად, ქვეყანას ეფექტიანი კიბერპოლიტიკა სჭირდება.[10] ეს გამოწვევაც დღეს აქტუალურია, რადგან საქართველო კვლავ რჩება კიბერშპიონაჟისა და ფინანსურ სექტორზე მიზანმიმართული შეტევების სამიზნედ.[11]

ამ გლობალური და ეროვნული მასშტაბის საფრთხეების ფონზე, თემის აქტუალობას კიდევ უფრო ამძაფრებს ის სამართლებრივი ქაოსი, რომელიც კიბერდანაშაულის კვალიფიკაციის სფეროში არსებობს. კიბერდანაშაულის

---

7 იქვე.

8 ბიბიჩაძე, თ. და ოვაკიმიან, შ. კიბერუსაფრთხოება, როგორც მთავარი გამოწვევა საერთაშორისო ურთიერთობებში (საქართველოს, უკრაინის, ესტონეთის შემთხვევების ანალიზი). ჟ. სტუდენტთა ჟურნალი სოციალურ მეცნიერებებში. 2024, 26, გვ. 5-9.

9 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 21-26.

10 ბიბიჩაძე, თ. და ოვაკიმიან, შ. კიბერუსაფრთხოება, როგორც მთავარი გამოწვევა საერთაშორისო ურთიერთობებში (საქართველოს, უკრაინის, ესტონეთის შემთხვევების ანალიზი). ჟ. სტუდენტთა ჟურნალი სოციალურ მეცნიერებებში. 2024, 26, გვ. 5-9.

11 იქვე., გვ. 5-9.

ერთიანი, საყოველთაოდ აღიარებული დეფინიციის არარსებობა, მისი შემადგენლობების უსისტემო განლაგება სისხლის სამართლის კოდექსში და ტრადიციული დანაშაულებისგან გამიჯვნის სირთულეები სერიოზულ პრობლემებს უქმნის როგორც კანონმდებელს, ისე სამართალგამომყენებელს. ეს ვითარება იწვევს ნორმათა არასასურველ კონკურენციას, ქმედების არასწორ კვალიფიკაციასა და, საბოლოო ჯამში, მართლმსაჯულების ეფექტიანობის შემცირებას. შესაბამისად, კიბერდანაშაულის კვალიფიკაციის დოქტრინალური და პრაქტიკული პრობლემების დაწვრილებითი კვლევა, მათი მიზეზების დადგენა და გადაჭრის გზების ძიება თანამედროვე ქართული სისხლის სამართლის მეცნიერებისთვის ერთ-ერთ საკვანძო ამოცანას წარმოადგენს.

წინამდებარე კვლევის მთავარი პრობლემაა კიბერსივრცეში განხორციელებულ ქმედებათა სისხლისსამართლებრივი კვალიფიკაციის პროცესში არსებული დოქტრინალური და პრაქტიკული სირთულეები. ეს პრობლემა რამდენიმე ძირითადი, ერთმანეთთან მჭიდროდ დაკავშირებული ასპექტისგან შედგება, რაც არაერთგვაროვანი და ხშირად წინააღმდეგობრივი სამართალგამოყენების პრაქტიკის საფუძველს ქმნის. უპირველეს ყოვლისა, პრობლემის სათავე „კიბერდანაშაულის“ ცნების დეფინიციის არარსებობაშია. არ არსებობს ამ ტერმინის ერთიანი, საყოველთაოდ მიღებული და, რაც მთავარია, საკანონმდებლო დონეზე განმტკიცებული განმარტება. დოქტრინაში არსებული დეფინიციები კი იმდენად განსხვავებული და ზოგჯერ ურთიერთგამომრიცხავია, რომ პრაქტიკული მიზნებისთვის ვერ გამოდგება.[12] ცნების ეს ბუნდოვანება პირდაპირ აისახება კრიმინალიზაციის პროცესზე და „აძნელებს როგორც ქმედების საკანონმდებლო, ისე სასამართლო კვალიფიკაციას“.[13] ეს პრობლემა საერთაშორისო დონეზეც მწვავედ დგას. მაგალითად, ბუდაპეშტის კონვენციაც კი, რომელიც ამ სფეროში ძირითად დოკუმენტად ითვლება, გაკრიტიკებულია იმის გამო, რომ ტექნოლოგიურად ნეიტრალური ტერმინოლოგიის გამოყენებით „სიზუსტე ეფექტიანობას შესწირა“, რამაც წევრ სახელმწიფოებში განსხვავებული განხორციელება და ჰარმონიზაციის დაბალი ხარისხი გამოიწვია.[14]

12 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 11-18.

13 იქვე., გვ. 11-18.

14 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, pp. 30-34.

დეფინიციის არარსებობასთან ერთად, არსებობს მეორე არსებითი პრობლემაც: კიბერდანაშაულებრივი შემადგენლობების უსისტემო და ფრაგმენტული განლაგება საქართველოს სისხლის სამართლის კოდექსში. მსგავსი შინაარსის დანაშაულები, რომლებიც კიბერტექნოლოგიების გამოყენებას უკავშირდება (მაგალითად, კიბერტერორიზმი, პირადი ცხოვრების საიდუმლოს ხელყოფა და სხვ.), კოდექსის სხვადასხვა თავშია გაბნეული და ერთ ლოგიკურად გამართულ სისტემაში არ არის თავმოყრილი.[15] ასეთი არაორგანიზებული სტრუქტურა იწვევს ნორმათა კონკურენციას, როდესაც ერთი და იმავე ქმედების მიმართ შესაძლოა რამდენიმე ნორმის გამოყენება განიხილებოდეს. ეს კი ქმნის „ქმედების დანაშაულთა ერთობლიობით კვალიფიკაციის უსამართლო შემთხვევებს“, როდესაც, ფაქტობრივად, ერთი უმართლობა რამდენიმე, შინაარსობრივად მსგავსი მუხლით ფასდება.[16] სწორედ ამ პრობლემების გამო ჩნდება საფუძვლიანი კითხვები: „რამ განაპირობა „კიბერდანაშაულებრივ“ ქმედებათა კრიმინალიზაციის საჭიროება დამოუკიდებელ შემადგენლობებად?“ და „ხომ არ შექმნა მსგავსმა პროცესმა სისხლისსამართლებრივ ნორმათა კონკურენციის ისეთი დონე, როდესაც მათი გამიჯვნა სირთულესთანაა დაკავშირებული ან/და შეუძლებელი ხდება?“.[17]

ამრიგად, კვლევის პრობლემა კიბერდანაშაულის კვალიფიკაციის მარეგულირებელი საკანონმდებლო ბაზის არასრულყოფილებაა, რაც ცნების დეფინიციის არარსებობით, კოდექსში შემადგენლობების უსისტემო განლაგებითა და, შედეგად, სამართალგამოყენების პრაქტიკაში წარმოშობილი სირთულეებით გამოიხატება.

წინამდებარე ნაშრომის მიზანია კიბერდანაშაულის კვალიფიკაციასთან დაკავშირებული დოქტრინალური და პრაქტიკული პრობლემების სრულყოფილი ანალიზი, ამ პრობლემების გამომწვევი მიზეზების დადგენა და ქართული სისხლის სამართლის კანონმდებლობისა და პრაქტიკის სრულყოფის მიზნით მეცნიერულად დასაბუთებული რეკომენდაციების შემუშავება. ამ მიზნის მისაღწევად ნაშრომში დაისახა შემდეგი ამოცანები: კიბერდანაშაულის ცნებისა და მისი დამახასიათებელი ნიშნების შესწავლა, არსებული დოქტრინალური მიდგომებისა და დეფინიციასთან დაკავშირებული პრობლემების ანალიზი;

15 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 121-122.
16 იქვე., გვ. 36-43.
17 იქვე., გვ. 121-127.

კიბერდანაშაულის ძირითადი სახეების კლასიფიკაცია და მათი სპეციფიკური მახასიათებლების გამოკვეთა; კიბერდანაშაულთან ბრძოლის საერთაშორისო და ეროვნული სამართლებრივი ჩარჩოს ანალიზი, მისი ძლიერი და სუსტი მხარეების დადგენა; კიბერდანაშაულის შემადგენლობის ობიექტური და სუბიექტური მხარის თავისებურებების კვლევა; კიბერდანაშაულის სხვა მონათესავე დანაშაულებისგან გამიჯვნის პრობლემებისა და ნორმათა კონკურენციის საკითხების ანალიზი; კიბერდანაშაულის ჩადენის დროისა და ადგილის განსაზღვრის პრობლემისა და მასთან დაკავშირებული იურისდიქციული საკითხების შესწავლა; ადამიანის უფლებათა ევროპული სასამართლოს, უცხო ქვეყნებისა და საქართველოს სასამართლო პრაქტიკის ანალიზი კიბერდანაშაულის კვალიფიკაციის კუთხით; კიბერდანაშაულის საქმეებზე არსებული მტკიცებულებითი სტანდარტებისა და გამოძიების პროცესში წარმოქმნილი სირთულეების კვლევა.

ნაშრომის კვლევის ობიექტს წარმოადგენს ის სოციალურ-სამართლებრივი ურთიერთობები, რომლებიც ყალიბდება კიბერსივრცეში განხორციელებული ქმედებების სისხლისსამართლებრივი კვალიფიკაციის, მათი კრიმინალიზაციისა და დამტკიცების პროცესში, ხოლო კვლევის საგანს შეადგენს კიბერდანაშაულის კვალიფიკაციის თეორიული, დოქტრინალური და პრაქტიკული პრობლემები, კიბერდანაშაულის მარეგულირებელი საერთაშორისო და საქართველოს ეროვნული სისხლისა და სისხლის საპროცესო სამართლის ნორმები, ასევე, შესაბამისი სასამართლო პრაქტიკა.

ნაშრომი შედგება შესავლის, სამი ძირითადი თავის, დასკვნისა და გამოყენებული ლიტერატურის ნუსხისგან. შესავალში დასაბუთებულია თემის აქტუალობა, ჩამოყალიბებულია კვლევის პრობლემა, მიზანი და ამოცანები, განისაზღვრება კვლევის ობიექტი და საგანი. პირველ თავში, „კიბერდანაშაულის ზოგადი დახასიათება და კვალიფიკაციის დოქტრინალური პრობლემები“, განხილულია კიბერდანაშაულის ცნებასთან დაკავშირებული დეფინიციური სირთულეები და დოქტრინაში არსებული სხვადასხვა მიდგომა, ასევე წარმოდგენილია კიბერდანაშაულის სახეობათა კლასიფიკაცია და მათი სპეციფიკური მახასიათებლების ანალიზი. მეორე თავი, „კიბერდანაშაულის კვალიფიკაციის მარეგულირებელი ნორმები და მათი გამოყენების პრაქტიკული პრობლემები“, ეძღვნება კიბერდანაშაულის მარეგულირებელი საერთაშორისო (ბუდაპეშტის კონვენცია, ევროკავშირის დირექტივები) და ეროვნული სამართლებრივი ჩარჩოს ანალიზს. ამავე თავში დეტალურად არის

გამოკვლეული კიბერდანაშაულის შემადგენლობის ობიექტური და სუბიექტური მხარის თავისებურებები და გაანალიზებულია კიბერდანაშაულის სხვა მონათესავე დანაშაულებისგან გამიჯვნის პრობლემები, განსაკუთრებით ნორმათა კონკურენციის საკითხი. მესამე თავი, „კიბერდანაშაულის კვალიფიკაციის პრობლემები მართლმსაჯულების პრაქტიკაში“, ყურადღებას ამახვილებს პრაქტიკულ გამოწვევებზე. მასში განხილულია დანაშაულის დროისა და ადგილის განსაზღვრის სირთულეები, იურისდიქციული საკითხები და გაანალიზებულია ადამიანის უფლებათა ევროპული სასამართლოს, უცხო ქვეყნებისა და საქართველოს სასამართლოების კონკრეტული გადაწყვეტილებები. ამასთან, თავი ეხება კიბერდანაშაულის საქმეებზე არსებულ მტკიცებულებით სტანდარტებსა და გამოძიების პროცესში არსებულ ტექნიკურ და სამართლებრივ სირთულეებს. დასკვნით ნაწილში შეჯამებულია კვლევის ძირითადი შედეგები და წარმოდგენილია კონკრეტული რეკომენდაციები ქართული სისხლის სამართლის კანონმდებლობისა და პრაქტიკის გასაუმჯობესებლად.

თავი I. კიბერდანაშაულის ცნება, სახეები და სამართლებრივი ბაზა

1.1. კიბერდანაშაულის დეფინიცია და დოქტრინალური მიდგომები

კიბერდანაშაულის ერთიანი, საყოველთაოდ აღიარებული დეფინიციის არარსებობა თანამედროვე სისხლის სამართლის დოქტრინისა და პრაქტიკისთვის ერთ-ერთ მთავარ გამოწვევად რჩება. ეს პრობლემა საერთაშორისო დოკუმენტებსა და ეროვნულ კანონმდებლობებშიც აისახება, სადაც ტერმინის ლეგალური განმარტება, როგორც წესი, არ გვხვდება.[18] მეცნიერთა შორისაც კი არ არსებობს ერთიანი ხედვა, რაც ამ ფენომენის მრავალფეროვნებითა და მისი საზღვრების მუდმივი გაფართოებით აიხსნება.[19] შესაბამისად, დღემდე აქტუალურია დისკუსია იმის შესახებ, თუ რა არის კიბერდანაშაული, რა ნიშნებით ხასიათდება და სად გადის ზღვარი ტრადიციულ დანაშაულსა და მის კიბერანალოგს შორის.

ტერმინოლოგიური თვალსაზრისით, საინტერესოა ცნების ევოლუცია. თავდაპირველად, დაახლოებით 2000 წლამდე, დომინანტური ტერმინი იყო „კომპიუტერული დანაშაული“ (computer crime), თუმცა დროთა განმავლობაში, განსაკუთრებით ინტერნეტის ფართოდ გავრცელების შემდეგ, საყოველთაო გამოყენებაში ტერმინი „კიბერდანაშაული“ (cybercrime) დამკვიდრდა.[20] ამ ცვლილებასთან ერთად გაჩნდა დისკუსიაც, თუ რომელი ცნებაა უფრო ფართო. მაგალითად, გაეროს მიდგომით, კიბერდანაშაული ზოგადი, ვრცელი ცნებაა, ხოლო კომპიუტერული დანაშაული მისი ვიწრო გაგებაა, რაც კონკრეტულად კომპიუტერული სისტემების უსაფრთხოების ხელყოფას გულისხმობს.[21] მსგავს პოზიციაზეა პროფესორი ტ. ტროპინაც, რომელიც ამტკიცებს, რომ „კიბერდანაშაული“ ბევრად ზოგადი და ფართო ტერმინია, რადგან ის მოიცავს ტრადიციულ დანაშაულებსაც, რომლებიც კომპიუტერული ტექნიკის დახმარებით სრულდება, და უშუალოდ კომპიუტერული სისტემების წინააღმდეგ მიმართულ

18 იქვე., გვ. 96.

19 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 382.

20 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 381-382.

21 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 18-19.

ქმედებებსაც.[22] საქართველოს სისხლის სამართლის კოდექსიც, როგორც ჩანს, ამ ლოგიკას მისდევს, რადგან XXXV თავი „კიბერდანაშაულად“ არის დასათაურებული, თუმცა მასში შემავალი მუხლები ძირითადად კომპიუტერულ დანაშაულებს აერთიანებს.[23]

კიბერდანაშაულის დეფინიციის პრობლემა ნათლად ჩანს სამეცნიერო ლიტერატურაში არსებულ მრავალფეროვან და ხშირად ურთიერთსაწინააღმდეგო განმარტებებში. მაგალითად, 1983 წელს პარიზში ექსპერტთა ჯგუფმა კიბერდანაშაული განმარტა, როგორც „კანონით აკრძალული, არაეთიკური ქმედება, რომელიც აფერხებს მონაცემთა ბაზების ავტომატიზებულ მუშაობას ან ინფორმაციის გადაცემას“.[24] ეს განმარტება მალევე გააკრიტიკეს მისი არასრულყოფილების გამო, რადგან ტერმინი „არაეთიკური ქმედება“ ბუნდოვანია, ხოლო დანაშაულის ობიექტების ჩამონათვალი - შეზღუდული.[25] მოგვიანებით, 2000 წელს შემოთავაზებულ იქნა უფრო ფართო დეფინიცია: „კომპიუტერის მეშვეობით განხორციელებული აქტივობები, რომლებიც ან უკანონოა, ან გარკვეული მხარეების მიერ მიუღებლად ითვლება და რომელთა განხორციელებაც შესაძლებელია გლობალური ელექტრონული ქსელებით“.[26] ამ განმარტების უპირატესობა ისაა, რომ ის აქცენტს კიბერსივრცეზე, როგორც დანაშაულის ჩადენის ახალ გარემოზე, აკეთებს. ასევე, ერთ-ერთი ხშირად ციტირებადი დეფინიციით, კიბერდანაშაულია „ნებისმიერი დანაშაული, რომელიც ხელშეწყობილია ან ჩადენილია კომპიუტერის, ქსელის ან აპარატული მოწყობილობის გამოყენებით“.[27] ეს მიდგომა ხაზს უსვამს ტექნოლოგიის, როგორც ინსტრუმენტის, მნიშვნელობას.

განსხვავებული მიდგომებიდან ყველაზე ხშირად ერთმანეთს კიბერდანაშაულის ვიწრო და ფართო გაგებას უპირისპირებენ. ვიწრო გაგებით, კიბერდანაშაული არის ქმედება, რომელიც უშუალოდ ინტერნეტის, მონაცემთა

---

22 იქვე., გვ. 19.

23 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 11.

24 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 17.

25 იქვე., გვ. 17.

26 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 382.

27 იქვე.

ბაზებისა და საინფორმაციო სისტემების წინააღმდეგაა მიმართული.[28] ხოლო ფართო გაგებით, კიბერდანაშაულს მიეკუთვნება ყველა სისხლისსამართლებრივი დანაშაული, რომელიც საინფორმაციო-საკომუნიკაციო ტექნოლოგიების გამოყენებით ხორციელდება.[29] ეს დაყოფა, მართალია, გავრცელებულია, მაგრამ ზოგიერთი ავტორის აზრით, არამიზანშეწონილია. მაგალითად, ერთი მოსაზრებით, ორივე შემთხვევაში საფუძვლად დანაშაულის შემადგენლობის ობიექტური მხარის ელემენტებია აღებული - დანაშაულის ჩადენის საშუალება (ფართო გაგება) და კანონით დაცული ობიექტი (ვიწრო გაგება), რაც ამგვარ დაყოფას ხელოვნურს ხდის.[30] ასევე, ეწინააღმდეგებიან კიბერდანაშაულის ფართო გაგებას და ამტკიცებენ, რომ ისეთი ქმედებები, როგორიცაა ბავშვთა პორნოგრაფიის გავრცელება ან რასისტული შეურაცხყოფა სოციალურ ქსელში, მხოლოდ იმიტომ არ უნდა ჩაითვალოს კიბერდანაშაულად, რომ მათი ჩადენა კომპიუტერის საშუალებით მოხდა.[31] ამავე პოზიციით, კიბერდანაშაულში მხოლოდ ის ქმედებები უნდა იგულისხმებოდეს, რომელთა მიზანი კომპიუტერული სისტემისა და მონაცემის ხელყოფაა.[32]

კიბერდანაშაულის განმარტების სირთულე მჭიდროდ უკავშირდება „კიბერსივრცის“ ცნების განუსაზღვრელობას. ერთი მიდგომით, კიბერდანაშაულად მიიჩნევა ყველა დანაშაული, რომელიც კიბერსივრცეშია ჩადენილი.[33] ანალოგიურად, კიბერდანაშაული განიმარტება როგორც დისტანციურად, კომპიუტერული ტექნოლოგიებით შექმნილ სივრცეში განხორციელებული დანაშაული.[34] ამ მიდგომის თანახმად, კიბერსივრცე დანაშაულის განხორციელების აუცილებელი სფეროა და ნებისმიერი ქმედება, რომელიც ამ სივრცეში ხდება, კიბერდანაშაულად უნდა ჩაითვალოს, მიუხედავად მისი ხერხისა და მეთოდისა.[35] ამ მოსაზრების მხარდამჭერები მიიჩნევენ, რომ კიბერდანაშაულის არსის განსაზღვრა სწორედ „კიბერსივრცის“ შინაარსის განმარტების კვალდაკვალ უნდა მოხდეს, რადგან კომპიუტერული

28 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 94-95.
29 იქვე., გვ. 94-95.
30 იქვე., გვ. 94-95.
31 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 18.
32 იქვე., გვ. 19.
33 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 96.
34 იქვე., გვ. 96-97.
35 იქვე., გვ. 97.

სისტემები, მონაცემები და საინფორმაციო ტექნოლოგიები კიბერსივრცის მატერიალურ შემადგენელ ნაწილებს წარმოადგენენ.[36] თუმცა, პრობლემა იმაშია, რომ თავად „კიბერუსაფრთხოებას“, რომლის ნაწილიც არის კიბერდანაშაული, არ გააჩნია ერთიანი, ყველასთვის მისაღები დეფინიცია.[37] ამ სფეროს სიფართოვის გამო, სხვადასხვა სპეციალისტი განსხვავებულ პასუხს იძლევა და ეს იმას არ ნიშნავს, რომ რომელიმე მათგანი ცდება.[38]

განსხვავებული შეხედულებების მიუხედავად, ავტორთა ნაწილი ცდილობს, ჩამოაყალიბოს კიბერდანაშაულის შედარებით სრულყოფილი განმარტება, რომელიც მის სპეციფიკურ ნიშნებს გაითვალისწინებს. ერთ-ერთი სრულყოფილი განმარტებით, „კიბერდანაშაული წარმოადგენს დანაშაულთა ერთობლიობას, ჩადენილს კიბერსივრცეში, კომპიუტერული სისტემებისა თუ კომპიუტერული ქსელების მეშვეობით... ისევე როგორც კომპიუტერული სისტემების, ქსელებისა და მონაცემების წინააღმდეგ მიმართული ქმედებები“.[39] ეს დეფინიცია ორივე ძირითად ასპექტს აერთიანებს: დანაშაულს, რომელიც კიბერსივრცეში ხდება და დანაშაულს, რომელიც კიბერსივრცის კომპონენტების წინააღმდეგაა მიმართული. დოქტრინაში გამოთქმული მოსაზრებების შეჯამებით, მკვლევრები მაინც გამოყოფენ კიბერდანაშაულის ისეთ დამახასიათებელ ნიშნებს, როგორიცაა ვირტუალური სივრცე, დისტანციურობა, უკიდურესი ლატენტურობა, ტრანსნაციონალური ხასიათი და უნივერსალობა.[40] ეს ნიშან-თვისებები, მართალია, არ არის ამომწურავი, მაგრამ კიბერდანაშაულს სოციალურად საშიში ქმედების სპეციფიკურ სახედ წარმოაჩენს.[41]

კიბერდანაშაულის დეფინიციის ირგვლივ არსებული გაურკვევლობა პირდაპირ აისახება სამართალგამოყენების პრაქტიკაზე და ქმნის ნორმათა კონკურენციის პრობლემებს. როდესაც კანონმდებლობა ცალკეულ შემადგენლობებად აყალიბებს ტრადიციული დანაშაულების კიბერანალოგებს (მაგალითად, კიბერთაღლითობა, კიბერტერორიზმი, კიბერმუქარა), ფაქტობრივად, ხდება ერთი და იმავე ქმედების დუბლირება.[42] ეს ართულებს ქმედების სწორ კვალიფიკაციას, განსაკუთრებით საგამოძიებო პრაქტიკაში, და

36 იქვე., გვ. 96-97.
37 იქვე., გვ. 90.
38 იქვე., გვ. 90.
39 იქვე., გვ. 96.
40 იქვე., გვ. 97.
41 იქვე., გვ. 97-98.
42 იქვე., გვ. 98-99.

ხშირად იწვევს ქმედების არასწორ კვალიფიკაციას დანაშაულთა ერთობლიობით, მაშინ როდესაც საქმე ერთ უმართლობას ეხება.[43] მაგალითად, თბილისის საქალაქო სასამართლოს ერთ-ერთ განაჩენში, ბრალდებულებს ბრალი ედებათ საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერული პროგრამის უნებართვო დამზადება), 285-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა), 158-ე (კომპიუტერული მონაცემების უნებართვო გამოყენება) და ამავდროულად 177-ე (ქურდობა) მუხლებით.[44] ეს საქმე ნათლად აჩვენებს, თუ როგორ ხდება კიბერელემენტების შემცველი ქმედებების კვალიფიკაცია როგორც სპეციალური, ისე ტრადიციული დანაშაულის მუხლებით, რაც დეფინიციის არარსებობით გამოწვეული სისტემური პრობლემის პრაქტიკული გამოვლინებაა.

კანონმდებლობის ანალიზი აჩვენებს, რომ პრობლემას არა მხოლოდ დეფინიციის არარსებობა, არამედ კრიმინალიზებული ქმედებების კოდექსში უსისტემო განლაგებაც ქმნის. მაგალითად, ჩნდება ლეგიტიმური კითხვა: თუ კიბერტერორიზმი ან პირადი ინფორმაციის კომპიუტერული ტექნოლოგიებით გავრცელება კიბერდანაშაულია, რატომ არ ხდება მათი გაერთიანება კიბერდანაშაულთა ერთ სამართლებრივ სისტემაში, ანუ სსკ-ის XXXV თავში?.[45] ეს უსისტემობა შეიძლება აიხსნას საკანონმდებლო ტექნიკის ნიუანსებით, მაგრამ რეალური პრობლემა გაცილებით არსებითია და სამართალგამოყენების სირთულეებში ვლინდება.[46] საერთაშორისო დონეზეც კი, მაგალითად, ბუდაპეშტის კონვენცია „კიბერდანაშაულის შესახებ“ აქცენტს აკეთებს კომპიუტერულ სისტემებსა და მონაცემებზე მიმართულ ქმედებებზე, რაც ბევრი ავტორის აზრით, არასრულყოფილი მიდგომაა და ვერ ფარავს კიბერდანაშაულის მთელ სპექტრს.[47] გაეროს ნარკოტიკებისა და დანაშაულის ოფისის კვლევაც ადასტურებს, რომ საერთაშორისო სამართლებრივი ინსტრუმენტების უმრავლესობა თავს არიდებს კიბერდანაშაულის ზუსტი დეფინიციის ჩამოყალიბებას და ამის ნაცვლად, ამჯობინებს იმ კონკრეტული ქმედებების ჩამონათვალის განსაზღვრას, რომლებიც კრიმინალიზაციას

43 იქვე., გვ. 92.
44 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, 2-3.
45 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 91-92.
46 იქვე., გვ. 92.
47 იქვე., გვ. 93-94.

ექვემდებარება.[48] ეს მიდგომა, მართალია, პრაგმატულია, მაგრამ ვერ წყვეტს ცნების ზოგადთეორიულ პრობლემას და ხელს უწყობს ფრაგმენტული და უსისტემო საკანონმდებლო რეგულაციების ჩამოყალიბებას.

აღსანიშნავია ისიც, რომ კიბერდანაშაულის ფენომენი სტატიკური არ არის. ის მუდმივად ვითარდება ტექნოლოგიურ პროგრესთან ერთად, რაც კიდევ უფრო ართულებს მისი ამომწურავი დეფინიციის შექმნას.[49] კიბერდანაშაულის დინამიური ბუნება, ანონიმურობა და ტრანსსასაზღვრო ხასიათი მოითხოვს არა მხოლოდ სამართლებრივ, არამედ მულტიდისციპლინურ მიდგომას კვლევის პროცესში.[50] კიბერდანაშაულის ცნების დაკავშირება მხოლოდ კონკრეტული ტექნოლოგიების გამოყენებასთან ან არსებულ კანონმდებლობასთან ზღუდავს ფენომენის სრულყოფილად გააზრების შესაძლებლობას და არ იძლევა საშუალებას, გავითვალისწინოთ მომავალში წარმოშობილი დანაშაულის ახალი ფორმები.[51] შესაძლოა, მომავალში უფრო ეფექტური იყოს კლასიფიკაცია, რომელიც დაეფუძნება არა ტექნოლოგიას, არამედ დამნაშავის მოტივაციასა და განზრახვას.[52] ადამიანის უფლებათა ევროპული სასამართლოც თავის პრაქტიკაში აღიარებს ონლაინ ძალადობას, როგორც პირადი ცხოვრების ხელყოფის სერიოზულ ფორმას, რომელიც სახელმწიფოს მხრიდან სისხლისსამართლებრივი რეაგირების ვალდებულებას წარმოშობს. მაგალითად, ერთ-ერთ საქმეში ევროპულმა სასამართლომ დაადგინა, რომ ინტიმური ფოტოების გამოქვეყნება და GPS-ით თვალთვალი იმდენად სერიოზული ქმედებები იყო, რომ სამოქალაქო-სამართლებრივი დაცვის მექანიზმები არასაკმარისი იქნებოდა და სახელმწიფოს პოზიტიური ვალდებულება ჰქონდა, ეფექტიანი სისხლისსამართლებრივი დაცვა უზრუნველეყო.[53] ეს ხაზს უსვამს, რომ დეფინიციის პრობლემის მიუხედავად, პრაქტიკა მაინც ითხოვს კიბერსივრცეში ჩადენილი ქმედებების სამართლებრივ შეფასებასა და მათგან დაცვას.

საბოლოოდ, კიბერდანაშაულის დეფინიციის საკითხი კვლავ ღიად რჩება. სამეცნიერო ლიტერატურისა და საერთაშორისო დოკუმენტების ანალიზი

48 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, pp. 42.
49 Haj-Ahmed, M. H. Research in Cybercrime: Why to not use the Black-letter Approach?. International Journal of Law Management & Humanities. 2026, 9, 2, pp. 3089.
50 იქვე.
51 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 396.
52 იქვე.
53 CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024, par. 23.

გვიჩვენებს, რომ ტერმინი უფრო აღწერით, კრებით ხასიათს ატარებს, ვიდრე მკაცრ სამართლებრივ კატეგორიას წარმოადგენს.[54] მიუხედავად იმისა, რომ უამრავი მცდელობა იყო ერთიანი ცნების ჩამოყალიბებისა, ვერც ერთმა მათგანმა ვერ მოიპოვა საყოველთაო აღიარება, რაც ამ ფენომენის სირთულითა და მუდმივი ცვალებადობით აიხსნება.[55] ეს ვითარება საგრძნობ პრობლემებს უქმნის როგორც კანონმდებელს, რომელიც ცდილობს ადეკვატური რეგულაციების შექმნას, ისე სამართალგამომყენებელს, რომელსაც კონკრეტული ქმედების კვალიფიკაცია ევალება. როგორც ჩანს, უახლოეს მომავალშიც კიბერდანაშაულის მკაფიო კონცეპტუალიზაცია კვლავ გამოწვევად დარჩება და დისკუსია ვიწრო და ფართო გაგებებს, ასევე ტექნოლოგიურ და მოტივაციურ მიდგომებს შორის, კვლავ გაგრძელდება.[56]

1.2. კიბერდანაშაულის სახეები და კლასიფიკაცია

კიბერდანაშაულის ერთიანი, საყოველთაოდ მიღებული დეფინიციის არარსებობა მის კლასიფიკაციას საგრძნობლად ართულებს.[57] ეს ფენომენი იმდენად მრავალფეროვან და დინამიურ ქმედებებს მოიცავს, რომ მათი ერთ სისტემაში მოქცევა რთულია. თავდაპირველად, როცა ეს სფერო ახალ ფენომენს წარმოადგენდა, დომინირებდა ტერმინი „კომპიუტერული დანაშაული“, თუმცა დაახლოებით 2000 წლიდან მას თანდათან ჩაენაცვლა უფრო ფართო შინაარსის „კიბერდანაშაული“.[58] მიუხედავად ტერმინოლოგიური დებატებისა, პრაქტიკაში შემუშავდა კლასიფიკაციის რამდენიმე მიდგომა, რომელიც ამ ფენომენის სტრუქტურირებას ისახავს მიზნად.

ერთ-ერთი გავრცელებული კლასიფიკაციით, დანაშაულები სამ ძირითად კატეგორიად იყოფა: დანაშაული ინდივიდების, საკუთრებისა და მთავრობის

54 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, pp. 42.

55 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 17-20.

56 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 396.

57 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 3.

58 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., and Aiken, M. P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences. 2022, 2, 2, pp. 2.

წინააღმდეგ.[59] ეს მიდგომა კიბერდანაშაულს ტრადიციული კრიმინოლოგიური კატეგორიების ჭრილში განიხილავს. მაგალითად, ინდივიდების წინააღმდეგ მიმართულ ქმედებებში ერთიანდება კიბერგადაკიდება და პორნოგრაფიის გავრცელება, საკუთრების წინააღმდეგ ჩადენილ დანაშაულებში - საბანკო დეტალების მოპარვა და თაღლითობა, ხოლო მთავრობის წინააღმდეგ მიმართული ქმედებები კი კიბერტერორიზმად კვალიფიცირდება.[60] უფრო დეტალურია უოლის ტიპოლოგია, რომელიც კიბერდანაშაულს ოთხ ჯგუფად ყოფს: კიბერშეღწევა (ჰაკინგი), კიბერთაღლითობა და ქურდობა (საკრედიტო ბარათების მონაცემების მოპარვა), კიბერპორნოგრაფია და კიბერძალადობა (სიძულვილის ენა და კიბერგადაკიდება).[61] აღნიშნული კლასიფიკაცია კიბერდანაშაულებრივი ქმედებების არსებულ სამართლებრივ კატეგორიებთან დაკავშირებაში გვეხმარება, თუმცა ის სრულად ვერ ასახავს იმ თვისებრივად ახალ ნიშნებს, რომლებიც ამ დანაშაულებს ახასიათებს.[62]

საერთაშორისო ორგანიზაციებიც ცდილობენ კიბერდანაშაულის სისტემატიზაციას. მაგალითად, ევროკომისია მას სამ ფართო ჯგუფად ჰყოფს: დანაშაულები, რომლებიც სპეციფიკურია ინტერნეტისთვის (ფიშინგი და საინფორმაციო სისტემებზე თავდასხმა); ონლაინ თაღლითობა და დოკუმენტების გაყალბება (მათ შორის, იდენტობის ქურდობა); და არალეგალური ონლაინ კონტენტი (ბავშვთა პორნოგრაფია და რასობრივი სიძულვილის გაღვივება).[63] გაეროს ნარკოტიკებისა და დანაშაულის ოფისის (UNODC) კვლევა კიბერდანაშაულებს კიდევ უფრო დეტალურად აკლასიფიცირებს და მოიცავს ისეთ ქმედებებს, როგორიცაა: კომპიუტერულ მონაცემებსა და სისტემებზე უკანონო წვდომა და ჩარევა, მავნე მოწყობილობების ბოროტად გამოყენება, კომპიუტერთან დაკავშირებული თაღლითობა, იდენტობის ქურდობა, საავტორო უფლებების დარღვევა, სპამის გაგზავნა, რასიზმისა და ქსენოფობიის შემცველი მასალების გავრცელება, ბავშვთა პორნოგრაფიის დამზადება-გავრცელება,

59 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, pp. 22.
60 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, pp. 23.
61 Marion, N. E., Twede, J. Introduction. ABC-CLIO. 2020, pp. 1-2; Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, p. 22.
62 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, pp. 22.
63 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, pp. 23.

ბავშვთა დაყოლიება (grooming) და ტერორიზმის მხარდაჭერასთან დაკავშირებული ქმედებები.[64]

კლასიფიკაციის მცდელობების მიუხედავად, კიბერდანაშაულის სრულყოფილი სურათის შესაქმნელად მისი კონკრეტული სახეობების ანალიზია საჭირო. ერთ-ერთი ყველაზე ცნობილი ქმედებაა ჰაკინგი, რაც სხვის კომპიუტერულ სისტემაში უნებართვო შეღწევას გულისხმობს.[65] ჰაკერები სხვადასხვა მოტივით შეიძლება მოქმედებდნენ. „თეთრი ქუდის“ ჰაკერები, ანუ „კეთილი“ ჰაკერები, ხშირად სისტემის სისუსტეების აღმოსაჩენად და უსაფრთხოების გასაუმჯობესებლად მოქმედებენ. მათგან განსხვავებით, „შავი ქუდის“ ჰაკერები პირადი გამორჩენის მიზნით, ფულის ან მონაცემების მოსაპარად მოქმედებენ და ყველაზე საშიშ კატეგორიას წარმოადგენენ. არსებობენ „ნაცრისფერი ქუდის“ ჰაკერებიც, რომლებიც ამ ორ კატეგორიას შორის დგანან და ხან პირადი გამორჩენისთვის მოქმედებენ, ხან კი - არა. ასევე, გამოყოფენ „სკრიპტ-კიდებს“ (Scriptkiddies), რომლებიც ნამდვილი ჰაკერები არ არიან და სხვის მიერ შექმნილ მზა პროგრამებს იყენებენ სისტემაში შესაღწევად.[66] საქართველოს სისხლის სამართლის კოდექსში ჰაკერობა პირდაპირ არ არის მოხსენიებული, თუმცა ეს ქმედება შეიძლება დაკვალიფიცირდეს სსკ-ის 284-ე მუხლით, რომელიც კომპიუტერულ სისტემაში უნებართვო შეღწევას გულისხმობს.[67]

მავნე პროგრამები კიბერდანაშაულის ჩადენის ერთ-ერთ მთავარ ინსტრუმენტს წარმოადგენს. ასეთი პროგრამები მიზნად ისახავს ქსელიდან კომპიუტერის გამოთიშვას ან მომხმარებლის პირად ინფორმაციაზე წვდომის მოპოვებას.[68] ამ კატეგორიაში შედის ტროიანები (Trojans), რომლებიც თავს უწყინარ პროგრამებად (მაგალითად, თამაშად ან სისტემურ განახლებად) ასაღებენ, რათა მომხმარებელმა თავად გადმოწეროს და გააქტიუროს ისინი. ტროიანების სახეებია: „ბექდორ“ (Backdoor) ტროიანები, რომლებიც დამნაშავეს სისტემაზე დისტანციური წვდომის საშუალებას აძლევს; საბანკო

64 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS. 2013, pp. 287-289.

65 მინაშვილი ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 18.

66 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, p. 25.

67 მინაშვილი ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 19.

68 იქვე., გვ. 20.

ტროიანები, რომლებიც ფინანსური ინფორმაციის მოსაპარად არის შექმნილი (მაგალითად, ცნობილი Zeus-ის ვირუსი); და გამოსასყიდი პროგრამები (Ransomware), რომლებიც შიფრავს ფაილებს და მათ აღსადგენად გამოსასყიდს ითხოვს.[69] თბილისის საქალაქო სასამართლოს ერთ-ერთ გახმაურებულ საქმეში, ორგანიზებული ჯგუფი იყენებდა „Gozi“ ვირუსს, რომელიც ჰიბრიდული მავნე კოდი იყო და ამერიკული კომპანიების საბანკო ანგარიშებიდან თანხების მოპარვას ემსახურებოდა. დამნაშავეები ვირუსის დასაშიფრად ე.წ. „კრიპტერებს“, ხოლო გასავრცელებლად „სპამერებს“ იყენებდნენ.[70]

ფიშინგი (Phishing) და მასთან დაკავშირებული თაღლითობები კიბერდანაშაულის ყველაზე გავრცელებული ფორმაა. 2022 წელს აშშ-ის ინტერნეტ დანაშაულის საჩივრების ცენტრს (IC3) ყველაზე მეტმა, დაახლოებით 300,497 ადამიანმა სწორედ ფიშინგის შესახებ აცნობა.[71] ფიშინგის დროს დამნაშავე მსხვერპლს უგზავნის ელექტრონულ წერილს, რომელიც თითქოს ლეგიტიმური ორგანიზაციისგან, მაგალითად ბანკისგან, არის გამოგზავნილი. ასეთი წერილი ხშირად კომპანიის ლოგოსა და ოფიციალურ სტილს იყენებს, რათა დამაჯერებლად გამოიყურებოდეს და მსხვერპლს სთხოვს, განაახლოს ანგარიშის პაროლი ან სხვა პირადი მონაცემები.[72] სწორედ ამ მეთოდს იყენებდა ზემოხსენებული ქართული დანაშაულებრივი ჯგუფი, რომელიც ამერიკულ კომპანიებს უგზავნიდა ვირუსულ ლინკებს, რომლებიც თითქოს ბანკისგან იყო. როდესაც კომპანიის თანამშრომელი ხსნიდა წერილს, მისი კომპიუტერი ინფიცირდებოდა და დამნაშავეები ეუფლებოდნენ ინტერნეტ-ბანკის მონაცემებს.[73] ამ სქემით ჯგუფმა ჯამში 1,260,521 აშშ დოლარის მითვისება სცადა, საიდანაც 316,955 დოლარს რეალურად დაეუფლა.[74] მოპარული თანხის განაღდება ე.წ. „დროპერების“ მეშვეობით ხდებოდა, ხოლო ჯგუფის წევრებს შორის თანხა კრიპტოვალუტით, კერძოდ ბიტკოინებით, ნაწილდებოდა.[75]

---

69 Chapter 1:- Introduction to Cyber Crime and Cyber Security. n.d., p. 24.

70 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 3-4.

71 Cernomoreț, S., Nastas, A. Comparative Analysis of Cybercrime in the Criminal Law System. 2020, p. 62.

72 Marion, N. E., Twede, J. Introduction. ABC-CLIO. 2020, p. 2.

73 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 5-6.

74 იქვე., გვ. 8.

75 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 4, 10.

სერვისზე უარის შეტევები (DoS/DDoS) მიზნად ისახავს, კონკრეტული სერვისი ან ვებგვერდი მომხმარებლებისთვის მიუწვდომელი გახადოს. DoS (Denial-of-Service) შეტევის დროს ერთი წყაროდან ხდება სერვერის გადატვირთვა არალეგიტიმური მოთხოვნების დიდი რაოდენობით. DDoS (Distributed Denial-of-Service) შეტევა კი უფრო რთულია, რადგან შეტევა მრავალი, ხშირად ათასობით, დავირუსებული კომპიუტერიდან (ე.წ. ბოტნეტიდან) ერთდროულად ხორციელდება, რაც მის აღმოჩენასა და შეჩერებას ძალიან ართულებს.[76] ისტორიულად, ამ ტიპის შეტევებისთვის გამოიყენებოდა ისეთი პროგრამები, როგორიცაა 2000-იანი წლების დასაწყისში გავრცელებული Trinoo, TFN (Tribe Flood Network) და Stacheldraht („ეკლიანი მავთული“ გერმანულად), რომლებიც თავდამსხმელს საშუალებას აძლევდა, კოორდინირებულად ემართა ათასობით დაპყრობილი კომპიუტერი (ე.წ. დემონი) და განეხორციელებინა მასშტაბური შეტევა.[77] ასეთი შეტევები ხშირად გამოიყენება როგორც „ელექტრონული პროტესტის“ ფორმა, რომელიც მიზნად ისახავს ციფრული სივრცის ბლოკირებას, ქუჩის აქციების ანალოგიურად.[78]

იდენტობის ქურდობა კიბერდანაშაულის ერთ-ერთი ყველაზე მზარდი პრობლემაა. ამ დროს დამნაშავე ეუფლება მსხვერპლის პირად მონაცემებს - საბანკო ანგარიშის, საკრედიტო ბარათის, დაზღვევისა და სხვა ინფორმაციას, და შემდეგ ამ ინფორმაციას მისი ნების გარეშე იყენებს ფულადი ტრანზაქციებისა და კრედიტების ასაღებად.[79] ამ ქმედებამ შეიძლება გამოიწვიოს როგორც მატერიალური ზიანი, ასევე გააფუჭოს დაზარალებულის საკრედიტო ისტორია. საქართველოს სისხლის სამართლის კოდექსში იდენტობის ქურდობის ცალკე მუხლი არ არსებობს, ამიტომ ასეთი ქმედების კვალიფიკაცია ორი მუხლის ერთობლიობით ხდება: სსკ-ის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა) მუხლებით.[80]

კიბერდანაშაულის სხვა გავრცელებულ სახეებს მიეკუთვნება კიბერგადაკიდება (Cyberstalking), რომლის დროსაც დამნაშავე ინტერნეტის

76 Chapter 1:- Introduction to Cyber Crime and Cyber Security. n.d., pp. 26-27.

77 Sinrod, E. J., Reilly, W. P. CYBER-CRIMES: A PRACTICAL APPROACH TO THE APPLICATION OF FEDERAL COMPUTER CRIME LAWS. SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL, 2000, 16 (2), pp. 18-19.

78 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, p. 37.

79 მინაშვილი ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 19-20.

80 იქვე., გვ. 20.

საშუალებით უთვალთვალებს, ავიწროებს და აშანტაჟებს მსხვერპლს, რაც მასზე მძიმე ფსიქოლოგიურ გავლენას ახდენს. ეს ქმედება განსაკუთრებით საყურადღებო გახდა მას შემდეგ, რაც მკვეთრად გაიზარდა ინტერნეტ-შეურაცხყოფის საფუძველზე თვითმკვლელობის შემთხვევები.[81] ასევე, სერიოზულ პრობლემას წარმოადგენს ბავშვთა ექსპლუატაცია, რაშიც შედის ბავშვთა პორნოგრაფიის დამზადება-გავრცელება და არასრულწლოვნების დაყოლიება სექსუალურ ქმედებებზე სოციალური ქსელების მეშვეობით.[82] აგრეთვე აღსანიშნავია საავტორო უფლებების დარღვევა, ანუ „კიბერქურდობა“, რაც ინტერნეტიდან პირატული მასალის (ფილმები, მუსიკა, პროგრამები) გადმოწერას გულისხმობს.[83]

კიბერდანაშაულის სახეების მრავალფეროვნება და მათი ტრადიციული დანაშაულებისგან განსხვავებული სტრუქტურა სერიოზულ პრობლემებს ქმნის საკანონმდებლო რეგულირებისთვის. კიბერსივრცე მუდმივად გვთავაზობს სოციალურად საშიში ქმედებების ახალ ფორმებს, რაზეც კანონმდებელი იძულებულია, დაუყოვნებლივ მოახდინოს რეაგირება და შეიმუშაოს დანაშაულის ახალი შემადგენლობები.[84] ამ ტენდენციამ შეიძლება მიგვიყვანოს იქამდე, რომ ტრადიციული დანაშაულების (ქურდობა, თაღლითობა, ტერორიზმი) პარალელურად გაჩნდეს მათი კიბერ-ანალოგები (კიბერქურდობა, კიბერთაღლითობა, კიბერტერორიზმი), რაც უკვე ბევრი ქვეყნის კანონმდებლობაში გვხვდება.[85] ასეთი მიდგომა, ერთი მხრივ, უზომოდ ზრდის სისხლის სამართლის კოდექსის მოცულობას და ართულებს სამართალგამოყენებას, მეორე მხრივ კი, ქმნის ნორმათა კონკურენციის პრობლემას, როდესაც რთული ხდება ზოგადი და სპეციალური ნორმების გამიჯვნა.[86]

სწორედ ამ პრობლემის გამო, ზოგიერთი მოსაზრებით, უფრო მიზანშეწონილია „კიბერდანაშაულის“ ელემენტების გათვალისწინება უკვე არსებულ, ტრადიციულ დანაშაულთა შემადგენლობებში, როგორც დამამძიმებელი გარემოების.[87] მაგალითად, იმის ნაცვლად, რომ შეიქმნას

---

81 იქვე., გვ. 20.
82 იქვე., გვ. 20-21.
83 იქვე., გვ. 19.
84 ამაშუკელი გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 28.
85 იქვე., გვ. 28-29.
86 იქვე., გვ. 36.
87 იქვე., გვ. 36.

„კიბერტერორიზმის“ ცალკე მუხლი, კომპიუტერული ტექნოლოგიების გამოყენება შეიძლება ტერორიზმის მუხლის მაკვალიფიცირებელ ნიშნად იქცეს. ასეთი მიდგომა თავიდან აგვარიდებდა ნორმათა კონკურენციას და გაამარტივებდა როგორც კვალიფიკაციის პროცესს, ისე სასამართლო პრაქტიკის ერთგვაროვნების დამკვიდრებას.[88] ეს პრობლემა ქართულ რეალობაშიც ნათლად ჩანს, რადგან სისხლის სამართლის კოდექსი არ იცნობს ტერმინს „ციფრული დანაშაული“ და როდესაც ასეთი ქმედება ხდება, მისი კვალიფიკაცია სხვადასხვა, ხშირად რამდენიმე მუხლის ერთობლიობით ხდება, რაც იმაზე მიუთითებს, რომ კანონმდებლობა ფეხს ვერ უბამს კიბერდანაშაულის განვითარებას.[89]

ამრიგად, კიბერდანაშაულის კლასიფიკაცია რთული საკითხია. არსებული ტიპოლოგიები, რომლებიც დანაშაულს ობიექტის (ინდივიდი, საკუთრება, სახელმწიფო) ან ჩადენის ხერხის (შეღწევა, თაღლითობა, ძალადობა) მიხედვით აჯგუფებს, ამ ფენომენის ზოგადი სურათის აღქმაში გვეხმარება, თუმცა მის ყველა ასპექტს ვერ ფარავს. კიბერდანაშაულის კონკრეტული ფორმები, როგორიცაა ფიშინგი, DDoS შეტევები თუ იდენტობის ქურდობა, თავისი სტრუქტურითა და მასშტაბებით უნიკალურ გამოწვევებს უქმნის სამართალდამცავ ორგანოებსა და კანონმდებელს, რის გამოც მათი კლასიფიკაციისა და სამართლებრივი მოწესრიგების საკითხი კვლავაც აქტუალურია.

1.3. საერთაშორისო და ეროვნული სამართლებრივი ჩარჩო

კიბერდანაშაულთან ბრძოლის ეფექტიანობა დიდწილად საერთაშორისო თანამშრომლობასა და ერთიანი სამართლებრივი სტანდარტების არსებობაზეა დამოკიდებული. ვინაიდან კიბერდანაშაული, თავისი ბუნებით, ხშირად ტრანსნაციონალურია და ფიზიკურ საზღვრებს სცდება, ცალკეული სახელმწიფოების მიერ იზოლირებულად გატარებული ღონისძიებები არასაკმარისია.[90] ამიტომ საერთაშორისო საზოგადოებამ ერთიანი მიდგომების ჩამოყალიბებაზე დაიწყო მუშაობა, რის შედეგადაც არაერთი საერთაშორისო დოკუმენტი შეიქმნა. ამ პროცესში ცენტრალური ადგილი ევროსაბჭოს 2001 წლის ბუდაპეშტის კონვენციას უკავია, რომელიც კიბერდანაშაულთან ბრძოლას საფუძვლად დაედო.

---

88 იქვე., გვ. 36.

89 მინაშვილი ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 18.

90 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 28.

კიბერდანაშაულის წინააღმდეგ ბრძოლაში ერთ-ერთ უმთავრეს დოკუმენტს ევროსაბჭოს 2001 წლის 23 ნოემბრის კონვენცია „კიბერდანაშაულის შესახებ“ წარმოადგენს, რომელიც ბუდაპეშტში შემუშავდა.[91] ეს იყო მსოფლიო მასშტაბით პირველი სერიოზული მცდელობა, შექმნილიყო ერთიანი სტრატეგია კიბერუსაფრთხოების დასაცავად და სახელმწიფოთა შორის თანამშრომლობის გასაძლიერებლად. კონვენციას, ევროპის ქვეყნების გარდა, ხელი მოაწერეს ისეთმა სახელმწიფოებმა, როგორებიცაა კანადა, იაპონია, სამხრეთ აფრიკა და აშშ, რაც მის გლობალურ მასშტაბზე მიუთითებს.[92] აღსანიშნავია, რომ 2008 წელს რუსეთის ფედერაციამ კონვენციის ხელმოწერაზე უარი განაცხადა, მაშინ როდესაც იმავე წელს მას აზერბაიჯანი შეუერთდა.[93] ამ დოკუმენტის მთავარი ღირსება მის სისტემურ მიდგომაშია, რაც ერთდროულად რამდენიმე მიმართულებას მოიცავს.[94]

კონვენცია, პირველ რიგში, ხელმომწერ სახელმწიფოებს ავალდებულებს, მოახდინონ სისხლის სამართლის კანონმდებლობის ჰარმონიზაცია და დასჯადად გამოაცხადონ დანაშაულთა ოთხი ძირითადი კატეგორია. ესენია: დანაშაულები კომპიუტერული მონაცემებისა და სისტემების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის წინააღმდეგ (მაგალითად, უნებართვო შეღწევა); კომპიუტერთან დაკავშირებული თაღლითობა და ყალბი დოკუმენტების დამზადება; შინაარსთან დაკავშირებული დანაშაულები, როგორიცაა ბავშვთა პორნოგრაფიის გავრცელება; და საავტორო და მომიჯნავე უფლებების დარღვევა.[95] ამასთან, კონვენცია განსაზღვრავს ისეთ ტერმინებს, როგორებიცაა „კომპიუტერული სისტემა“, „მომსახურების მიმწოდებელი“ (service provider) და „ტრაფიკის მონაცემები“ (traffic data), რაც ერთიანი სამართლებრივი ენის ჩამოყალიბებას ემსახურება.[96] მეორე

---

91 ზაქაშვილი უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14.

92 ზაქაშვილი უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14; Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, p. 28.

93 ზაქაშვილი უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14.

94 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, p. 28.

95 Council of Europe. Explanatory Report to the Convention on Cybercrime. Council of Europe. 2001, pp. 8-9.

96 Council of Europe. 2001. Explanatory Report to the Convention on Cybercrime. Council of Europe. p. 7-8.

მიმართულება საპროცესო სამართლის ნორმების დახვეწაა, რაც საგამოძიებო ორგანოებს აძლევს ისეთ ინსტრუმენტებს, როგორიცაა შენახული კომპიუტერული მონაცემების სასწრაფოდ შენარჩუნება (expedited preservation), მონაცემთა გამოთხოვა (production order) და კომპიუტერული სისტემების ჩხრეკა და ამოღება.[97]

მესამე, ასევე არსებითი კომპონენტი, საერთაშორისო თანამშრომლობის ეფექტიანი სისტემის შექმნაა. კონვენციის 35-ე მუხლი წევრ სახელმწიფოებს ავალდებულებს, შექმნან 24/7 რეჟიმში მომუშავე საკონტაქტო პუნქტები (ე.წ. „ცხელი ხაზი“), რათა კიბერდანაშაულის გამოძიების პროცესში ერთმანეთს სწრაფი დახმარება აღმოუჩინონ, იქნება ეს ტექნიკური რჩევის მიცემა, მტკიცებულებების მოპოვება თუ დამნაშავის ადგილსამყოფლის დადგენა.[98] ეს ქსელი გადამწყვეტია ტრანსნაციონალური დანაშაულების ოპერატიულად გამოძიებისთვის. ამავდროულად, კონვენცია ითვალისწინებს ადამიანის უფლებათა დაცვის გარანტიებს. კერძოდ, მე-15 მუხლი მოითხოვს, რომ საგამოძიებო უფლებამოსილებების გამოყენება პროპორციულობის პრინციპს ეფუძნებოდეს და ექვემდებარებოდეს სასამართლო ან სხვა დამოუკიდებელ ზედამხედველობას.[99]

მიუხედავად ბუდაპეშტის კონვენციის მნიშვნელობისა, მისი რატიფიცირების პროცესი ევროპის ბევრ ქვეყანაში დროში გაიწელა. ამ გარემოებამ, ნაწილობრივ, განაპირობა ევროკავშირის საბჭოს 2005 წლის 24 თებერვლის №2005/222 ჩარჩო გადაწყვეტილების მიღება „საინფორმაციო სისტემებზე თავდასხმის წინააღმდეგ“.[100] ამ დოკუმენტის მიზანი წევრი ქვეყნების სისხლისსამართლებრივი ნორმების დაახლოება და მართლმსაჯულების ორგანოებს შორის თანამშრომლობის გაუმჯობესება იყო.[101] ჩარჩო

---

97 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, p. 28; Council of Europe. 2001. Explanatory Report to the Convention on Cybercrime. Council of Europe. p. 30-31.

98 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 35; ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14.

99 Council of Europe. 2001. Explanatory Report to the Convention on Cybercrime. Council of Europe. p. 30.

100 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14-15.

101 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 35; Guðbrandsdóttir, M. B. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. 2015, p. 19.

გადაწყვეტილება იმეორებდა კონვენციის ძირითად პრინციპებს და ავალდებულებდა წევრ სახელმწიფოებს, კრიმინალიზაცია მოეხდინათ ისეთი ქმედებებისა, როგორიცაა საინფორმაციო სისტემაში უნებართვო შეღწევა (მუხლი 2), სისტემის ფუნქციონირებაში უნებართვო ჩარევა (მუხლი 3) და კომპიუტერული მონაცემების უნებართვო წაშლა ან დაზიანება (მუხლი 4).[102] აღსანიშნავია, რომ გადაწყვეტილებაში გამოყენებულია ტერმინი „საინფორმაციო სისტემა“, რომელიც უფრო ფართო და სრულყოფილად მიიჩნევა, ვიდრე კონვენციის ტერმინი „კომპიუტერული სისტემა“, რადგან ის მონაცემთა ავტომატური დამუშავების გარდა, მათ შენახვას, აღდგენასა და გადაგზავნასაც მოიცავს.[103]

თუმცა, ამ გადაწყვეტილების განხორციელებაც პრობლემური აღმოჩნდა. 2007 წლის 16 მარტისთვის, დაწესებულ ვადაში, ვალდებულებები სრულად მხოლოდ შვედეთმა შეასრულა, ხოლო ისეთი ქვეყნები, როგორიცაა პოლონეთი, ესპანეთი, მალტა და სლოვაკეთი, ანგარიშის წარდგენას 2008 წლის ივლისამდე აგვიანებდნენ.[104] მეტიც, ავსტრიამ, ჩეხეთმა, ლატვიამ და ფინეთმა უნებართვო შეღწევის დასჯადობა დანაშაულებრივი შედეგის (ზიანის) დადგომას დაუკავშირეს, რაც ეწინააღმდეგებოდა გადაწყვეტილების სულისკვეთებას, რომლის მიხედვითაც დანაშაული შეღწევის მომენტიდანვე დამთავრებულად ითვლება.[105] ამ ხარვეზებისა და ახალი გამოწვევების საპასუხოდ, მათ შორის 2007 წელს ესტონეთზე განხორციელებული კიბერშეტევების გამო, 2013 წელს ევროპარლამენტმა და საბჭომ ახალი დირექტივა 2013/40/EU მიიღეს, რომელმაც 2005 წლის ჩარჩო გადაწყვეტილება ჩაანაცვლა.[106] ეს ახალი დირექტივა კიდევ უფრო აფართოებს დასჯადი ქმედებების წრეს და

---

102 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 16.

103 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 16; Guðbrandsdóttir, M. B. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. 2015, p. 19.

104 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 16; Guðbrandsdóttir, M. B. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. 2015, p. 23.

105 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 17.

106 Guðbrandsdóttir, M. B. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. 2015, p. 24; Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, p. 28.

კრიმინალიზებულად აცხადებს კომპიუტერული მონაცემების უკანონო მიყურადებასა (intercepting) და კიბერდანაშაულის ჩასადენად საჭირო ინსტრუმენტების (მაგალითად, მავნე პროგრამების) დამზადებას, გაყიდვასა და გავრცელებას.[107]

საქართველოს სისხლის სამართლის კანონმდებლობა კიბერდანაშაულის მიმართულებით არსებითად განვითარდა, თუმცა ეს პროცესი არათანმიმდევრული იყო. დიდი ხნის განმავლობაში ეს სფერო ქართველი მეცნიერების კვლევის საგანი იშვიათად ხდებოდა, ხოლო საკანონმდებლო რეგულაციები ხშირად სხვა ქვეყნების, კერძოდ, რუსეთის ფედერაციის კანონმდებლობის პირდაპირ გადმოღებას წარმოადგენდა.[108] გარდამტეხი მომენტი 2009-2010 წლებში ევროსაბჭოს ორგანიზებით განხორციელებული „კიბერდანაშაულის პროექტი საქართველოში“ აღმოჩნდა, რომლის შედეგადაც მომზადდა საკანონმდებლო ცვლილებები ბუდაპეშტის კონვენციის მოთხოვნების შესაბამისად. რის შემდეგაც საქართველო კონვენციას შეუერთდა და სისხლის სამართლის კოდექსში კიბერდანაშაულის მარეგულირებელი ახალი ნორმები გაჩნდა.[109]

დღესდღეობით, საქართველოს სისხლის სამართლის კოდექსში კიბერდანაშაულს ეძღვნება XXXV-ე თავი, რომელიც ხუთი შემადგენლობისგან შედგება (284-286² მუხლები).[110] აგრეთვე, კიბერსივრცესთან დაკავშირებული სხვა დანაშაულებრივი ქმედებები კოდექსის სხვა თავებშია გაბნეული. მაგალითად, 157-ე, 158-ე და 159-ე მუხლები, რომლებიც პირადი ცხოვრებისა და კომუნიკაციის საიდუმლოებას ეხება, კიბერდანაშაულებრივ ელემენტებს შეიცავს, ისევე როგორც 324¹ მუხლი (კიბერტერორიზმი).[111] ასეთი სტრუქტურული მოუწესრიგებლობა სამართალგამოყენების პრაქტიკაში სირთულეებს ქმნის, რადგან მსგავსი შინაარსის ნორმები სხვადასხვა თავშია მოქცეული. ეს განსაკუთრებით პრობლემურია ნორმათა კონკურენციის დროს,

---

107 Guðbrandsdóttir, M. B. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. 2015, p. 25.

108 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 129.

109 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 14, 129.

110 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 121.

111 იქვე., გვ. 121-122.

როდესაც ერთი ქმედება შეიძლება რამდენიმე მუხლით დაკვალიფიცირდეს. მაგალითად, ხშირია შემთხვევები, როდესაც კომპიუტერული სისტემიდან თანხის ფარულად დაუფლება ერთდროულად კვალიფიცირდება როგორც ქურდობა (177-ე მუხლი), ასევე კომპიუტერულ სისტემაში უნებართვო შეღწევა (284-ე მუხლი).[112]

ამგვარი მიდგომის თვალსაჩინო მაგალითია თბილისის საქალაქო სასამართლოს 2019 წლის 11 დეკემბრის განაჩენი, სადაც ორგანიზებული ჯგუფი „ფიშინგის“ მეთოდითა და „Gozi“ ვირუსის გამოყენებით იპარავდა ამერიკული კომპანიების საბანკო ანგარიშებიდან თანხებს.[113] დანაშაულებრივ სქემაში ჩართულები იყვნენ როგორც ვირუსის გამავრცელებლები („სპამერები“), ასევე ვირუსის დამშიფრავები („კრიპტერები“) და თანხის განაღდებაზე პასუხისმგებელი პირები („დროპერები“), მათ შორის ბულგარეთისა და უკრაინის მოქალაქეები.[114] სასამართლომ ბრალდებულების ქმედებები ერთობლიობაში დააკვალიფიცირა სსკ-ის რამდენიმე მუხლით: 284-ე (კომპიუტერული პროგრამის უნებართვო დამზადება და გავრცელება), 158-ე (კომპიუტერული მონაცემების უნებართვო შენახვა და გამოყენება), 285-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა დიდი ოდენობით, ჩადენილი ორგანიზებული ჯგუფის მიერ).[115] ეს საქმე ნათლად აჩვენებს, თუ როგორ იწვევს კანონმდებლობის არსებული სტრუქტურა დანაშაულთა ერთობლიობით კვალიფიკაციის აუცილებლობას, რაც დებატებს იწვევს იმაზე, ხომ არ იქნებოდა უფრო სწორი, კომპიუტერული ტექნოლოგიების გამოყენება დამამძიმებელ გარემოებად ჩათვლილიყო და არა დამოუკიდებელ დანაშაულად.[116]

ეროვნული კანონმდებლობის ანალიზისას სხვა პრობლემებიც ვლინდება. მაგალითად, ერთ-ერთი კვლევის თანახმად, გაუგებარია 284-ე მუხლის მე-2 ნაწილში „მნიშვნელოვანი ზიანის“ დამამძიმებელ გარემოებად მითითება, რადგან უნებართვო შეღწევა ფორმალური შემადგენლობის დანაშაულია და მისი

---

112 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 120; მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 21.

113 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, 3-5.

114 იქვე., გვ. 30.

115 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, 2-3, 27.

116 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 120.

დასრულებისთვის შედეგის დადგომა საჭირო არ არის.[117] ასევე, პრობლემურია 285-ე მუხლის ფორმულირება, რომელიც დასჯადად აცხადებს კომპიუტერული პროგრამის დამზადებას „ამ თავით და ამ კოდექსის 158-ე მუხლით“ გათვალისწინებული დანაშაულის ჩადენის მიზნით. კავშირი „და“ ქმნის უცნაურ ვითარებას, თითქოს პირმა ერთდროულად ორივე კატეგორიის დანაშაულის ჩადენა უნდა განიზრახოს, რაც პრაქტიკაში გამოყენებას ართულებს.[118] გარდა ამისა, ქართული კანონმდებლობა არ იცნობს კიბერგადაკიდების (cyberstalking) ცალკე შემადგენლობას, თუმცა ასეთი ქმედება შეიძლება თვითმკვლელობამდე მიყვანის (სსკ-ის 115-ე მუხლი) შემადგენლობით დაკვალიფიცირდეს, თუ ის სისტემატურ დამცირებას მოიცავს.[119]

სხვა ქვეყნების გამოცდილებაც საინტერესოა. მაგალითად, უკრაინის სისხლის სამართლის კოდექსსაც გააჩნია ცალკე თავი კომპიუტერული დანაშაულებისთვის, მაგრამ, საქართველოსგან განსხვავებით, თაღლითობას კომპიუტერული ტექნოლოგიების გამოყენებით განიხილავს, როგორც ამავე დანაშაულის (თაღლითობის) დამამძიმებელ გარემოებას და არა დამოუკიდებელ კიბერდანაშაულად.[120] გერმანიის კანონმდებლობაში კი კიბერდანაშაულები ცალკე თავში თავმოყრილი არ არის და კოდექსის სხვადასხვა ნაწილშია გადანაწილებული, რაც ქართული მოდელისგან ასევე განსხვავდება.[121] ეს მაგალითები აჩვენებს, რომ კიბერდანაშაულთა კრიმინალიზაციისა და სისტემატიზაციის უნივერსალური მოდელი არ არსებობს, თუმცა ბუდაპეშტის კონვენცია ადგენს მინიმალურ სტანდარტს, რომელსაც ეროვნული კანონმდებლობები უნდა შეესაბამებოდეს. ამ კუთხით, მიუხედავად მიღწეული პროგრესისა, საქართველოს კანონმდებლობა ჰარმონიზაციის დასასრულებლად და პრაქტიკული პრობლემების გადასაჭრელად კვლავ საჭიროებს დახვეწას.

ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაც ხაზს უსვამს სახელმწიფოთა პოზიტიურ ვალდებულებას, ეფექტიანად გამოიძიონ ონლაინ

---

117 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 130.

118 იქვე., გვ. 130.

119 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 21.

120 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 85.

121 იქვე., გვ. 83.

სივრცეში ჩადენილი დანაშაულები. საქმეში M.Ș.D. v. ROMANIA, სასამართლომ დაადგინა, რომ ონლაინ შევიწროება, მათ შორის ინტიმური ფოტოების უნებართვოდ გავრცელება („შურისძიების პორნო“), წარმოადგენს პირადი ცხოვრების ხელყოფას (ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლი) და სახელმწიფოსგან სისხლისსამართლებრივ რეაგირებას მოითხოვს.[122] სამოქალაქო-სამართლებრივი დაცვის მექანიზმები ასეთ მძიმე შემთხვევებში არასაკმარისად მიიჩნევა. საქმეში ILAREVA AND OTHERS v. BULGARIA კი გამოიკვეთა ონლაინ სივრცეში ჩადენილი შეურაცხყოფის ავტორის დადგენის სირთულეები და ის საგამოძიებო მოქმედებები, რომლებსაც სასამართლოები მიმართავენ, მაგალითად, ლინგვისტური ექსპერტიზის დანიშვნა.[123] ეს გადაწყვეტილებები ცხადყოფს, რომ ეროვნულმა კანონმდებლობამ დანაშაულის შემადგენლობების განსაზღვრასთან ერთად, ეფექტიანი გამოძიებისთვის საჭირო პროცედურული ინსტრუმენტებიც უნდა უზრუნველყოს.

კიბერდანაშაულთან ბრძოლის სამართლებრივი ჩარჩო, როგორც საერთაშორისო, ისე ეროვნულ დონეზე, დინამიკურ განვითარებას განიცდის. ბუდაპეშტის კონვენცია რჩება ამოსავალ წერტილად, რომელიც სახელმწიფოებს სისხლის სამართლის მატერიალური და საპროცესო ნორმების ჰარმონიზაციის ერთიან მოდელს სთავაზობს. ევროკავშირის დირექტივებმა კი კიდევ უფრო დახვეწა და გააფართოვა ეს ჩარჩო ევროპულ სივრცეში. საქართველომ, ბუდაპეშტის კონვენციასთან მიერთებით, არსებითი ნაბიჯი გადადგა საერთაშორისო სტანდარტებთან დაახლოების გზაზე, თუმცა ანალიზი აჩვენებს, რომ ეროვნულ კანონმდებლობაში კვლავ რჩება არაერთი პრობლემური საკითხი. ესენია: კიბერდანაშაულის შემადგენლობების სტრუქტურული მოუწესრიგებლობა კოდექსში, ტერმინოლოგიური ბუნდოვანება და ნორმათა კონკურენციის შედეგად წარმოქმნილი კვალიფიკაციის სირთულეები. სასამართლო პრაქტიკა აჩვენებს, რომ კანონმდებლობის არსებული სახით გამოყენება ხშირად დანაშაულთა ერთობლიობით რთულ კვალიფიკაციას მოითხოვს, რაც აჩენს კითხვებს სისტემის ეფექტიანობასთან დაკავშირებით. შესაბამისად, ამ ხარვეზების აღმოფხვრა და უფრო თანმიმდევრული, პრაქტიკაზე მორგებული სამართლებრივი ბაზის შექმნა მომავალი რეფორმების მიზანი უნდა გახდეს.

122 CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024, par. 22-24.
123 CASE OF ILAREVA AND OTHERS v. BULGARIA [ECtHR], 2025, par. 16.

თავი II. კიბერდანაშაულის კვალიფიკაციის დოქტრინალური პრობლემები

2.1. ობიექტური და სუბიექტური შემადგენლობის თავისებურებები

კიბერდანაშაულის შემადგენლობის ანალიზისას, ერთ-ერთ მთავარ საკითხს დანაშაულის ობიექტის განსაზღვრა წარმოადგენს. დანაშაულის სწორი კვალიფიკაციისთვის აუცილებელია გვარეობითი, სახეობითი და უშუალო ობიექტების ერთმანეთისგან გამიჯვნა. საქართველოს სისხლის სამართლის კოდექსში კომპიუტერული დანაშაულის თავი მოთავსებულია მეცხრე კარში, სათაურით „დანაშაული საზოგადოებრივი უშიშროებისა და წესრიგის წინააღმდეგ“, რაც ნიშნავს, რომ კანონმდებელმა ამ დანაშაულთა გვარეობით ობიექტად საზოგადოებრივი უშიშროება და წესრიგი განსაზღვრა.[124] სახეობითი ობიექტი უფრო ვიწროა და აერთიანებს საზოგადოებრივ ურთიერთობათა იმ ჯგუფს, რომელიც კომპიუტერული სისტემისა და მონაცემების უსაფრთხო და მართლზომიერ გამოყენებას უზრუნველყოფს.[125] რაც შეეხება უშუალო ობიექტს, მაგალითად, სსკ-ის 284-ე მუხლის (კომპიუტერულ სისტემაში უნებართვო შეღწევა) შემთხვევაში, ეს არის ინფორმაციის კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა, ასევე თავად კომპიუტერული სისტემის დაცულობა.[126]

განსაკუთრებით საინტერესოა კიბერდანაშაულის საგნისა და ჩადენის საშუალების გამიჯვნის საკითხი. ხშირად ისმება კითხვა, თავად კომპიუტერული ტექნიკა დანაშაულის საგანს წარმოადგენს, მის იარაღს თუ არც ერთს. სამართლის დოქტრინაში გამოთქმულია მოსაზრება, რომლის მიხედვითაც დანაშაულებრივი ხელყოფა მიმართულია კომპიუტერში არსებულ სისტემაზე, მონაცემსა თუ პროგრამაზე და არა მის ფიზიკურ ნაწილებზე.[127] შესაბამისად, კომპიუტერი, როგორც ტექნიკური მოწყობილობა, დანაშაულის ობიექტად არ განიხილება. მაგალითად, თუ პირი სხვის კომპიუტერულ სისტემაში უნებართვოდ აღწევს, ამით ზიანი სისტემის უსაფრთხოებას ადგება და არა ფიზიკურად

124 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 24; მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 10.

125 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 24.

126 იქვე., გვ. 25.

127 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. თბილისი: ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 26.

კომპიუტერს, რომელიც არც ცვეთას განიცდის და არც მწყობრიდან გამოდის.[128] კომპიუტერის ეკრანის დამტვრევა ნივთის დაზიანებად დაკვალიფიცირდება და არა ციფრულ დანაშაულად, მიუხედავად იმისა, რომ მოტივი კომპიუტერში შენახული ინფორმაციის განადგურება იყო.[129] ამიტომ აუცილებელია „კომპიუტერული დანაშაულისა“ და „კომპიუტერულ ტექნიკასთან დაკავშირებული დანაშაულების“ გამიჯვნა, სადაც მეორე შემთხვევაში კომპიუტერი მხოლოდ ტექნიკური საშუალებაა ტრადიციული დანაშაულის ჩასადენად, როგორიცაა თაღლითობა ან ყალბი დოკუმენტის დამზადება.[130]

აქედან გამომდინარე, კიბერდანაშაულის საგანია არამატერიალური, კოდების სახით წარმოდგენილი ციფრული ინფორმაცია და არა მატერიალური ნივთი.[131] მართალია, კლასიკური დეფინიციით დანაშაულის საგანი მატერიალური ნივთია, რომელზეც დამნაშავის მოქმედებაა მიმართული, თუმცა ეს განმარტება იმ პერიოდში ჩამოყალიბდა, როცა კიბერდანაშაული ჯერ კიდევ არ არსებობდა.[132] თანამედროვე რეალობაში კი დანაშაულის საგნად როგორც კომპიუტერული სისტემა, ისე კომპიუტერული მონაცემი უნდა მოვიაზროთ.[133] ეს უკანასკნელი მოიცავს ნებისმიერი სახის ინფორმაციას, იქნება ეს ტექსტური, გრაფიკული თუ ბგერითი, რომელიც ციფრული კოდების ერთობლიობას წარმოადგენს.[134] ამერიკელი ექსპერტების აზრითაც, დანაშაულის საგანი შეიძლება იყოს კომპიუტერი ან მასში შენახული ინფორმაცია, თუმცა ისინი არ აკონკრეტებენ, კომპიუტერში მის ტექნიკურ ნაწილს გულისხმობენ თუ სისტემას.[135] მოლდოვის სისხლის სამართლის კანონმდებლობის ანალიზიც

---

128 იქვე., გვ. 26.

129 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. თბილისი: მერიდიანი, 2019, გვ. 13.

130 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. თბილისი: ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 25-26.

131 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. თბილისი: მერიდიანი, 2019, გვ. 11.

132 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. თბილისი: ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 27.

133 იქვე., გვ. 27.

134 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. თბილისი: მერიდიანი, 2019, გვ. 12.

135 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. თბილისი: ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 28.

აჩვენებს, რომ დანაშაულის მატერიალურ თუ არამატერიალურ საგნად კომპიუტერული ინფორმაცია, სისტემა ან ქსელი განიხილება.[136]

კიბერდანაშაულის ობიექტური მხარე უმეტესად მართლსაწინააღმდეგო მოქმედებით ხასიათდება.[137] ასეთ მოქმედებებს განეკუთვნება კიბერტერორიზმი, ჰაკერობა, იდენტიფიკაციის ქურდობა, ვირუსული პროგრამების გავრცელება და სხვა.[138] თბილისის საქალაქო სასამართლოს ერთ-ერთ გახმაურებულ საქმეში[139] ნათლად ჩანს, თუ რა რთული და მრავალეტაპიანი შეიძლება იყოს დანაშაულის ობიექტური მხარე. ბრალდებულები იყენებდნენ ე.წ. „ფიშერულ“ სქემას, რაც გულისხმობდა ვირუსის შექმნას, მის დაშიფვრას „კრიპტერების“ მეშვეობით, შემდეგ „სპამერების“ მიერ ელექტრონული ფოსტით გავრცელებას, კომპიუტერების დაინფიცირებას და საბოლოოდ, საბანკო ანგარიშებიდან თანხების მოპარვას „დროპერების“ დახმარებით.[140] ეს საქმე ცხადყოფს, რომ კიბერდანაშაულის ჩადენის ხერხი და საშუალება კომპიუტერული სისტემაა, ხოლო შედეგი - ციფრულ ინფორმაციაზე ზემოქმედება.[141] თუმცა, ზოგიერთ იურისდიქციაში, მაგალითად მოლდოვაში, ცალკეული კიბერდანაშაულის ჩადენა შესაძლებელია როგორც მოქმედებით, ისე უმოქმედობითაც.[142] აღსანიშნავია ისიც, რომ დანაშაულები შეიძლება იყოს როგორც მატერიალური (როცა დამდგარი შედეგია აუცილებელი), ისე ფორმალური (როცა თავად ქმედებაა დასრულებული დანაშაული).[143]

სუბიექტური მხარის ანალიზისას, კიბერდანაშაულების უმრავლესობა განზრახი ფორმით ხასიათდება. გაეროს ნარკოტიკებისა და დანაშაულის ოფისის კვლევის თანახმად, საერთაშორისო ინსტრუმენტების დიდი ნაწილი მოითხოვს, რომ ქმედება დასჯადი იყოს „განზრახ ჩადენისას“.[144] პრაქტიკაში კი განზრახვის, განსაკუთრებით სუბიექტური ელემენტის, „ცოდნის“ დადგენა, ერთ-

136 Cernomoreț S., Nastas A., Comparative Analysis of Cybercrime in the Criminal Law System. 2020, გვ. 39.
137 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. თბილისი: მერიდიანი, 2019, გვ. 13.
138 იქვე., გვ. 13.
139 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631.
140 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, 3-5.
141 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. თბილისი: მერიდიანი, 2019, გვ. 14.
142 Cernomoreț S., Nastas A., Comparative Analysis of Cybercrime in the Criminal Law System. 2020, გვ. 40-41.
143 იქვე., გვ. 41.
144 UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, გვ. 79.

ერთ უდიდეს სირთულეს წარმოადგენს. ამ პრობლემას ამძაფრებს კანონმდებლობის ხშირი ბუნდოვანება, რის გამოც მოსამართლეებს ემპირიულ შეფასებებზე უწევთ დაყრდნობა, რაც სხვადასხვა რეგიონსა და საქმეში განსხვავებულ პრაქტიკას წარმოშობს.[145] მაგალითად, ხშირია დავა იმის თაობაზე, „იცოდა“ მოიცავს თუ არა „უნდა სცოდნოდა“-ს კატეგორიას.[146] ზოგიერთი მიიჩნევს, რომ „უნდა სცოდნოდა“ პრინციპის გამოყენება ეფექტიანია კიბერდანაშაულთან ბრძოლაში, სხვები კი ამტკიცებენ, რომ ეს არღვევს პასუხისმგებლობის პრინციპს და შლის ზღვარს განზრახვასა და გაუფრთხილებლობას შორის.[147]

ამერიკული სამართლის პრაქტიკაც ადასტურებს, თუ რამდენად რთულია განზრახვის ფარგლების განსაზღვრა. გახმაურებულ საქმეში აშშ მორისის წინააღმდეგ, სასამართლომ დაადგინა, რომ განზრახვა ვრცელდებოდა მხოლოდ კომპიუტერულ სისტემაში უნებართვო შეღწევის (წვდომის) ელემენტზე და არა მის შედეგად გამოწვეულ ზიანზე.[148] ეს ნიშნავს, რომ პირი შეიძლება დამნაშავედ ცნონ მაშინაც კი, თუ ზიანი გაუფრთხილებლობით ან უნებლიეთ გამოიწვია, მთავარია, თავად შეღწევა ყოფილიყო განზრახი. თუმცა, ამ საქმემ პასუხგაუცემელი დატოვა კითხვა, უნდა სცოდნოდა თუ არა ბრალდებულს, რომ მისი წვდომა უნებართვო იყო.[149] ზოგიერთი შტატის კანონმდებლობა ამ საკითხს უფრო ნათლად არეგულირებს და მოითხოვს იმის მტკიცებას, რომ პირმა იმოქმედა „იმის ცოდნით, რომ ასეთი გამოყენება ნებართვის გარეშე ხდებოდა“.[150] ეს სირთულეები ხშირად იწვევს სასამართლო პრაქტიკაში შეუსაბამობებს, როცა თითქმის იდენტურ საქმეებზე სხვადასხვა მოსამართლე სრულიად განსხვავებულ გადაწყვეტილებებს იღებს.[151]

მართალია, კიბერდანაშაულების ძირითადი ნაწილი განზრახ კატეგორიას მიეკუთვნება, მაგრამ სულ უფრო აქტუალური ხდება გაუფრთხილებლობით

---

145 Liu Y., Study on the Subjective Knowledge Element of Cybercrime Assistance Based on Quantitative Methods. Advances in Social Science, Education and Humanities Research. 2025, გვ. 2-4.
146 იქვე., გვ. 4.
147 იქვე., გვ. 4.
148 Clough J., PRINCIPLES OF CYBERCRIME. Cambridge: Cambridge University Press, 2010, გვ. 94.
149 იქვე., გვ. 94.
150 იქვე., გვ. 94.
151 Liu Y., Study on the Subjective Knowledge Element of Cybercrime Assistance Based on Quantitative Methods. Advances in Social Science, Education and Humanities Research. 2025, გვ. 5.

ჩადენილი ქმედებების კრიმინალიზაციის საკითხი. თუ კიბერდანაშაულად მხოლოდ სსკ-ის XXXV თავით გათვალისწინებულ ქმედებებს მივიჩნევთ, მაშინ საქმე მხოლოდ განზრახ დანაშაულებთან გვექნება, მაგრამ თუ ამ თავის მიღმაც გავიხედავთ, აღმოჩნდება, რომ გაუფრთხილებლობა კიბერდანაშაულისთვის „კარხსნილია“.[152] მაგალითად, დღეს არსებული სამხედრო, საავიაციო თუ სატრანსპორტო ტექნიკის სისტემები მთლიანად კომპიუტერიზებულია, ამიტომ ექსპლუატაციის წესების დარღვევა, ფაქტობრივად, კომპიუტერულ ტექნოლოგიათა არასწორ გამოყენებას ნიშნავს.[153] ჩერნობილის ატომურ სადგურზე მომხდარი ტრაგედია ან კრუიზული გემის, „კონკორდიას“ ჩაძირვა, არსებითად, გაუფრთხილებელი დანაშაულის მაგალითებია, რომელთა საფუძველშიც ტექნოლოგიური სისტემების გაუმართაობა ან არასწორი მართვა იდგა.[154] ზოგიერთი საერთაშორისო დოკუმენტიც პირდაპირ უშვებს გაუფრთხილებლობით ჩადენილი ქმედებების დასჯადობას. მაგალითად, აფრიკის კავშირის კონვენციის პროექტი ითვალისწინებს პერსონალური მონაცემების დამუშავების წესების დარღვევის კრიმინალიზაციას „თუნდაც გაუფრთხილებლობით“.[155]

გაუფრთხილებლობის კონტექსტში განსაკუთრებულ მნიშვნელობას იძენს სპეციალური სუბიექტის როლი. ის, რაც შეიძლება მისატევებელი იყოს რიგითი მომხმარებლისთვის, დაუშვებელია პასუხისმგებელი პირისთვის, რომელსაც სამსახურებრივი ვალდებულება აკისრია.[156] მაგალითად, გემის კაპიტანი ვალდებულია, სრულყოფილად ფლობდეს სანავიგაციო ტექნოლოგიებს, რასაც ვერ მოვთხოვთ რიგით თანამშრომელს.[157] „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონიც დეტალურად განსაზღვრავს კრიტიკული ინფორმაციის შენახვისა და კომპიუტერულ ინციდენტებზე რეაგირების შესაბამის სუბიექტებს, რაც მათზე დაკისრებულ მომეტებულ პასუხისმგებლობაზე მიუთითებს.[158] ამ სფეროებში ადამიანური შეცდომა გარდაუვალია, თუმცა

---

152 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 16-17.

153 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 17, 128.

154 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 126.

155 UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, გვ. 79.

156 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 16, 130.

157 იქვე., გვ. 130.

158 იქვე., გვ. 130.

როდესაც ასეთი ურთიერთობები უკვე რეგულირდება ადმინისტრაციული სამართლის ნორმებით, ეს სისხლისსამართლებრივი რეგულირების აუცილებლობაზეც მიანიშნებს.[159] ამასთან, კიბერდანაშაულის გაუფრთხილებლობით ჩადენილი ქმედებების კრიმინალიზაციას თან სდევს რისკი, რომ სისხლის სამართლის კოდექსი ვერ დაიტევს შემადგენლობათა უსასრულო რაოდენობას.[160] ამიტომ ერთ-ერთ გამოსავლად მიიჩნევა კიბერტექნოლოგიების გამოყენების გათვალისწინება უკვე არსებულ შემადგენლობებში, როგორც მაკვალიფიცირებელი გარემოებისა.[161]

სუბიექტური მხარის კვალიფიკაციის პრობლემები კარგად გამოჩნდა საგამოძიებო პრაქტიკაშიც, კერძოდ, პირადი ცხოვრების ამსახველი კადრების გავრცელების საქმეზე. გამოძიების ფარგლებში პასუხისგებაში მიეცა პირთა დიდი რაოდენობა, რომლებიც აღნიშნულ კადრებს ინახავდნენ. ერთ-ერთი ბრალდებულის, ვ-ს მიმართ, თავდაპირველად ბრალდება დამძიმდა გავრცელების ეპიზოდით, რადგან მისმა მეგობარმა შემთხვევით ნახა ეს კადრები მის ტელეფონში და სხვებს გაუზიარა.[162] თუმცა, შემდგომ ეტაპზე დადგინდა, რომ ვ-ს მხრიდან ინფორმაციის გავრცელება განპირობებული იყო გაუფრთხილებლობით და არა განზრახვით, რის გამოც მას გავრცელების ეპიზოდი მოეხსნა. ეს იმიტომ მოხდა, რომ პირადი ცხოვრების საიდუმლოს ხელყოფის შემადგენლობა[163] მხოლოდ განზრახი ბრალით ჩადენას გულისხმობს.[164] ეს შემთხვევა ნათლად აჩვენებს, რომ მსგავსი ქმედებების შინაარსი სავსებით თავსებადია გაუფრთხილებლობის ბუნებასთან, მაგრამ კანონმდებლობა ჯერჯერობით არ ითვალისწინებს ასეთი ქმედებების გაუფრთხილებლობით ჩადენის შესაძლებლობას, რაც პრაქტიკაში კვალიფიკაციის სირთულეებს ქმნის.[165]

კიბერდანაშაულის შემადგენლობის ელემენტების ანალიზი ცხადყოფს, რომ ტრადიციული სისხლისსამართლებრივი ცნებების პირდაპირი გადმოტანა ციფრულ სამყაროში არაერთ პრობლემას წარმოშობს. დანაშაულის საგნის

---

159 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 16.
160 იქვე., გვ. 17.
161 იქვე., გვ. 17-18.
162 იქვე., გვ. 128-129.
163 საქართველოს სისხლის სამართლის კოდექსი, მუხლი 157[1].
164 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. თბილისი: კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 129.
165 იქვე., გვ. 129.

არამატერიალური ბუნება, მოქმედების ტექნოლოგიურად რთული ხასიათი და, რაც მთავარია, სუბიექტური მხარის, განსაკუთრებით „ცოდნის“ ელემენტის, დამტკიცების სირთულეები სამართალდამცავ ორგანოებსა და სასამართლოებს სერიოზული გამოწვევების წინაშე აყენებს. მართალია, ეროვნული კანონმდებლობები და სასამართლო პრაქტიკა ცდილობს ამ პრობლემებთან გამკლავებას, მაგრამ კიბერსივრცის მუდმივი განვითარება და დანაშაულის ახალი ფორმების გაჩენა დოქტრინისა და კანონმდებლობის მუდმივ სრულყოფას მოითხოვს, რათა სამართლებრივი რეაგირება ადეკვატური და ეფექტიანი იყოს.

2.2. დანაშაულის დროისა და ადგილის განსაზღვრის პრობლემა

კიბერდანაშაულის ტრანსნაციონალური ბუნება სამართალდამცავი ორგანოებისა და სასამართლო სისტემებისთვის ერთ-ერთ უდიდეს სირთულეს ქმნის, რადგან ტრადიციული, ტერიტორიულ საზღვრებზე დაფუძნებული იურისდიქციის პრინციპები კიბერსივრცის უსაზღვრო ბუნებასთან ხშირად შეუსაბამოა. ეს მდგომარეობა იწვევს იურისდიქციულ ქაოსს, რასაც დამნაშავეები წარმატებით იყენებენ გამოძიებისა და სისხლისსამართლებრივი დევნისგან თავის ასარიდებლად.[166] კიბერდამნაშავეს, რომელსაც ინტერნეტზე წვდომა აქვს, შეუძლია დანაშაული მსოფლიოს ნებისმიერი წერტილიდან ჩაიდინოს, რაც ტრადიციული საგამოძიებო მეთოდებისა და იურისდიქციული ნორმების ეფექტიანობას საგრძნობლად ამცირებს.[167]

დანაშაულის ადგილის, ანუ locus delicti-ს დასადგენად, კლასიკური სისხლის სამართალი რამდენიმე თეორიას იყენებს, რომელთა კიბერსივრცეში გადმოტანაც რთული აღმოჩნდა. ესენია: ქმედების განხორციელების ადგილის თეორია, სადაც დამნაშავემ ქმედება ჩაიდინა; შედეგის დადგომის ადგილის თეორია, სადაც დანაშაულებრივი შედეგი დადგა; და უბიქვიტურობის თეორია, რომელიც იურისდიქციას ორივე ადგილას აღიარებს. კიბერდანაშაულის შემთხვევაში, ეს თეორიები ხშირად რამდენიმე სახელმწიფოს ერთდროულად ანიჭებს იურისდიქციას; მაგალითად, დამნაშავე A ქვეყნიდან არღვევს B ქვეყანაში მდებარე სერვერს და ზიანს აყენებს C ქვეყანაში მყოფ მსხვერპლს.[168] ასეთ ვითარებაში იურისდიქციის მქონე სახელმწიფოთა რიცხვი მკვეთრად

166 Coupland H., Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 20-24.
167 იქვე., გვ. 6-9.
168 იქვე., გვ. 6-9.

იზრდება, რაც საქმეს კიდევ უფრო ართულებს.[169] პრაქტიკაში, ზოგიერთი ქვეყნის, მაგალითად, ინდონეზიის გამომძიებლები დანაშაულის ადგილის დასადგენად „ატვირთვის თეორიას“ (ქმედების ადგილი) და „ჩამოტვირთვის თეორიას“ (შედეგის ადგილი) იყენებენ (ჰერავატი, 2024, 20-26).

იურისდიქციული პრინციპების ფართო გამოყენება კონკურენტული იურისდიქციების პრობლემას წარმოშობს, როდესაც ერთსა და იმავე ქმედებაზე რამდენიმე სახელმწიფო აცხადებს პრეტენზიას.[170] ეს ვითარება ქმნის როგორც სამართლებრივი გაურკვევლობის, ასევე ne bis in idem პრინციპის (ერთი და იმავე დანაშაულისთვის პირის ორჯერ გაუსამართლებლობა) დარღვევის რისკს. პრობლემას ისიც ართულებს, რომ გლობალურ დონეზე არ არსებობს ne bis in idem პრინციპის უნივერსალური აღიარება და სახელმწიფოები ხშირად უარს ამბობენ უცხოური სასამართლოს გადაწყვეტილების (res iudicata) ცნობაზე.[171] გარდა ამისა, შესაძლოა, სახელმწიფოები ვერც კი შეთანხმდნენ იმაზე, თუ რა წარმოადგენს „იგივე ქმედებას“ (idem), განსაკუთრებით მაშინ, როდესაც კანონმდებლობა არაჰარმონიზებულია, რაც ორმაგი დასჯის საშიშროებას ზრდის.[172]

საერთაშორისო ინსტრუმენტები ამ კონფლიქტების მოგვარების სხვადასხვა მექანიზმს გვთავაზობს, თუმცა განსხვავებული ეფექტიანობით. მაგალითად, ევროპის საბჭოს კიბერდანაშაულის კონვენციის 22-ე მუხლის მე-5 პუნქტი მხარეებს „შესაბამის შემთხვევებში“ კონსულტაციების გამართვას სთავაზობს, მაგრამ ეს ვალდებულებას არ წარმოადგენს და, შესაბამისად, მისი ეფექტიანობა მცირდება (ბრატა, 2021, 4-6; ბუსოლატი, 2020, 225-228). ამისგან განსხვავებით, არაბულ სახელმწიფოთა ლიგის კონვენცია იურისდიქციული დავების გადასაწყვეტად პრიორიტეტების დეტალურ სიას აწესებს: პირველ ადგილზეა სახელმწიფო, რომლის უსაფრთხოებას ან ინტერესებს შეექმნა საფრთხე (დამცავი პრინციპი); მეორეზე - სახელმწიფო, რომლის ტერიტორიაზეც ჩაიდინეს დანაშაული; და მესამეზე - დამნაშავის მოქალაქეობის სახელმწიფო.[173] აღსანიშნავია, რომ არაბული კონვენცია უპირატესობას დამცავ პრინციპს ანიჭებს ტრადიციულად უფრო ძლიერ

169 Bussolati N., Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, გვ. 221-224.
170 UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, გვ. 224-226.
171 Bussolati N., Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, გვ. 225-228.
172 იქვე., გვ. 225-228.

ტერიტორიულობის პრინციპთან შედარებით.[174] ევროკავშირის ინსტრუმენტები კი საქმის წარმოების ერთ სახელმწიფოში „ცენტრალიზებას“ ცდილობენ და კონფლიქტური სიტუაციების გადასაწყვეტად ევროჯასთის (Eurojust) მექანიზმს იყენებენ.[175]

ბევრი ქვეყანა, რომელსაც იურისდიქციული კონფლიქტების მოსაგვარებლად სპეციალური კანონმდებლობა არ გააჩნია, არაფორმალურ კონსულტაციებსა და საერთაშორისო ორგანიზაციების, როგორიცაა ინტერპოლი და ევროპოლი, დახმარებას ეყრდნობა.[176] სანიმუშოა ამერიკის ერთ-ერთი ქვეყნის პრაქტიკა, სადაც სისხლისსამართლებრივი დევნა ფრაგმენტული დანაშაულების მიმართ მხოლოდ მაშინ იწყება, თუ დამნაშავე ან მსხვერპლი ამ ქვეყნის მოქალაქეა, ხოლო სხვა შემთხვევები ინტერპოლის არხებით შესაბამის ქვეყნებს გადაეცემა.[177] ამის საპირისპიროდ, აშშ-ის ზოგიერთ შტატს, მაგალითად, არკანზასსა და ოჰაიოს, მიღებული აქვს კანონები, რომლებიც იურისდიქციას ადგენს იმ შემთხვევაში, თუ დანაშაულებრივი მონაცემთა გადაცემა შტატის ტერიტორიიდან დაიწყო ან შტატის ტერიტორიაზე იქნა მიღებული (ბრატა, 2021, 4-6).

იურისდიქციული ბუნდოვანების ნათელ მაგალითს წარმოადგენს საქმე Yahoo!, Inc. v. LICRA. საფრანგეთის სასამართლომ დაავალა Yahoo-ს, დაებლოკა ფრანგი მომხმარებლებისთვის წვდომა ნაცისტური ატრიბუტიკის ონლაინ-აუქციონზე, მიუხედავად იმისა, რომ ასეთი მასალის გაყიდვა აშშ-ის კანონმდებლობით ლეგალური იყო.[178] ამ საქმემ ცხარე დებატები გამოიწვია იმის შესახებ, თუ რა საზღვრებში შეუძლია ერთ სახელმწიფოს, საკუთარი კანონები დაუწესოს უცხოურ კომპანიებს, რომლებიც ონლაინ ოპერირებენ (ბრატა, 2021, 4-6). ეს შემთხვევა ნათლად აჩვენებს ეროვნული სუვერენიტეტისა და

173 UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, გვ. 224-226; Bussolati N., Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, გვ. 225-228.

174 Bussolati N., Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, გვ. 221-224.

175 იქვე., გვ. 225-228.

176 UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, გვ. 224-226.

177 იქვე., გვ. 224-226.

178 Coupland H., Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 6-9.

ინტერნეტის გლობალური ბუნების შეჯახებას, რაც იურისდიქციული უფლებამოსილების ფარგლების შესახებ არსებით კითხვებს აჩენს.[179]

კიდევ ერთი საყურადღებო საქმეა Microsoft Ireland, სადაც აშშ-ის მთავრობა ცდილობდა, მაიკროსოფტი ირლანდიაში მდებარე სერვერებზე შენახული ელექტრონული ფოსტის გადაცემაზე დაეყოლიებინა. ამ საქმემ ხაზი გაუსვა საზღვარგარეთ შენახულ მონაცემებზე ეროვნული კანონების ექსტრატერიტორიული გამოყენების სამართლებრივ გაურკვევლობას. მართალია, ეს საკითხი შემდგომში აშშ-ში CLOUD Act-ის მიღებით ნაწილობრივ დარეგულირდა, რომელიც ამერიკის ხელისუფლებას უცხოეთში შენახული მონაცემების მოთხოვნის უფლებას ანიჭებს, მაგრამ ამით ვერ აღმოიფხვრა დაპირისპირება ეროვნულ სუვერენიტეტსა და გლობალურ ციფრულ ინფრასტრუქტურას შორის.[180]

იურისდიქციასთან ერთად, სერიოზული პრობლემაა ორმაგი დანაშაულებრიობის პრინციპი, რაც ნათლად გამოჩნდა „Love Bug“ ვირუსის საქმეში. ფილიპინელმა სტუდენტმა, ონელ დე გუზმანმა, შექმნა და გაავრცელა ვირუსი, რომელმაც დიდი ზიანი მიაყენა კომპიუტერულ სისტემებს აშშ-ში. თუმცა, მისი ექსტრადიცია აშშ-ში ვერ მოხერხდა, რადგან იმ დროისთვის ჰაკინგი და ვირუსის გავრცელება ფილიპინების კანონმდებლობით დანაშაულად არ ითვლებოდა. ეს შემთხვევა ცხადყოფს, რომ ექსტრადიციისთვის აუცილებელი მოთხოვნა - ქმედება ორივე სახელმწიფოში დანაშაულად იყოს ცნობილი - კიბერდამნაშავეებს დაუსჯელობის შესაძლებლობას აძლევს იმ ქვეყნებში, სადაც კანონმდებლობა ტექნოლოგიურ განვითარებას ჩამორჩება (ბრატა, 2021, 6-8).

მაშინაც კი, როდესაც იურისდიქცია დადგენილია, მისი აღსრულება არაკოოპერირებად სახელმწიფოში მყოფი დამნაშავის მიმართ პრაქტიკულად შეუძლებელი შეიძლება აღმოჩნდეს. ამის მაგალითია United States v. Gorshkov საქმე, სადაც რუსი ჰაკერის, გორშკოვის, წინააღმდეგ აშშ-მა დაიწყო დევნა, მაგრამ რუსეთთან ექსტრადიციის ხელშეკრულების არარსებობის გამო, ამერიკის ხელისუფლებამ ხრიკს მიმართა და დამნაშავე აშშ-ის ტერიტორიაზე მოტყუებით შემოიყვანა მის დასაკავებლად (ბრატა, 2021, 6-8). ანალოგიური სირთულეები გამოიკვეთა United States v. Ivanov საქმეშიც, სადაც რუსი ჰაკერის წინააღმდეგ გამოტანილი განაჩენის აღსრულება ვერ მოხერხდა,

179 იქვე., გვ. 6-9.
180 იქვე., გვ. 6-9.

რადგან დამნაშავე არასათანამშრომლო იურისდიქციაში იმყოფებოდა.[181] ეს საქმეები ცხადყოფს, რომ მხოლოდ იურისდიქციის არსებობა, საერთაშორისო თანამშრომლობის გარეშე, ხშირად არასაკმარისია დამნაშავის პასუხისგებაში მისაცემად.

ტრანსნაციონალური კიბერდანაშაულის გამოძიების პრაქტიკა საქართველოშიც არსებობს, რაც თბილისის საქალაქო სასამართლოს ერთ-ერთ გახმაურებულ საქმეში გამოვლინდა. საქმე ეხებოდა ორგანიზებულ ჯგუფს, რომელშიც საქართველოსა და ბულგარეთის მოქალაქეები მონაწილეობდნენ. ისინი ე.წ. „ფიშინგის“ მეთოდითა და „G-----“ სახელწოდების ვირუსის გამოყენებით აშშ-ში რეგისტრირებულ კომპანიათა საბანკო ანგარიშებიდან დიდი ოდენობით თანხებს იპარავდნენ (თბილისის საქალაქო სასამართლო, 2019, 1-9). დანაშაულებრივი სქემა მოიცავდა სხვადასხვა როლების მქონე პირებს, მათ შორის „სპამერებს“ (ვირუსის გამავრცელებელი), „კრიპტერებს“ (ვირუსის დამშიფრავი ანტივირუსული პროგრამებისგან დასამალად) და „დროპერებს“ (თანხის გამნაღდებელი) (თბილისის საქალაქო სასამართლო, 2019, 33-42). ჯგუფმა სცადა 1,260,521 აშშ დოლარის მითვისება, საიდანაც ფაქტობრივად 316,955 დოლარს დაეუფლა (თბილისის საქალაქო სასამართლო, 2019, 20-28). გამოძიება მიმდინარეობდა აშშ-ის გამოძიების ფედერალურ ბიუროსთან (FBI) მჭიდრო თანამშრომლობით, რაც ხაზს უსვამს საერთაშორისო კოოპერაციის აუცილებლობას ასეთი რთული საქმეების გასახსნელად (თბილისის საქალაქო სასამართლო, 2019, 20-28). საბოლოოდ, სასამართლომ ბრალდებულები დამნაშავედ ცნო საქართველოს სისხლის სამართლის კოდექსის რამდენიმე მუხლით, მათ შორის 177-ე (ქურდობა), 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 285-ე (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა) მუხლებით.[182]

იურისდიქციული პრობლემების ფონზე, ჩნდება კითხვა: ხომ არ არის საჭირო ცალკე, „კიბერსივრცის“ განზომილებაზე მორგებული იურისდიქციის შექმნა? გაეროს ნარკოტიკებისა და დანაშაულის ოფისის შეფასებით, ამ ეტაპზე ამის საჭიროება არ დგას. კვლევის ავტორები მიიჩნევენ, რომ კიბერდანაშაულთა უმრავლესობა თითქმის ყოველთვის შეიძლება დაუკავშირდეს კონკრეტულ სახელმწიფოს ტერიტორიულობისა და მოქალაქეობის პრინციპების გამოყენებით, რადგან კიბერსივრცეში

181 იქვე., გვ. 6-9.
182 თბილისის საქალაქო სასამართლო, 2019 გადაწყვეტილება, 26-35.

განხორციელებული ტრანზაქციები რეალურ ადამიანებს ეხება, რომლებიც კონკრეტულ ტერიტორიულ იურისდიქციებში იმყოფებიან (გაეროს ნარკოტიკებისა და დანაშაულის ოფისი, 2013, 226-229). მათი აზრით, მონაცემთა გლობალურ ცენტრებში გაფანტვა და მობილურობა უფრო მეტად მტკიცებულებების შეგროვების პრობლემას ქმნის, ვიდრე იურისდიქციის დადგენისას (გაეროს ნარკოტიკებისა და დანაშაულის ოფისი, 2013, 226-229).

სწორედ მტკიცებულებების შეგროვება და საერთაშორისო თანამშრომლობის სირთულეებია მთავარი დაბრკოლება. ტრადიციული მექანიზმები, როგორიცაა სამართლებრივი ურთიერთდახმარების ხელშეკრულებები (MLATs), კიბერდანაშაულის სისწრაფისთვის ზედმეტად ნელი და ბიუროკრატიულია.[183] გაეროს კვლევის მონაცემებით, ფორმალური მოთხოვნების პასუხის დრო, როგორც ექსტრადიციის, ისე ურთიერთდახმარების შემთხვევაში, ხშირად თვეებით იზომება (გაეროს ნარკოტიკებისა და დანაშაულის ოფისი, 2013, 226-229). ეს კი კრიტიკულად დიდი დროა, როდესაც საქმე ეხება ციფრულ მტკიცებულებებს, რომელთა განადგურება ან შეცვლა წამებშია შესაძლებელი. არსებული ვითარება ქმნის საშიშროებას, რომ შეიქმნას ქვეყნების დახურული „კლასტერები“, რომლებიც ეფექტიანად თანამშრომლობენ ერთმანეთთან, ხოლო სხვა ქვეყნებთან ურთიერთობა კვლავ ტრადიციულ, მოძველებულ რეჟიმში რჩება, რაც გლობალურ ბრძოლას აფერხებს (გაეროს ნარკოტიკებისა და დანაშაულის ოფისი, 2013, 226-229).

პრობლემის გადაჭრისთვის რამდენიმე მიმართულებით არის ნაბიჯები გადასადგმელი. უპირველესად, აუცილებელია კანონმდებლობის საერთაშორისო ჰარმონიზაცია, თუმცა ეს პროცესი რთულია, რადგან სახელმწიფოები, განსაკუთრებით ავტორიტარული რეჟიმები, ხშირად ეწინააღმდეგებიან ისეთ ცვლილებებს, რომლებიც ინტერნეტზე მათ კონტროლს შეზღუდავს.[184] აგრეთვე, გადამწყვეტია ე.წ. მულტისტეიკჰოლდერული მიდგომა, რომელიც მოიცავს არა მხოლოდ სამართალდამცავ ორგანოებს, არამედ კერძო სექტორსაც, განსაკუთრებით ტექნოლოგიურ კომპანიებს. ეს კომპანიები, რომლებსაც ზოგი მკვლევარი „ციფრულ სუვერენებს“ უწოდებს, ხშირად უკეთეს მდგომარეობაში არიან, შექმნან და უზრუნველყონ კიბერდანაშაულთან

183 Coupland H., Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 6-9.
184 იქვე., გვ. 20-24.

ბრძოლისთვის საჭირო მოწინავე ტექნოლოგიები და ინფორმაცია.[185] ამასთან, განიხილება ისეთი იდეებიც, როგორიცაა კიბერსივრცისთვის საერთაშორისო კრიმინალური ტრიბუნალის (ICTC) შექმნა, რომელსაც იურისდიქცია ექნება საერთაშორისო ხელშეკრულებების დამრღვევ და კრიტიკული ინფრასტრუქტურისთვის საფრთხის შემცველ კიბერდანაშაულებზე (ბრატა, 2021, 6-8).

ამრიგად, კიბერდანაშაულის შემთხვევაში დროისა და ადგილის დადგენის პრობლემა არსებული იურისდიქციული ჩარჩოების არაადეკვატურობასა და საერთაშორისო თანამშრომლობის ნაკლოვანებებში მდგომარეობს. მიუხედავად იმისა, რომ ახალი, სპეციალური „კიბერსივრცის იურისდიქციის“ შექმნა ამ ეტაპზე გამართლებულად არ მიიჩნევა, აშკარაა, რომ აუცილებელია არსებული პრინციპების ინოვაციური გამოყენება და, რაც მთავარია, სახელმწიფოებს შორის სწრაფი და ეფექტიანი საკომუნიკაციო არხების ჩამოყალიბება. ციფრული მტკიცებულებების დასაშვებობის შესახებ წესების გადახედვა, საერთაშორისო საგამოძიებო ჯგუფების შექმნა და კერძო სექტორთან მჭიდრო თანამშრომლობა ის პრაქტიკული ნაბიჯებია, რომლებმაც შეიძლება შეამციროონ ის იურისდიქციული ხარვეზები, რომლებითაც დღეს კიბერდამნაშავეები სარგებლობენ.

2.3. კიბერდანაშაულის გამიჯვნა სხვა მონათესავე დანაშაულებისგან

კიბერდანაშაულის კვალიფიკაციისას მთავარ სირთულეს მისი სხვა, ტრადიციული დანაშაულებისგან გამიჯვნა წარმოადგენს. ტექნოლოგიურმა განვითარებამ ისე წაშალა ზღვარი ძველ და ახალ დანაშაულებრივ ქმედებებს შორის, რომ ერთი ქმედება ხშირად ერთდროულად რამდენიმე სისხლისსამართლებრივი ნორმის რეგულირების სფეროში ექცევა. ეს კი ნორმათა კონკურენციისა და დანაშაულთა ერთობლიობით კვალიფიკაციის სირთულეებს იწვევს, რაც სერიოზულ გამოწვევას უქმნის კანონმდებელსა და პრაქტიკოს იურისტებს.[186] ამიტომ აუცილებელია იმ კრიტერიუმების გაანალიზება, რომლებითაც კიბერდანაშაული ქონებრივი და პიროვნების წინააღმდეგ მიმართული დანაშაულებისგან გაიმიჯნება.

კიბერდანაშაულების გამიჯვნა ტრადიციული ქონებრივი დანაშაულებისგან განსაკუთრებით რთულია, რადგან ციფრული ტექნოლოგიები ხშირად სწორედ

185 იქვე., გვ. 20-24.

186 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 36.

ქონებრივი სარგებლის მიღების იარაღად გამოიყენება. თავდაპირველად, როდესაც სპეციალური კიბერდანაშაულებრივი ნორმები არ არსებობდა, სამართალდამცავი ორგანოები ცდილობდნენ, ახალი ტიპის ქმედებები ქურდობის, თაღლითობის ან დოკუმენტის გაყალბების არსებულ შემადგენლობებში მოექციათ, თუმცა ეს მიდგომა ბევრ პრობლემას აწყდებოდა. მაგალითად, ტრადიციული სამართლებრივი დოქტრინით, ქურდობა ნივთის მფლობელობიდან ფიზიკურად გამოყვანას გულისხმობს, ხოლო კომპიუტერული მონაცემების კოპირებისას მფლობელი მას არ კარგავს, რაც ქურდობის შემადგენლობას გამორიცხავდა.[187] ასევე, კონფიდენციალური ინფორმაცია, თავისი არამატერიალური ბუნების გამო, ტრადიციულად არ განიხილებოდა „ქონებად“, რომლის მოპარვაც შეიძლებოდა. ამგვარად, არსებული კანონების ახალ რეალობაზე მორგების მცდელობა ხშირად „პროკრუსტეს სარეცელზე“ ფაქტების მორგებას ემსგავსებოდა, რადგან ეს კანონები უბრალოდ არ იყო შექმნილი ასეთი შემთხვევებისთვის.[188]

საქართველოს სისხლის სამართლის კოდექსიც ამ პრობლემას ვერ ასცდა. კიბერდანაშაულების უმეტესობა სწორედ ქონებრივი სარგებლის მიღებას ისახავს მიზნად, რა დროსაც კომპიუტერი დანაშაულის ჩადენის იარაღს წარმოადგენს.[189] ამის ნათელი მაგალითია თბილისის საქალაქო სასამართლოს ერთ-ერთი საქმე,[190] რომელშიც ორგანიზებულმა ჯგუფმა რთული დანაშაულებრივი სქემა შეიმუშავა. ისინი იყენებდნენ „G-----“ სახელწოდების ჰიბრიდულ ვირუსს, რომელსაც ე.წ. „სპამერების“ მეშვეობით ამერიკულ კომპანიებს უგზავნიდნენ. როდესაც კომპანიის თანამშრომელი ვირუსიან ელექტრონულ წერილს ხსნიდა, მისი კომპიუტერი ინფიცირდებოდა, რაც დამნაშავეებს ინტერნეტბანკის მონაცემებზე წვდომის საშუალებას აძლევდა. ამის შემდეგ, ჯგუფის სხვა წევრები, ე.წ. „თანხის გადამრიცხავები“, ამ მონაცემებით შედიოდნენ კომპანიის ანგარიშზე და თანხა გადაჰქონდათ „დროპერების“ ანგარიშებზე, რომლებიც მას ანაღდებდნენ და კრიპტოვალუტის სახით ჯგუფის წევრებს უნაწილებდნენ.[191]

---

187 Clough, J. PRINCIPLES OF CYBERCRIME. Cambridge University Press. 2010, 95.

188 იქვე., გვ. 95-96.

189 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 27.

190 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631.

191 თბილისის საქალაქო სასამართლო გადაწყვეტილება #330100119003053631, 3-5.

ამ კონკრეტულ შემთხვევაში, ჯგუფის წევრებს ბრალი დანაშაულთა ერთობლიობისთვის წაუყენეს, რაც სპეციფიკურ კიბერდანაშაულებსა და ტრადიციულ ქონებრივ დანაშაულს მოიცავდა. კერძოდ, მათი ქმედება დაკვალიფიცირდა საქართველოს სისხლის სამართლის კოდექსის 284-ე, 285-ე, 158-ე და 177-ე მუხლებით (ქურდობა, ჩადენილი ორგანიზებული ჯგუფის მიერ დიდი ოდენობით).[192] ეს საქმე ნათლად აჩვენებს, რომ ერთი დანაშაულებრივი განზრახვა (თანხის ფარული დაუფლება) ქმედებათა ჯაჭვით ხორციელდება, რომელთაგან თითოეული ცალკე დანაშაულის შემადგენლობას ქმნის. სასამართლომ საბოლოო სასჯელის განსაზღვრისას სსკ-ის 59-ე მუხლი გამოიყენა და უფრო მძიმე სასჯელით დაფარა ნაკლებად მძიმეები, რაც დანაშაულთა რეალური ერთობლიობის ტიპური მაგალითია.[193]

სწორედ ასეთი შემთხვევები წარმოშობს დოქტრინალურ დებატებს იმის თაობაზე, თუ რამდენად გამართლებულია ცალკეული კიბერდანაშაულებრივი შემადგენლობების არსებობა, როდესაც ისინი ტრადიციული დანაშაულების ჩადენის ხერხს წარმოადგენენ. მაგალითად, ქართულ კანონმდებლობაში არსებული „კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით“ (სსკ-ის 286[1] მუხლი) შინაარსობრივად ძალიან ახლოს დგას თაღლითობასთან. ასეთი დუბლირება ნორმათა კონკურენციას იწვევს და ხშირად ქმედების უსამართლო კვალიფიკაციას ორი, თითქმის იდენტური შინაარსის მუხლით. ამ პრობლემის თავიდან აცილება შესაძლებელი იქნებოდა, კანონმდებელს კომპიუტერული ტექნოლოგიების გამოყენება დამოუკიდებელ დანაშაულად კი არ განეხილა, არამედ ტრადიციული დანაშაულის (მაგალითად, თაღლითობის ან ქურდობის) მაკვალიფიცირებელ ნიშნად.[194] ეს მიდგომა გაამარტივებდა კვალიფიკაციის პროცესს და ამავდროულად, ერთგვაროვანი სასამართლო პრაქტიკის ჩამოყალიბებასაც შეუწყობდა ხელს.[195]

ქონებრივი დანაშაულების გარდა, კიბერსივრცე პიროვნების წინააღმდეგ მიმართული დანაშაულების ჩასადენადაც აქტიურად გამოიყენება. ასეთია კიბერბულინგი, კიბერგადაკიდება (cyberstalking), ცილისწამება და პირადი ცხოვრების საიდუმლოს ხელყოფა, რომელთა მიზანი ხშირად მსხვერპლის

192 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, 2-3.
193 თბილისის საქალაქო სასამართლო გადაწყვეტილება #330100119003053631, 35-36.
194 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 121-127.
195 იქვე., გვ. 36-43.

რეპუტაციის შელახვა, დაშინება ან ფსიქოლოგიური ზიანის მიყენებაა.[196] საქართველოს კანონმდებლობა „კიბერგადაკიდების“ ცალკე შემადგენლობას არ იცნობს, თუმცა, როდესაც ასეთი ქმედება მძიმე შედეგს, მაგალითად, თვითმკვლელობას იწვევს, შესაძლებელია მისი კვალიფიკაცია სსკ-ის იმ მუხლით, რომელიც პასუხისმგებლობას აწესებს პატივისა და ღირსების სისტემატური დამცირებით თვითმკვლელობამდე მიყვანისთვის.[197] ესეც მიუთითებს იმაზე, რომ პრაქტიკა იძულებულია, ახალი ტიპის ქმედებები არსებულ, ტრადიციულ ნორმებს „მოარგოს“, რაც ყოველთვის ეფექტიანი არ არის.

დანაშაულთა ერთობლიობის პრობლემა განსაკუთრებით მწვავედ დგას ისეთი ქმედებების დროს, სადაც ციფრული კომპონენტი დანაშაულის ჩადენის აუცილებელი, თუმცა არა ერთადერთი, ელემენტია. ქართულ პრაქტიკაში დამკვიდრდა მიდგომა, რომლის მიხედვითაც ასეთი ქმედებები რამდენიმე მუხლის ერთობლიობით კვალიფიცირდება. მაგალითად, „კიბერქურდობა“, რაც ინტერნეტიდან საავტორო უფლებების დარღვევით ინფორმაციის გადმოწერას გულისხმობს, კვალიფიცირდება სსკ-ის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189-ე (საავტორო უფლების ხელყოფა) მუხლების ერთობლიობით. ანალოგიურად, „იდენტიფიკაციის ქურდობა“, როდესაც დამნაშავე სხვისი პერსონალური მონაცემების გამოყენებით კრედიტს იღებს, 284-ე (შეღწევა) და 177-ე (ქურდობა) მუხლებით კვალიფიცირდება.[198]

ასეთი მიდგომა პრობლემურია, რადგან ერთიან დანაშაულებრივ ქმედებას ხელოვნურად შლის შემადგენელ ნაწილებად და ნორმათა არასასურველ კონკურენციას იწვევს. კიბერტექნოლოგიების როლი დანაშაულის ჩადენის პროცესში ისეთივე ბუნებრივი და გარდაუვალი ხდება, როგორც, მაგალითად, ცეცხლსასროლი იარაღის გამოყენება, რაც აუცილებლად აყენებს ქმედების დანაშაულთა ერთობლიობით კვალიფიკაციის პრობლემას, რომელიც სამართლებრივ ნორმათა განმარტებით უნდა გადაიჭრას.[199] პრობლემას ისიც ართულებს, რომ კიბერსივრცისთვის დამახასიათებელი ტერმინების

196 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, 8.

197 მინაშვილი ი., ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“, 2019, გვ. 20.

198 იქვე., გვ. 19-20.

199 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 121-127.

ინტერპრეტაცია თავისთავად რთული და ხანგრძლივი პროცესია, რაც კვალიფიკაციის საკითხს კიდევ უფრო ბუნდოვანს ხდის.[200]

ამ პრობლემების ფონზე, სამართლებრივ თეორიაში აქტიურად განიხილება საკითხი, არის თუ არა კიბერდანაშაული სრულიად „ახალი“ დანაშაული, თუ იგი „ძველი ღვინოა ახალ ბოთლებში“.[201] კიბერდანაშაულს მართლაც აქვს უნიკალური მახასიათებლები: დამნაშავეს შეუძლია იმოქმედოს ანონიმურად, მსხვერპლისგან ფიზიკურად დაშორებით და მინიმალური ძალისხმევით ერთდროულად შეუტიოს ათასობით ადამიანს. გარდა ამისა, ციფრული მტკიცებულებები, ტრადიციული დანაშაულის კვალისგან (მაგალითად, თითის ანაბეჭდებისგან) განსხვავებით, ადვილად ნადგურდება და მათი მოპოვება რთულია.[202] ეს მახასიათებლები, ერთი შეხედვით, კიბერდანაშაულის სპეციფიკურობასა და მის დამოუკიდებელ ფენომენად განხილვას ამართლებს.

თუმცა, კიბერდანაშაულის კრიმინალიზაციისას კანონმდებლის მთავარი საზრუნავი ხშირად ის ტრადიციული სამართლებრივი სიკეთეა, რომელსაც საფრთხე ექმნება, და არა თავად ტექნოლოგია. კიბერდანაშაულების კლასიფიკაციაც ხომ ამ პრინციპს ემყარება: დანაშაულები კომპიუტერული მონაცემების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის წინააღმდეგ, კომპიუტერის გამოყენებით ჩადენილი დანაშაულები (მაგალითად, თაღლითობა, გაყალბება) და შინაარსთან დაკავშირებული დანაშაულები (მაგალითად, ბავშვთა პორნოგრაფია).[203] დანაშაულის ობიექტური მხარის ელემენტები (ხერხი, საშუალება), და არა სუბიექტური მხარე, განსაზღვრავს კიბერშემადგენლობათა სპეციფიკას.[204]

ამ ლოგიკიდან გამომდინარე, უფრო გამართლებული ჩანს მიდგომა, რომელიც კიბერდანაშაულს ტრადიციული დანაშაულების გამოვლინების სპეციფიკურ ფორმად განიხილავს და არა სრულიად იზოლირებულ ფენომენად. ასეთ შემთხვევაში, საკანონმდებლო რეგულირება ახალი, დამოუკიდებელი შემადგენლობების უსასრულოდ შექმნის ნაცვლად, კიბერელემენტების

200 იქვე., გვ. 121-127.
201 Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. 2016, 8-11.
202 იქვე., გვ. 8-11.
203 UNITED NATIONS OFFICE ON DRUGS AND CRIME Comprehensive Study on Cybercrime. UNITED NATIONS. 2013, 48-50.
204 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 36-43.

ინტეგრირებას უნდა ისახავდეს მიზნად უკვე არსებულ, ტრადიციულ შემადგენლობებში, რაც „ფიზიკურად ვერ დაიტევს და ვერ გადახარშავს“ სისხლის სამართლის კანონმდებლობას.[205] მაგალითად, კიბერტერორიზმის დამოუკიდებელ შემადგენლობად გამოყოფის ნაცვლად, უფრო ლოგიკური იქნებოდა მისი, როგორც ტერორიზმის მაკვალიფიცირებელი გარემოების, გათვალისწინება. ეს ავტომატურად გადაჭრიდა გაუფრთხილებლობით კიბერტერორიზმის ჩადენის შესაძლებლობის აბსურდულ თეორიულ საკითხსაც, ვინაიდან ტერორიზმი თავისი არსით მხოლოდ განზრახი დანაშაულია.[206]

საყურადღებოა, რომ საერთაშორისო დონეზეც კი არ არსებობს სრული კონსენსუსი კიბერსივრცესთან დაკავშირებული ყველა ქმედების კრიმინალიზაციაზე. მაგალითად, ისეთი ქმედებები, როგორიცაა სპამი, საავტორო უფლებების დარღვევა ან ბავშვთა გრუმინგი, მიუხედავად იმისა, რომ ბევრ ქვეყანაში დასჯადია, არ სარგებლობს იმგვარი საყოველთაო აღიარებით, რომ მათი უპირობო შეტანა საერთაშორისო კონვენციებში მომხდარიყო.[207] ეს გარემოება კიდევ ერთხელ უსვამს ხაზს კიბერდანაშაულის დეფინიციისა და კვალიფიკაციის სირთულეებს. როდესაც საერთაშორისო დონეზეც კი ვერ თანხმდებიან, რა არის დანაშაული, ეროვნულ დონეზე არასისტემური და ფრაგმენტული რეგულირება სამართალგამოყენების პრაქტიკაში კიდევ უფრო მეტ ქაოსს იწვევს.[208]

საბოლოოდ, კიბერდანაშაულისა და სხვა მონათესავე დანაშაულების გამიჯვნის პრობლემა საკანონმდებლო პოლიტიკის საკითხია. არსებული ქაოსური მდგომარეობა, როდესაც კიბერდანაშაულებრივი შემადგენლობები სისხლის სამართლის კოდექსის სხვადასხვა თავშია გაბნეული და ხშირად ერთმანეთსაც ეწინააღმდეგება, სასამართლო პრაქტიკაში სერიოზულ სიძნელეებს ქმნის. კვალიფიკაციის პროცესში ნორმათა კონკურენციის პრობლემის გადაჭრა და დანაშაულთა ერთობლიობის საკითხის სწორად დარეგულირება ერთიანი, ლოგიკური და სისტემური საკანონმდებლო მიდგომის გარეშე შეუძლებელია. დოქტრინაში გამოთქმული მოსაზრება, რომლის თანახმადაც უმჯობესია კიბერელემენტების ინტეგრირება ტრადიციულ

205 იქვე., გვ. 36-43.

206 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 36-43, 121-127.

207 Tennis, M. M. A UNITED NATIONS CONVENTION ON CYBERCRIME. Capital University Law Review. 2020, 48, 24-27.

208 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 121-127.

შემადგენლობებში მაკვალიფიცირებელ გარემოებებად, ამ პრობლემების გადაჭრის ერთ-ერთ რაციონალურ გზად მოჩანს. ეს თავიდან აგვარიდებდა ნორმების არასასურველ კონკურენციასა და ქმედების უსამართლო კვალიფიკაციას რამდენიმე, შინაარსობრივად მსგავსი მუხლით.

თავი III. კიბერდანაშაულის კვალიფიკაციის პრაქტიკული გამოწვევები საქართველოსა და საერთაშორისო პრაქტიკაში

3.1. საქართველოს სასამართლო პრაქტიკის ანალიზი

კიბერდანაშაულის სფეროში არსებული დოქტრინალური პრობლემების პარალელურად, საინტერესოა, თუ როგორ ართმევს თავს ამ გამოწვევებს ქართული მართლმსაჯულება. სასამართლო პრაქტიკის ანალიზი გვაძლევს საშუალებას, დავინახოთ, რამდენად ერთგვაროვანია მიდგომები, რა სახის სირთულეები იკვეთება კონკრეტული დანაშაულების კვალიფიკაციისას და როგორ ხდება კანონის ნორმების ინტერპრეტაცია რეალურ საქმეებში. წინამდებარე ნაწილში სწორედ საქართველოს სასამართლოების მიერ მიღებულ გადაწყვეტილებებს განვიხილავთ, რათა გამოვავლინოთ კიბერდანაშაულის კვალიფიკაციასთან დაკავშირებული ძირითადი ტენდენციები და პრობლემური ასპექტები. ეს ანალიზი დაგვეხმარება იმის შეფასებაში, თუ რამდენად პასუხობს პრაქტიკა თეორიულ დონეზე არსებულ მოლოდინებსა და გამოწვევებს.[209]

სასამართლო პრაქტიკის ანალიზისას ერთ-ერთი პირველი პრობლემა, რომელიც იკვეთება, ე.წ. „DoS“ (Denial-of-service) შეტევების კვალიფიკაციას ეხება. ამ ტიპის დანაშაული ვებგვერდის სერვერზე ერთდროულად ათასობით მოთხოვნის გაგზავნას გულისხმობს, რაც მის პარალიზებას იწვევს.[210] საინტერესოა შალვა ბენდელიანის (სახელი შეცვლილია) საქმე, სადაც პირს ბრალი ედებოდა საინფორმაციო პორტალებზე „presa.ge“ და „droni.ge“ კიბერშეტევის განხორციელებაში. გამოძიების ვერსიით, ბენდელიანმა დაამზადა და გაავრცელა კომპიუტერული პროგრამა, რომელმაც ამ საიტების ფუნქციონირების განზრახ შეფერხება გამოიწვია. საბოლოოდ, სასამართლომ მისი ქმედება საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლის პირველი ნაწილით გათვალისწინებულ დანაშაულად შეაფასა, რაც კომპიუტერული პროგრამის უნებართვო დამზადებასა და გავრცელებას გულისხმობს კიბერდანაშაულის ჩადენის მიზნით.[211]

---

209 ამაშუკელი გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 36.

210 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 72.

211 იქვე., გვ. 72-73.

თუმცა, ამავე საქმეში პრობლემურია, თუ რატომ არ მოხდა ქმედების დამატებით კვალიფიკაცია სსკ-ის 286-ე მუხლით, რომელიც კომპიუტერული მონაცემის უნებართვო დაზიანებას, წაშლას, შეცვლას ან გადაცემას ეხება, რამაც კომპიუტერული სისტემის ფუნქციონირების მნიშვნელოვანი შეფერხება გამოიწვია. როგორც ჩანს, მთავარი სირთულე ტერმინ „უნებართვობის“ განმარტებამ შექმნა. ვინაიდან საინფორმაციო ვებგვერდები საჯაროა და ნებისმიერ მომხმარებელს შეუძლია მათზე შესვლა, რთული დასამტკიცებელია, რომ ათასობით მოთხოვნის გაგზავნა „უნებართვო“ ქმედება იყო. ამ ლოგიკით, მაშინაც კი, თუკი დადასტურდება, რომ სისტემის მუშაობა განზრახ და მნიშვნელოვნად შეფერხდა, ქმედების „უნებართვობის“ კომპონენტის არარსებობის გამო, 286-ე მუხლის გამოყენება კითხვის ნიშნის ქვეშ დგება.[212] ეს შემთხვევა ნათლად აჩვენებს, როგორ შეიძლება დოქტრინალურმა გაურკვევლობამ კონკრეტული ნორმის გამოყენება პრაქტიკაში გაართულოს.

კვალიფიკაციის პრობლემები ჩნდება სსკ-ის 286-ე მუხლის სხვა ნაწილების გამოყენებისასაც, განსაკუთრებით მაშინ, როდესაც საქმე ეხება „კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვან შეფერხებას“. სასამართლო პრაქტიკიდან ცნობილია ორი საქმე, სადაც პირთა ჯგუფს ბრალი ედებოდა კომპიუტერული მონაცემის უნებართვო შეცვლაში. პირველ შემთხვევაში, საუბარი იყო საკონტროლო-სალარო აპარატის ფისკალური მეხსიერების შეცვლაზე, გადასახადებისთვის თავის არიდების მიზნით.[213] მეორე შემთხვევაში კი, პირებმა ავტომანქანის გავლილი მანძილის მაჩვენებელი შეცვალეს. ორივე შემთხვევაში სასამართლომ გამოიყენა სსკ-ის 286-ე მუხლის მე-3 ნაწილი და დაადგინა, რომ მონაცემთა შეცვლამ კომპიუტერული სისტემის „მნიშვნელოვანი შეფერხება“ გამოიწვია.[214]

სალარო აპარატის შემთხვევაში სასამართლოს ლოგიკა მეტ-ნაკლებად გასაგებია, რადგან მონაცემთა სისწორე პირდაპირ კავშირშია საგადასახადო ვალდებულებებთან, მაგრამ ავტომანქანის გარბენის მაჩვენებლის შეცვლისას სრულიად გაუგებარია, როგორ გამოიწვია ამ ქმედებამ კომპიუტერული სისტემის „მნიშვნელოვანი შეფერხება“.[215] ეს მაგალითი კარგად წარმოაჩენს, თუ როგორ ხდება საკანონმდებლო ტერმინის ფართო და ზოგჯერ დაუსაბუთებელი

212 იქვე., გვ. 71-73.
213 იქვე., გვ. 73-74.
214 იქვე., გვ. 82-83.
215 იქვე., გვ. 83.

ინტერპრეტაცია, რაც არაერთგვაროვანი პრაქტიკის ჩამოყალიბებას უწყობს ხელს. ასეთი მიდგომა ქმნის რისკს, რომ დანაშაულის კვალიფიკაცია მოსამართლის სუბიექტურ შეფასებაზე გახდეს დამოკიდებული და არა კანონის ზუსტ და მკაცრ მოთხოვნებზე, რაც საბოლოო ჯამში მართლმსაჯულების პროგნოზირებადობას ამცირებს.

სასამართლო პრაქტიკაში კიბერდანაშაულთა კვალიფიკაციისას ხშირად ვხვდებით დანაშაულთა ერთობლიობას, როდესაც ერთი დანაშაულებრივი სქემის ფარგლებში ჩადენილი ქმედებები რამდენიმე მუხლით კვალიფიცირდება. ამის ნათელი მაგალითია თბილისის საქალაქო სასამართლოს 2019 წლის 11 დეკემბრის განაჩენი[216] ორგანიზებული ჯგუფის მიერ ჩადენილი კიბერდანაშაულის საქმეზე. დანაშაულებრივი სქემა მოიცავდა ე.წ. „ფიშინგის“ გზით ამერიკული კომპანიების საბანკო ანგარიშებიდან თანხების ქურდობას, რისთვისაც ბრალდებულები იყენებდნენ სპეციალურად მოდიფიცირებულ ვირუსს („G-----“), „კრიპტერებს“ (ვირუსის დამშიფრავებს) და „სპამერებს“ (ვირუსის გამავრცელებლებს).[217] დაზარალებულები იღებდნენ წერილს, რომელიც თითქოს ბანკისგან იყო გამოგზავნილი, ხსნიდნენ მასზე მიბმულ ბმულს, რის შედეგადაც მათი კომპიუტერი ვირუსით ინფიცირდებოდა და დამნაშავეები ინტერნეტბანკის მონაცემებს ეუფლებოდნენ.[218] ჯამში, ჯგუფმა 1,260,521.69 აშშ დოლარის დაუფლება სცადა, საიდანაც რეალურად 316,955.12 აშშ დოლარის მითვისება მოახერხა.[219]

ამ რთულ საქმეში სასამართლომ ბრალდებულების ქმედებები დანაშაულთა ერთობლიობად შეაფასა და სისხლის სამართლის კოდექსის ოთხი სხვადასხვა მუხლი გამოიყენა: 284-ე (კომპიუტერული პროგრამის უნებართვო დამზადება, შენახვა და გავრცელება), 158-ე (კომპიუტერული მონაცემების უნებართვო შენახვა, გამოყენება და გავრცელება), 285-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა დიდი ოდენობით, ჩადენილი ორგანიზებული ჯგუფის მიერ).[220] ეს მიდგომა, როდესაც ერთი ქმედება რამდენიმე შემადგენლობით კვალიფიცირდება, პრაქტიკოს სამართალდამცველებში საკმაოდ გავრცელებულია. მაგალითად, ერთ-ერთ

216 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631.
217 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 3-4.
218 თბილისის საქალაქო სასამართლო, 2019 გადაწყვეტილება, 7-9.
219 თბილისის საქალაქო სასამართლო, 2019 გადაწყვეტილება, 8, 22.
220 თბილისის საქალაქო სასამართლო, 2019 გადაწყვეტილება, 27.

კვლევაში, რომელიც შსს-ს გამომძიებლებში ჩატარდა, გამოკითხულთა 56% მხარს უჭერს კიბერდანაშაულისა და, მაგალითად, თაღლითობის შემადგენლობების ერთობლიობით კვალიფიკაციას.[221]

თუმცა, სწორედ ეს პრაქტიკა აჩენს კითხვებს ნორმათა კონკურენციისა და სამართლიანი კვალიფიკაციის შესახებ. როდესაც კანონმდებლობაში კომპიუტერული დანაშაულისთვის სპეციალური ნორმები არსებობს, რამდენად გამართლებულია ამავე ქმედების ზოგადი ნორმით (მაგალითად, ქურდობით) კვალიფიკაციაც? ამგვარი მიდგომა „უსამართლო კვალიფიკაციის“ რისკს ქმნის, როდესაც ერთი და იმავე შინაარსის ქმედება ორი სხვადასხვა შემადგენლობით ფასდება.[222] ამ პრობლემის თავიდან ასაცილებლად, ზოგიერთი მკვლევარი გვთავაზობს, რომ კიბერდანაშაულის ელემენტები დამამძიმებელ გარემოებად გაითვალისწინონ უკვე არსებულ, ტრადიციულ შემადგენლობებში და არა ცალკე დანაშაულად. ეს მიდგომა თავიდან აგვარიდებდა ნორმათა არასასურველ კონკურენციას და, ამავდროულად, ხელს შეუწყობდა კვალიფიკაციის პროცესის გამარტივებასა და ერთგვაროვანი სასამართლო პრაქტიკის დამკვიდრებას.[223]

სასამართლო პრაქტიკაში კიბერდანაშაულთა სუბიექტური მხარის შეფასებისას, როგორც წესი, საქმე გვაქვს განზრახ დანაშაულებთან. ევროპის საბჭოს კონვენციაც კი მიუთითებს, რომ დასჯადი უნდა იყოს განზრახ ჩადენილი კომპიუტერული დანაშაული.[224] საქართველოს სისხლის სამართლის კოდექსის მე-9 მუხლის მიხედვით, განზრახვა ქმედების ცოდნას, ნებელობასა და მართლწინააღმდეგობის შეგნებას გულისხმობს.[225] მაგალითად, საქმეში, სადაც მოქალაქე ბ. დიდავამ ინტერნეტკაფეში დაიმახსოვრა სხვა პირის მომხმარებლის სახელი და პაროლი, ხოლო შემდეგ მის პირად გვერდზე უნებართვოდ შევიდა, სასამართლომ ქმედება სსკ-ის 284-ე მუხლით შეაფასა. ამ შემთხვევაში აშკარად იკვეთება პირდაპირი განზრახვა, რადგან ბრალდებულის

221 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 151.
222 ამაშუკელი გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 36.
223 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 37.
224 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 85.
225 იქვე., გვ. 85-86.

ნებელობა და ქმედების წინასწარი მომზადება (პაროლის დამახსოვრება) თვალსაჩინო იყო.[226]

მიუხედავად იმისა, რომ პრაქტიკაში ძირითადად განზრახ დანაშაულებს ვხვდებით, საყურადღებოა, რომ სამართალდამცველებში არსებობს მყარი აზრი გაუფრთხილებლობით ჩადენილი კიბერდანაშაულის კრიმინალიზაციის აუცილებლობის შესახებ. ამაშუკელის მიერ ჩატარებულ კვლევაში, გამოკითხული 145 გამომძიებლიდან ყველა (100%) კატეგორიულად ემხრობა გაუფრთხილებლობის ინსტიტუტის კრიმინალიზებას ამ სფეროში.[227] ეს განსაკუთრებით აქტუალური შეიძლება გახდეს ისეთ სფეროებში, როგორიცაა სატრანსპორტო ან ენერგეტიკული სისტემების მართვა, სადაც კიბერტექნოლოგიებისადმი გაუფრთხილებელმა დამოკიდებულებამ შესაძლოა მძიმე შედეგები გამოიწვიოს.[228] ამ ეტაპზე ქართული სასამართლო პრაქტიკა ამ მიმართულებით ჩამოყალიბებული არ არის, რაც ლოგიკურიცაა, რადგან მოქმედი კანონმდებლობა ძირითადად განზრახ ქმედებებზეა ორიენტირებული. თუმცა, პრაქტიკოსთა ეს მოთხოვნა მომავლის გამოწვევაზე მიუთითებს, რომელზეც კანონმდებელსა და სასამართლოს პასუხის გაცემა მოუწევთ.

სასამართლო პრაქტიკის განხილვისას ასევე აღსანიშნავია, რომ სასამართლოები კიბერდანაშაულს, განსაკუთრებით მის ტრანსნაციონალურ ფორმებს, სოციალურად მომეტებული საფრთხის მქონე ქმედებად აფასებენ. მაგალითად, უკვე ნახსენებ 2019 წლის განაჩენში სასამართლო პირდაპირ მიუთითებს, რომ ბრალდებულის მიერ ჩადენილი კიბერდანაშაული „ატარებს ტრანსნაციონალურ ხასიათს და საფრთხეს უქმნის მსოფლიო საბანკო სისტემის ნორმალურ ფუნქციონირებასა და ბანკში დაცულ საკუთრებას“.[229] ასეთი შეფასება გავლენას ახდენს სასჯელის ზომის განსაზღვრაზე და ხაზს უსვამს ამ ტიპის დანაშაულების წინააღმდეგ ბრძოლის მნიშვნელობას. თუმცა, სასჯელის შეფარდებისას, სასამართლოები ითვალისწინებენ ისეთ შემამსუბუქებელ გარემოებებსაც, როგორიცაა, მაგალითად, ბრალდებულის ჯანმრთელობის

226 იქვე., გვ. 86.
227 ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 151.
228 იქვე., გვ. 37.
229 თბილისის საქალაქო სასამართლოს 2019 წლის გადაწყვეტილება #330100119003053631, გვ. 28.

მძიმე მდგომარეობა, რამაც შეიძლება სასჯელის მოხდის პირობებზე იქონიოს გავლენა.[230]

ამავე დროს, სასამართლო პრაქტიკა აჩვენებს, რომ საქართველოს სისხლის სამართლის კანონმდებლობაში არსებული ხარვეზები პირდაპირ აისახება გამოძიებასა და საბოლოო განაჩენებზე. მაგალითად, როდესაც 2008 წლის აგვისტოს ომის დროს ქართულ სამთავრობო საიტებზე კიბერიერიში განხორციელდა, გამოძიება, როგორც ჩანს, არ დაწყებულა საბოტაჟის მუხლით (სსკ-ის 318-ე), მიუხედავად იმისა, რომ ასეთი ქმედება, განსაკუთრებით ომის პირობებში, სასიცოცხლო ობიექტების მწყობრიდან გამოყვანას ისახავდა მიზნად.[231] ეს ფაქტი მიუთითებს როგორც საგამოძიებო ორგანოების, ისე ზოგადად სამართლებრივი სისტემის მოუმზადებლობაზე, ადეკვატურად უპასუხოს კიბერაგრესიის ახალ ფორმებს. ასეთ შემთხვევებში, სწორი კვალიფიკაციის არარსებობა დამნაშავეთა იდენტიფიკაციასაც ართულებს და მომავალში მსგავსი ქმედებების პრევენციასაც.

საბოლოოდ, საქართველოს სასამართლო პრაქტიკის ანალიზი გვიჩვენებს, რომ კიბერდანაშაულის კვალიფიკაცია კვლავ რჩება ერთ-ერთ მთავარ გამოწვევად. მართალია, სასამართლოები აქტიურად იყენებენ როგორც სპეციალურ (კიბერდანაშაულის თავი), ისე ზოგად მუხლებს, მაგრამ კვალიფიკაციის პროცესში არსებითი პრობლემები იკვეთება. კერძოდ, პრობლემურია ისეთი ცნებების განმარტება, როგორიცაა „უნებართვობა“ და „მნიშვნელოვანი შეფერხება“, რაც არაერთგვაროვანი და ზოგჯერ საკამათო გადაწყვეტილებების საფუძველი ხდება. ასევე, დანაშაულთა ერთობლიობით კვალიფიკაციის გავრცელებული პრაქტიკა აჩენს კითხვებს ნორმათა კონკურენციისა და ორმაგი დასჯის თავიდან აცილების პრინციპთან დაკავშირებით. პრაქტიკა ძირითადად განზრახ დანაშაულებზეა ფოკუსირებული, მაშინ როცა სამართალდამცველები გაუფრთხილებლობითი კიბერდანაშაულის კრიმინალიზაციის საჭიროებაზე მიუთითებენ. ეს ყველაფერი ცხადყოფს, რომ კიბერსივრცეში ჩადენილ ქმედებათა სამართლებრივი რეგულირება და

230 თბილისის საქალაქო სასამართლო, 2019 გადაწყვეტილება, 28-29.

231 ზაქაშვილი უ., კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2013, გვ. 70-71.

სასამართლო პრაქტიკის დახვეწა კვლავაც აქტუალურ ამოცანად რჩება ქართული მართლმსაჯულებისთვის.[232]

3.2. ევროპული სასამართლოსა და უცხო ქვეყნების პრაქტიკა

კიბერდანაშაულის გამოძიება და კვალიფიკაცია რთულ სამართლებრივ საკითხებს წარმოშობს, განსაკუთრებით პირადი ცხოვრების ხელშეუხებლობის უფლებასთან მიმართებით. ადამიანის უფლებათა ევროპული სასამართლო (ECHR) ამ საკითხს კონვენციის მე-8 მუხლის ჭრილში განიხილავს, რომელიც პირადი და ოჯახური ცხოვრების, საცხოვრისისა და მიმოწერა-კომუნიკაციის პატივისცემის უფლებას იცავს. ეს უფლება აბსოლუტური არ არის და შეიძლება შეიზღუდოს, მაგალითად, დანაშაულის პრევენციის მიზნით, მაგრამ ნებისმიერი ასეთი ჩარევა კანონით უნდა იყოს გათვალისწინებული, დემოკრატიულ საზოგადოებაში აუცილებელი და პროპორციული.[233] ევროპული სასამართლოს პრაქტიკით, გამოძიების ფარგლებში განხორციელებული ღონისძიებები, მათ შორის, ფარული მოსმენა, კანონის ზუსტ და მკაფიო საფუძველს უნდა ეყრდნობოდეს, რათა თვითნებური ჩარევა გამოირიცხოს. მაგალითად, საქმეში Khan v. the United Kingdom, სასამართლომ მე-8 მუხლის დარღვევა დაადგინა, რადგან ფარული მოსასმენი მოწყობილობების გამოყენება კანონით კი არა, მხოლოდ მინისტრის დეპარტამენტის გაიდლაინებით რეგულირდებოდა.[234]

ევროპული სასამართლო სულ უფრო მეტ ყურადღებას უთმობს ონლაინ სივრცეში ჩადენილ ძალადობასა და სახელმწიფოს პოზიტიურ ვალდებულებებს. საქმეში M.Ș.D. v. ROMANIA, რომელიც ყოფილი პარტნიორის მიერ ინტიმური ფოტოების შურისძიების მოტივით გავრცელებას ეხებოდა, სასამართლომ დაადგინა, რომ ადამიანის დამცირებისკენ მიმართული მსგავსი ქმედებები იმდენად სერიოზულია, რომ სახელმწიფოსგან სისხლისსამართლებრივ რეაგირებას მოითხოვს.[235] სასამართლოს შეფასებით, ასეთ დროს სამოქალაქო-სამართლებრივი დაცვის მექანიზმები არასაკმარისია და სახელმწიფოს აკისრია ვალდებულება, შექმნას და ეფექტიანად გამოიყენოს კანონმდებლობა,

232 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022. URL (accessed 07.06.2026).; ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013. URL (accessed 07.06.2026).

233 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, გვ. 195. URL (accessed 07.06.2026).

234 იქვე.

235 CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024, par. 24-26. URL (accessed 07.06.2026).

რომელიც ონლაინ ძალადობის ყველა ფორმას დასჯადს გახდის.[236] ამავე საქმეში სასამართლომ ხაზგასმით აღნიშნა გამოძიების არაეფექტიანობა და გაჭიანურება, რაც, მისივე შეფასებით, დაუსჯელობის განცდას აძლიერებს და სახელმწიფოს პოზიტიური ვალდებულების შეუსრულებლობას წარმოადგენს.[237] მსგავსი პოზიცია ჩანს საქმეში AYTAJ AHMADOVA v. AZERBAIJAN, სადაც სასამართლომ კვლავ გაუსვა ხაზი სახელმწიფოს ვალდებულებას, ჩაატაროს სწრაფი და ეფექტიანი გამოძიება კიბერსივრცეში პირადი ცხოვრების ხელყოფის ფაქტებზე.[238] ეს სტანდარტები პირდაპირ ეხება საქართველოსაც, სადაც, მაგალითად, კიბერგადაკიდება ცალკე დანაშაულად არ არის მიჩნეული და სხვა, ზოგადი მუხლებით კვალიფიცირდება, რაც, შესაძლოა, არაეფექტიანი იყოს.[239]

ამერიკის შეერთებული შტატების კანონმდებლობა კიბერდანაშაულის მიმართ ერთ-ერთი ყველაზე მკაცრი და დეტალურია. 1986 წელს მიღებული „კომპიუტერთან დაკავშირებული თაღლითობისა და მისი ბოროტად გამოყენების შესახებ“ კანონი მრავალჯერ შეიცვალა და ახალი შემადგენლობებით შეივსო.[240] აშშ-ის კანონმდებლობა, გერმანულ-რომანული სამართლისგან განსხვავებით, კიბერდანაშაულის გაუფრთხილებლობით ჩადენის ფორმასაც ცნობს და უმკაცრეს სანქციებს ითვალისწინებს, ზოგჯერ 30 წლამდე თავისუფლების აღკვეთასაც კი პირობით ვადამდე გათავისუფლების უფლების გარეშე.[241] აღსანიშნავია, რომ ფედერალური კანონმდებლობის გარდა, ცალკეულ შტატებს, მაგალითად, ფლორიდასა და ტეხასს, საკუთარი კანონები აქვთ, სადაც დეტალურადაა განმარტებული ისეთი ტერმინები, როგორიცაა „კომპიუტერული ვირუსი“, „ზიანი“, „ხელმისაწვდომობა“ და სხვა, რაც კანონის გამოყენებას აადვილებს და ორაზროვნებას გამორიცხავს.[242] ეს განსხვავდება ქართული რეალობისგან, სადაც სპეციფიკური ტერმინოლოგიის ნაკლებობა კვლავ პრობლემად რჩება.[243]

---

236 CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024, par. 22-24. URL (accessed 07.06.2026).

237 CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024, par. 31-34. URL (accessed 07.06.2026).

238 CASE OF AYTAJ AHMADOVA v. AZERBAIJAN [ECtHR], 2025, par. 12-14. URL (accessed 07.06.2026).

239 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 21. URL (accessed 07.06.2026).

240 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 82-87. URL (accessed 07.06.2026).

241 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 82. URL (accessed 07.06.2026).

242 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 87. URL (accessed 07.06.2026).

243 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 24. URL (accessed 07.06.2026).

გერმანიის სისხლის სამართლის კოდექსიც დეტალურად არეგულირებს კიბერდანაშაულს. მაგალითად, 303-ე მუხლის „ა“ პუნქტი სჯის მონაცემების მართლსაწინააღმდეგო წაშლას ან დამალვას, ხოლო „ბ“ პუნქტი - სხვისთვის მნიშვნელოვანი მონაცემების დამუშავების პროცესში ხელის შეშლას.[244] 202b მუხლი კი კრძალავს მონაცემების ხელში ჩაგდებას არასაჯარო გადაცემის პროცესში, მაგალითად, უკაბელო ინტერნეტის ან ელექტრონული ფოსტის საშუალებით.[245] გერმანიაში ასევე კარგად არის განვითარებული ინსტიტუციური სისტემა: 2011 წელს შეიქმნა ეროვნული კიბერთავდაცვის ცენტრი (NCAZ), რომელიც კოორდინაციას უწევს სხვადასხვა სამთავრობო უწყების, მათ შორის, თავდაცვის სამინისტროსა და პოლიციის საქმიანობას. ამასთან, ფუნქციონირებს ინფორმაციული უსაფრთხოების ფედერალური ოფისი (BSI) 400-ზე მეტი თანამშრომლით.[246]

დიდი ბრიტანეთის მიდგომა გერმანულის მსგავსია და 1990 წლიდან მოქმედებს კანონი „კომპიუტერული ტექნოლოგიის არასანქცირებული გამოყენების შესახებ“ (Computer Misuse Act), რომელიც დასჯადად აცხადებს კომპიუტერში უნებართვო შეღწევას, ინფორმაციის ბლოკირებას, მოდიფიცირებასა და კოპირებას.[247] 2011 წელს დიდმა ბრიტანეთმა კიბერდანაშაულის შესახებ ევროპის საბჭოს კონვენციის რატიფიცირებით კანონმდებლობის ჰარმონიზაციისკენ არსებითი ნაბიჯი გადადგა.[248] ბრიტანეთშიც, გერმანიის მსგავსად, შექმნილია სპეციალიზებული სტრუქტურები, როგორიცაა „კიბერ-ოპერაციებისგან თავდაცვის ჯგუფი“ თავდაცვის სამინისტროს დაქვემდებარებაში.[249]

ქართული და უცხოური სასამართლო პრაქტიკის შედარებისას საინტერესო განსხვავებები იკვეთება. მაგალითად, თბილისის საქალაქო სასამართლოს 2019 წლის ერთ-ერთ საქმეში[250] ბრალდებულებს ედავებოდნენ რთული,

---

244 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 36. URL (accessed 07.06.2026).

245 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 37. URL (accessed 07.06.2026).

246 იქვე.

247 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 38. URL (accessed 07.06.2026).

248 ამაშუკელი, გ. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. 2022, გვ. 82-87. URL (accessed 07.06.2026).

249 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 39. URL (accessed 07.06.2026).

250 თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631.

ორგანიზებული სქემის შექმნას, რომელიც მოიცავდა ვირუსის შექმნასა და მოდიფიცირებას, ე.წ. „კრიპტერების“ (დამშიფრავების) და „სპამერების“ (გამავრცელებლების) გამოყენებას, დაზარალებულთა საბანკო ანგარიშებიდან თანხების მოპარვასა და შემდეგ ე.წ. „დროპერების“ (განმაღდებლების) მეშვეობით მის ლეგალიზაციას.[251] სასამართლომ ბრალდებულები დამნაშავედ ცნო სსკ-ის რამდენიმე მუხლით, მათ შორის, კომპიუტერულ სისტემაში უნებართვო შეღწევისთვის (284-ე მუხლი), კომპიუტერული მონაცემების უნებართვო გამოყენებისთვის (158-ე მუხლი) და ქურდობისთვის (177-ე მუხლი).[252] ეს საქმე აჩვენებს, რომ ქართული მართლმსაჯულება რთულ ტრანსნაციონალურ კიბერდანაშაულებს არსებული კანონმდებლობის ფარგლებში განიხილავს, თუმცა, როგორც წესი, კვალიფიკაცია რამდენიმე ზოგადი მუხლის ერთობლიობით ხდება.

ქართულ კანონმდებლობაში არსებულ ხარვეზებზე მკვლევრებიც მიუთითებენ. მაგალითად, ე.წ. „DoS“ (Denial-of-Service) შეტევის კვალიფიკაცია პრობლემურია, რადგან ასეთი შეტევა საიტზე ერთდროულად ათასობით მოთხოვნის გაგზავნას გულისხმობს, რაც თავისთავად „უნებართვო“ ქმედებად ძნელად განიხილება, რადგან საჯარო ვებგვერდზე შესვლა ყველასთვის ხელმისაწვდომია. ამიტომ არსებული 286-ე მუხლი, რომელიც კომპიუტერული მონაცემის უნებართვო გადაცემას ეხება, შესაძლოა, „DoS“ შეტევას ვერ მოერგოს.[253] ამ პრობლემის გადასაჭრელად ზოგიერთი ავტორი „DoS“ შეტევისთვის ცალკე მუხლის შემოღებას მიიჩნევს მიზანშეწონილად.[254]

იურისდიქციის საკითხიც ერთ-ერთი მთავარი გამოწვევაა, რადგან კიბერდანაშაული ხშირად ტრანსსასაზღვრო ხასიათისაა. ამერიკულ პრაქტიკაში ცნობილია Microsoft Ireland-ის საქმე, სადაც აშშ-ის სასამართლომ ირლანდიაში მდებარე სერვერზე შენახული ელექტრონული ფოსტის მონაცემების გადაცემა მოითხოვა. ამ საქმემ საბოლოოდ „CLOUD Act“-ის მიღება დააჩქარა, რომელიც ამერიკულ სამართალდამცავ ორგანოებს უფლებას აძლევს, მოითხოვონ

---

251 თბილისის საქალაქო სასამართლო. თბილისის საქალაქო სასამართლო გადაწყვეტილება #330100119003053631, გვ. 26-35. URL (accessed 07.06.2026).

252 თბილისის საქალაქო სასამართლო. თბილისის საქალაქო სასამართლო გადაწყვეტილება #330100119003053631, გვ. 1-9. URL (accessed 07.06.2026).

253 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 71-72. URL (accessed 07.06.2026).

254 ზაქაშვილი, უ. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 2013, გვ. 72. URL (accessed 07.06.2026).

მონაცემები ამერიკული კომპანიებისგან, მიუხედავად იმისა, თუ სად ინახება ეს მონაცემები ფიზიკურად.[255] ბუდაპეშტის კონვენციაც, რომლის ხელმომწერიც საქართველოა, არეგულირებს იურისდიქციის საკითხებს და ადგენს, რომ ქვეყანას იურისდიქცია აქვს, თუ დანაშაული მის ტერიტორიაზე, მის დროშით მცურავ გემზე, მის კანონმდებლობით რეგისტრირებულ თვითმფრინავზე ან მისი მოქალაქის მიერაა ჩადენილი.[256]

უცხოური და საერთაშორისო პრაქტიკის ანალიზი საქართველოსთვის რამდენიმე დასკვნის გამოტანის საშუალებას იძლევა. პირველ რიგში, ევროპული სასამართლოს სტანდარტები, განსაკუთრებით მე-8 მუხლთან დაკავშირებით, პირდაპირ ავალდებულებს საქართველოს, უზრუნველყოს პირადი ცხოვრების დაცვის ეფექტიანი მექანიზმები კიბერსივრცეში და სათანადოდ მოახდინოს რეაგირება ონლაინ ძალადობაზე. მეორეც, აშშ-ის, გერმანიისა და დიდი ბრიტანეთის გამოცდილება დეტალური, სპეციფიკური კანონმდებლობისა და ძლიერი ინსტიტუციური ბაზის შექმნის აუცილებლობაზე მიუთითებს. ქართულმა კანონმდებლობამ, მიზანშეწონილია, გაითვალისწინოს ამ ქვეყნების მოდელები ისეთი ქმედებების კრიმინალიზაციისთვის, როგორიცაა „DoS“ შეტევები ან კიბერგადაკიდება, და დახვეწოს ტერმინოლოგია. საერთაშორისო თანამშრომლობა და კანონმდებლობის ჰარმონიზაცია ბუდაპეშტის კონვენციის ფარგლებში აუცილებელია, რადგან კიბერდანაშაულთან ბრძოლა ერთი ქვეყნის ძალისხმევით შეუძლებელია.[257]

3.3. მტკიცებულებითი სტანდარტები და გამოძიების სირთულეები

კიბერდანაშაულის გამოძიება ტრადიციული კრიმინალისტიკისგან არსებითად განსხვავებულ გამოწვევებს აწყდება, რაც, პირველ რიგში, მტკიცებულებათა სპეციფიკური ბუნებითაა განპირობებული. თუ ტრადიციულ დანაშაულში საქმე გვაქვს ფიზიკურ, მატერიალურ ობიექტებთან, კიბერდანაშაულის მთავარი ბირთვი ციფრული საგანი, ანუ ციფრული ინფორმაციაა.[258] სწორედ ეს ციფრული ინფორმაცია, რომელიც სასამართლო

255 Mustaque, A. M. Jurisdictional Issues in Adjudication of Cyber Crimes. High Court of Kerala. 2000, გვ. 13. URL (accessed 07.06.2026).

256 Mustaque, A. M. Jurisdictional Issues in Adjudication of Cyber Crimes. High Court of Kerala. 2000, გვ. 23. URL (accessed 07.06.2026).

257 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, გვ. 201-202. URL (accessed 07.06.2026).

258 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 9-10. URL (accessed 07.06.2026).

პროცესში მტკიცებულების სახეს იძენს, ქმნის მთავარ სირთულეს. ფიზიკური ნივთებისგან განსხვავებით, რომელთა დეგრადაციაც ყოველი კოპირებისას ხდება, ციფრული მონაცემის უსასრულოდ გამრავლებაა შესაძლებელი ხარისხის გაუარესების გარეშე, რაც მას გაყალბებისადმი მეტად მოწყვლადს ხდის.[259] ამიტომაც კიბერდანაშაულის გამოძიების ეფექტიანობა პირდაპირაა დამოკიდებული იმ მეთოდებსა და სტანდარტებზე, რომლებითაც ხდება ციფრული მტკიცებულებების მოპოვება, შენახვა და ანალიზი.

ციფრული მტკიცებულების ცნება საკმაოდ ფართოა და მოიცავს ნებისმიერ მონაცემს, რომელიც შექმნილი, შენახული ან გადაცემულია კომპიუტერული სისტემის მიერ და საქმის გადაწყვეტისთვის შესაბამის ინფორმაციას შეიცავს.[260] ეს შეიძლება იყოს ელექტრონული ფოსტა, ციფრული ფოტოები, ბანკომატის ტრანზაქციების ჩანაწერები, ტექსტური დოკუმენტები, ინტერნეტბრაუზერის ისტორია და სხვა.[261] კრიმინალისტიკური თვალსაზრისით, მათი კლასიფიკაცია საყურადღებოა. მაგალითად, ერთმანეთისგან უნდა განვასხვავოთ „სტატიკური მონაცემები“, რომლებიც მყარ დისკზე ან სერვერზე ინახება, და „დინამიკური“, ანუ „ტრანზიტული მონაცემები“, რომლებიც გადაცემის პროცესშია.[262] განსაკუთრებით პრობლემურია „არასტაბილური მონაცემების“ (Volatile Data) შენახვა, რადგან ისინი ძალიან მცირე დროით ინახება და მარტივად იშლება ან იცვლება; ასეთებია, მაგალითად, ოპერატიული მეხსიერების (RAM) შიგთავსი, ქეშირებული ფაილები, გახსნილი ქსელური კავშირები ან პაროლები.[263] ასევე, არსებობს დაყოფა შინაარსის მიხედვით: „შიგთავსის მონაცემები“ (Content data), რომელიც კომუნიკაციის არსს მოიცავს, და „მეტამონაცემები“ (Metadata), რომელიც ინფორმაციას გვაწვდის თავად კომუნიკაციის შესახებ, მაგალითად, მისი წარმომავლობა, დანიშნულება, დრო, ზომა და ხანგრძლივობა.[264] სწორედ

259 Coupland, H. Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 16. URL (accessed 07.06.2026).
260 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, გვ. 161. URL (accessed 07.06.2026).
261 Stoilkovski, M. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. 2022, გვ. 22. URL (accessed 07.06.2026).
262 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, გვ. 161. URL (accessed 07.06.2026).
263 Stoilkovski, M. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. 2022, გვ. 29. URL (accessed 07.06.2026).
264 Bussolati, N. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. 2020, გვ. 161. URL (accessed 07.06.2026).

ამ მრავალფეროვნებისა და არასტაბილურობის გამო ციფრული მტკიცებულებების მოპოვება განსაკუთრებულ სიფრთხილეს მოითხოვს.

ციფრული მტკიცებულების დასაშვებობის საკითხი სასამართლოში ერთ-ერთ მთავარ გამოწვევად რჩება. იმისათვის, რომ ციფრული მონაცემი სასამართლომ დასაშვებ მტკიცებულებად ცნოს, ის რამდენიმე მკაცრ კრიტერიუმს უნდა აკმაყოფილებდეს. პირველ რიგში, აუცილებელია მისი ავთენტურობისა და მთლიანობის (Integrity) დამტკიცება, ანუ იმის ჩვენება, რომ მტკიცებულება თავდაპირველი სახითაა წარმოდგენილი და მისი შეცვლა ან გაყალბება არ მომხდარა.[265] გამოკითხული ქვეყნების დაახლოებით 70%-ში ელექტრონული მტკიცებულების დასაშვებობა სწორედ მონაცემთა მთლიანობის დემონსტრირებაზე, სასამართლოს დისკრეციასა და მოპოვების კანონიერ პროცედურებზეა დამოკიდებული.[266] ამასთან, ზოგიერთ ქვეყანაში ელექტრონული მტკიცებულება საერთოდ დაუშვებლად მიიჩნევა, რაც კიბერდანაშაულის წარმატებით გამოძიებისთვის სერიოზულ დაბრკოლებას ქმნის.[267] აუცილებელია, რომ მტკიცებულებაზე ჩატარებული ანალიზი სრულ სურათს ასახავდეს და არ იყოს რომელიმე მხარისთვის სასურველ პერსპექტივაზე მორგებული; ასევე, მისი მოპოვების მეთოდები სამართლიანი და პროპორციული უნდა იყოს.[268]

მტკიცებულების ავთენტურობის უზრუნველყოფის მთავარი მექანიზმი მტკიცებულებათა ჯაჭვის (Chain of Custody) ზედმიწევნით დაცვაა. ეს არის დოკუმენტირებული ჩანაწერი მტკიცებულების მოძრაობისა და მასთან შეხების შესახებ, რომელიც მის მთლიანობასა და სასამართლოში დასაშვებობას უზრუნველყოფს.[269] ციფრულ სამყაროში ამ პრინციპის დაცვა განსაკუთრებით რთულია, რადგან მტკიცებულება ხშირად რამდენიმე იურისდიქციას კვეთს, რაც მის გაყალბებასა და მანიპულაციას აადვილებს.[270] მტკიცებულებათა ჯაჭვის

265 Stoilkovski, M. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. 2022, გვ. 32. URL (accessed 07.06.2026).
266 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS. 2013, გვ. 196. URL (accessed 07.06.2026).
267 UNITED NATIONS OFFICE ON DRUGS AND CRIME. Comprehensive Study on Cybercrime. UNITED NATIONS. 2013, გვ. 195. URL (accessed 07.06.2026).
268 Stoilkovski, M. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. 2022, გვ. 32. URL (accessed 07.06.2026).
269 MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. DIGITAL NOTES ON CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS. MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. 2024, გვ. 110-116. URL (accessed 07.06.2026).
270 Coupland, H. Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 16. URL (accessed

მთავარი ელემენტებია: დეტალური დოკუმენტაცია (შეგროვების, შენახვისა და გადაცემის თარიღი, დრო, ადგილი, მონაწილე პირები), უსაფრთხო შენახვა (სპეციალური კონტეინერები, დაშვების კონტროლი), უსაფრთხო ტრანსპორტირება და ყველა მოქმედების აღრიცხვა.[271] გამოძიების პროცესში განხორციელებული ყველა ქმედება ისე უნდა იყოს აღწერილი, რომ დამოუკიდებელმა მესამე პირმა შეძლოს ამ მოქმედებების გამეორება და იგივე შედეგის მიღება.[272] სწორედ ამ პროცედურების დარღვევა ხშირად ხდება დაცვის მხარის მიერ მტკიცებულების დასაშვებობის ეჭვქვეშ დაყენების საფუძველი.

საგამოძიებო მოქმედებების, კერძოდ, ჩხრეკა-ამოღების დროს, ციფრული მტკიცებულებების სპეციფიკა დამატებით სირთულეებს ქმნის. პრაქტიკაში გამომძიებლები ხშირად იღებენ კომპიუტერთან დაკავშირებულ ყველა მოწყობილობას, მათ შორის პრინტერს, სკანერსა და მაუსსაც კი, მაშინ როცა საქმისთვის, შესაძლოა, მხოლოდ ინფორმაციის მატარებელი მოწყობილობა, მაგალითად, მყარი დისკი იყოს საჭირო.[273] ეს პრობლემა განსაკუთრებით მწვავედ დგას პირადი ცხოვრების ხელშეუხებლობის უფლებასთან მიმართებით. კომპიუტერულ მოწყობილობებზე არსებული ინფორმაციის მოცულობისა და მრავალფეროვნების გამო, სასამართლოს განჩინება ამოღების შესახებ მაქსიმალურად დეტალური უნდა იყოს. განჩინებაში, სულ მცირე, მითითებული უნდა იყოს ამოსაღები კომპიუტერული მონაცემების შესანახი საშუალებები, მათი მახასიათებლები და დასაბუთება, თუ რატომ არის საჭირო კონკრეტული ნივთის ამოღება.[274]

ამერიკული სასამართლო პრაქტიკაც ამაზე მიუთითებს. მაგალითად, საქმეში აშშ რიკარდის წინააღმდეგ, სასამართლომ ჩხრეკის ორდერი ზედმეტად ფართო შინაარსის მატარებლად მიიჩნია, რადგან ის გამომძიებლებს უფლებას აძლევდა, ამოეღოთ არა მხოლოდ კომპიუტერი, არამედ მასთან დაკავშირებული ყველა მოწყობილობა, მათ შორის პრინტერები და მოდემებიც. სასამართლოს განმარტებით, ორდერი არ იყო შემოფარგლული რომელიმე

07.06.2026).

271 MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. DIGITAL NOTES ON CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS. MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. 2024, გვ. 110-116. URL (accessed 07.06.2026).

272 Stoilkovski, M. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. 2022, გვ. 30. URL (accessed 07.06.2026).

273 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 54. URL (accessed 07.06.2026).

274 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 54-55. URL (accessed 07.06.2026).

კონკრეტული დანაშაულის მამხილებელი ფაილებით და გამომძიებლებს ფაქტობრივად ნებისმიერი ინფორმაციის მოძიების საშუალებას აძლევდა, ბავშვთა პორნოგრაფიიდან დაწყებული საგადასახადო დარღვევებით დამთავრებული.[275] ამიტომ, განჩინებამ მკაფიოდ უნდა დაადგინოს ობიექტური კრიტერიუმი, რომლითაც გამომძიებელი შეძლებს ამოღებას დაქვემდებარებული საგნების გარჩევას იმ საგნებისგან, რომელთა ამოღებაც არ უნდა მოხდეს.[276] ეს პრობლემა კიდევ უფრო მწვავდება, როდესაც ტრადიციული საგამოძიებო მეთოდები ციფრულ სამყაროსთან შეუსაბამო ხდება, რადგან ისინი ფიზიკური დანაშაულის ადგილებისთვისაა შემუშავებული და ვერ ითვალისწინებს ციფრული მტკიცებულების ფრაგმენტულ, მრავალ ლოკაციაზე განაწილებულ და საზღვრებს მიღმა არსებულ ბუნებას.[277]

გამოძიების პროცესში ერთ-ერთ მთავარ ტექნიკურ ბარიერს მონაცემთა დაშიფვრა (encryption) წარმოადგენს. დამნაშავეები აქტიურად იყენებენ დაშიფვრის ტექნოლოგიებს როგორც კომუნიკაციისთვის, ისე მტკიცებულებების დასამალად, რაც სამართალდამცავ უწყებებს ინფორმაციაზე წვდომას საგრძნობლად ურთულებს.[278] ბოლო წლებში რამდენიმე წარმატებული ოპერაცია განხორციელდა, რომელთა შედეგადაც გატყდა კრიმინალების მიერ გამოყენებული დაშიფრული საკომუნიკაციო პლატფორმები, როგორიცაა EncroChat, Sky ECC და Exclu. ამ ოპერაციებმა სამართალდამცავებს უპრეცედენტო რაოდენობის ინფორმაცია მიაწოდა კრიმინალური ქსელებისა და მათი საქმიანობის შესახებ, დაწყებული ძალადობრივი თავდასხმებიდან, დამთავრებული ფართომასშტაბიანი ნარკოტრაფიკით.[279] თუმცა, ასეთი პლატფორმების დახურვის შემდეგ, დამნაშავეები მუდმივად ეძებენ კომუნიკაციის ახალ, უფრო დაცულ გზებს.

პრობლემას ამწვავებს თანამედროვე ტელეკომუნიკაციის ტექნოლოგიებიც. მაგალითად, 5G სტანდარტები ხმოვანი ზარებისთვის ბოლოდან ბოლომდე დაშიფვრას (E2EE) იყენებს, რაც შეუძლებელს ხდის

275 მინაშვილი, ი. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. 2019, გვ. 55. URL (accessed 07.06.2026).
276 იქვე.
277 Coupland, H. Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. n.d., გვ. 16. URL (accessed 07.06.2026).
278 Eurojust and Europol. Common Challenges in Cybercrime 2024 Review by Eurojust and Europol. Publications Office of the European Union, Luxembourg. 2025, გვ. 6. URL (accessed 07.06.2026).
279 იქვე.

კანონიერ მოსმენას.[280] მსგავსი გამოწვევა არსებობს 4G ქსელებშიც, როდესაც მომხმარებელი როუმინგით სარგებლობს და მისი კომუნიკაცია ისევ საშინაო ქსელის გავლით მუშავდება (Home Routing), რის გამოც ადგილობრივ სამართალდამცავებს არ შეუძლიათ მისი მოსმენა.[281] გარდა ამისა, დაშიფვრის სავალდებულო გაუქმება ან ე.წ. „უკანა კარის“ შექმნა სახელმწიფოსთვის, სამოქალაქო თავისუფლებების კუთხით სერიოზულ დებატებს იწვევს, რადგან მონაცემთა კონფიდენციალურობა ძირითად უფლებად განიხილება.[282] ამიტომ, ნებისმიერი საკანონმდებლო ინიციატივა ამ მიმართულებით რთული ბალანსის დაცვას მოითხოვს სახელმწიფო უსაფრთხოებასა და პირადი ცხოვრების ხელშეუხებლობას შორის.

დაშიფვრასთან ერთად, გამოძიების ერთ-ერთი მთავარი თავსატეხია ანონიმურობა და დამნაშავის იდენტიფიკაცია, ანუ ატრიბუცია. კიბერდანაშაულის გამოძიებაში ატრიბუცია „ყველაზე რთულ საკითხად“ მიიჩნევა.[283] ეს იმითაა განპირობებული, რომ დამნაშავესა და მსხვერპლს შორის ყოველთვის დგას შუამავალი მოწყობილობა, რაც ართულებს ქმედების კონკრეტულ პიროვნებასთან პირდაპირ დაკავშირებას.[284] ხშირად ერთადერთი გზა ირიბი, გარემოებითი მტკიცებულებების ერთობლიობაა, როგორიცაა, მაგალითად, საკომუნიკაციო მოწყობილობის ფლობის დამტკიცება, სააბონენტო ინფორმაცია, კომუნიკაციის შინაარსის ანალიზი და მოწყობილობის კრიმინალისტიკური ექსპერტიზა.[285]

ანონიმურობის პრობლემა განსაკუთრებით მწვავედ ვლინდება ბნელ ქსელში (dark web), სადაც დახვეწილი ანონიმიზაციის ტექნოლოგიები დამნაშავეებს საშუალებას აძლევს, უკვალოდ განახორციელონ ისეთი ქმედებები, როგორიცაა ნარკოტრეფიკინგი ან პირადობის ქურდობა.[286] ვითარებას კიდევ უფრო ართულებს „კიბერდანაშაული როგორც სერვისის“

---

280 Eurojust and Europol. Common Challenges in Cybercrime 2024 Review by Eurojust and Europol. Publications Office of the European Union, Luxembourg. 2025, გვ. 7. URL (accessed 07.06.2026).

281 იქვე.

282 [1] H. Coupland, Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them, n.d., 15.

283 [1] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, 199.

284 იქვე., გვ. 198.

285 იქვე., გვ. 198-199.

286 [1] H. Coupland, Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them, n.d., 15.

(Cybercrime-as-a-Service, CaaS) მოდელის გავრცელება. ეს მოდელი დაბალი კვალიფიკაციის მქონე პირებსაც კი საშუალებას აძლევს, იქირაონ ან შეიძინონ რთული ჰაკერული ინსტრუმენტები, რაც ზრდის როგორც თავდასხმების სიხშირეს, ისე სირთულეს.[287] CaaS-ის პირობებში დამნაშავეები ერთდროულად რამდენიმე იურისდიქციიდან მოქმედებენ, რაც ატრიბუციის პროცესს თითქმის შეუძლებელს ხდის.[288] სწორედ ასეთ რთულ, ორგანიზებულ დანაშაულებრივ სქემასთან გვქონდა საქმე თბილისის საქალაქო სასამართლოს ერთ-ერთ გახმაურებულ გადაწყვეტილებაში.

კიბერდანაშაულის გამოძიების სირთულეს კარგად ასახავს თბილისის საქალაქო სასამართლოს 2019 წლის 11 დეკემბრის განაჩენი,[289] რომელიც ეხებოდა ორგანიზებული ჯგუფის მიერ ვირუს „Gozi“-ს გამოყენებით ამერიკული კომპანიების საბანკო ანგარიშებიდან დიდი ოდენობით თანხების ქურდობას. საქმის მასალებიდან ირკვევა, რომ დანაშაულებრივი სქემა ტრანსნაციონალურ ხასიათს ატარებდა და მასში ჩართული იყო სხვადასხვა როლის მქონე პირთა მთელი ქსელი: „სპამერები“ (ვირუსის გამავრცელებლები), „კრიპტერები“ (ვირუსის დამშიფრავები), თანხის გადამრიცხველები და „დროპერები“ (თანხის გამნაღდებლები).[290] ჯგუფი იყენებდა ფიშინგის ტექნიკას: პოტენციურ მსხვერპლ კომპანიებს ეგზავნებოდათ ელექტრონული წერილი, რომელიც, ერთი შეხედვით, სანდო წყაროდან (მაგალითად, ბანკიდან) იყო და შეიცავდა ვირუსულ ბმულს. ბმულზე გადასვლის შემდეგ კომპანიის კომპიუტერული სისტემა ინფიცირდებოდა, ხოლო ვირუსი ინტერნეტბანკის ავტორიზაციის მონაცემებს (მომხმარებლის სახელი, პაროლი) იპარავდა და ცენტრალურ სერვერზე აგზავნიდა.[291] საერთო ჯამში, ჯგუფი შეეცადა დაუფლებოდა 1,260,521 აშშ დოლარს, საიდანაც რეალურად 316,955 აშშ დოლარის მოპარვა მოახერხა.[292]

ამ საქმის გამოძიება ნათლად აჩვენებს იმ პრაქტიკულ სირთულეებს, რომლებიც კიბერდანაშაულს ახასიათებს. ჯგუფის წევრები ერთმანეთთან საკომუნიკაციოდ იყენებდნენ დაშიფრულ მესენჯერს „ჯაბერს“ (Jabber), სადაც მათ ზედმეტსახელები ჰქონდათ რეგისტრირებული, რაც მათ იდენტიფიკაციას

287 იქვე., გვ. 18.
288 იქვე., გვ. 18.
289 ¹ თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631.
290 იქვე., გვ. 30-31.
291 ¹ თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, გვ. 3-4, 11.
292 ¹ თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, გვ. 35.

ართულებდა.[293] გამოძიებისთვის საჭირო გახდა საერთაშორისო თანამშრომლობა აშშ-ის გამოძიების ფედერალურ ბიუროსთან (FBI) და ბულგარეთის სამართალდამცავ უწყებებთან, რათა მომხდარიყო ჯგუფის წევრების, მათ შორის ბულგარეთის მოქალაქის, იდენტიფიკაცია და დაკავებაც.[294] მტკიცებულებების სახით საქმეში ფიგურირებდა კომპიუტერულ-ტექნიკური ექსპერტიზის დასკვნები, ამოღებული ლეპტოპები და მყარი დისკები, „ჯაბერის“ მიმოწერები და სამართლებრივი დახმარების ფარგლებში აშშ-დან გადმოგზავნილი მასალები.[295] ეს საქმე იმის დასტურია, რომ კიბერდანაშაული საზღვრებს სცდება და მის ეფექტიან გამოძიებას როგორც მაღალტექნოლოგიური კრიმინალისტიკური მეთოდები, ისე მჭიდრო საერთაშორისო კოორდინაცია სჭირდება.

კიბერდანაშაულის ტრანსნაციონალური ბუნება სამართლებრივი თანამშრომლობის კუთხითაც სერიოზულ პრობლემებს ქმნის. ციფრული მტკიცებულებები ხშირად მიმოფანტულია სხვადასხვა ქვეყნის სერვერებზე, რაც გამოძიებას აიძულებს, მიმართოს სამართლებრივი ურთიერთდახმარების მექანიზმებს (MLATs). თუმცა, ეს პროცესი, როგორც წესი, მეტად ნელია და ვერ პასუხობს კიბერგამოძიების სისწრაფის მოთხოვნებს.[296] ეს შეფერხება დამნაშავეებს აძლევს დროს, გადაიტანონ ან წაშალონ მონაცემები, ან ისარგებლონ სხვადასხვა ქვეყნის კანონმდებლობას შორის არსებული შეუსაბამობებით. ამის გამო, ზოგიერთი მკვლევარი გამოსავალს საერთაშორისო კრიმინალისტიკური სტანდარტების შემუშავებაში ხედავს, თუმცა ეს ფართო პოლიტიკურ და სამართლებრივ თანამშრომლობას მოითხოვს.[297]

აგრეთვე, პრობლემურია თავად ეროვნული კანონმდებლობების მოძველებული ბუნებაც. კიბერდანაშაულის მარეგულირებელი მრავალი საპროცესო ნორმა თავდაპირველად ფიზიკური ობიექტებისა და ტრადიციული ტექნოლოგიებისთვის, მაგალითად, სატელეფონო კომუნიკაციებისთვის, შეიქმნა

293 [1] თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, გვ. 10, 21.
294 [1] თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, გვ. 12, 14.
295 [1] თბილისის საქალაქო სასამართლოს გადაწყვეტილება #330100119003053631, გვ. 21, 25.
296 [1] H. Coupland, Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them, n.d., 17.
297 იქვე., გვ. 17.

და ისინი ვერ ერგება ციფრულ სამყაროს.[298] ტექნოლოგიური განვითარება ბევრად უსწრებს საკანონმდებლო ცვლილებებს, რაც ქმნის ე.წ. „სამართლებრივ ჩამორჩენას“ ("law lag").[299] ამის შედეგად, სამართალდამცავები ან ვერ იყენებენ ახალ საგამოძიებო ინსტრუმენტებს, ან იყენებენ მათ ზუსტი სამართლებრივი საფუძვლის გარეშე, რაც ეჭვქვეშ აყენებს როგორც გამოძიების კანონიერებას, ისე ეჭვმიტანილის უფლებების დაცვას.[300] ამ ფონზე აქტიურია დებატები იმის შესახებ, უნდა მოხდეს თუ არა არსებული სამართლებრივი ჩარჩოების ადაპტაცია ციფრულ სამყაროსთან („კიბერ-არაგანსაკუთრებულობა“), თუ საჭიროა სრულიად ახალი, ტრანსნაციონალური სამართლებრივი არქიტექტურის შექმნა, რომელიც ციფრული სივრცის უსაზღვრო ბუნებას უკეთ გაითვალისწინებს.[301]

ტექნოლოგიური და სამართლებრივი გამოწვევების გარდა, კიბერდანაშაულის გამოძიების ეფექტიანობას საგრძნობლად აფერხებს ადამიანური ფაქტორი - კვალიფიციური კადრებისა და რესურსების ნაკლებობა. ბევრ სამართალდამცავ უწყებაში მუშაობენ ოფიცრები, რომლებსაც ციფრული კრიმინალისტიკისა და კიბერდანაშაულის გამოძიების კუთხით შეზღუდული ცოდნა აქვთ.[302] ეს პრობლემა განსაკუთრებით მწვავეა მცირე იურისდიქციებში, რომლებსაც, დიდი სააგენტოებისგან განსხვავებით, არ გააჩნიათ სპეციალიზებული კიბერდანაშაულის დანაყოფები და შესაბამისი რესურსები. ასეთი რეგიონები კი კიბერდამნაშავეებისთვის ერთგვარ „უსაფრთხო თავშესაფრად“ შეიძლება იქცეს.[303] განვითარებად ქვეყნებში ბევრი უწყება აღიარებს, რომ მათ არ აქვთ საკმარისი შესაძლებლობები და რესურსები, რათა სრულად დანერგონ თანამედროვე ტექნიკური სტანდარტები.[304]

ეს პრობლემა საქართველოსთვისაც აქტუალურია. შიდა ქართლის საგამოძიებო სამსახურის 145 თანამშრომელთან ჩატარებულმა კვლევამ აჩვენა, რომ მიუხედავად იმისა, რომ გამოკითხულთა 100% ემხრობა კიბერდანაშაულებრივი ქმედებების კრიმინალიზაციას, არ არსებობს ერთიანი,

298 [1] N. Bussolati, Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam, 2020, 159.
299 იქვე., გვ. 159.
300 იქვე., გვ. 159.
301 [1] H. Coupland, Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them, n.d., 20-21.
302 იქვე., გვ. 20.
303 იქვე., გვ. 21.
304 [1] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime. UNITED NATIONS, 2013, 199.

მკაფიო ხედვა იმის შესახებ, უნდა ჩამოყალიბდეს თუ არა ეს ქმედებები დამოუკიდებელ დანაშაულებრივ შემადგენლობებად.[305] ეს მიუთითებს იმაზე, რომ პრაქტიკოსებს შორისაც კი არ არის კონსენსუსი კიბერდანაშაულის სწორ სამართლებრივ კვალიფიკაციაზე, რაც, სავარაუდოდ, სწორედ ამ სფეროში არსებულ სირთულეებსა და ცოდნის არაერთგვაროვნებაზე მეტყველებს. ამ ფონზე, გამომძიებელთა და ზოგადად, სამართალდამცავთა მუდმივი გადამზადება და რესურსებით უზრუნველყოფა მთავარ ამოცანად რჩება.

ამ გამოწვევების ფონზე, გამოძიების ეფექტიანობის გაზრდის მიზნით სულ უფრო აქტიურად განიხილება ხელოვნური ინტელექტისა (AI) და მანქანური სწავლების (ML) ტექნოლოგიების გამოყენება. ხელოვნურ ინტელექტს შეუძლია უზარმაზარი მოცულობის მონაცემების დამუშავება და ანალიზი, რათა გამოავლინოს ფარული კავშირები და კანონზომიერებები, მოახდინოს საქმეების პრიორიტეტიზაცია და გამომძიებლებს დანაშაულებრივი ქცევის პროგნოზირებაშიც კი დაეხმაროს.[306] თუმცა, ამ ტექნოლოგიების დანერგვა გარკვეულ რისკებსაც შეიცავს. ხელოვნური ინტელექტის სისტემები იმდენად კარგია, რამდენადაც კარგია მონაცემები, რომლებზეც ისინი „ივარჯიშებენ“. არასრული ან მიკერძოებული მონაცემების გამოყენებამ შეიძლება მცდარი დასკვნები და, შედეგად, უსამართლო ბრალდებები გამოიწვიოს.[307] გარდა ამისა, არსებობს ეთიკური კითხვები პროგნოზირებადი პოლიციის მოდელების შესახებ, რადგან მათ შეუძლიათ საზოგადოებაში არსებული სოციალური უთანასწორობისა და სტერეოტიპების გაღრმავება.[308] შესაბამისად, ახალი ტექნოლოგიების დანერგვა უნდა მოხდეს ძალიან ფრთხილად, მათი პოტენციური სარგებლისა და შესაძლო რისკების გულდასმით შეფასების საფუძველზე.

---

305 [1] ამაშუკელი გ., კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი, 2022, გვ. 152.

306 [1] H. Coupland, Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them, n.d., 18.

307 იქვე., გვ. 18-19.

308 იქვე., გვ. 19.

დასკვნა

ჩატარებულმა კვლევამ აჩვენა, რომ კიბერდანაშაულის კვალიფიკაცია თანამედროვე ქართული სისხლის სამართლის ერთ-ერთ ყველაზე აქტუალურ და რთულ გამოწვევას წარმოადგენს. კვლევის მიზანი იყო კვალიფიკაციასთან დაკავშირებული დოქტრინალური და პრაქტიკული პრობლემების გამოვლენა და ანალიზი. შედეგად, გამოიკვეთა რამდენიმე სისტემური ხარვეზი, რომელიც მართლმსაჯულების ეფექტიან განხორციელებასა და ერთგვაროვანი პრაქტიკის ჩამოყალიბებას აფერხებს.

კვლევის შედეგად დადასტურდა, რომ კიბერდანაშაულის ერთიანი დეფინიციის არარსებობა არა უბრალოდ ტერმინოლოგიური, არამედ ფუნდამენტური, პრაქტიკული შედეგების მომტანი პრობლემაა. თუ შესავალში ეს საკითხი დაისვა, როგორც კვლევის ამოსავალი წერტილი, კვლევის პროცესში გამოჩნდა, რომ დეფინიციის არარსებობა პირდაპირ კვებავს სამართალგამოყენების არაერთგვაროვან პრაქტიკას და ქმნის „მოქნილი კვალიფიკაციის“ მანკიერ შესაძლებლობას, სადაც ბრალდების მხარეს შეუძლია ქმედების ხელოვნურად დამძიმება დანაშაულთა იდეალური ერთობლიობის გამოყენებით. ეს არ არის მხოლოდ კანონმდებლობის ფრაგმენტულობის შედეგი, არამედ სამართალდამცავი სისტემის მიერ ამ ფრაგმენტულობის, როგორც ინსტრუმენტის, გამოყენების პრაქტიკა, რაც ეჭვქვეშ აყენებს არა მხოლოდ კვალიფიკაციის სისწორეს, არამედ მართლმსაჯულების პროგნოზირებადობის პრინციპსაც. როგორც ამაშუკელი (2022) და Cernomoreț (2020) აღნიშნავენ, ასეთი ქაოსი ძირს უთხრის სამართლებრივი უსაფრთხოების განცდას და ქმნის ნოყიერ ნიადაგს შერჩევითი მართლმსაჯულებისთვის.

ასევე გამოიკვეთა, რომ ტრადიციული სისხლისსამართლებრივი ინსტიტუტები და ცნებები რთულად ერგება კიბერსივრცის სპეციფიკას. დანაშაულის საგნის არამატერიალური ბუნება, დანაშაულის ადგილისა და დროის განსაზღვრის სირთულე მისი ტრანსნაციონალური ხასიათის გამო და სუბიექტური მხარის, კერძოდ, განზრახვის („ცოდნის“) დამტკიცების სირთულე, არსებითად აძნელებს როგორც გამოძიების პროცესს, ისე სასამართლო განხილვას. ამასთან, კვლევის თანახმად, მოქმედი კანონმდებლობა ფაქტობრივად არ ითვალისწინებს გაუფრთხილებლობით ჩადენილი კიბერდანაშაულის შესაძლებლობას, მაშინ როდესაც ტექნოლოგიურად მართულ კრიტიკულ ინფრასტრუქტურებში გაუფრთხილებლობამ შესაძლოა

კატასტროფული შედეგები გამოიწვიოს, პრაქტიკოსი სამართალდამცველები კი ერთხმად უჭერენ მხარს ასეთი ქმედებების კრიმინალიზაციას.

გამოძიების ეტაპზე მთავარ ბარიერებს ციფრული მტკიცებულებების მოპოვების, შენახვისა და ანალიზის სირთულეები ქმნის. მონაცემთა დაშიფვრა, დამნაშავეთა ანონიმურობა, მტკიცებულებათა არასტაბილური ბუნება და საერთაშორისო სამართლებრივი თანამშრომლობის მექანიზმების ბიუროკრატიულობა ის ფაქტორებია, რომლებიც კიბერდამნაშავეებს ხშირად დაუსჯელობის განცდას უქმნის. ამას ემატება კვალიფიციური კადრებისა და რესურსების ნაკლებობა, რაც განსაკუთრებით აფერხებს რთული, ტრანსნაციონალური საქმეების ეფექტიან გამოძიებას.

ადამიანის უფლებათა ევროპული სასამართლოსა და უცხო ქვეყნების პრაქტიკის ანალიზი აჩვენებს, რომ, მიუხედავად ბუდაპეშტის კონვენციასთან მიერთებით კანონმდებლობის ჰარმონიზაციისკენ გადადგმული არსებითი ნაბიჯისა, ეროვნული კანონმდებლობა და პრაქტიკა კვლავ ჩამორჩება განვითარებული ქვეყნების სტანდარტებს ნორმების დეტალიზაციისა და ინსტიტუციური მოწყობის თვალსაზრისით. ევროპული სასამართლო კი სახელმწიფოებს სულ უფრო მკაცრ პოზიტიურ ვალდებულებებს უწესებს ონლაინ სივრცეში ჩადენილი დანაშაულების, განსაკუთრებით პირადი ცხოვრების ხელყოფის ფაქტების, სწრაფი და ეფექტიანი გამოძიების უზრუნველსაყოფად.

აღნიშნული პრობლემების გადასაჭრელად და ქართული სისხლის სამართლის კანონმდებლობისა და პრაქტიკის სრულყოფის მიზნით, მიზანშეწონილად მიგვაჩნია შემდეგი რეკომენდაციების წარმოდგენა:

1. საკანონმდებლო პოლიტიკის გადახედვა: უმთავრესი რეკომენდაციაა, კანონმდებელმა უარი თქვას ტრადიციული დანაშაულების კიბერანალოგების დამოუკიდებელ შემადგენლობებად კრიმინალიზაციის პრაქტიკაზე. ამის ნაცვლად, კომპიუტერული ტექნოლოგიების გამოყენება გასათვალისწინებელია როგორც ტრადიციული დანაშაულების (ქურდობა, თაღლითობა, ტერორიზმი და სხვ.) ჩადენის მაკვალიფიცირებელი (დამამძიმებელი) ნიშანი. ეს მიდგომა გადაჭრის ნორმათა კონკურენციის პრობლემას, თავიდან აგვარიდებს ქმედების უსამართლო, ორმაგ კვალიფიკაციას და, ამავდროულად, გაამარტივებს სამართალგამოყენების პროცესს და ხელი შეუწყობს ერთიანი სასამართლო პრაქტიკის ჩამოყალიბებას.

2. სისხლის სამართლის კოდექსის სისტემატიზაცია: აუცილებელია სისხლის სამართლის კოდექსის სრული გადახედვა და კიბერსივრცესთან დაკავშირებული ყველა დანაშაულის ერთ, ლოგიკურად გამართულ სისტემაში თავმოყრა. სასურველია, რომ კიბერდანაშაულის ყველა შემადგენლობა, რომლებიც დღეს კოდექსის სხვადასხვა თავშია გაბნეული, გაერთიანდეს ერთ, განახლებულ და სტრუქტურულად გამართულ თავში, რაც კანონმდებლობას უფრო გასაგებსა და ადვილად გამოყენებადს გახდის.

3. კანონმდებლობის დახვეწა და ახალი შემადგენლობების შემოღება: საჭიროა სისხლის სამართლის კოდექსის XXXV თავში არსებული ნორმების ტერმინოლოგიურად დახვეწა და იმ ბუნდოვანებების აღმოფხვრა, რომლებიც პრაქტიკაში განმარტების სირთულეებს ქმნის (მაგ., ცნებები „მნიშვნელოვანი შეფერხება“, „უნებართვობა“). ამასთან, უცხოური გამოცდილების გათვალისწინებით, მიზანშეწონილია ისეთი ქმედებების დამოუკიდებელ შემადგენლობებად კრიმინალიზაცია, რომლებსაც მოქმედი კანონმდებლობა სრულფასოვნად ვერ ფარავს, კერძოდ, კიბერგადაკიდების (Cyberstalking) და სერვისზე უარის შეტევების (DoS/DDoS). ასევე, გასათვალისწინებელია გაუფრთხილებლობით ჩადენილი კიბერდანაშაულების კრიმინალიზაციის საკითხი, განსაკუთრებით კრიტიკული ინფორმაციული სისტემების უსაფრთხოებასთან დაკავშირებით.

4. ინსტიტუციური და ადამიანური რესურსების გაძლიერება: კიბერდანაშაულთან ეფექტიანი ბრძოლა შეუძლებელია შესაბამისი ინსტიტუციური მოწყობის გარეშე. აუცილებელია სამართალდამცავ სტრუქტურებში სპეციალიზებული კიბერდანაშაულის დანაყოფების შექმნა და გაძლიერება, მათი თანამედროვე ტექნიკური საშუალებებით აღჭურვა. თუმცა, უმთავრესია ადამიანურ რესურსებში ინვესტირება: გამომძიებლების, პროკურორებისა და მოსამართლეების მუდმივი, საფუძვლიანი გადამზადება ციფრული კრიმინალისტიკის, მტკიცებულებათა მოპოვებისა და კიბერდანაშაულის ტექნიკური ასპექტების შესახებ.

5. საერთაშორისო და კერძო სექტორთან თანამშრომლობის გაღრმავება: ვინაიდან კიბერდანაშაულს საზღვრები არ გააჩნია, იზოლირებული ბრძოლა უშედეგოა. საქართველომ აქტიურად უნდა გამოიყენოს ბუდაპეშტის კონვენციით გათვალისწინებული 24/7 საკონტაქტო ქსელი და სხვა არაფორმალური თანამშრომლობის მექანიზმები, რათა დაჩქარდეს მტკიცებულებების გაცვლა და

ერთობლივი საგამოძიებო ჯგუფების შექმნა. გარდა ამისა, გადამწყვეტია კერძო სექტორთან, განსაკუთრებით ტელეკომუნიკაციისა და ტექნოლოგიურ კომპანიებთან, მჭიდრო პარტნიორობის ჩამოყალიბება, რადგან ხშირად სწორედ მათ ხელშია ის ინფორმაცია და ტექნიკური შესაძლებლობები, რომლებიც დანაშაულის გახსნისთვის აუცილებელია.

კიბერდანაშაული მუდმივად ცვალებადი მოვლენაა, რომელიც სამართლებრივ სისტემას მუდმივი მისადაგების საჭიროების წინაშე აყენებს. ნაშრომში განხილული პრობლემები და შემუშავებული რეკომენდაციები აჩვენებს, რომ კიბერდანაშაულთან ეფექტიანი ბრძოლისთვის საჭიროა სისტემური მიდგომა, რომელიც მოიცავს კანონმდებლობის დახვეწას, ინსტიტუციების გაძლიერებას, კადრების გადამზადებასა და საერთაშორისო თანამშრომლობის გაღრმავებას. მხოლოდ ასეთი ერთობლივი ძალისხმევითაა შესაძლებელი იმ საფრთხეების შემცირება, რომლებსაც ციფრული ეპოქა უქმნის საზოგადოებრივ უსაფრთხოებასა და მოქალაქეთა უფლებებს.

გამოყენებული ლიტერატურა

Berris, P. G. 2023. Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes. Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R47557/R47557.2.pdf (accessed 07.06.2026).

Bussolati, N. 2020. Harmonisation of Cybercrime Law: Past Solutions, Present Tensions, and Future Challenges. Universiteit van Amsterdam. https://pure.uva.nl/ws/files/51253937/Thesis.pdf (accessed 07.06.2026).

Cernomoreț, S. and A. Nastas. 2020. Comparative Analysis of Cybercrime in the Criminal Law System. https://www.adjuris.ro/books/cacc/Comparative%20Analysis%20of%20Cybercrime%20in%20the%20Criminal%20Law%20System.pdf (accessed 07.06.2026).

Clough, J. 2010. PRINCIPLES OF CYBERCRIME. Cambridge University Press. https://ugcollege.ge/storage/books/April2023/Tp9d8vOmUTINUOQaaliz.pdf (accessed 07.06.2026).

Council of Europe. 2001. Explanatory Report to the Convention on Cybercrime. Council of Europe. https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf (accessed 07.06.2026).

Council of Europe. 2025. Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2025 to implement the outcomes of the WSIS. Commission on Science and Technology for Development (CSTD). https://unctad.org/system/files/official-document/tcsdtlinf2025d2_en.pdf (accessed 07.06.2026).

Coupland, H. 2019. Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. https://www.york.ac.uk/media/law/documents/eventsandnewsdocs/2.%20Inv

estigating%20Cybercrime_The%20Key%20Jurisdictional%20and%20Technical%20Challenges%20Faced%20by%20Law%20Enforcement%20and%20Ways%20to%20Address%20Them.pdf (accessed 07.06.2026).

Eurojust. 2020. Challenges and best practices from Eurojust casework in the area of cybercrime. Eurojust. https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_cybercrime_report.pdf (accessed 07.06.2026).

Eurojust and Europol. 2025. Common Challenges in Cybercrime 2024 Review by Eurojust and Europol. Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf (accessed 07.06.2026).

Suspect in cyber-crime related offences would not be exposed to a real risk of ill-treatment if he were extradited to the United States [ECtHR], 2014. European Court of Human Rights. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-4832292-5894912&filename=Judgment%20Calovskis%20v.%20Latvia%20-%20extradition%20to%20USA%20of%20suspect%20in%20cyber-related%20offences.pdf (accessed 07.06.2026).

CASE OF M.Ș.D. v. ROMANIA [ECtHR], 2024. ECHR (HUDOC). (accessed 07.06.2026).

CASE OF AYTAJ AHMADOVA v. AZERBAIJAN [ECtHR], 2025. ECHR (HUDOC). (accessed 07.06.2026).

CASE OF VYACHESLAVOVA AND OTHERS v. UKRAINE [ECtHR], 2025. ECHR (HUDOC). (accessed 07.06.2026).

CASE OF ILAREVA AND OTHERS v. BULGARIA [ECtHR], 2025. ECHR (HUDOC). (accessed 07.06.2026).

Europol. 2022. The European Union Agency for Law Enforcement Cooperation. Europol. (accessed 07.06.2026).

Gautam, Y. and R. Renu. 2024. Integrating Artificial Intelligence into Cybercrime Investigation: Challenges and Future Directions. International Journal for Multidisciplinary Research (IJFMR) 6 (5): 1-4. https://www.ijfmr.com/papers/2024/5/28909.pdf (accessed 07.06.2026).

Guðbrandsdóttir, M. B. 2015. European Union Cyber Security: A Viable Solution?. Háskóla Íslands. https://skemman.is/bitstream/1946/19512/3/Cyber%20Security%20-%20BA%20.pdf (accessed 07.06.2026).

Haj-Ahmed, M. H. 2026. Research in Cybercrime: Why to not use the Black-letter Approach?. International Journal of Law Management & Humanities 9 (2): 3076-3092. https://ijlmh.com/paper/research-in-cybercrime-why-to-not-use-the-black-letter-approach/ (accessed 07.06.2026).

Kshetri, N. 2019. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management 22 (2): 77-81. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2019.pdf (accessed 07.06.2026).

Liu, Y. 2025. Study on the Subjective Knowledge Element of Cybercrime Assistance Based on Quantitative Methods. Advances in Social Science, Education and Humanities Research: 183-192. https://www.atlantis-press.com/article/126015479.pdf (accessed 07.06.2026).

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. 2024. DIGITAL NOTES ON CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS. MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. https://mrcet.com/downloads/digital_notes/CSEDS/CYBER%20CRIME%20INVESTIGATIONS%20AND%20DIGITAL%20FORENSICS.pdf (accessed 07.06.2026).

Marion, N. E. and J. Twede. 2020. Introduction. ABC-CLIO. https://cod.pressbooks.pub/app/uploads/sites/96/2021/08/Cybercrime-an-encyclopedia-of-digital-crime.pdf (accessed 07.06.2026).

Mathur, K. 2019. International conventions on cybercrime and the challenges of harmonisation. International Journal of Advanced Research and

Development 4 (4): 74-78. https://www.multireviewjournal.com/assets/archives/2019/vol4issue4/4-4-23-109.pdf (accessed 07.06.2026).

MOISE, A. C. 2015. Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level. Journal of Law and Administrative Sciences (Special Issue): 374-377. https://jolas.ro/wp-content/uploads/2015/07/jolas_sia38.pdf (accessed 07.06.2026).

Murphy, C. 2024. Understanding cybercrime. EPRS | European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf (accessed 07.06.2026).

Mustaque, A. M. 2000. Jurisdictional Issues in Adjudication of Cyber Crimes. High Court of Kerala. https://nja.gov.in/Concluded_Programmes/2022-23/P-1299_PPTs/2.Jurisdictional%20Issues%20in%20Adjudication%20of%20Cyber%20Crimes.pdf (accessed 07.06.2026).

Panel on Cybercrime Classification and Measurement. 2025. Cybercrime Classification and Measurement. National Academies of Sciences, Engineering, and Medicine. https://static1.squarespace.com/static/5b7ea2794cde7a79e7c00582/t/680f9449b73a5c15bb3ab9aa/1745851470777/29048.pdf (accessed 07.06.2026).

Phillips, K., J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, and M. P. Aiken. 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences 2 (2): 379-398. https://www.semanticscholar.org/reader/f2bc792c2a19af231963e8eaed48487a14cf3e2d (accessed 07.06.2026).

Putnam, T. L. and D. D. Elliott. 1999. International Responses to Cyber Crime. Hoover Press: 35-38. https://www.hoover.org/sites/default/files/uploads/documents/0817999825_35.pdf (accessed 07.06.2026).

Sinrod, E. J. and W. P. Reilly. 2000. CYBER-CRIMES: A PRACTICAL APPROACH TO THE APPLICATION OF FEDERAL COMPUTER CRIME LAWS. SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL 16 (2). https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1258&context=chtlj (accessed 07.06.2026).

Stoilkovski, M. 2022. GUIDELINES ON CYBERCRIME INVESTIGATION. OSCE. https://albania.osce.org/sites/default/files/f/documents/a/8/534684.pdf (accessed 07.06.2026).

Tennis, M. M. 2020. A UNITED NATIONS CONVENTION ON CYBERCRIME. Capital University Law Review 48: 189-192. https://www.capitallawreview.org/article/12972-a-united-nations-convention-on-cybercrime.pdf (accessed 07.06.2026).

UNITED NATIONS OFFICE ON DRUGS AND CRIME. 2013. Comprehensive Study on Cybercrime. UNITED NATIONS. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 07.06.2026).

Verleysen, C. 2016. Cybercrime: A theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series. https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf (accessed 07.06.2026).

ამაშუკელი, გ. 2022. კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა. კავკასიის საერთაშორისო უნივერსიტეტი. https://dspace.nplg.gov.ge/bitstream/1234/419560/1/Amashukeli_Giorgi_Disertacia.pdf (accessed 07.06.2026).

ბიბიჩაძე, თ. და შ. ოვაკიმიან. 2024. კიბერუსაფრთხოება, როგორც მთავარი გამოწვევა საერთაშორისო ურთიერთობებში (საქართველოს, უკრაინის, ესტონეთის შემთხვევების ანალიზი). ჟ. სტუდენტთა ჟურნალი სოციალურ მეცნიერებებში (26): 36-38. https://sjss.tsu.ge/img/3.%20%E1%83%91%E1%83%98%E1%83%91%E1%83%98%E1%83%A9%E1%83%90%E1%83%AB%E1%83%94%20%E1%83%9D%E1%83%95%E1%83%90%E1%83%99%E1%83%98%E1%83%9B%E1%83%98%E1%83%90%E1%83%9C%E1%83%98.pdf (accessed 07.06.2026).

ზაქაშვილი, უ. 2013. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. https://openscience.ge/bitstreams/109e4b2e-b6e3-4c06-a791-eba78eae40b8/download (accessed 07.06.2026).

თბილისის სააპელაციო სასამართლო. n.d. თბილისის სააპელაციო სასამართლო გადაწყვეტილება #330100117001817465. თბილისის სააპელაციო სასამართლო. (accessed 07.06.2026).

თბილისის საქალაქო სასამართლო. n.d. თბილისის საქალაქო სასამართლო გადაწყვეტილება #330100119003053631. თბილისის საქალაქო სასამართლო. (accessed 07.06.2026).

მინაშვილი, ი. 2019. ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდიკა. გამომცემლობა „მერიდიანი“. (accessed 07.06.2026).

მშვიდობაძე, თ. და გ. ხელაძე. 2014. სახელმწიფო კიბერუსაფრთხოების პოლიტიკა. ილიას სახელმწიფო უნივერსიტეტი. (accessed 07.06.2026).

საქართველოს საკონსტიტუციო სასამართლო. 2025. საქართველოს საკონსტიტუციო სასამართლოს პლენუმის გადაწყვეტილება №3/9/1818,1861. (accessed 07.06.2026).

საქართველოს საკონსტიტუციო სასამართლო. 2025. საქართველოს საკონსტიტუციო სასამართლოს პლენუმის განმწესრიგებელი სხდომის საოქმო ჩანაწერი №3/5/1861. (accessed 07.06.2026).

საქართველოს საკონსტიტუციო სასამართლო. 2026. საქართველოს საკონსტიტუციო სასამართლოს პლენუმის განჩინება №3/6/1919. (accessed 07.06.2026).

საქართველოს უზენაესი სასამართლო. 2019. საქართველოს უზენაესი სასამართლოს გადაწყვეტილება #ბს-1499(კ-18). (accessed 07.06.2026).

საქართველოს უზენაესი სასამართლო. 2022. საქართველოს უზენაესი სასამართლოს გადაწყვეტილება #ბს-416(კს-22). (accessed 07.06.2026).

საქართველოს უზენაესი სასამართლო. 2024. საქართველოს უზენაესი სასამართლოს გადაწყვეტილება #ბს-1169(კ-22). (accessed 07.06.2026).

ჯღარკავა, ი. 2021. საქართველოს კიბერუსაფრთხოების პოლიტიკა, გამოწვევები და შესაძლებლობები. აშშ-ის საელჩო საქართველოში; საქართველოს სტრატეგიის და განვითარების ცენტრი. (accessed 07.06.2026).