September 2022 (№23)
Volume 8; Issue 3; Page No. 153-168
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/8.3.10


# Analysis of Procedural Problems in Cybercrime Investigations

Irakli Nadareishvili
*Doctor of Law, Affiliated Associated professor of Caucasus International University Head of The Department to Investigate Offenses Committed in the Course of Legal Proceedings The Office of The General Prosecutor of Georgia*

Shota Kakulia
*Master of Law, Prosecutor of The Department to Investigate Offenses Committed in the Course of Legal Proceedings*

ARTICLE INFO

*Article History:*

Received 09.09.2022
Accepted 26.09.2022
Published 30.09.2022

*Keywords:*

Budapest Convention, Preservation of Computer Data, Requesting Information, Digital Evidence, Cybercrime

ABSTRACT

The approach used to investigate cybercrime in developed nations is examined in this article, along with the innovations that might be implemented in Georgia to ensure successful investigations. Detailing the procedures outlined under the Budapest Convention on Computer Crimes, attention is given to the procedural issues that crop up while gathering and presenting electronic evidence in criminal investigations. The convention's individual articles are examined, including those that deal with information requests, and a comparison between the convention's legal provisions and the standards incorporated into Georgian law is made. The article examines the practice of collaboration between developed country law enforcement bodies and Internet service providers. The absence of computer data classification in Georgian law is highlighted, which results in the existence of a single, all-encompassing rule for all forms of electronic information. The paper also covers court rulings on the admissibility of electronic evidence and offers advice on whether it would be wise to clarify or improve the criminal procedure laws. The article explains the need for varied time limits and tactics for getting and maintaining information from internet service providers based on the classification of cybercrimes into distinct crime categories, such as serious, particularly serious, and crimes against national security.

# კიბერდანაშაულის გამოძიებისას არსებული პროცედურული პრობლემების ანალიზი

**ირაკლი ნადარეიშვილი**

*სამართლის დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის აფილირებული ასოცირებული პროფესორი. საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი*

**შოთა კაკულია**

*სამართლის მაგისტრი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის პროკურორი*

**საკვანძო სიტყვები:** ინტერნეტ-ტრაფიკი, მონაცემების რეზერვაცია, ელექტრონული მტკიცებულებების გამოთხოვა, კიბერდანაშაული

## შესავალი

საინფორმაციო ტექნოლოგიების განვითარებამ ფუნდამენტურად შეცვალა საზოგადოების მიდგომები და აღნიშნული ტენდენცია, დიდი ალბათობით, შენარჩუნდება უახლოეს მომავალშიც. ტექნოლოგიების მხარდაჭერით ბევრი საკითხის გადაწყვეტა გაცილებით ნაკლები ადამიანური რესურსით გახდა შესაძლებელი. თუკი საწყის ეტაპზე მხოლოდ საზოგადოების გარკვეულმა ნაწილმა მოახდინა საქმიანობის რაციონალიზაცია საინფორმაციო ტექნოლოგიებით, ამჟამად თითქმის არ დარჩა სფერო, რომელსაც ცვლილებები არ შეხებია.

საინფორმაციო ტექნოლოგიების განვითარების თვალსაჩინო მახასიათებელია მისი გავლენა სატელეკომუნიკაციო ტექნოლოგიების ევოლუციის პროცესში. მაგალითისთვის: კლასიკური ტელეფონი, რომელიც გამოიყენებოდა ადამიანის ხმის გადასაცემად, ჩანაცვლდა ისეთი ტექნოლოგიური მიღწევებით, რომლითაც შესაძლებელი გახდა როგორც ხმის, ასევე ტექსტის, მუსიკის, მოძრავი და სტატიკური სურათების ტრანსფერი. აღნიშნული სახის ინფორმაციის გაცვლა აღარ ხდება მხოლოდ ადამიანებს შორის, არამედ შესაძლებელია გაცვლის სუბიექტები იყვნენ საკუთრივ კომპიუტერები. თანამედროვე მიღწევების ფონზე აქტუალობა დაკარგა ადამიანთა შორის მხოლოდ პირდაპირი კავშირის დამყარების საჭიროებამ, კომუნიკაციისათვის ახლა უკვე საკმარისია კონკრეტული დანიშნულების მისამართის ცოდნა ან კომპიუტერული ფაილის საჯაროდ ხელმისაწვდომობის ფუნქციის გააქტიურება.

კომპიუტერულ სისტემებში არსებული ინფორმაციის ხელმისაწვდომობისა და მოკვლევის სიმარტივემ, სწრაფად გაცვლისა და გავრცელების პრაქტიკულად შეუზღუდავ შესაძლებლობებთან ერთად, გამოიწვია სიახლეებისადმი შემეცნების ბუმი, რაც თავისთავად ტექნოლოგიების შემდგომი განვითარების წინაპირობაა.

აღნიშნულმა მოვლენებმა უპრეცედენტო ბიძგი მისცეს ეკონომიკური და სოციალური სფეროს განვითარებას, თუმცა მათ აქვთ ნეგატიური მხარეც. კერძოდ, ტექნოლგიების განვითარებამ გამოიწვია როგორც ახალი ტიპის კიბერდანაშაულის გაჩენა, ასევე, ხელი შეუწყო ტრადიციული დანაშაულის ტიპების ტექნოლოგიების გამოყენებით ჩადენის გავრცელებას. კრიმინალური ქცევა ნაკლებად პროგნოზირებადი და რთულად დასადგენი გახდა. ახალი ტექნოლოგიები დიდ გამოწვევად იქცა ტრადიციული სამართლებრივი კონცეფციებისთვის. ინფორმაციისა და კომუნიკაციის ნაკადები მარტივად და მოქნილად მიედინება მთელ მსოფლიოში და მათ ვერ აფერხებს ქვეყნებს შორის არსებული გეოგრაფიული საზღვრები.[1]

## კონვენცია კომპიუტერული დანაშაულის შესახებ

ტექნოლოგიური განვითარების პერმანენტული და სწრაფი ტემპების გათვალისწინებით, კრიტიკულ მნიშვნელობას იძენს კომპიუტერულ სისტემებთან/მონაცემებთან მოპყრობის მარეგულირებელი ნორმატიული რეგულაციების პარალელურ რეჟიმში განვითარება და სრულყოფა, სათანადო და მოქნილი სამართლებრივი მექანიზმების შექმნა, რათა თანამედროვე გამოწვევებზე ადეკვატური რეაგირების მიზნით ერთი მხრივ, უზრუნველყოფილ იქნას სამართალდამცავი ორგანოების შესაძლებლობა – განახორციელონ ეფექტიანი გამოძიება, ხოლო, მეორე მხრივ, სათანადო პროცედურული გარანტიებით დაცულ იქნას პირადი ცხოვრების ხელშეუხებლობის უფლება.

აღნიშნული პროცესის მართებულად წარმართვისა და კიბერდანაშაულთან ბრძოლაში კოორდინაციის გაზრდის, ასევე, კანონმდებლობის ჰარმონიზაციისა და საერთაშორისო სფეროში თანამშრომლობის გაღრმავების მიზნით, 2001 წლის 8 ნოემბერს, ევროპის საბჭოს მინისტრთა კომიტეტის მიერ, მიღებულ იქნა „კონვენცია კიბერდანაშაულის შესახებ“ (ე.წ. „ბუდაპეშტის კონვენცია“), რომელიც ძალაში შევიდა 2004 წლის 1-ელ ივლისს. საქართველოს მიერ კონვენციის რატიფიცირება განხორციელდა 2012 წლის 6 ივნისს და ძალაში შევიდა იმავე წლის 1-ელ ოქტომბერს.

აღნიშნული კონვენცია წარმოადგენს პირველ საერთაშორისო, სავალდებულო ძალის მქონე აქტს, რომელმაც საერთაშორისო დონეზე განსაზღვრა ფუნდამენტური ცნებები და წარმმართველი როლი ითამაშა ტერმინთა უნიფიცირებისა და ეროვნული კანონმდებლობების ჰარმონიზაციის მიმართულებით.

კიბერდანაშაულის გამოძიების მიმართულებით ერთიანი სისხლის სამართლის პოლიტიკის შექმნის, კომპიუტერული დანაშაულებისგან საზოგადოების დაცვის, შესაბამისი კანონმდებლობის მიღებისა და საერთაშორისო თანამშრომლობის ხელშეწყობის მიზნით, ე.წ. „ბუდაპეშტის კონვენციის“ მეორე თავში განისაზღვრა ცალკეული კიბერდანაშაულების დეფინიცია. მაგალითად, განისაზღვრა უნებართვო წვდომა (მუხლი 2), მონაცემთა ხელში ჩაგდება ნებართვის გარეშე (მუხლი 3), მონაცემთა ხელყოფა (მუხლი 4), სისტემაში ჩარევის (მუხლი 5) და ა.შ. ცნებები. კონვენციის მე-2 თავის მე-2 ნაწილი ეთმობა უშუალოდ იმ პროცედურული მექანიზმების განსაზღვრას, რომლებიც გამოიყენება კომპიუტერულ დანაშაულების გამოძიების დროს. ამგვარ მექანიზმებს, კონვენციის მიხედვით, განეკუთვნება კომპიუტერული მონაცემების დაჩქარებული დაცვა (მუხლი 16); ტრაფიკის მონაცემის დაჩქარებული დაცვა და ნაწილობრივი გადმოცემა (მუხლი 17); დოკუმენტთა/ინფორმაციის გამოთხოვის ბრძანება (მუხლი 18); შენახული კომპიუტერული მონაცემების ჩხრეკა და ამოღება (მუხლი 19); ინტერნეტ ტრაფიკის მონაცემების მიმდინარე შეგროვება (მუხლი 20); კომუნიკაციის შინაარსობრივი მონაცემების ხელში ჩაგდება (მუხლი 21).[2]

კიბერდანაშაულის ეფექტიანი გამოძიების უზრუნველსაყოფად მნიშვნელოვანია, ქვეყანას ჰყავდეს შესაბამისი ცოდნით აღჭურვილი საგამოძიებო უწყების წარმომადგენლები, რომლებსაც გავლილი ექნებათ სათანადო ინ-

1 Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. P. 1. <https://rm.coe.int/16800cce5b> [ბოლო წვდომა: 9 სექტემბერი, 2022]

2 “Convention on Cybercrime” (2001). Articles 2 – 5 and 16 – 21, Council of Europe. <https://rm.coe.int/1680081561> [ბოლო წვდომა: 9 სექტემბერი, 2022].

სტრუქტაჟი. ასევე, აუცილებელია სპეციალიზირებული საგამოძიებო დანაყოფების თანამედროვე ტექნოლოგიებით უზრუნველყოფა, რომლითაც შესაძლებელი გახდება გამოძიებისთვის კრიტიკულად მნიშვნელოვანი ინფორმაციის ოპერატიულად მოპოვება. განვითარებულ ქვეყნებში შემუშავებულია სხვადასხვა სახის გზამკვლევები, რომლითაც ხელმძღვანელობენ სამართალდამცავები. საქართველოში კიბერდანაშაულის სხვადასხვა ტიპის დანაშაულების ზრდის ტემპის პარალელურად, აუცილებელია, რომ სახელმწიფომ გაიზიაროს განვითარებული ქვეყნების გამოცდილება, გადაამზადოს პერსონალი, დანერგოს გამოძიების მეთოდოლოგიის ძირითადი პრინციპები და შეიძინოს სრულყოფილი გამოძიების ჩასატარებლად აუცილებელი ტექნიკური აღჭურვილობა.

## გამოძიების პროცედურული მექანიზმები

„კომპიუტერული დანაშაულის შესახებ“ ბუდაპეშტის კონვენციის მე-14 მუხლი განსაზღვრავს, რომ ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს ისეთი საჭირო საკანონმდებლო და სხვა ზომები, რომლებიც უზრუნველყოფს სისხლის სამართლის კონკრეტული საქმის გამოძიების ან დევნის შესაბამისი უფლებამოსილებისა და პროცედურების დანერგვას.

კონვენციამ მოუწოდა ხელშემკვრელ სახელმწიფოებს, რომ კანონმდებლობაში დაენერგათ პროცედურული მექანიზმები, რომლებიც იქნებოდა მოქნილი და, ამავდროულად, გამოძების სრულყოფილად ჩატარებაზე ორიენტირებული. აღნიშნული პროცედურებიდან შესაძლებელია განვიხილოთ რამდენიმე, რომელთა ეფექტურ დანერგვაზე პირდაპირპროპორციულად არის დამოკიდებული გამოძიების ხარისხი. კონვენციის მე-16 მუხლი მოუწოდებს სახელმწიფოებს, რომ შეიმუშავონ საკანონმდებლო ან სხვა სახის ზომები, რომლებიც უზრუნველყოფენ შენახულ კომპიუტერულ მონაცემთა დაჩქარებულ დაცვას. აღნიშნული ნორმის მიზანს წარმოადგენს გამოძიებისთვის რელევანტური კომპიუტერული მონაცემების შესაძლო დაკარგვის ან შეცვლის საფრთხის პრევენცია.

გამოძიების წარმოებისთვის აუცილებელი კიდევ ერთი მექანიზმი – ინფორმაციის გამოთხოვა – გათვალისწინებულია კონვენციის მე-18 მუხლით და გულისხმობს წევრი სახელმწიფოების კომპეტენტური ორგანოებისთვის შემდეგი უფლებამოსილების მინიჭების შესაძლებლობას:

*„ა) დაავალდებულონ მათ ტერიტორიაზე მყოფი პირი – წარმოადგინოს კონკრეტული კომპიუტერული მონაცემი, რომელიც ამ პირის მფლობელობაში ან კონტროლის ქვეშაა და ინახება კომპიუტერულ სისტემაში ან კომპიუტერული მონაცემების შემნახავ საშუალებაში;*

*ბ) დაავალდებულონ მომსახურების მიმწოდებელი (რომელიც მომსახურების მიწოდებას ახორციელებს) – მათ ტერიტორიაზე წარმოადგინოს მომხმარებლის შესახებ ინფორმაცია, რომელიც დაკავშირებულია ამგვარ მომსახურებასთან და რომელსაც ფლობს ან/და აკონტროლებს აღნიშნული მომსახურების მიმწოდებელი“.*[3]

კონვენციის მე-19 მუხლით, ასევე, გათვალისწინებულია შენახულ კომპიუტერულ მონაცემთა ჩხრეკა და ამოღების შესაძლებლობა, ხოლო მე-20 მუხლი ითვალისწინებს ინტერნეტ ტრაფიკის მიმდინარე შეგროვებას. კონვენციის მე-18 მუხლის ახსნა-განმარტებითი ბარათის 170-ე პუნქტი განსაზღვრავს ინფორმაციის გამოთხოვის, როგორც ერთ-ერთი საგამოძიებო მოქმედების კანონმდებლობაში დანერგვის მთავარ ლეგიტიმურ მიზანს. კერძოდ, ბარათში ვკითხულობთ, რომ სახელმწიფოების მხრიდან მესამე პირებთან მიმართებით, სისტემატურად ისეთი იძულების ღონისძიებების გამოყენების შესამცირებლად, როგორსაც წარმოადგენს მონაცემების ჩხრეკა და ამოღება, მნიშვნელოვანია, რომ მათ ეროვნულ კანონმდებლობაში ჰქონდეთ ალტერნატიული საგამოძიებო მექანიზმები, რომლებიც იძლევიან ნაკლებად ინტენსიური ჩარევის შესაძლებლობას იმ კომპიუტერული ინფორმაციის მოსაპოვებლად, რომელიც დაკავშირებულია დანაშაულის გამოძიებასთან. [4]

---

3 “Convention on Cybercrime” (2001). Article 18, Council of Europe. <https://rm.coe.int/1680081561> [ბოლო წვდომა: 9 სექტემბერი, 2022].

4 Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. P. 29. <https://rm.coe.int/16800cce5b> [ბოლო წვდომა: 9 სექტემბერი, 2022].

„კიბერ-დანაშაულთან ბრძოლის შესახებ“ კონვენციის ხელმოწერის შემდეგ, 2010 წელს ცვლილება შევიდა საქართველოს სისხლის სამართლის საპროცესო კოდექსში და მას დაემატა თავი კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების შესახებ. აღნიშნული თავი, კონვენციის მე-18 მუხლის იმპლემენტირების მიზნით, შეიცავს სსსკ 136-ე მუხლს ინფორმაციის ან დოკუმენტის გამოთხოვის შესახებ, რომლის პირველი ნაწილის მიხედვითაც: *„თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში, ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, პროკურორი უფლებამოსილია გამოძიების ადგილის მიხედვით მიმართოს სასამართლოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით“*.[5] აღნიშნულ ნაწილს 2022 წლის 24 მაისის ცვლილებით დაემატა შემდეგი სახის ჩანაწერი – *„გადაუდებელი აუცილებლობის შემთხვევაში ამ მუხლით გათვალისწინებული საგამოძიებო მოქმედება შესაძლებელია ჩატარდეს პროკურორის დადგენილების საფუძველზე, ამ კოდექსის 112-ე მუხლის მე-5 ნაწილით განსაზღვრული წესით“*.[6] საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის 2022 წლის 24 მაისამდე მოქმედი რედაქციის თანახმად, ინფორმაციის გამოთხოვის პროცედურაზე ვრცელდებოდა ფარული საგამოძიებო მოქმედებების შესახებ თავის ($143^2$-$143^{10}$ მუხლების) მოქმედება, რაც დამატებით, აბსურდულ ბარიერს წარმოადგენდა, ზოგადად, ნებისმიერი სახის გამოძიების წარმოებისთვის, სადაც საჭირო იყო კომპიუტერული მონაცემების მოპოვება და განსაკუთრებულ პრობლემებს ქმნიდა კიბერდანაშაულის კატეგორიის დანაშაულის გამოძიების პროცესში. კერძოდ, ირელევანტური იყო, თუ რამდენად ატარებდა მოსაპოვებელი ინფორმაცია ან დოკუმენტი სენსიტიურ ხასიათს და არ ხდებოდა კომპიუტერული მონაცემების კატეგორიზაცია. ნებისმიერი სახის კომპიუტერული მონაცემი ექცეოდა ერთიანი „ქოლგის“ ქვეშ და ინფორმაციის გამოთხოვის შესახებ შუამდგომლობის ავტორისგან ითხოვდა სისხლის სამართლის საპროცესო კოდექსის ფარული საგამოძიებო მოქმედებების შესახებ თავში გათვალისწინებული გარანტიების დაცვას და ზედმეტად მყარ დასაბუთებას.

2022 წლის 24 მაისს, 136-ე მუხლში განხორციელებული ცვლილებებით, გარკვეულწილად გამარტივდა კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში არსებული ინფორმაციის ან დოკუმენტის გამოძიების მიერ მოპოვების შესაძლებლობა, რადგან განხორციელებული ცვლილებებით მათზე აღარ ვრცელდება ფარული საგამოძიებო მოქმედებების ჩატარების წესი, რაც ცალსახად დაგვიანებულ, თუმცა წინ გადადგმულ ნაბიჯად უნდა ჩაითვალოს.

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლი ვრცელი შინაარსისაა და ადგენს ერთიან უნიფიცირებულ წესს ნებისმიერი სახის ინფორმაციის მოსაპოვებლად, რომელიც შენახულია კომპიუტერული ფაილის სახით. XXI-ე საუკუნეში ორგანიზაციების უდიდესი ნაწილი მათ ხელთ არსებულ ინფორმაციას/დოკუმენტაციას ელექტრონული ფორმით ინახავს. შედეგად, ვიღებთ რეალობას, რა დროსაც საჯარო თუ კერძო დაწესებულებებიდან ინფორმაციის მოსაპოვებლად აუცილებელია მოსამართლისგან ინფორმაციის გამოთხოვის თაობაზე განჩინების მიღება, მიუხედავად იმისა, გამოსათხოვი ინფორმაცია ნაკლებად სენსიტიურია თუ თავისი არსით არის საჯარო და ხელმისაწვდომი ნებისმიერი პირისთვის. აღნიშნული წარმოადგენს დამატებით ბიუროკრატიულ ბარიერს მოქნილი და ეფექტური გამოძიების წარმოებისთვის.

საქართველოში მოქმედი კანონმდებლობა არ ახდენს გამოთხოვას დაქვემდებარებული ინფორმაციის დიფერენცირებას კატეგორიის მიხედვით. კატეგორიზაციის თვალსაზრისით, ერთადერთ გამონაკლისს წარმოადგენს 136-ე მუხლის მე-3 ნაწილით გათვალისწინებული „მომხმარებლის მაიდენტიფიცირებელი მონაცემი“, რომელიც პირდაპირ არის გადმოტანილი ბუდაპეშტის კონვენციიდან. მოცემულ

---

5 საქართველოს სისხლის სამართლის საპროცესო კოდექსი (2009). მუხლი 136 (13.04.2022 წლის რედაქცია). საქართველოს საკანონმდებლო მაცნე. <https://www.matsne.gov.ge/document/view/90034?publication=143> [ბოლო წვდომა: 9 სექტემბერი, 2022]

6 საქართველოს სისხლის სამართლის საპროცესო კოდექსი (2009). მუხლი 136 (21.06.2022 წლის რედაქცია). საქართველოს საკანონმდებლო მაცნე. <https://www.matsne.gov.ge/ka/document/view/90034?publication=146> [ბოლო წვდომა: 9 სექტემბერი, 2022]

შემთხვევაში პრობლემას წარმოადგენს არა ის, თუ როგორ არის ასახული „მომხმარებლის მაიდენტიფიცირებელი მონაცემი“ სისხლის სამართლის საპროცესო კოდექსში, არამედ მიდგომა, რომლის თანახმადაც მის მოსაპოვებლად განსაზღვრულია იგივე პროცედურული მექანიზმი, როგორიც გამოიყენება ნებისმიერი სხვა სახის ელექტრონული ინფორმაციის მოპოვების შემთხვევაში.

*„კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის კონვენციის მე-18 მუხლის მიზნებისთვის ტერმინი „ინფორმაცია მომხარებლის შესხებ“ არის ნებისმიერი ინფორმაცია, რომელსაც მომსახურების მომწოდებელი ინახავს კომპიუტერული მონაცემების ან სხვა ნებისმიერი ფორმით, რომელიც დაკავშირებულია მისი მომსახურების მომხმარებლებთან, განსხვავდება ინტერნეტ ტრაფიკისა და შინაარსობრივი მონაცემებისგან და რომლის მიხედვითაც შესაძლებელია დადგინდეს/განისაზღვროს:*

*ა) გამოყენებული კომუნიკაციის მომსახურების ტიპი, გამოყენებული ტექნიკური საშუალებები და მომსახურების დრო;*

*ბ) მომხმარებლის ვინაობა, საფოსტო ან საცხოვრებელი მისამართი, ტელეფონის და სხვა საკონტაქტო ნომრები, ინფორმაცია ანგარიშისა და გადასახადების შესახებ, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე;*

*გ) დამონტაჟებული საკომუნიკაციო აღჭურვილობის ადგილმდებარეობის თაობაზე არსებული ნებისმიერი სხვა ინფორმაცია, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე“.*[7]

მოცემულ შემთხვევაში, აუცილებელია სწორად იქნას გაგებული კანონმდებლის მიზანი, თუ რას ემსახურებოდა კომპიუტერულ მონაცემთა დაყოფა მომხმარებლის, კომუნიკაციის მაიდენტიფიცირებელი მონაცემებისა და კომუნიკაციის შინაარსობრივი/ინტერნეტ ტრაფიკის მონაცემების კატეგორიებად. ნებისმიერი პირის პირადი ცხოვრების ხელშეუხებლობა დაცულია კონსტიტუციითა და შესაბამისი ნორმატიული აქტებით. აღნიშნული უფლება არ არის აბსოლუტური ხასიათის და კანონმდებლობა ითვალისწინებს მისი შეზღუდვის შესაძლებლობას ლეგიტიმური მიზნის მისაღწევად. ლოგიკურია, რომ უფლების შეზღუდვის სიმძიმის გათვალისწინებით უნდა განსხვავდებოდეს სამართლებრივი პროცედურებიც, წინააღმდეგ შემთხვევაში აზრი დაეკარგებოდა კომპიუტერული მონაცემების დიფერენცირებას მომხმარებლისა და შინაარსობრივი ინფორმაციის კატეგორიებად. აღნიშნულის თაობაზე საუბარია კიბერდანაშაულთან ბრძოლის საზედამხედველო კომიტეტის შემფასებელი მისიის დასკვნაში[8] და შესაბამის რეკომენდაციაში, ამაზე მეტყველებს, ასევე, ევროპული ქვეყნების გამოცდილებაც. მაგალითისთვის შესაძლოა მოყვანილ იქნას ისეთი ქვეყნები, როგორიც არის ლატვია, ლიტვა, ესტონეთი, გერმანია, ესპანეთი, დანია, მონტენეგრო, სლოვენია, ფინეთი და ნორვეგია.[9]

გამოთხოვის მექანიზმი გათვალისწინებულია „კიბერ-დანაშაულთან ბრძოლის ევროპული კონვენციის“ მე-18 მუხლით. კონვენციის განმარტებითი ბარათის 171-ე პუნქტის შესაბამისად, *„გამოთხოვა წარმოადგენს მოქნილ მექანიზმს, რომლის გამოყენებაც საგამოძიებო ორგანოებს შეუძლიათ მრავალ შემთხვევაში, განსაკუთრებით იმ ღონისძიებების ნაცვლად, რომლებიც თავისი არსით უფრო იძულებითია. ამგვარი ღონისძიებების ეროვნულ კანონმდებლობაში არსებობა და მათი გამოყენება ასევე სასარგებლოა მესამე პირებისთვის, რომლებიც ინახავენ მონაცემებს, როგორებიც არიან, მაგალითად, მომსახურების მიმწოდებლები, რომლებიც ხშირად მზად არიან დახმარება გაუწიონ სამართალდამცავ ორგანოებს ნებაყოფლობით საწყისზე იმ მონაცემების ნებაყოფლობით მიწოდებით, რომელიც მათ კონტროლ ქვეშაა, თუმცა ამჯობინებენ შესაბამისი სამართლებრივი საფუძვლის ქონას ამგვარი დახმარების აღმო-*

7 “Convention on Cybercrime” (2001). Article 18, Paragraph 3, Council of Europe. <https://rm.coe.int/1680081561> [ბოლო წვდომა: 9 სექტემბერი, 2022]

8 Kunappu. M., Jurich. M. (2017). Report on Georgia, “Draft legislation supplementing and amending various issues related to cybercrime and electronic evidence”. Cybercrime Convention Committee bureau and Council of Europe. p. 7. <https://rm.coe.int/3608-20-georgia-cybercrime-law-reform-review-final-19-april-2017/168076be28> [ბოლო წვდომა: 9 სექტემბერი, 2022]

9 Cybercrime Convention Committee (2014). “Rules on obtaining subscriber information”. Report adopted by the T-CY at its plenary, Directorate General of Human Rights and Rule of Law, Council of Europe. P. 17-20. <https://rm.coe.int/16802e7ad1> [ბოლო წვდომა: 9 სექტემბერი, 2022]

*ჩენისთვის, ჰაც მათ გაათავისუფლებს ნებისმიერი სახის სახელშეკრულებო ან არა სახელშეკრულებო ვალდებულებისაგან“.*[10]

ამგვარად, გამოთხოვის მექანიზმი განიხილება, როგორც ამავე კონვენციის მე-19 მუხლით გათვალისწინებული კომპიუტერული მონაცემების ჩხრეკა-ამოღების ალტერნატიული, ნაკლებად რეპრესიული მექანიზმი, რომლის ძირითადი არსი გამოიხატება შემდეგში: თუ სუბიექტი, რომლისგანაც უნდა განხორციელდეს ინფორმაციის გამოთხოვა, სანდოა (მაგალითად, ინფორმაცია გამოთხოვილ უნდა იქნას მომსახურების მიმწოდებლისგან: მაგთიკომი, ჯეოსელი, Meta, Google და ა.შ.) და მას არ გააჩნია ობიექტური დაინტერესება – შეცვალოს ან გაანადგუროს გამოთხოვილი მონაცემები, ამოღების საგამოძიებო მოქმედების ნაცვლად გამოყენებულ უნდა იქნას ნაკლებად რეპრესიული გამოთხოვის მექანიზმი.

## მომსახურების მომწოდებლებსა და სამართალდამცავ ორგანოებს შორის თანამშრომლობა და მასთან დაკავშირებული პრობლემები

კიბერდანაშაულის გამოძიებისას დამნაშავის იდენტიფიცირების მიზნით ძირითადად აუცილებელია ტრაფიკის მონაცემების ანალიზი. მათ შორის, IP მისამართები და სხვადასხვა ელექტრონული მოწყობილობების მახასიათებლები, რომლებსაც იყენებს დამნაშავე დანაშაულის ჩადენის პროცესში, წარმოადგენს გამოძიებისთვის კრიტიკულად მნიშვნელოვან ინფორმაციას. გარდა იმისა, რომ ზოგადად დიდ სირთულესთან არის დაკავშირებული კონკრეტული IP მისამართის დადგენა და კიბერდამნაშავის იდენტიფიცირება, დამატებით ბარიერს ქმნის ის გარემოება, რომ გამოძიებისთვის საინტერესო ტრაფიკის მონაცემები შესაძლოა ავტომატურად წაიშალოს დროის საკმაოდ მცირე მონაკვეთში.

აღნიშნული პრობლემის დაძლევის მიზნით, „კომპიუტერული დანაშაულის შესახებ“ ბუდაპეშტის კონვენციის მე-16 მუხლით გათვალისწინებულია მომსახურების მომწოდებლების მერ შენახულ კომპიუტერულ მონაცემთა დაჩქარებული დაცვის პროცედურული სამართლებრივი მექანიზმი. კონვენციის ხელმომწერი თითოეული სახელმწიფო ვალდებულია მიიღოს ისეთი საკანონმდებლო რეგულაციები, რომლებიც უფლებამოსილ სამართალდამცავ ორგანოებს უფლებას მიანიჭებენ – გასცენ შესაბამისი ბრძანება და უზრუნველყონ კომპიუტერული მონაცემების შენახვა მომსახურების მომწოდებლებთან. აღნიშნული განსაკუთრებით ეხება იმ შემთხვევებს, როდესაც არსებობს მნიშვნელოვანი კომპიუტერული მონაცემის დაკარგვის ან გამოცვლის საფრთხე.[11]

კონვენციის 29-ე მუხლის თანახმად, კონვენციის წევრმა სახელმწიფომ შესაძლოა მოსთხოვოს სხვა წევრ სახელმწიფოს, რომ მოხდეს მის ტერიტორიაზე არსებული კონკრეტული კომპიუტერული მონაცემების დაჩქარებული დაცვა, რათა შემდგომ, ურთიერთდახმარების მოთხოვნის საფუძველზე, მოახდინოს მათი გამოთხოვა. აღნიშნული სახის მოთხოვნა უნდა აკმაყოფილდებოდეს გარკვეულ კრიტერიუმებს და შეიცავდეს უფლებამოსილი ორგანოს დასახელებას, რომელიც ითხოვს ინფორმაციის შენახვას, ასევე, მითითებული უნდა იყოს დანაშაული, რომელზეც მიმდინარეობს გამოძიება და/ან ხორციელდება სისხლისსამართლებრივი დევნა, შესანახი კომპიუტერული მონაცემების კავშირი აღნიშნულ დანაშაულთან და შენახვის აუცილებლობა.[12]

კომპიუტერული მონაცემების შენახვის რეგულაციები წარმოადგენენ მნიშვნელოვან სამართლებრივ საგამოძიებო ინსტრუმენტს კომპიუტერული დანაშაულის გამოძიების მიზნებისთვის. კომპიუტერული მონაცემების ცვალებადი ბუნების გათვალისწინებით, მაღალია მათი შესაძლო გამოცვლის ან დაკარგვის რისკი. აღნიშნულიდან გამომდინარე, გამოძიებისთვის მნიშვნელოვანი მტკიცებულება

10 Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. P. 29. <https://rm.coe.int/16800cce5b> [ბოლო წვდომა: 9 სექტემბერი, 2022]

11 “Convention on Cybercrime” (2001). Article 16, Council of Europe. <https://rm.coe.int/1680081561> [ბოლო წვდომა: 9 სექტემბერი, 2022]

12 “Convention on Cybercrime” (2001). Article 29, Council of Europe. <https://rm.coe.int/1680081561> [ბოლო წვდომა: 9 სექტემბერი, 2022]

შესაძლოა დაიკარგოს შენახვის არასწორი მენეჯმენტის, უყურადღებობის, განზრახი მანიპულაციის/წაშლის ან იმის გამო, რომ მომსახურების მომწოდებლებს არ ჭირდებათ მათი შენახვა და ავტომატურად შლიან ინფორმაციას. მიზეზი ამ ავტომატური წაშლის არის ის გარემოება, რომ თითოეული მოქმედების განხორციელებისას წარმოშობილი ტრაფიკის მონაცემების შენახვა წარმოუდგენლად დიდ დანახარჯებთან არის დაკავშირებული და გაზრდის მომსახურების საფასურს.

უფლებამოსილი ორგანოების მიერ, ბუდაპეშტის კონვენციით გათვალისწინებული დებულებების შესაბამისად, მომსახურების მომწოდებლების დავალდებულება – მოახდინონ გამოძიებისთვის საინტერესო კომპიუტერული მონაცემების რეზერვაცია – შესაძლოა დაკავშირებული იყოს დამატებით ხარჯებთან, თუმცა, ჩხრეკისა და ამოღების საგამოძიებო მოქმედებებთან შედარებით, არ უშლის ხელს მათ ნორმალურ ფუნქციონირებას. აქვე უნდა აღინიშნოს, რომ კომპიუტერული დანაშაულის დიდი ნაწილი ჩადენილია კომპიუტერული სისტემების გამოყენებით განხორციელებული კომუნიკაციების გზით. აღნიშნული კომუნიკაციები შესაძლოა იყოს დანაშაულებრივი ქმედებების ამსახველი და შეიცავდეს მნიშვნელოვან მტკიცებულებებს ისეთ მძიმე დანაშაულებზე, როგორიც არის ბავშვთა პორნოგრაფია, ნარკოტიკებით ვაჭრობა, კომპიუტერული სისტემების ნორმალური ფუნქციონირებისთვის ხელის შეშლა და ა.შ. შესაბამისად, წყაროს ან დანიშნულების მისამართის გაშიფვრა შესაძლოა დაეხმაროს სამართალდამცავ ორგანოებს დამნაშავეების იდენტიფიცირებაში, აღნიშნულისთვის კი აუცილებელია განხორციელებული კომუნიკაციის ტრაფიკის არსებობა და მისი ანალიზი.[13]

ყოველივე ზემოაღნიშნულის გათვალისწინებით, სამართალდამცავ ორგანოებსა და ინტერნეტის მომსახურების მომწოდებლებს შორის მჭიდრო თანამშრომლობა ყოველთვის წარმოადგენდა კიბერდანაშაულის წინააღმდეგ ეფექტიანი ბრძოლის მნიშვნელოვან წინაპირობას. ბუდაპეშტის კონვენცია შეიცავს დებულებებს, რომელიც ავალდებულებს წევრ სახელმწიფოებს – შექმნან შესაბამისი საკანონმდებლო ბაზა მომსახურების მომწოდებლებთან ინფორმაციის შენახვისა და მათგან ინფორმაციის გამოთხოვის თვალსაზრისით, თუმცა საბოლოოდ ყველაზე მნიშვნელოვანია, თუ როგორ აისახა/აისახება აღნიშნული წევრი სახელმწიფოების ეროვნულ კანონმდებლობებში.

მსოფლიოს სხვადასხვა ქვეყანაში არსებობს მომსახურების მომწოდებლებთან თანამშრომლობის განსხვავებული პრაქტიკა. აღნიშნული თანამშრომლობა შესაძლებელია ატარებდეს ნებაყოფლობით ხასიათს ან შემუშავებული იყოს საკანონმდებლო ჩარჩო. იმ ქვეყნებში, სადაც მომსახურების მომწოდებლების მიერ კომპიუტერული მონაცემების სამართალდამცავი ორგანოებისთვის მიწოდება ან შესაბამისი მოთხოვნის საფუძველზე მათი შენახვა წარმოებს ნებაყოფლობით, სამართალდამცავ ორგანოებს შეუძლიათ მოითხოვონ აღნიშნული მოქმედების განხორციელება მაშინაც კი, როდესაც არ გააჩნიათ სათანადო საფუძველი. მსგავსი მიდგომა იმ ქვეყნებში არის შესაძლებელი, სადაც არ არის დაწესებული შეზღუდვები მომსახურების მომწოდებლების ქმედებებზე.

აშშ-ის 1986 წლის კომუნიკაციებისა და კონფიდენციალურობის კანონი (ECPA) არის საკმაოდ მოქნილი სამართალდამცავ ორგანოებთან თანამშრომლობის თვალსაზრისით და მომსახურების მომწოდებლებს ანიჭებს უფლებას ნებაყოფლობით გაამჟღავნონ არაშინაარსობრივი სახის კომპიუტერული მონაცემები. აღნიშნული კანონი მომსახურების მომწოდებლებს უკრძალავს ნებაყოფლობით გაამჟღავნონ შინაარსობრივი კომპიუტერული მონაცემები, გარდა საგანგებო შემთხვევებისა.[14]

სამართალდამცავ ორგანოებსა და მომსახურების მომწოდებლებს შორის ინფორმაციის შენახვისა და წარმოდგენის თაობაზე თანამშრომლობის ნებაყოფლობით საწყისებზე დაფუძნება დადებით მხარეებთან ერთად

13 Council of Europe (2001). "Explanatory Report to the Convention on Cybercrime", Council of Europe. P. 25-26. <https://rm.coe.int/16800cce5b> [ბოლო წვდომა: 9 სექტემბერი, 2022]

14 Council of Europe (2008). "Cooperation between law enforcement and Internet service providers against cybercrime", Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. p. 17. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [ბოლო წვდომა: 9 სექტემბერი, 2022].

შეიცავს უარყოფით ელემენტებსაც. კერძოდ, სამართალდამცავ ორგანოებს არ შეუძლიათ წინასწარ განჭვრიტონ – წარმოადგენს თუ არა მომსახურების მომწოდებელი ინფორმაციას და დადებით შემთხვევაში – რა მოცულობით. საერთაშორისო თანამშრომლობის ფარგლებში ევროპის სამართალდამცავ ორგანოებს შეუძლიათ მიიღონ მონაცემები აშშ-ში დაფუძნებული სერვისის პროვაიდერებისგან, თუმცა აშშ ვერ გამოიყენებს იგივე შესაძლებლობას, რადგან ევროპაში მომსახურების მიმწოდებლებს აქვთ მკაცრად რეგულირებული სამართლებრივი ვალდებულებები, რომლებიც დაკავშირებულია მათი მომხმარებლების უფლებების დაცვასა და პირადი მონაცემების შენახვასთან.

საქართველოში 2010 წელს ხელი მოეწერა ურთიერთგაგების მემორანდუმს სამართალდამცავ ორგანოებსა და 10 უმსხვილეს ინტერნეტის მომსახურების მომწოდებელს შორის. აღნიშნული მემორანდუმით განსაზღვრულია თანამშრომლობის ძირითადი პრინციპები კიბერდანაშაულის გამოძიების პროცესში სამართალდამცავ ორგანოებსა და მომსახურების მომწოდებლებს შორის. დოკუმენტში, ასევე, გაწერილია რომ მომსახურების მომწოდებლები ვალდებულები არიან გამოყონ საკონტაქტო პირები სამართალდამცავ ორგანოებთან თანამშრომლობის მიზნით, რაც მნიშვნელოვნად ამცირებს მოთხოვნილი ინფორმაციის დამუშავების პროცესს.[15]

აღნიშნული მემორანდუმის ფარგლებში გაწერილია მომსახურების მომწოდებლების უფლებები და ვალდებულებები. კერძოდ, ისინი ვალდებულები არიან, საქართველოს კანონმდებლობით დადგენილი წესების შესაბამისად, სამართალდამცავებს წერილობით მიაწოდონ მათ ხელთ არსებული ინფორმაცია. იმ შემთხვევაში, თუ მომსახურების მომწოდებელი უარს იტყვის ინფორმაციის გაცემაზე, მან უნდა დაასაბუთოს, თუ რამ განაპირობა მოთხოვნის შეუსრულებლობა. მემორანდუმი, ასევე, ითვალისწინებს სამართალდამცავი ორგანოების ვალდებულებას – მიაწოდონ მომსახურების მომწოდებლებს გამოძიების შესახებ მაქსიმალური ინფორმაცია, რომლის გამჟღავნებაც არ ეწინააღმდეგება გამოძების ინტერესებს.[16]

აღნიშნული საკითხის დეტალურად შესწავლის თვალსაზრისით, საინტერესოა ინტერნეტის მომსახურების მომწოდებლებსა და ბუდაპეშტის კონვენციის ხელმოწმერ სხვადასხვა ქვეყნებს შორის ურთიერთობის მოკლე ანალიზი. დანიაში სამართალდამცავ ორგანოებსა და მომსახურების მომწოდებლებს შორის თანამშრომლობა ეფუძნება არაფორმალურ შეთანხმებებს ინფორმაციის გაცვლის თაობაზე, რომლის ძირითადი პრინციპები თანხვედრაშია ელექტრონული კომუნიკაციების ქსელებისა და მომსახურების კანონთან. სამართალდამცავ ორგანოებსა და სხვა კერძო სექტორის კომპიუტერულ მონაცემთა მფლობელებთან ურთიერთანამშრომლობა განისაზღვრება თითოეულ შემთხვევაში ინდივიდუალურად.

ევროსაბჭოსა და ევროკავშირის ხელშეწყობით, 2007 წელს შეიქმნა სამუშაო ჯგუფი, რომელმაც შეიმუშავა სამართალდამცავ ორგანოებსა და მომსახურების მომწოდებლებს შორის თანამშრომლობის გზამკვლევი. აღნიშნული პროექტის ფარგლებში განხილულ იქნა სხვადასხვა ქვეყნებში არსებული პრაქტიკა. ანგარიშის მიხედვით, საფრანგეთში შინაგან საქმეთა სამინისტროსა და მომსახურების მომწოდებლებს შორის დადებულია პარტნიორობის შეთანხმება, რომლის თანახმადაც ინფორმაციის გადმოცემა ხდება ნებაყოფლობით. ძირითადად ხდება 3 კატეგორიის ინფორმაციის გამოთხოვა: 1) ზოგად საკითხებზე; 2) ინდივიდებისა და ქონების მიმართ ჩადენილ მძიმე დაზიანებებზე; 3) ტერორიზმთან და ქვეყნის ეროვნულ ინტერესებთან დაკავშირებულ საკითხებზე. უნგრეთში მიღებულია კანონმდებლობა, რომელიც პირდაპირ ავალდებუ-

15 Council of Europe (2008). "Cooperation between law enforcement and Internet service providers against cybercrime", Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. p. 18. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [ბოლო წვდომა: 9 სექტემბერი, 2022].

16 Georgian National Communications Commission, Ministry of Internal Affairs and Internet Service Providers, (2010). "Memorandum of Understanding between Georgian law enforcement and Internet providers based on the principles of cooperation in the field of cybercrime". pp. 2-3. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fe136> [ბოლო წვდომა: 9 სექტემბერი, 2022].

ლებს მომსახურების მომწოდებლებს, რომ მათ წარმოადგინონ მათ ხელთ არსებული კომპიუტერული მონაცემები, რომელიც მნიშვნელოვანია სამართალდამცავი ორგანოებისთვის. აღნიშნული რეგულირდება სისხლის სამართლებრივი პროცედურების თაობაზე 1998 წელს მიღებული კანონით. აღნიშნული კანონის გარდა, უნგრეთის პოლიციასა და ინტერნეტის მომსახურების მომწოდებლებს შორის დადებულია შეთანხმებებიც თანამშრომლობის თაობაზე. იაპონიაში სამსართალდამცავებსა და მომსახურების მომწოდებლებს შორის არის მჭიდრო თანამშრომლობა ინფორმაციის გაცვლასთან დაკავშირებით, რომლის მთავარ მიზანს წარმოადგენს გამოძიებისთვის მნიშვნელოვანი ამოსაღები ინფორმაციის ადგილმდებარეობისა და მოცულობის ზუსტი განსაზღვრა, რაც ემსახურება მომსახურების მომწოდებლების საქმიანობის შეუფერხებლად გაგრძელებას და, ასევე, მესამე პირთა უფლებების მაქსიმალურად დაცვას.[17]

რაც შეეხება კომპიუტერული ინფორმაციის მომსახურების მომწოდებლების მიერ რეზერვაციას, აღნიშნული დღემდე წარმოადგენს პრობლემურ საკითხს. ევროპისა და მსოფლიოს ქვეყნების უმეტეს ნაწილში არ არსებობს რეგულაციები, რომლებიც დაავალდებულებენ მომსახურების მომწოდებლებს – შეინახონ განხორციელებული ტრაფიკის თაობაზე ინფორმაცია ხანგრძლივი პერიოდის განმავლობაში. აღნიშნული გამოიწვევს კოლოსალურ ხარჯს და პირდაპირ დაკავშირებულია სერვისის საფასურის ზრდასთან. ამასთანავე, მომსახურების მომწოდებლებს ცალკე ვალდებულებები გააჩნიათ მომხმარებელთა ინტერესების დაცვის კუთხით და კომპიუტერული შინაარსობრივი მონაცემების დიდი პერიოდის განმავლობაში შენახვა ეწინააღმდეგება მათ კონფიდენციალურობის პოლიტიკას.

აშშ-ში მომსახურების მომწოდებლების მიერ ძირითადად ხდება ინფორმაციის შენახვა რამდენიმე თვის განმავლობაში, თუმცა არ არის მკაცრად დადგენილი კონკრეტული ვადა. აღნიშნული ატარებს ნებაყოფლობით ხასიათს და არ არის განსაზღვრული ნორმატიული აქტით. ევროკავშირის ქვეყნებში მოქმედი მომსახურების მომწოდებლებისგან ინფორმაციის მიღება გაცილებით პრობლემურია, რადგან ისინი, ძირითადად, დიდი დროით არ ინახავენ ინფორმაციას შესაბამისი სამართლებრივი რეგულაციის არარსებობის პირობებში და, საჭიროების შემთხვევაში, ინფორმაციის რეზერვაცია უნდა მოხდეს რაც შეიძლება სწრაფად, რათა გამოირიცხოს მტკიცებულების გამოცვლის, წაშლის ან დაკარგვის რისკი.

## ელექტრონული მტკიცებულებების დამაგრება სისხლის სამართლის საქმეზე

ელექტრონული მტკიცებულება არის ინფორმაცია, რომელიც ელექტრონული სახით ინახება კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში. საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის თანახმად, აღნიშნული სახის კომპიუტერული ინფორმაციის მოსაპოვებლად აუცილებელია ინფორმაციის გამოთხოვის თაობაზე სასამართლოს განჩინების მიღება.

აღსანიშნავია, რომ საქართველოს კანონმდებლობა არ ახდენს კომპიუტერული ინფორმაციის/მონაცემის დიფერენცირებას. შესაბამისად, იმ შემთხვევაში, თუ გამომძიებელი სისხლის სამართლის საქმეზე გამოძიების ჩატარებისას გადაწყვეტს, რომ მოიპოვოს ინფორმაცია ან მტკიცებულება, რომელიც ინახება კომპიუტერულ სისტემაში ან ელექტრონულ მატარებელზე (მეხსიერების ბარათი, კომპაქტ დისკი და ა.შ.), პროკურორი უპირობოდ ვალდებულია, რომ აღნიშნული ინფორმაციის გამოთხოვის მიზნით მიმართოს სასამართლოს შუამდგომლობით განჩინების გაცემის თაობაზე. ამასთანავე, ვინაიდან ელექტრონული მტკიცებულების მოდიფიკაცია უკვე არ წარმოადგენს დიდ სირთულეს, მოსაპოვებელი მტკიცებულების დაკარგვის ან გამოცვლის რისკის პრევენციის მიზნით,

17 Council of Europe (2008). "Cooperation between law enforcement and Internet service providers against cybercrime", Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. pp. 17 – 19. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [ბოლო წვდომა: 9 სექტემბერი, 2022]

პრაქტიკაში გამომძიებელი, ძირითადად, გადაუდებელი აუცილებლობიდან გამომდინარე იღებს კომპიუტერული ინფორმაციის მატარებელ მოწყობილობას და შემდგომ პროკურორი მიმართავს სასამართლოს აღნიშნული საგამოძიებო მოქმედების კანონიერად ცნობის თაობაზე შუამდგომლობით. აღნიშნული საგამოძიებო მოქმედების (ამოღების) კანონიერად ცნობის შემდეგ, პროკურორი უკვე მიმართავს სასამართლოს გამოძიების ხელთ კანონიერად არსებული ელექტრონული მოწყობილობიდან ინფორმაციის გამოთხოვის შუამდგომლობით.

ზემოთ აღწერილი პრაქტიკის ჩამოყალიბებას ხელი შეუწყო როგორც სსსკ-ის 136-ე მუხლის ზოგადმა დეფინიციამ და ელექტრონული მტკიცებულებების მოპოვებისას რაიმე სახის კატეგორიზაციის არარსებობამ, ასევე საქართველოს საერთო სასამართლოებში ელექტრონული მტკიცებულებებს მოპოვების წესთან და მათ დასაშვებობასთან დაკავშირებულმა არაერთგვაროვანმა პრაქტიკამ.

თბილისის სააპელაციო სასამართლოს 2016 წლის 30 მარტის №1გ/548-16 განჩინებაში მოსამართლემ იმსჯელა, რომ *„მიკჰოსაფინანსო ოჰაგანიზაცია „თ.-ს“ კამეჩით აღბეჭდილი ვიდეოჩანაწერები, უდავოა, რომ წარმოადგენს კომპიუტერულ სისტემაში დაცულ კომპიუტერულ მონაცემს, ხოლო გამოძიებისთვის წარდგენილი დისკი არის კომპიუტერულ მონაცემთა შესანახი საშუალება, რომელშიც საქმისათვის მნიშვნელოვანი ინფორმაცია აღბეჭდილია ვიდეოჩანაწერის სახით. შესაბამისად, იმის გამო, რომ ვიდეოჩანაწერები გამოთხოვილი იქნა მხოლოდ მიმართვის წერილების საფუძველზე, საგამოძიებო კოლეგიას მიაჩნია, რომ აღნიშნულით არ იქნა დაცული შესაბამისი სტანდარტი. კერძოდ, ის, რომ დაუშვებელია მიმართვის საფუძველზე საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით განსაზღვრული ინფორმაციის გამოთხოვა. საქმეში არ არის უფლებამოსილი პირის შესაბამისი მოქმედების ამსახველი საპროცესო დოკუმენტი და ყველა მონაცემი მიუთითებს იმის შესახებ, რომ კომპიუტერულ მონაცემთა შესანახ საშუალებაში დაცული მონაცემები იქნა გამოთხოვილი გამომძიებლის მიერ წერილის საშუალებით, რაც თავისთავად დაუშვებელია და დათვალიერების ოქმი და ვიდეოდისკები კანონის დარღვევით დაუშვებელ მტკიცებულებად უნდა იქნას დატოვებული“.*[18]

თბილისის სააპელაციო სასამართლოს 2017 წლის 19 ივლისის №1გ/960-17 განჩინებით სასამართლომ დაადგინა, რომ *„ბრალდების მხარის მიერ მოთხოვნილია კომპიუტერულ სისტემაში დაცული ინფორმაციის, მობილური ტელეფონში არსებული ინფორმაციის ამოღება. კერძოდ, გამოძიების ინტერესშია ა. ჩ.-ს კუთვნილ „აიფონი“-ს ფირმის მობილური ტელეფონში ნანახი საქმისათვის მნიშვნელოვანი ინფორმაციის ამოღება და არა კონკრეტულად მხოლოდ მობილური ტელეფონის, როგორც ნივთის ამოღება, რამეთუ მობილური ტელეფონი ცალკე აღებული მასში არსებული ინფორმაციის გარეშე საქმისათვის მნიშვნელოვანი არ არის. ამ შემთხვევაში ხსენებული მობილური ტელეფონი წარმოადგენს სწორედ კომპიუტერულ სისტემას, რომელშიც შენახულია ინფორმაცია. მობილური ტელეფონი ცალკე ნივთის სახით ამოღების ობიექტი შეიძლება იყოს მხოლოდ მაშინ, თუ იგი დანაშაულის იარაღი ან საგანია ან თავად ტელეფონი არის მტკიცებულების მატარებელი, ხოლო როდესაც მობილური ტელეფონის ამოღების მოთხოვნა მიმართულია ჰეალუად მასში არსებული ინფორმაციის შემდგომი გამოყენებისათვის, ასეთ ვითარებაში დაცული უნდა იქნეს სასამართლოსთვის მიმართვის კანონით დადგენილი ფორმა და წესი. ხსენებული ინფორმაციის მოპოვების სპეციალური წესი კი იმპერატიულად არის დადგენილი საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით“.*[19]

სასამართლოს აღნიშნული გადაწყვეტილების შეფასებისას მნიშვნელოვან გარემოებას წარმოადგენს ის ფაქტი, რომ ბრალდების მხარე ითხოვდა, გადაუდებელი აუცილებლობიდან გამომდინარე, ამოღებული მობილური ტელეფონის ამოღების კანონიერად ცნობას, ვინაიდან მასში დაცული მონაცემები წარმოადგენდა გამოძიებისთვის მნიშვნელოვან ინფორმაციას. სასამართლომ იმსჯელა, რომ

18 №1გ/548-16 განჩინება (2016). “საჩივრის დაკმაყოფილებაზე უარის თქმის შესახებ“. თბილისის სააპელაციო სასამართლო. <http://library.court.ge/judgements/92352016-04-04.pdf> [ბოლო წვდომა: 9 სექტემბერი, 2022].

19 №1გ/960-17 განჩინება (2017). “საჩივრის დაკმაყოფილებაზე უარის თქმის შესახებ“. თბილისის სააპელაციო სასამართლო. <http://library.court.ge/judgements/5582017-07-25.pdf> [ბოლო წვდომა: 9 სექტემბერი, 2022].

გამოძიების ინტერესის საგანი იყო არა თავად ობიექტი (მობილური ტელეფონი), არამედ მასში არსებული ინფორმაცია, შესაბამისად, უნდა მომხდარიყო ინფორმაციის გამოთხოვა. ამ დროს უნდა გავითვალისწინოთ, რომ ინფორმაციის გამოთხოვის თაობაზე სასამართლოსთვის მიმართვის შემთხვევაში არ არსებობს ინფორმაციის მატარებელი ობიექტის გამოძიების ფარგლებში დატოვების შესაძლებლობა, რაც, თავის მხრივ, ზრდის მასში არსებული ელექტრონული მტკიცებულების შესაძლო გამოცვლის ან დაკარგვის რისკს. საქართველოს კანონმდებლობა, ასევე, არ შეიცავს განსხვავებულ წესს საჯაროდ ხელმისაწვდომი ელექტრონული მტკიცებულების სისხლის სამართლის საქმეზე დამაგრების თვალსაზრისითაც. აღნიშნულ შემთხვევაშიც სასამართლო მხარეებისგან ითხოვს, რომ ზედმიწევნით დაიცვან საქართველოს სსსკ-ის 136-ე მუხლით განსაზღვრული ზოგადი წესი და მომსახურების მომწოდებლებისგან (რომელთა სათაო ოფისიც ძირითად შემთხვევაში საზღვარგარეთ მდებარეობს) გამოითხოვონ საჯაროდ ხელმისაწვდომი ინფორმაცია. გამონაკლისს არ წარმოადგენს გარემოება, როდესაც გამოძიების ინტერესის საგანს წარმოადგენს არა თავად მოსაპოვებელი მტკიცებულების კომპიუტერული ელემენტი, არამედ ზოგადად ვიზუალურად ასახული ინფორმაცია (ფოტო, ვიდეო, ტექსტი და ა.შ.).

## დასკვნა

საქართველოს კანონმდებლობაში ელექტრონული მტკიცებულებების კატეგორიზაციის არარსებობა და ინფორმაციის გამოთხოვის მიმართ არაერთგვაროვანი პრაქტიკა წარმოშობს გარკვეულ პროცესუალურ ბარიერებს, განსაკუთრებით, კიბერდანაშაულის გამოძიების მიმართულებით.

საკანონმდებლო ცვლილებების მიღებისას და კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის კონვენციით გათვალისწინებული დებულებების სწორი იმპლემენტაციის მიზნით, აუცილებლია სწორად იქნას გაგებული კანონმდებლის მიზანი. კერძოდ, კონვენციის მე-18 მუხლით გათვალისწინებული დოკუმენტის/ინფორმაციის გამოთხოვის ბრძანების ძირითად მიზანს წარმოადგენდა ჩხრეკა-ამოღების ალტერნატიული, ნაკლებად რეპრესიული მექანიზმის შემუშავება იმ შემთხვევებში, როდესაც სუბიექტი, საიდანაც ხდება ინფორმაციის გამოთხოვა, არის სანდო და სახეზე არ არის ელექტრონული მტკიცებულების შესაძლო დაკარგვის ან გამოცვლის რისკი. ნაცვლად იმისა, რომ კანონმდებლობის დონეზე მომხდარიყო კომპიუტერული მონაცემების დიფერენცირება, რომელთა გამოთხოვაც შესაძლებელი იქნებოდა გამომძიებლის ან პროკურორის წერილობითი მოთხოვნით (როგორც ეს მიღებულია ევროპის ბევრ ქვეყანაში), ჩამოყალიბდა პრაქტიკა, რომლის მიხედვითაც სასამართლოები დასაშვებად მიიჩნევენ კომპიუტერული სისტემის, როგორც ფიზიკური ობიექტის ამოღებას, თუმცა, ამოღების შემდეგ კომპიუტერულ სისტემაში არსებულ ინფორმაციაზე წვდომისთვის აუცილებელია დამატებით მოსამართლის განჩინების აღება კომპიუტერულ სისტემაში არსებული მონაცემების გამოთხოვის შესახებ. ამგვარად, კომპიუტერული მონაცემებზე წვდომის მიზნით, საგამოძიებო ორგანოს ფაქტობრივად ესაჭიროება მოსამართლის ორი განჩინების მოპოვება – კომპიუტერული სისტემის ამოღებაზე და ამოღებული კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვაზე, რასაც არ გააჩნია ანალოგი მსოფლიო პრაქტიკაში. ამასთან, გაუგებარია, თუ ვისგან უნდა გამოითხოვონ ინფორმაცია, რომელიც ისედაც საგამოძიებო ორგანოს ხელშია.

უნდა აღინიშნოს, რომ მომსახურების მომწოდებლებსა და სამართალდამცავ ორგანოებს შორის მჭიდრო თანამშრომლობაზე დიდწილად არის დამოკიდებული კიბერდანაშაულის გამოძიების ეფექტიანობის ხარისხი. ამდენად, მიზანშეწონილია, გაზიარებულ იქნას რიგი ქვეყნების გამოცდილება და მოხდეს დანაშაულთა და კიბერდანაშაულთა კატეგორიზაცია, რომელთა მიხედვითაც შემუშავდება მომსახურების მომწოდებლებისგან ინფორმაციის გამოთხოვისა და რეზერვაციის განსხვავებული მიდგომები. კერძოდ, იმ შემთხვევაში, როდესაც საკითხი დაკავშირებულია მძიმე ან განსაკუთრებით მძიმე დანაშაულთან ან ეხება ქვეყნის უსაფრთხოების ინტერესებს, მომსახურების მომწოდებლებისგან ინფორმაციის რეზერვაცია უნდა განხორციელდეს

დაუყოვნებლივ, ხოლო გარკვეული სახის არაშინაარსობრივი ინფორმაციის მოპოვება სასამართლოს განჩინების გარეშე გახდეს ნებადართული. ხსენებული მიდგომის იმპლემენტირებისთვის საჭიროა როგორც საკანონმდებლო ცვლილებები, ასევე თანამშრომლობის თაობაზე მემორანდუმის გაფორმება საგამოძიებო უწყებებსა და მომსახურების მომწოდებლებს შორის.

---


**ბიბლიოგრაფია:**

**საკანონმდებლო აქტები:**

1. კონვენცია „კომპიუტერული დანაშაულის შესახებ“ (2001). მუხლები: 2 – 5 და 16 – 21, ევროპის საბჭო. <https://rm.coe.int/1680081561>
2. საქართველოს სისხლის სამართლის საპროცესო კოდექსი (2009). მუხლი 136 (13.04.2022 წლის რედაქცია). საქართველოს საკანონმდებლო მაცნე. <https://www.matsne.gov.ge/document/view/90034?publication=143>
3. საქართველოს სისხლის სამართლის საპროცესო კოდექსი (2009). მუხლი 136 (21.06.2022 წლის რედაქცია). საქართველოს საკანონმდებლო მაცნე. <https://www.matsne.gov.ge/ka/document/view/90034?publication=146>

**სასამართლო გადაწყვეტილებები:**

1. №1გ/548-16 განჩინება (2016). „საჩივრის დაკმაყოფილებაზე უარის თქმის შესახებ“. თბილისის სააპელაციო სასამართლო. <http://library.court.ge/judgements/92352016-04-04.pdf>
2. №1გ/960-17 განჩინება (2017). „საჩივრის დაკმაყოფილებაზე უარის თქმის შესახებ“. თბილისის სააპელაციო სასამართლო. <http://library.court.ge/judgements/5582017-07-25.pdf>

**უცხოენოვანი ლიტერატურა:**

1. Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. <https://rm.coe.int/16800cce5b>
2. Kunappu. M., Jurich. M. (2017). Report on Georgia, “Draft legislation supplementing and amending various issues related to cybercrime and electronic evidence”. Cybercrime Convention Committee bureau and Council of Europe. <https://rm.coe.int/3608-20-georgia-cybercrime-law-reform-review-final-19-april-2017/168076be28>
3. Cybercrime Convention Committee (2014). “Rules on obtaining subscriber information”. Report adopted by the T-CY at its plenary, Directorate

**BIBLIOGRAPHY:**

**Legal Acts:**

1. “Convention on Cybercrime” (2001). Articles 2 – 5 and 16 – 21, Council of Europe. <https://rm.coe.int/1680081561> (In English)
2. Criminal Procedure Code of Georgia (2009). Article 136, Paragraph I, (13.04.2022 Edition). Legislative Herald of Georgia. <https://www.matsne.gov.ge/document/view/90034?publication=143> (In Georgian)
3. Criminal Procedure Code of Georgia (2009). Article 136, Paragraph I, (21.06.2022 Edition). Legislative Herald of Georgia. <https://www.matsne.gov.ge/ka/document/view/90034?publication=146> (In Georgian)

**Court Orders:**

1. Tbilisi Court of Appeals order №1გ/548-16 (2016). “Order on inadmissability of evidence”. Tbilisi Court of Appeals. <http://library.court.ge/judgements/92352016-04-04.pdf> (In Georgian)
2. Tbilisi Court of Appeals order №1გ/960-17 (2017). “Order on inadmissability of evidence”. Tbilisi Court of Appeals. <http://library.court.ge/judgements/5582017-07-25.pdf> (In Georgian)

**Used Literature:**

1. Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. <https://rm.coe.int/16800cce5b> (In English)
2. Kunappu. M., Jurich. M. (2017). Report on Georgia, “Draft legislation supplementing and amending various issues related to cybercrime and electronic evidence”. Cybercrime Convention Committee bureau and Council of Europe. <https://rm.coe.int/3608-20-georgia-cybercrime-law-reform-review-final-19-april-2017/168076be28> (In English)
3. Cybercrime Convention Committee (2014). “Rules on obtaining subscriber information”. Report adopted by the T-CY at its plenary, Directorate General of Human Rights and Rule of Law, Coun-

General of Human Rights and Rule of Law, Council of Europe. <https://rm.coe.int/16802e7ad1>
4. Council of Europe (2008). "Cooperation between law enforcement and Internet service providers against cybercrime", Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7>
5. Georgian National Communications Commission, Ministry of Internal Affairs and Internet Service Providers, (2010). "Memorandum of Understanding between Georgian law enforcement and Internet providers based on the principles of cooperation in the field of cybercrime". <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fe136>

cil of Europe. <https://rm.coe.int/16802e7ad1> (In English)
4. Council of Europe (2008). "Cooperation between law enforcement and Internet service providers against cybercrime", Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> (In English)
5. Georgian National Communications Commission, Ministry of Internal Affairs and Internet Service Providers, (2010). "Memorandum of Understanding between Georgian law enforcement and Internet providers based on the principles of cooperation in the field of cybercrime". <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fe136> (In English)

**NOTES:**

1. Council of Europe (2001). "Explanatory Report to the Convention on Cybercrime", Council of Europe. p. 1. <https://rm.coe.int/16800cce5b> [Last access: 9 September, 2022]
2. "Convention on Cybercrime" (2001). Articles 2 – 5 and 16 – 21, Council of Europe. <https://rm.coe.int/1680081561> [Last access: 9 September, 2022]
3. "Convention on Cybercrime" (2001). Article 18, Council of Europe. <https://rm.coe.int/1680081561> [Last access: 9 September, 2022]
4. Council of Europe (2001). "Explanatory Report to the Convention on Cybercrime", Council of Europe. P. 29. <https://rm.coe.int/16800cce5b> [Last access: 9 September, 2022]
5. Legislative Herald of Georgia, Criminal Procedure Code of Georgia (Date of Issuing: 09.10.2009, Article 136, Paragraph I, 13.04.2022 Edition (Last Accessed 09.09.2022) <https://www.matsne.gov.ge/document/view/90034?publication=143> [Last access: 9 September, 2022]
6. Legislative Herald of Georgia, Criminal Procedure Code of Georgia (Date of Issuing: 09.10.2009, Article 136, Paragraph I, 21.06.2022 Edition (Last Accessed 09.09.2022) <https://www.matsne.gov.ge/ka/document/view/90034?publication=146> [Last access: 9 September, 2022]
7. "Convention on Cybercrime" (2001). Article 18, Paragraph 3, Council of Europe. <https://rm.coe.int/1680081561> [Last access: 9 September, 2022]
8. Kunappu. M., Jurich. M. (2017). Report on Georgia, "Draft legislation supplementing and amending various issues related to cybercrime and electronic evidence". Cybercrime Convention Committee bureau and Council of Europe. p. 7. <https://rm.coe.int/3608-20-georgia-cybercrime-law-reform-review-final-19-april-2017/168076be28> [Last access: 9 September, 2022]
9. Cybercrime Convention Committee (2014). "Rules on obtaining subscriber information". Report adopted by the T-CY at its plenary, Directorate General of Human Rights and Rule of Law, Council of Europe. pp. 17-20. <https://rm.coe.int/16802e7ad1> [Last access: 9 September, 2022]
10. Council of Europe (2001). "Explanatory Report to the Convention on Cybercrime", Council of Europe. p. 29. <https://rm.coe.int/16800cce5b> [Last access: 9 September, 2022]
11. "Convention on Cybercrime" (2001). Article 16, Council of Europe. <https://rm.coe.int/1680081561> [Last access: 9 September, 2022]

12. “Convention on Cybercrime” (2001). Article 29, Council of Europe. <https://rm.coe.int/1680081561> [Last access: 9 September, 2022]
13. Council of Europe (2001). “Explanatory Report to the Convention on Cybercrime”, Council of Europe. pp. 25-26. <https://rm.coe.int/16800cce5b> [Last access: 9 September, 2022]
14. Council of Europe (2008). “Cooperation between law enforcement and Internet service providers against cybercrime”, Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. p. 17. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [Last access: 9 September, 2022]
15. Council of Europe (2008). “Cooperation between law enforcement and Internet service providers against cybercrime”, Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. p. 18. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [Last access: 9 September, 2022]
16. Georgian National Communications Commission, Ministry of Internal Affairs and Internet Service Providers, (2010). “Memorandum of Understanding between Georgian law enforcement and Internet providers based on the principles of cooperation in the field of cybercrime”. pp. 2-3. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fe136> [Last access: 9 September, 2022]
17. Council of Europe (2008). “Cooperation between law enforcement and Internet service providers against cybercrime”, Common guidelines. Cybercrime Programme Office of the Council of Europe (C-PROC), Council of Europe. pp. 17 – 19. <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [Last access: 9 September, 2022]
18. Tbilisi Court of Appeals order №1ბ/548-16 (2016). “Order on inadmissability of evidence”. Tbilisi Court of Appeals. <http://library.court.ge/judgements/92352016-04-04.pdf> [Last access: 9 September, 2022]
19. Tbilisi Court of Appeals order №1ბ/960-17 (2017). “Order on inadmissability of evidence”. Tbilisi Court of Appeals. <http://library.court.ge/judgements/5582017-07-25.pdf> [Last access: 9 September, 2022]