თორნიკე ხიდეშელი*

# კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან

*ნაშრომი ეხება ისეთ აქტუალურ საკითხს, როგორიცაა კომპიუტერული მონაცემის გამოთხოვის საკანონმდებლო მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციასთან. საგამოძიებო მოქმედებას, რომლის მნიშვნელობა განსაკუთრებულია შენახული ელექტრონული კომუნიკაციის შინაარსობრივი თუ მაიდენტიფიცირებელი მონაცემების, მომხმარებლის მაიდენტიფიცირებელი მონაცემებისა თუ ზოგადად, კომპიუტერული ინფორმაციის მოსაპოვებლად. პრინციპულად მნიშვნელოვანია გამართული ეროვნული საკანონმდებლო ბაზა, რომელიც თანხვედრაშია საერთაშორისო სამართლის მოთხოვნებთან. შესაბამისად, ნაშრომის მიზანს სსსკ-ის 136-ე მუხლის ე.წ. „ბუდაპეშტის“ კონვენციასთან შესაბამისობის წარმოჩენა წარმოადგენს, ხოლო წინააღმდეგობის აღმოჩენის შემთხვევაში არსებული უზუსტობების გამოკვეთა, გაანალიზება.*

***საკვანძო სიტყვები:*** *კომპიუტერული სისტემა, კომპიუტერული მონაცემი, ციფრული მტკიცებულება, ელექტრონული მტკიცებულება*

## 1. შესავალი

თანამედროვე მსოფლიოში კიბერდანაშაული რეალურ საფრთხეს წარმოადგენს ინდივიდებისთვის, ბიზნესისთვის და სახელმწიფო უწყებებისთვის.[1] საინფორმაციო ტექნოლოგიების განვითარებამ დანაშაულის ჩადენის განსხვავებულ ფორმას დაუდო დასაბამი და ამასთან, ზეგავლენა ტრადიციულ დანაშაულზეც მოახდინა. არსებული რეალობის გათვალისწინებით უდაოა, რომ ელექტრონული ინფორმაცია არის ყველგან, დღითიდღე მსოფლიო უფრო მეტად ხდება ურთიერთდაკავშირებული და ჩვენი ყოველდღიურობა რთული წარმოსადგენია ელექტრონული მოწყობილობის გარეშე. პარალელურ რეჟიმში, თანდათან იზრდება ელექტრონული მტკიცებულების მნიშვნელობა დანაშაულის გამოძიების პროცესში[2], იქნება ეს წვრილმანი დანაშაული, კიბერტერორიზმი თუ ორგანიზებული დანაშაული.[3]

ელექტრონული მტკიცებულების სიჭარბის, დინამიურობისა და ვოლატიურობიდან გამომდინარე, გამოძიების პროცესში განსაკუთრებულ მნიშვნელობას იძენს ეფექტური პროცედურული მექანიზმების ხელმისაწვდომობა. მათი არსებობის აუცილებლობა უფრო ნათელი ხდება ქსელური დანაშაულის გამოძიებისას, რა დროსაც კიბერკრიმინალები სანიმუშოდ დახვეწილ თავდასხმებს ახორციელებენ კომპიუტერულ სისტემებზე და შედეგად დიდი მოცულობის პერსონალური ინფორმაციის, მომხმარებლის სახე-

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, მოწვეული ლექტორი.

1 *Schwerha J.J.,* Transborder Acquisition of Electronic Evidence from “Cloud Computing Providers”, 2010, 4.

2 *Kerr S.O.,* Searches and Seizures in Digital World, Harvard Law Review, Vol. 119, USA, 2006, 1.

3 *Arnes A. (ed.),* Forensic Science, Digital Forensics, Norway, 2018, 1.

ლების, დაბადების თარიღების, მისამართების გამჟღავნება ხდება.[4] ასეთ დროს, სირთულეს წარმოადგენს დამნაშავის იდენტიფიცირება და სამართლებრივ სიკეთეზე ქმედების უარყოფითი ზეგავლენის შეფასება. შესაბამისად, სწრაფ და ზოგჯერ ფარულ მოქმედებებს, გადამწყვეტი მნიშვნელობა აქვს წარმატებული გამოძიებისათვის.[5]

„კიბერდანაშაულის შესახებ“ კონვენციის მეშვეობით ევროპის საბჭო წარმატებით უმკლავდება არსებულ გამოწვევებს[6] და კომპიუტერული მონაცემის გადაცემის ბრძანებასთან ერთად არაერთ საპროცესო ღონისძიებას გვთავაზობს, რაც ხელს უწყობს სახელმწიფოს პოზიტიური ვალდებულების სრულყოფილად შესრულებას, დაიცვას ინდივიდები დანაშაულისგან, მათ შორის კიბერდანაშაულისგან და გამოძიება აწარმოოს ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვითა და პატივისცემით.

შესაბამისად, ამ მიზნით კონვენციაში მატერიალურ და პროცესუალურ დებულებებთან ერთად, გათვალისწინებულია მთელი რიგი წინაპირობები, რომელთაც სახელმწიფოებმა ნორმის იმპლემენტირებისას განსაკუთრებული ყურადღება უნდა მიაქციონ. ვინაიდან, სსსკ-ის 136-ე მუხლით გათვალისწინებული „დოკუმენტის ან ინფორმაციის გამოთხოვის“ საგამოძიებო მოქმედება „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლის „კომპიუტერული მონაცემის წარმოდგენის ბრძანების“ ეროვნულ კანონმდებლობაში იმპლემენტირების შედეგია და ამავდროულად, ეროვნულ კანონმდებლობაში იგი წარმოადგენს შენახული ელექტრონული მტკიცებულების მოპოვების ქმედით მექანიზმს, მნიშვნელოვანია მისი თანხვედრა საერთაშორისო სამართლის მოთხოვნებთან. სწორედ ამიტომ, მოცემულ წერილში ყურადღება გამახვილდება როგორც „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებსა და საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლზე, ისე ამ უკანასკნელის შესაბამისობაზე კონვენციით განსაზღვრულ წინაპირობებთან.

## 2. „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნები

### 2.1. ნორმის იმპლემენტაცია

კომპიუტერული მონაცემის გადაცემის ბრძანების ძირითადი მიზანი სამართალდამცავი ორგანოების ნებისმიერი კატეგორიის კომპიუტერული მონაცემის, მათ შორის მომხმარებლის შესახებ ინფორმაციის მოპოვების უფლებამოსილებით აღჭურვა წარმოადგენს. თუ ამ საგამოძიებო მოქმედებას „კიბერდანაშაულის შესახებ“ კონვენციის მე-15 მუხლის (პირობები და გარანტიები) პერსპექტივიდან შევხედავთ, დავინახავთ, რომ მისი მიზანი ასევე იძულებით ღონისძიებებს შორის ალტერნატიული საგამოძიებო უფლებამოსილების არსებობაა, რომელიც საგამოძიებო უწყებებს სისხლის სამართლის საქმესთან დაკავშირებული ელექტრონული მტკიცებულების უფლების ნაკლები ინტენსი-

4 *Flaglien O. A.,* The Digital Forensics Process, Digital Forensics, *Arnes A. (ed.),* Norway, 2018, 13.

5 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, §133.

6 *Schwerha J.J.,* Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from “Cloud Computing Providers” France, 2010, 4.

ვობით შეზღუდვის ხარჯზე მოპოვებაში დაეხმარება.[7] განსაკუთრებით მაშინ, როდესაც ინფორმაციის მფლობელები მზად არიან გამოძიებასთან თანამშრომლობისთვის, თუმცა ამისთვის მკაფიოდ განსაზღვრული სამართლებრივი საფუძველი და მოქმედების ფარგლები სჭირდებათ.[8]

შესაბამისად, კომპიუტერული მონაცემის წარმოდგენის ბრძანების სათანადო იმპლემენტირებისათვის რამდენიმე წინაპირობის გათვალისწინებაა აუცილებელი. ყურადღება უნდა მიექცეს შემდეგ ფაქტორებს: **1. კონკრეტული საპროცესო ინსტრუმენტი გათვალისწინებულია თუ არა როგორც დამოუკიდებელი საგამოძიებო მოქმედება ეროვნული კანონმდებლობით; 2. აკმაყოფილებს თუ არა ეროვნული კანონმდებლობა სიზუსტისა და განჭვრეტადობის მოთხოვნებს; და 3. შეიცავს თუ არა უფლებაში თვითნებური ჩარევისგან დასაცავ ქმედით პროცესუალურ გარანტიებს.**[9] ამასთან, კანონმდებლობით შესაძლოა განისაზღვროს გამონაკლისი ინფორმაციის გადაცემის ვალდებულებისგან. მაგალითისთვის, პრივილეგირებულ კომუნიკაციასა და ინფორმაციაზე, რომელიც ადვოკატისა და კლიენტის ურთიერთობას ეხება და სხვა.[10] უფლებამოსილების განხორციელებისთვის მიზანშეწონილია სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობის განხორციელება, თუმცა აღნიშნული თითოეული კატეგორიის მონაცემთან დაკავშირებით ინდივიდუალურად უნდა გადაწყდეს.

### 2.2. პროცედურული ღონისძიებების მოქმედების ფარგლები

„კიბერდანაშაულის შესახებ“ კონვენციის მე-14 მუხლი აწესრიგებს ისეთ მნიშვნელოვან საკითხს, როგორიცაა საგამოძიებო ღონისძიებების, მათ შორის „კომპიუტერული მონაცემის წარმოდგენის ბრძანების“ მოქმედების ფარგლები და მიზნები.

ნორმის მიხედვით, საპროცესო ღონისძიებების გამოყენება დასაშვებია, **ა) თავად კონვენციით გათვალისწინებული დანაშაულის გამოსაძიებლად; ბ) იმგვარი დანაშაულის გამოსაძიებლად, რომელიც კომპიუტერული სისტემის გამოყენებით არის ჩადენილი და გ) ნებისმიერი დანაშაულის გამოძიებისას, სადაც შესაძლებელია მტკიცებულება ელექტრონული ფორმით არსებობდეს.**[11] მოქმედების ფარგლების ასე ფართოდ განსაზღვრა არის მცდელობა ციფრულ სივრცეში, კომპეტენტური ორგანოების მაქსიმალურად ეფექტური და სრული უფლებამოსილებით აღჭურვის, როგორც ეს მათ ტრადიციული მტკიცებულებების მოპოვებისას გააჩნიათ. ამასთან, ეს არის დასტური

---

7 Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

8 იქვე.

9 Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 9. <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].

10 Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 30.

11 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 7. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

იმისა, რომ ელექტრონული ინფორმაცია შესაძლოა გამოყენებულ იქნას როგორც მტკიცებულება სასამართლოს წინაშე, მიუხედავად დანაშაულის ხასიათისა და სიმძიმისა.[12]

მიუხედავად პროცედურული ღონისძიებების მოქმედების ფარგლებთან დაკავშირებული ზოგადი და ფართო ხასიათის დათქმისა, კონვენცია გარკვეული სახის შეზღუდვას მაინც ითვალისწინებს. ეროვნულ კანონმდებლობაში საერთაშორისო-სამართლებრივი ნორმების იმპლემენტირებისას, კერძოდ კი, შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვების საგამოძიებო ღონისძიების დანერგვისას, მისი მოქმედების ფარგლები „მძიმე დანაშაულთა“ (Serious Offence) კატეგორიით უნდა შეიზღუდოს. დათქმას, საგამოძიებო მოქმედების ფარული და პირადი ცხოვრების უფლების მაღალი ინტენსივობით მზღუდავი ხასიათი განაპირობებს. რაც შეეხება „მძიმე დანაშაულთა“ დეფინიციას, კონვენცია ნეიტრალურ პოზიციას ინარჩუნებს, მის განმარტებას ხელშემკვრელ მხარეს ანდობს და საკითხის გადაწყვეტას იმის მიხედვით სთავაზობს თუ რომელი დანაშაული ითვლება მძიმედ ეროვნული კანონმდებლობით.[13] თუმცა, ეს არ გამორიცხავს სახელმწიფოს შესაძლებლობას თავად განსაზღვროს დანაშაულთა ჩამონათვალი და ღონისძიების მოქმედების ფარგლები.

შინაარსობრივი მონაცემების მოპოვების დანაშაულთა წრით შეზღუდვის მოთხოვნა იმპერატიული ხასიათისაა. ტრაფიკის მონაცემების შეგროვების შემთხვევაში შეზღუდვის დაწესება კი ხელშემკვრელი მხარეების დამოუკიდებელი არჩევანია. შესაძლებელია ცალკე აღებული ტრაფიკის მონაცემების შეგროვებით ვერ მივიღოთ ინფორმაცია კომუნიკაციის შინაარსთან დაკავშირებით და ამით ვერ გაუთანაბრდეს იგი პირადი ცხოვრების უფლების შეზღუდვის ხასიათით შინაარსობრივი მონაცემების შეგროვებას. თუმცა, მისი დახმარებით შესაძლებელია კომუნიკაციის წყაროს და დანიშნულების ადგილის განსაზღვრა, შესაბამისად პირის იდენტიფიცირებაც. ამრიგად, სახელმწიფო უფლებამოსილია შეხედულებისამებრ მიიღოს გადაწყვეტილება მისი მოქმედების ფარგლების შეზღუდვასთან დაკავშირებით. თუმცა შეზღუდვისას ყურადღება უნდა მიაპყროს კონვენციის იმპერატიულ მოთხოვნას, რომ დანაშაულთა წრე, რომელთა არსებობის შემთხვევაშიც შესაძლებელი იქნება ტრაფიკის მონაცემების მიმდინარე რეჟიმში შეგროვება, არ შეზღუდოს იმაზე მეტად ვიდრე ეს შინაარსობრივი მონაცემების მოპოვების შემთხვევაში იქნება გათვალისწინებული.[14]

შეჯამებისთვის, კონვენციის მე-14 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი მოქმედების ფარგლებს ამავე დოკუმენტით განსაზღვრული დანაშაულებით ზღუდავს, თუმცა „ბ“ და „გ“ ქვეპუნქტები იმგვარად არის ფორმულირებული, რომ პროცედურული მექანიზმების გამოყენება ნებისმიერი დანაშაულის გამოძიების დროს იყოს შესაძლებელი.[15] იმპერატიული ხასიათის დათქმას, დანაშაულთა წრით შეზღუდვაზე, მხოლოდ შინაარსობრივი მონაცემების მოპოვების ნაწილში ვაწყდებით. ხოლო, ტრაფიკის მონაცემების შემთხვევაში, შეზღუდვის დაწესება ხელშემკვრელი სახელმწიფოს თავისუფალ ნებაზეა

12 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 22.
13 იქვე.
14 იქვე, 23.
15 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 100.

დამოკიდებული. თუმცა, უნდა ითქვას, რომ განმარტებითი ბარათის მიხედვით, ტრაფიკის მონაცემების შეგროვებით კომუნიკაციის წყაროსა და ადგილმდებარეობის განსაზღვრის გაადვილების მიზნით, ამგვარი შეზღუდვის დაწესება არერეკომენდირებულია.[16] გარდა შინაარსობრივი მონაცემების შეგროვების შემთხვევისა, საპროცესო დებულებების მოქმედების ფარგლების ფართოდ განმარტება მიზანშეწონილია, ვინაიდან ცნობილია, რომ ქმედებისათვის პასუხისმგებლობის დამდგენ ღონისძიებას გააჩნია შემაკავებელი ეფექტი, ხოლო თუ არ არსებობს რეალური დამნაშავის იდენტიფიცირებისა და მართლმსაჯულების წინაშე წარდგენის პროცესუალური საშუალება, ეს ეფექტი შემცირებული და შეზღუდულია.[17] ამასთან, საყურადღებოა, რომ კონვენცია არ ზღუდავს საგამოძიებო მოქმედებების გამოყენების შესაძლებლობას სისხლის სამართლის პროცესის არცერთ სტადიაზე. მთავარია, საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელი დასაბუთებული ვარაუდის სტანდარტი იყოს დაკმაყოფილებული.[18]

### 2.3. პირობები და გარანტიები

კომპიუტერული მონაცემის გადაცემის ბრძანება, რომელიც ეროვნულ კანონმდებლობაში დოკუმენტის ან ინფორმაციის გამოთხოვის სახელით არის ცნობილი, ტექნოლოგიურ სამყაროზე მორგებული და განახლებული ტრადიციული ჩხრეკა-ამოღების საგამოძიებო მოქმედება, მონაცემთა დაჩქარებული დაცვის ბრძანება, ინტერნეტ-ტრაფიკისა და შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვების შესაძლებლობა, იძულებითი ხასიათის ღონისძიებებს განეკუთვნებიან. იძულებითი ღონისძიებების გამოყენებით კი მნიშვნელოვნად იზღუდება პირადი ცხოვრების უფლება, თავისუფლების უფლება, გამოხატვის თავისუფლება, საკუთრების უფლება და ამასთან, ძირითადად ისინი ადრესატის თანხმობისა და ინფორმირების გარეშე გამოიყენება.[19] აქედან გამომდინარე, „კიბერდანაშაულის შესახებ“ კონვენციის მე-15 მუხლი საპროცესო ღონისძიებების გამოყენების პროცესში ადამიანის ძირითადი უფლებების დაცვის ვალდებულებას ითვალისწინებს. უფლებათა ადეკვატური დაცვის სათანადოდ უზრუნველსაყოფად კი მიზანშეწონილია ა) ადამიანის უფლებათა დაცვის საერთაშორისო ინსტრუმენტებით ნაკისრი ვალდებულებების პატივისცემა; ბ) უფლებაში ჩარევის გამამართლებელი საფუძვლის არსებობა; გ) პროპორციულობის პრინციპის დაცვა; დ) უფლებამოსილების ხანგრძლივობისა და ფარგლების შეზღუდვა; ე) სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობის განხორციელება,[20] ვ) მესამე მხარის უფლებების, ვალდე-

16 Explanatory Report to the Convention on Cybercrime, Council of Europe, Budapest, 23.11.2001, §143.
17 K. U. v. Finland, [2009], ECHR, №2872/02, §46.
18 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 100.
19 იქვე, 61.
20 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.09.2022].

ბულებებისა და კანონიერი ინტერესების პატივისცემა.[21] მიმოვიხილოთ თითოეული მათგანი:

**ა) ადამიანის უფლებათა დაცვის საერთაშორისო ინსტრუმენტებით ნაკისრი ვალდებულების პატივისცემა –** ძნელი წარმოსადგენია ადამიანის უფლებათა დაცვის სისტემის განმტკიცება ამ სფეროში არსებული საერთაშორისო ხელშეკრულებების სათანადო პატივისცემის გარეშე. როგორც წესი, დიდია მათი ზეგავლენა ნაციონალურ კანონმდელობასა და სასამართლო პრაქტიკაზე. ასეთს საქართველოსთვის, 1950 წლის ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია და ამავე დოკუმენტის საფუძველზე შექმნილი სასამართლოს გადაწყვეტილებები წარმოადგენენ. შესაბამისად, კონვენცია მოუწოდებს ხელშემკვრელ მხარეებს დაიცვან საერთაშორისო დოკუმენტებით გათვალისწინებული და ნაკისრი ვალდებულებები. კერძოდ, ევროპული კონვენციის მე-5 მუხლით განსაზღვრული თავისუფლებისა და უსაფრთხოების უფლება, მე-6 მუხლით გარანტირებული საქმის სამართლიანი განხილვის უფლება, მე-7 მუხლით გათვალისწინებული პრინციპი „არავითარი სასჯელი კანონის გარეშე“ (nullum poena sine lege) და მე-8 მუხლით დაცული პირადი და ოჯახური ცხოვრების უფლება.[22]

**ბ) ჩარევის გამამართლებელი საფუძვლის არსებობა –** როგორც ზემოთ ვახსენეთ, „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული ნებისმიერი პროცესუალური ღონისძიების განხორციელება გარკვეული ხარისხით პირთა პირად ცხოვრებაში ჩარევას გულისხმობს. შესაბამისად, ყოველი ასეთი ღონისძიების გამოყენების აუცილებლობა დასაბუთებული უნდა იყოს ვარგისი ცნობებითა და დასკვნებით, ხოლო დასაბუთება წარმოდგენილი და ხელმისაწვდომი საგამოძიებო მოქმედების განხორციელებამდე.[23] დასაბუთების ვალდებულება გარკვეულწილად გამორიცხავს უფლებაში თვითნებურ ჩარევასა და სახელმწიფო რესურსების არამიზნობრივ ხარჯვას.[24] ამასთან, საგამოძიებო ღონისძიების გამოყენების აუცილებელი წინაპირობაა სისხლის სამართლის საქმეზე გამოძიების მიმდინარეობა.

**გ) პროპორციულობის პრინციპი –** თუ დავაკვირდებით კონვენციის მუხლების წყობას, დავინახავთ, რომ ისინი გარკვეული თანმიმდევრობით არიან დალაგებულნი. კრიტერიუმი კი უფლების შეზღუდვის ინტენსივობაა. საპროცესო დებულებები იწყება კომპიუტერულ მონაცემთა დაჩქარებული დაცვით, უფლების ნაკლებად მზღუდავი საგამოძიებო მოქმედებით და მთავრდება მაღალი ინტენსივობით მზღუდავი შინაარსობრივ მონაცემთა შეგროვების ღონისძიებით. შეიძლება ითქვას, რომ ეს არის ერთგვარი ინდიკატორი პროპორციულობის დასაცავად. თუ დასახული მიზნის მიღწევა ნაკლებად მზღუდავი საგამოძიებო მოქმედებით შესაძლებელია, დაუშვებელია უფრო მძიმე ღო-

---

21 Convention on Cybercrime, Budapest, 23.11.2001, Article 15(3).

22 *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11.

23 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

24 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 99.

ნისძიების გატარება. არჩევანი კონკრეტული ღონისძიების გამოყენების თაობაზე, დანაშაულის ბუნებისა და საქმის გარემოებების პროპორციული უნდა იყოს.[25] აგრეთვე, პროპორციულობის პრინციპის ზუსტი გამოხატულებაა, კონვენციის 21-ე მუხლის 1-ლი ნაწილის მოთხოვნა, დანაშაულთა წრით შეიზღუდოს შინაარსობრივი მონაცემების შეგროვება.[26]

**დ) უფლებამოსილების ხანგრძლივობისა და ფარგლების შეზღუდვა –** აღნიშნულს განსაკუთრებული მნიშვნელობა კომპიუტერულ მონაცემთა მიმდინარე რეჟიმში შეგროვების დროს გააჩნია. იმის გარდა, რომ ინტერნეტ-ტრაფიკისა და შინაარსობრივი მონაცემების (იმპერატიული) მოქმედების ფარგლები „მძიმე დანაშაულთა“ კატეგორიით უნდა შემოიფარგლოს, აუცილებელია მათი გამოყენების ხანგრძლივობის შეზღუდვაც. რა თქმა უნდა, ნებართვის პერიოდულად გადახედვა და უფლებამოსილი ორგანოს მიერ მიყურადების გახანგრძლივება დასაშვებია.[27]

**ე) სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობა[28] –** სასამართლო ზედამხედველობა ყველაზე ეფექტურ საშუალებად ითვლება პირთა პირად ცხოვრებაში არამართლზომიერი ჩარევის თავიდან ასაცილებლად და ზოგადად, სამართლიანი სასამართლო უფლების უზრუნველსაყოფად. დამოუკიდებელ ზედამხედველობაზე საუბრისას მნიშვნელოვანია რომ ზედამხედველი ორგანო თუ პირი, ფუნქციურად და არა ფორმალურად, მხარეებისგან დამოუკიდებელი იყოს. მოსამართლის გარდა, ასეთი შეიძლება იყოს მონაცემთა დაცვაზე ზედამხედველი ორგანო, პარლამენტი, სპეციალური მიზნისთვის შექმნილი კომისიები და ა.შ.[29]

**ვ) მესამე მხარის უფლებების, ვალდებულებებისა და კანონიერი ინტერესების პატივისცემა**

უნდა ითქვას, რომ კონვენციის მე-15 მუხლის მე-3 ნაწილი მართლმსაჯულების ეფექტური განხორციელების ინტერესიდან გამომდინარე სახელმწიფოებს ავალდებულებს გაითვალისწინონ მესამე პირთა კანონიერი ინტერესები. პირების, რომლებიც არ არიან დაკავშირებულნი დანაშაულთან, თუმცა გამოძიების მიმდინარეობა და კონვენციით გათვალისწინებული საგამოძიებო ღონისძიებების გამოყენება ზეგავლენას ახდენს მათ უფლებრივ მდგომარეობაზე. საყურადღებოა, რომ კონვენცია არა კონკრეტული ზო-

---

25 General Report on Mapping the Current Strengths, Weaknesses, Opportunities and Risks of Public/private Cooperation on Cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 13. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

26 *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11.

27 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

28 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 101.

29 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

მების მიღების ვალდებულებას აკისრებს ხელშემკვრელ მხარეს, არამედ ინფორმაციას აწვდის მესამე პირთა კანონიერი ინტერესების დაცვის ვალდებულების შესახებ.[30]

მესამე პირთა ინტერესების გათვალისწინების ვალდებულებას პრაქტიკული ახსნა აქვს. მაგალითისთვის, აშშ-ის იუსტიციის დეპარტამენტმა 2012 წლის იანვარში, ერთერთი ცნობილი ვებ-გვერდი – www.megaupload.com დახურა, ხოლო მის მფლობელებსა და რამდენიმე პირს ბრალი საავტორო უფლებების დარღვევასა და რეკეტში წაუყენა. ვებ-გვერდის მომხმარებელთა რაოდენობა კი 66 მილიონს აჭარბებდა, რომელთაც საკუთარ ანგარიშებზე წვდომა შეეზღუდათ.[31] მიუხედავად იმისა, რომ სამართალწარმოება მხოლოდ რამდენიმე პირის მიმართ მიმდინარეობდა, გამოძიების მიმდინარეობამ ზეგავლენა მილიონობით მომხმარებელზე იქონია.

მესამე მხარის კანონიერი ინტერესების განმტკიცებას ემსახურება „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული „კომპიუტერული მონაცემის წარმოდგენის ბრძანება“. უფლების დაბალი ინტენსივობით მზღუდავი ბუნების უპირატესობის გარდა, მისი ეროვნულ კანონმდებლობაში დანერგვა მესამე პირებზე, განსაკუთრებით კი ინტერნეტ-პროვაიდერებზეც აისახება დადებითად, რაც საგამოძიებო უწყების წარმომადგენლებისთვის მომხმარებელთა პერსონალური მონაცემების კეთილი ნების და არა სამართლებრივი საფუძვლის ან ვალდებულების გარეშე გადაცემის ფაქტს გამორიცხავს.[32] განსაკუთრებით მაშინ, როდესაც ცნობები ელექტრონული საკომუნიკაციო ქსელების მომხმარებლების შესახებ და აგრეთვე მათ მიერ ქსელის მეშვეობით გადაცემული ინფორმაცია საიდუმლოა.[33]

შეჯამებისთვის, ზემოთგანხილული პირობები და გარანტიები, რა საკვირველია, ამომწურავად არ განსაზღვრავს ყველა საჭირო საკითხს ადამიანთა უფლებების სათანადო დაცვის უზრუნველსაყოფად, თუმცა წარმოადგენს ძირითად და აუცილებელ მოთხოვნებს პროცესუალური ღონისძიებების ეროვნულ კანონმდებლობაში დასანერგად. ხსენებულთან ერთად, ნებისმიერი საპროცესო ღონისძიების გამოყენებისას აუცილებელია უზრუნველყოფილი იყოს სხვა ძირითადი უფლებებისა და თავისუფლებების დაცვაც. მათ შორის, უდანაშაულობისა და თავისუფლების პრეზუმფცია, სამართლიანი სასამართლო უფლება, გამოხატვის თავისუფლება, განმეორებით მსჯავრდების აკრძალვის პრინციპი და სხვა.[34] კომპეტენტური ორგანოების მხრიდან უფლებამოსილების გამოყენებასა და პირთა უფლებების პატივისცემას შორის ბალანსის დაცვას გადამწყვეტი მნიშვნელობა აქვს ჩატარებული საგამოძიებო მოქმედების კანონიერებისა და შესაბამისად მოპოვებული ინფორმაციის დასაშვებ მტკიცებულად ცნობისათვის.[35]

---

30 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 102.

31 United States of America v. Kim Dotcom*,* (2012), US, №1:12CR3.

32 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

33 საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, სსმ, 02/06/2005, მუხ. 8 (1).

34 General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 8. <https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.2022].

35 იქვე.

### 3. კომპიუტერული მონაცემის გამოთხოვა ქართული საპროცესო კანონმდებლობის მიხედვით

„კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული საგამოძიებო ღონისძიება **„კომპიუტერული მონაცემის წარმოდგენის ბრძანება“**, საქართველოს სისხლის სამართლის საპროცესო კოდექსში **დოკუმენტის ან ინფორმაციის გამოთხოვის** სახელით არის ცნობილი.[36] რა თქმა უნდა, ნორმაში გამოყენებული სიტყვები „ინფორმაცია და დოკუმენტი“ არა ნებისმიერი სახის ინფორმაციას ან დოკუმენტს აერთიანებს, არამედ მხოლოდ ელექტრონული ფორმით არსებულს.

სსსკ-ის 136-ე მუხლის პირველი ნაწილის თანახმად „თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, პროკურორი (ახლა უკვე დაცვის მხარეც)[37] უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით“. ნათელია, რომ ნორმა შინაარსობრივად ზოგადი ხასიათისაა და კომპიუტერული სისტემიდან ან მონაცემთა შესანახი საშუალებებიდან სისხლის სამართლის საქმისათვის მნიშვნელოვანი ელექტრონული ინფორმაციის მოპოვებას ეხება. ამასთან, ყურადღება არ არის გამახვილებული მონაცემთა სახეებზე, რაც მისი მოქმედების თანაბარმნიშვნელობაზე მეტყველებს როგორც შინაარსობრივი ინფორმაციის, ისე სხვა ნებისმიერი კატეგორიის კომპიუტერულ მონაცემზე. შესაბამისად, როგორც ბრალდების, ისე დაცვის მხარე სასამართლო ნებართვის საფუძველზე უფლებამოსილნი არიან საქართველოს ტერიტორიაზე მყოფი პირის მფლობელობაში ან ზედამხედველობის ქვეშ არსებული კომპიუტერული სისტემიდან ან ინფორმაციის შემნახველი მოწყობილობიდან ნებისმიერი სახის ინფორმაცია მოიპოვონ.[38]

რაც შეეხება სსსკ-ის 136-ე მუხლის მე-2 ნაწილს, აქ უკვე კომპიუტერული მონაცემი მომსახურების მიმწოდებელს[39] ეკუთვნის და იმისათვის, რომ პროკურორმა მომხმარებლის შესახებ ელექტრონული ინფორმაცია[40] გამოითხოვოს, მან დასაბუთებული ვარაუ-

---

36 საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09/10/2009.

37 საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე: ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ №1/1/650,699.

38 Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

39 ტერმინი „მომსახურების მომწოდებელი“ პირთა ფართო წრეს აერთიანებს. მასში მოიაზრებიან, როგორც კერძო და საჯარო პირები, რომლებიც მომხმარებლებს კომპიუტერული სისტემის გამოყენებით ურთიერთობის შესაძლებლობით უზრუნველყოფენ, აგრეთვე, ის პირები, რომლებიც მომსახურების ან მომხმარებელთა სახელით ამუშავებენ ან ინახავენ კომპიუტერულ მონაცემს. მნიშვნელობა არ ენიჭება ამგვარი სერვისი ხელმისაწვდომია ყველასათვის თუ მხოლოდ შეზღუდულ პირთა წრისათვის, ფასიანი თუ უფასო. სერვისის მომწოდებელთა ცნებაში ექცევა დახურული საკომუნიკაციო ქსელიც.

40 მომხმარებლის შესახებ ინფორმაცია – ტრაფიკისა და შინაარსობრივი მონაცემებისგან განსხვავებულ ინფორმაციას წარმოადგენს, რომელსაც მომსახურების მომწოდებელი კომპიუტერული მონაცემის ან სხვა ნებისმიერი ფორმით ინახავს და ამ ინფორმაციის მეშვეობით შესაძლებელია: გამოყენებული კომუნიკაციის მომსახურების ტიპის ან ტექნიკური საშუალებისა და მომსახურების დროის განსაზღვრა. აგრეთვე, მომხმარებლის ვინაობის, მისი საფოსტო ან საცხოვრებელი მისამართის, ტელეფონისა და სხვა საკონტაქტო ნომრების, ანგარიშისა და გადასახადების შე-

დის სტანდარტით უნდა ამტკიცოს, რომ პირი დანაშაულებრივ ქმედებას კომპიუტერული სისტემის გამოყენებით ახორციელებს. როგორც ჩანს, მუხლის მეორე ნაწილი პირველთან შედარებით უფრო სპეციფიკური და ვიწროა. კერძოდ, მომხმარებლის შესახებ ინფორმაციის გამოთხოვაზე უფლებამოსილ პირს მხოლოდ პროკურორი წარმოადგენს და ამასთან, თუ გამოძიებისათვის მნიშვნელოვანი იქნება მომხმარებლის შესახებ არსებული კომპიუტერული მონაცემი, რომელიც ინფორმაციის ფართო სპექტრს მოიცავს და ეს პირი არ ჩადის დანაშაულს კომპიუტერული სისტემის გამოყენებით, კომპეტენტური ორგანო მოკლებული იქნება შესაძლებლობას მიმართოს სასამართლოს ამგვარი ინფორმაციის გამოთხოვის შუამდგომლობით.

გარდამტეხი მნიშვნელობისაა ამავე მუხლის მე-4 ნაწილი, რომელიც იმპერატიულად კომპიუტერული მონაცემის გამოთხოვას ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესის მიხედვით აწესრიგებს, რაც უპირველესად მისი მოქმედების ფარგლების შეზღუდვას გულისხმობს, ვინაიდან ფარული საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელ წინაპირობას, განზრახ მძიმე ან/და განსაკუთრებით მძიმე ან საქართველოს სისხლის სამართლის კოდექსის კონკრეტულ დანაშაულებზე დაწყებული გამოძიების ან სისხლისსამართლებრივი დევნის არსებობა წარმოადგენს.[41]

ცალკე საკითხია, თავისი ბუნებით კომპიუტერული მონაცემის გამოთხოვა რამდენად წარმოადგენს ფარულ საგამოძიებო მოქმედებას და აქვს თუ არა პირისთვის მოულოდნელობის ეფექტი[42], თუმცა კანონმდებლის ამგვარი დათქმა არ არის თანხვედრაში, არც კიბერდანაშაულის შესახებ კონვენციასთან და არც საერთაშორისო გამოცდილებასთან.[43]

შეჯამებისთვის, შინაარსობრივად საგამოძიებო მოქმედება ორ დამოუკიდებელ შემთხვევას აწესრიგებს. სსსკ-ის 136-ე მუხლის პირველი ნაწილი ფართო შინაარსისაა და პროცესის ორივე მხარეს შესაძლებლობას ანიჭებს ქვეყნის ტერიტორიაზე მყოფი პირის მფლობელობასა თუ კონტროლ ქვეშ არსებული კომპიუტერული სისტემიდან ან ელექტრონული მატარებლიდან, ინფორმაციის გამოთხოვის შუამდგომლობით მიმართონ სასამართლოს, ხოლო მე-2 ნაწილით მოწესრიგებულია გამოძიების მიზნებისთვის მომხმარებლის შესახებ ინფორმაციის მოპოვების პროცედურა, რომლის თანახმადაც სასამართლოს წინაშე შუამდგომლობით დაყენების უფლებამოსილება მხოლოდ პროკურორს გააჩნია. გარდა იმისა, რომ ზოგადად საგამოძიებო ღონისძიების გამოყენებისთვის უცილებელია საქმეზე ოფიციალური გამოძიების მიმდინარეობა ან პირის მიმართ დაწყებული სს დევნა, ისიც შეზღუდულად, სსსკ-ის $143^3$ -ე მუხლის მე-2 ნაწილის ფარგლებში, პროკურორმა, მომხმარებლის შესახებ ინფორმაციის გამოთხოვის შუამდგომლობის დაყენებისას დასა-

სახებ ინფორმაციის, დამონტაჟებული საკომუნიკაციო აღჭურვილობის ადგილმდებარეობისა და სხვა ინფორმაციის დადგენა, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე.

41 საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მუხ. $143^3$ ¯ ის მე-2 ნაწილის „ა“ ქვეპუნქტი, სსმ, 09/10/2009.

42 თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 6 მაისის გადაწყვეტილება საქმეზე №1გ/633-20, 3.

43 Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, France, 2014, 16-18, <https://rm.coe.int/16802e7ad1> [08.03.22].

ბუთებული ვარაუდის სტანდარტით უნდა ამტკიცოს, რომ პირი, ვის ინფორმაციასაც ითხოვს სერვისის მიმწოდებლისგან, დანაშაულს კომპიუტერული სისტემის გამოყენებით სჩადის. შესაბამისად, აღნიშნული კიდევ უფრო მეტად ზღუდავს სსსკ-ის 136-ე მუხლის მოქმედების ფარგლებს, რომლის მიზანშეწონილობის საკითხი „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებზე დაყრდნობით განხილული იქნება მოგვიანებით.

## 4. სსსკ-ის 136-ე მუხლის შესაბამისობა კონვენციის მოთხოვნებთან

კონვენციით გათვალისწინებული მოთხოვნებისა და საქართველოს საპროცესო კანონმდებლობის მიმოხილვის შემდეგ მნიშვნელოვანია ფუნდამენტური საკითხების შეჯამება. ძირითადად, ყურადსაღებია თუ რამდენად თანხვედრაშია სსსკ-ის 136-ე მუხლის საკანონმდებლო მოწესრიგება კონვენციით დადგენილ დათქმებთან საგამოძიებო ღონისძიებების მოქმედების ფარგლებსა და ადამიანის ძირითად უფლებათა და თავისუფლებათა დაცვისთვის აუცილებელ პირობებთან.

მოქმედების ფარგლების მხრივ კონვენციის მე-14 მუხლის მე-2 ნაწილი იმგვარად არის ფორმულირებული, რომ პროცედურული მექანიზმების, მათ შორის შენახული კომპიუტერული მონაცემის გამოთხოვის, გამოყენება ნებისმიერი დანაშაულის გამოძიების დროს იყოს შესაძლებელი. მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვის იმპერატიულ მოთხოვნას მხოლოდ შინაარსობრივი მონაცემების მიმდინარე რეჟიმში მოპოვების ნაწილში ვხვდებით, რომელიც ბუნებით ფარულ საგამოძიებო მოქმედებას მიეკუთვნება და მაღალი ინტენსივობით ერევა ადამიანის პირად ცხოვრებაში. ხოლო, კომპიუტერული მონაცემის გადაცემის ბრძანების არსებობის შემთხვევაში, რომელიც უფლების შეზღუდვის დაბალი ინტენსივობით გამოირჩევა და სამართლებრივ საფუძველს ქმნის საგამოძიებო ორგანოსა და ფიზიკურ თუ იურიდიულ პირებს შორის თანამშრომლობისთვის, მსგავსი შეზღუდვის დაწესება გაუმართლებელია. მეტიც, იგი ერთადერთი საგამოძიებო მოქმედებაა, რომელიც ჩხრეკა-ამოღებაზე მსუბუქი და ამავდროულად, ელექტრონული მტკიცებულების მოპოვების კუთხით ეფექტური მექანიზმია.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, სსსკ-ის 136-ე მუხლის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვა, არა მხოლოდ კონვენციის მოთხოვნებთან შეუსაბამოა, არამედ სხვადასხვა სახელმწიფოს კანონმდებლობისგანაც განსხვავდება.[44] როგორც ზემოთ ვახსენეთ, ფარული საგამოძიებო მოქმედებებისთვის დადგენილი საპროცესო რეჟიმის მსგავსად, ასევე ნორმის მოქმედებას მნიშვნელოვნად ზღუდავს სსსკ-ის 136-ე მუხლის მეორე ნაწილში არსებული ჩანაწერი „პირი დანაშაულებრივ ქმედებას ახორციელებს კომპიუტერული სისტემის გამოყენებით“. სწორად ამიტომ, აღმოსავლეთ პარტნიორობის ფარგლებში მომზადებულ სადისკუსიო ნაშრომში საქართველოს მიმართ გაცემულ იქნა რეკომენდაცია ნორმის მოქმედების არეალის გასაფართოებლად, რათა ელექტრონული მტკიცებულების, მათ შორის მომხმარებლის შესახებ ინფორმაცი-

[44] *Marion L., Degani M.,* Making the Most of Your Statutory Electronic Evidence Toolbox, *Donovan J. (eds.),* Cyber Misbehavior, USA, 2016, 58-60. იხ. Criminal Procedure Code of Austria, 30.12.1975, მუხ. 76a, 90(7); Telecommunications Act 2003, 19.08.2003, მუხ. 92(3); German Code of Criminal Procedure, 07/04/1987, მუხ. 100j; Telecommunications Act (TKG), 06/22/2004, მუხ. 113(3).

ის მოპოვება ნებისმიერი დანაშაულის გამოძიების ფარგლებში ხელმისაწვდომი გამხდარიყო.[45] თუმცა, კანონში დღემდე შესაბამისი ცვლილება არ განხორციელებულა.

რასაკვირველია, გამოძიების ინტერესებთან ერთად, მნიშვნელოვანია ეროვნული კანონმდებლობა, შესაბამისად, სსსკ-ის 136-ე მუხლი, უფლებაში თვითნებური ჩარევისგან დასაცავ პროცედურულ გარანტიებს ითვალისწინებდეს და თანხვედრაში მოდიოდეს კონვენციით გათვალისწინებულ პირობებთან და გარანტიებთან. ეროვნული კანონმდებლობით კი ქმედით გარანტიებს წარმოადგენს დოკუმენტის ან ინფორმაციის გამოთხოვისთვის ფორმალური და მატერიალური წინაპირობების დაკმაყოფილების აუცილებლობა.[46] კერძოდ, სისხლის სამართლის საქმეზე ოფიციალური გამოძიების წარმოება, სასამართლოს წინაშე მოტივირებული შუამდგომლობის დაყენება და დასაბუთებული ვარაუდის სტანდარტით ხელმძღვანელობის ვალდებულება,[47] Ex ante და Ex post (ბრალდების მხარის შემთხვევაში) სასამართლო კონტროლი[48] და აგრეთვე პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ზედამხედველობის განხორციელება საგამოძიებო ღონისძიებაზე.[49] ყოველივე ზემოთ ჩამოთვლილი ერთობლიობაში მყარ გარანტიას ქმნის ადამიანის ძირითადი უფლებებისა და თავისუფლებების სათანადო დაცვისათვის.

საკითხის განხილვა ცხადყოფს, რომ სსსკ-ის 136-ე მუხლი ადამიანის ძირითადი უფლებების დაცვის კუთხით სრულ თანხვედრაშია საერთაშორისო სამართლის მოთხოვნებთან. შეუსაბამობას მისი მოქმედების ფარგლების ნაწილში ვხვდებით, რაც მნიშვნელოვან ბარიერს ქმნის პრაქტიკული კუთხით.[50] განსაკუთრებით მომხმარებლის შესახებ ინფორმაცია, რომელიც მსოფლიო მასშტაბით დანაშაულის გახსნის მხრივ გადამწყვეტ როლს ასრულებს, და ტრაფიკისა და შინაარსობრივი მონაცემების მიმდინარე რეჟიმში მოპოვებასთან შედარებით, მსუბუქ მოწესრიგებას უნდა დაექვემდებაროს.[51] ამასთან, სსსკ-ის 136-ე მუხლის მიზნებისთვის მიზანშეწონილია მონაცემის სახეების გამოყოფა[52] და მათზე განსხვავებული სამართლებრივი რეჟიმის გავრცელება, უფლებამოსილი პირების განსაზღვრა. სასამართლო ნებართვის მოპოვების შემთხვევაში კი შუამდგომლობის სსსკ-ის 112-ე მუხლით დადგენილი წესით განხილვა.

---

45 *Dragicevic D., Juric M.,* Article 15 – Safeguards in the Eastern Partnership Region, Prepared under the Cybercrime EAP, Council of Europe, 2013, 44.

46 თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის გადაწყვეტილება საქმეზე №1გ/363-20, 3.

47 *Dragicevic D., Juric M.,* “Article 15 – Safeguards in the Eastern Partnership Region” Prepared under the Cybercrime EAP, Council of Europe, 2013, 38.

48 Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 44. <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].

49 საქართველოს პარლამენტის გადაწყვეტილებით 2022 წლის 1 მარტიდან სახელმწიფო ინსპექტორის სამსახური გაუქმებულია. ნაცვლად ორი უწყება – სპეციალური საგამოძიებო სამსახური და პერსონალურ მონაცემთა დაცვის სამსახური იფუნქციონირებს.

50 თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 ოქტომბრის №1გ/1614-16 გადაწყვეტილება, გვ. 9. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 25 დეკემბრის №1გ/2110-19 გადაწტვეტილება, 4-5; თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 26 დეკემბრის №1გ/2133-19 გადაწტვეტილება.

51 Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, Bucharest, 2017, 18.

52 შეიძლება გამოვყოთ: ელექტრონული კომუნიკაციის შინაარსობრივი მონაცემები; ელექტრონული კომუნიკაციისა და მომხმარებლის მაიდენტიფიცირებელი მონაცემები; საიდუმლო კომპიუტერული მონაცემები (პრივილეგირებული) და სხვა.

## 5. დასკვნა

თანამედროვე ეპოქაში რთული წარმოსადგენია დანაშაული, რომელსაც კავშირი არ აქვს ციფრულ განზომილებასთან.[53] კრიმინალები ხშირად იყენებენ კომპიუტერულ სისტემებს დანაშაულის ჩასადენად, კომუნიკაციისთვის, ფულის გასათეთრებლად, კრიტიკულ ინფრასტრუქტურებზე ჰაკერული თავდასხმებისთვის და ა.შ..[54] ონლაინ სივრცეში გადაინაცვლა ტრადიციულმა დანაშაულმაც. ონლაინ შავ ბაზარზე ხდება არალეგალური პროდუქციით ვაჭრობა. ვიდეო კამერის წინ სჩადიან სქესობრივ დანაშაულს და შემდეგ ჩანაწერს ინტერნეტ სივრცეში ავრცელებენ.[55]

თუ საერთოდ შესაძლებელია, რომ დანაშაულის ჩადენის დროს ტექნოლოგიის მზარდი გამოყენების „დადებით“ მხარეზე ვისაუბროთ, ამგვარ ასპექტად შეიძლება ელექტრონული მტკიცებულების სიმრავლე მივიჩნიოთ, რაც ხელს უწყობს სავარაუდო დამნაშავის დაკავებასა და სისხლის სამართლის საქმის გამოძიებას.[56] ხოლო ვინაიდან სისხლის სამართლის საქმის გამოძიების პროცესში ძირითად აქტივობას მტკიცებულებების შეგროვება წარმოადგენს,[57] ეს ეფექტურ, თანამედროვე ტექნოლოგიებსა და გამოწვევებზე მორგებული პროცედურულ მექანიზმების გარეშე წარმოუდგენელია. კომპიუტერულ სისტემაში, ელექტრონულ მატარებელსა თუ ვირტუალურ სერვერზე შენახული კომპიუტერული მონაცემის მოპოვების მხრივ კი ასეთს სსსკ-ის 136-ე მუხლით გათვალისწინებული „დოკუმენტის ან ინფორმაციის გამოთხოვა“ წარმოადგენს. შესაბამისად, მისი ეფექტურობის უზრუნველსაყოფად მნიშვნელოვანია საკითხის სრულყოფილად მოწესრიგება, საკანონმდებლო ბაზის თანხვედრა საერთაშორისო სამართლის მოთხოვნებთან. კონვენციის დებულებების, ეროვნული კანონმდებლობის განხილვამ და მათი შედარებითსამართლებრივმა ანალიზმა ცხადჰყო, რომ ელექტრონული მტკიცებულების გამოთხოვისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების სათანადოდ დაცვა უზრუნველყოფილია. დაცულია ნორმის ეროვნულ კანონმდებლობაში იმპლემენტირებისათვის აუცილებელი წინაპირობები. კერძოდ, ე.წ. „ბუდაპეშტის“ კონვენციის მე-18 მუხლით განსაზღვრული „კომპიუტერული მონაცემის გადაცემის ბრძანება“ ეროვნული კანონმდებლობით გათვალისწინებულია, როგორც დამოუკიდებელი საგამოძიებო მოქმედება, იგი აკმაყოფილებს სიზუსტისა და განჭვრეტადობის მოთხოვნებს და ამასთან ითვალისწინებს ძირითად უფლებაში თვითნებური ჩარევისგან დასაცავ ქმედით გარანტიებს.

თუმცა, მოთხოვნა, რომელსაც სსსკ-ის 136-ე მუხლი ვერ პასუხობს, ეს ნორმის მოქმედების ფარგლებია, ვინაიდან კონვენციის მე-14 მუხლის მე-2 ნაწილით შენახული კომპიუტერული მონაცემის გამოთხოვა და გამოძიების მიზნებისთვის მისი გამოყენება ნებისმიერი კატეგორიის დანაშაულის შემთხვევაშია შესაძლებელი, ხოლო ეროვნული

---

53 *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3.

54 იქვე, 3-4.

55 The Internet Organised Crime Threat Assessment (IOCTA), Europol, 2015, 29. <https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf> [08.03.22].

56 *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 5.

57 *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A*., (*eds.),* Norway, 2018, 95.

კანონმდებლობით კი მისი მოპოვება „დანაშაულთა წრით“ არის შეზღუდული.[58] შეზღუდულია მომხმარებლის შესახებ ინფორმაციის მოპოვების შესაძლებლობაც, მაშინ, როდესაც კონვენციის მიხედვით მომხმარებლის შესახებ ინფორმაციის გამოთხოვისთვის არ არის აუცილებელი პირი დანაშაულს კომპიუტერული სისტემის გამოყენებით ჩადიოდეს.

ყოველივეს გათვალისწინებით, კი ცხადია, რომ სსსკ-ის 136-ე მუხლის „კიბერდანაშაულის შესახებ“ კონვენციასთან აბსოლუტური თანხვედრისთვის აუცილებელია განხორციელდეს საკანონმდებლო ცვლილებები. კერძოდ, გაუქმდეს ფარული საგამოძიებო მოქმედებებისთვის დადგენილი რეჟიმი, რაც ავტომატურად გააფართოებს ნორმის მოქმედების ფარგლებს და პროცესის მხარეებისთვის ელექტრონული ინფორმაცია ხელმისაწვდომი გახდება ნებისმიერი კატეგორიის დანაშაულის გამოძიებისას. აგრეთვე, უნდა გაფართოვდეს სსსკ-136-ე მუხლის მე-2 ნაწილის ნორმატიული შინაარსი და მომხმარებლის შესახებ ინფორმაციის გამოთხოვაზე ზეგავლენას სიტყვები – „პირი დანაშაულებრივ ქმედებას კომპიუტერული სისტემის გამოყენებით ახორციელებს“ არ უნდა ახდენდეს. აღნიშნული, საერთაშორისო სამართლის მოთხოვნებთან დაახლოებასთან ერთად, მნიშვნელოვნად შეუწყობს ხელს მართლმსაჯულების ობიექტურად განხორციელებას.

**ბიბლიოგრაფია:**


1. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09/10/2009.
2. საქართველოს კანონი „ელექტრონული კომუნიკაციების შესახებ“, სსმ, 02/06/2005.
3. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 6 მაისის გადაწყვეტილება საქმეზე №1გ/633-20.
4. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის გადაწტვეტილება საქმეზე №1გ/363-20.
5. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 26 დეკემბრის გადაწტვეტილება საქმეზე №1გ/2133-19.
6. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 25 დეკემბრის გადაწტვეტილება საქმეზე №1გ/2110-19.
7. საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე: ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ №1/1/650,699.
8. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 ოქტომბრის გადაწყვეტილება საქმეზე №1გ/1614-16.
9. Telecommunications Act (TKG), 06/22/2004.
10. Telecommunications Act 2003, 19.08.2003.
11. Convention on Cybercrime, Budapest, 23.11.2001.
12. Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001.
13. German Code of Criminal Procedure, 07/04/1987.
14. Criminal Procedure Code of Austria, 30.12.1975.


[58] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მუხ. $143^3$ ¯ ის მე-2 ნაწილის „ა“ ქვეპუნქტი, სსმ, 09/10/2009.

15. *Arnes A. (ed.),* Forensic Science, Digital Forensics, Norway, 2018, 1.
16. *Casey E*., Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 3-5, 29.
17. *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership Region, Council of Europe, 2013, 11, 38, 44.
18. *Flaglien O. Anders,* The Digital Forensics Process, Digital Forensics, *Arnes A. (eds.),* Norway, 2018, 13.
19. *Kerr S.O.,* Searches and Seizures in Digital World, Harvard Law Review, Vol. 119, USA, 2006, 1.
20. *Marion L., Degani M.,* Making the Most of Your Statutory Electronic Evidence Toolbox, *Donovan J. (eds.),* Cyber Misbehavior, USA, 2016, 58-60.
21. *Schwerha J.J,* Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" France, 2010, 4.
22. *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, 2018, 95, 99, 100-102.
23. Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 9, 44.
<https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.03.22].
24. Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, Bucharest, 2017, 18.
25. General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership, Council of Europe, Cybercrime EAP, 2017, 7, 8, 13.
<https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [08.03.22].
26. The Internet Organised Crime Threat Assessment (IOCTA), Europol, 2015, 29. <ttps://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf> [08.03.22].
27. Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, France, 2014, 16-18.
< https://rm.coe.int/16802e7ad1> [08.03.22].
28. *United States of America v. Kim Dotcom,* (2012), US, №1:12CR3.
29. K. U. v. Finland, [2009], ECHR, №2872/02.