სსიპ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

იურიდიული ფაკულტეტი

სამართლის სადოქტორო საგანმანათლებლო პროგრამა

თორნიკე ხიდეშელი

კომპიუტერული მონაცემების გამოთხოვის სამართლებრივი საფუძვლები, ადამიანის უფლებათა საერთაშორისო სამართლის გათვალისწინებით

სამართლის დოქტორის აკადემიური ხარისხის მოსაპოვებლად წარმოდგენილი დისერტაცია

სამეცნიერო ხელმძღვანელი: ასოცირებული პროფესორი გიორგი თუმანიშვილი

სამეცნიერო თანახელმძღვანელი: ასოცირებული პროფესორი მაია ბითაძე

თბილისი
2023

აბსტრაქტი

ეროვნული კანონმდებლობისთვის კომპიუტერული მონაცემი და მასთან დაკავშირებული საგამოძიებო მოქმედებები მეტნაკლებად სიახლეს წარმოადგენენ. აქტიური განვითარების გზას გადის კომპიუტერული მონაცემის გამოთხოვის საპროცესო სამართლებრივი რეგულირება, რომლის ნათელი მაგალითია 2010 წლიდან დღემდე სსსკ-ის 136-ე მუხლთან დაკავშირებით განხორციელებული არაერთი მნიშვნელოვანი საკანონმდებლო ცვლილება.

მნიშვნელოვანია კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედება სრულყოფილად იყოს იმპლემენტირებული ეროვნულ კანონმდებლობაში, ხოლო ელექტრონული მტკიცებულების მოპოვების პროცესი ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვითა და პატივისცემით მიმდინარეობდეს. შესაბამისად, კვლევის მიზანია სადისერტაციო თემის ფარგლებში შეძლებისდაგვარად სრულყოფილად იქნას შესწავლილი კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედების არსი და თავისებურებანი, შეფასდეს ეროვნულ კანონმდებლობაში განხორციელებული ცვლილებები და სასამართლო პრაქტიკისა და „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნების ანალიზის საფუძველზე გამოიკვეთოს ამა თუ იმ საკანონმდებლო ცვლილების ნაკლოვანი მხარეები.

ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციისა და ევროპის კავშირის ძირითადი უფლებების ქარტიის მოთხოვნების, ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული სასამართლოს პრეცენდენტული სამართლით დადგენილი განმარტებების საფუძველზე შეფასდეს ეროვნული კანონმდებლობით გათვალისწინებული ძირითად უფლებაში თვითნებურად ჩარევისგან დაცვის გარანტიების ეფექტურობა. საზღვარგარეთის კანონმდებლობისა და გამოცდილების შესწავლის ფონზე გამოიკვეთოს კვლევის საგანთან დაკავშირებული განსხვავებული მიდგომები და დისერტაციაში განხილულ სხვადასხვა საკითხებთან თანხვედრაში შემუშავდეს სსსკ-ის 136-ე მუხლის სრულყოფისთვის საჭირო რეკომენდაციები.

კვლევის ფარგლებში დასახული მიზნების მისაღწევად გამოყენებულია ისტორიული, ანალიტიკური, სისტემური, დოგმატური, ფორმალურ-ლოგიკური და შედარებით-სამართლებრივი მეთოდები.

ნაშრომი შედგება შესავლისგან, 7 თავისაგან და დასკვნისგან. დისერტაციას თან ერთვის ბიბლიოგრაფია და 3 დანართი.

ნიშანდობლივია, რომ კვლევა, მასში განხილული საკითხების გათვალისწინებით წარმოადგენს სამეცნიერო სიახლეს. კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედების ბუნება და არსი, ელექტრონული მტკიცებულებების მახასიათებლები, „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნები და ეროვნული კანონმდებლობის მასთან შესაბამისობის საკითხი, წლების მანძილზე დაგროვილი საერთო სასამართლოების პრაქტიკა დოკუმენტის ან ინფორმაციის გამოთხოვის კუთხით და სხვა, იმ საკიხთა რიგს მიეკუთვნება, რომლებიც მეცნიერულად დაუმუშავებელია საქართველოში. აღნიშნულზე დაყრდნობით, დარწმუნებით შეიძლება ითქვას, რომ ნაშრომში მოყვანილი მოსაზრებები ღირებული იქნება როგორც პრაქტიკოსი, ისე მეცნიერი იურისტებისთვის.

Abstract

Computer data and related investigative actions are novel within national legislation. The Production order is undergoing active development, exemplified by a series of significant legislative changes implemented from 2010 to the present.

It is imperative that the investigative action of the production order be fully integrated into national legislation, ensuring that the collection of electronic evidence is carried out while safeguarding and respecting fundamental human rights and freedoms. Consequently, this research aims to comprehensively examine the essence and features of the production order, evaluate the modifications introduced in national legislation, and based on an analysis of judicial practice and the stipulations of the "Convention on Cybercrime," elucidate its shortcomings.

Based on the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union, and the case law of the European Court of Human Rights and the European Court of Justice, to evaluate the effectiveness of conditions and safeguards against arbitrary interference enshrined in national legislation. Furthermore, through the study of foreign legislation and experiences to identify diverse approaches pertinent to the research object, and formulate the recommendations for the enhancement of Article 136 of the GECPC.

A myriad of methodologies, including historical, analytical systematic, dogmatic, formal-logical, and comparative-legal methods are used and all aimed at attaining the research objectives.

The paper is comprised of an introduction, 7 chapters and a conclusion. The references and 3 annexes are enclosed to the dissertation.

Significantly, the research and the topics therein discussed constitute a scientific novelty. The nature and essence of the "Production Order," the attributes of electronic evidence, the requirements of the Convention on Cybercrime, and the alignment of national legislation therewith, as well as the extensive case law of Common Courts, belong to a range of issues that have remained unexplored within Georgian scholarly discourse. As a result, the opinions and assertions articulated within this paper hold substantial value for both practitioners and academic legal scholars.

სარჩევი

გამოყენებული აბრევიატურა

ქართულ ენაზე

მუხ. - მუხლი

ე.ი - ესე იგი

ე.წ. - ეგრედ წოდებული

ა.შ. - ასე შემდეგ

გვ. - გვერდი

იხ. - იხილე

მაგ. - მაგალითად

რედ. - რედაქტორი

კონვენცია - „კიბერდანაშაულის“ შესახებ კონვენცია

სსკ- სისხლის სამართლის კოდექსი

სსსკ - სისხლის სამართლის საპროცესო კოდექსი

სხვ. - სხვა

თბ. - თბილისი

აშშ - ამერიკის შეერთებული შტატები

ჟურნ. - ჟურნალი

ინგლისურ ენაზე

Art. – Article

Para – paragraph

v. – versus

vol. – volume

EU – European Union

ECHR – European Court of Human Rights

CJEU – Court of Justice of the European Union

Ed. - Edition

Eds. – Editors

Ser. – Series

FRA – European Union Agency for Fundamental Rights

NIJ – National Institute of Justice

U.S.C. – The United States Code

SCA – Stored Communications Act

ECPA – Electronic Communications Privacy Act

IP – Internet Protocol

IMEI – International Mobile Equipment Identity

IMSI – International Mobile Subscriber Identity

შესავალი

კვლევის აქტუალობა და მისი საგანი:

ციფრული ტექნოლოგიების დახვეწამ, ციფრული აპლიკაციების მზარდმა გამოყენებამ და პროცესების ავტომატიზაციამ საზოგადოებრივ ცხოვრებასთან ერთად, შეცვალა დანაშაულის ჩადენისა თუ გამოძიების ფორმაც. დასაბამი დაუდო დანაშაულთა ახალ სახეებს და ამასთან, გაიზარდა თანამედროვე ტექნოლოგიების ტრადიციული დანაშაულის დაგეგმვისა თუ ჩადენის მიზნით გამოყენების შემთხვევებიც. სწორედ ამიტომ, თანამედროვე სამყაროში წარმოუდგენელია დანაშაული, ციფრულ განზომილებასთან კავშირის გარეშე.[1] შესაბამისად, დღეს გამოძიების ინტერესებისთვის ელექტრონული მტკიცებულების გამოყენება არათუ განსაკუთრებულ მოვლენად, არამედ მის განუყოფელ ნაწილად განიხილება და დანაშაულის გამოძიების პროცესში მნიშვნელოვან დასაყრდენს წარმოადგენს.[2]

ზოგადად თუ შესაძლებელია, დანაშაულზე ტექნოლოგიათა ზეგავლენის „დადებით“ მხარეზე მსჯელობა, ამგვარად ელექტრონული მტკიცებულების სიმრავლე შეიძლება მივიჩნიოთ, რაც თავის მხრივ ხელს უწყობს სავარაუდო დამნაშავის იდენტიფიცირებასა და სიხლის სამართლის საქმის გამოძიებას.[3] საყურადღებოა, რომ ინფორმაციის სიმრავლის მიუხედავად, გამოძიებისთვის მნიშვნელოვანი მონაცემების შეგროვება თანამედროვე ტექნოლოგიებსა და გამოწვევებზე მორგებული პროცედურული მექანიზმების გარეშე წარმოუდგენელია. შესაბამისად, ასეთ ინსტრუმენტებს საქართველოსთვის სავალდებულო ძალის მქონე საერთაშორისო დოკუმენტი, ევროპის საბჭოს „კიბერდანაშაულის შესახებ“ კონვენცია, გვთავაზობს.

როდესაც კომპიუტერული სისტემიდან ან მონაცემთა შესანახი საშუალებიდან ინფორმაციის გამოთხოვაზე ვსაუბრობთ, უნდა გვახსოვდეს „კიბერდანაშაულის შესახებ კონვენციის“ მე-18 მუხლის შესაბამისად საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული „დოკუმენტის ან ინფორმაციის გამოთხოვის“ საგამოძიებო მოქმედება. საგამოძიებო მოქმედება,

---

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

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

[3] *Casey E.*, Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, 2011, 5. იხ. *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 238.

რომლის ეროვნულ კანონმდებლობაში ასახვა 2010 წლის 24 სექტემბრის ცვლილებით განხორციელდა და მასზე სსსკ-ის 112-ე მუხლის დებულებები გავრცელდა. თუმცა, საპროცესო კანონმდებლობაში მოგვიანებით განხორციელებული ცვლილებით (2014 წლის 1 აგვისტო) საგამოძიებო მოქმედების ჩატარება ფარული საგამოძიებო მოქმედებისათვის დადგენილ წესებს დაექვემდებარა. [4] აღნიშნულმა ცვლილებამ მნიშვნელოვნად გაართულა მთელი რიგი ნაკლებად მძიმე კატეგორიის დანაშაულის გამოძიების მიზნებისთვის ელექტრონული მტკიცებულების მოპოვება.

ასეთმა საკანონმდებლო მოწესრიგებამ და შეიძლება ითქვას ხარვეზმა, არაერთგვაროვან სასამართლო პრაქტიკას დაუდო საფუძველი. მხედველობაში გვაქვს ე.წ. „შემოვლითი“ პრაქტიკის დამკვიდრება, რა დროსაც მხარეები, საქმისთვის მნიშვნელოვანი ელექტრონული ინფორმაციის მოპოვებას, „დათვალიერების“, [5] ცალკეულ შემთხვევებში ელექტრონული ინფორმაციის მატარებლის ამოღების გზით ცდილობდნენ.[6]

ხანგრძლივი დროის მანძილზე მნიშვნელოვან ხარვეზს წარმოადგენდა ასევე დაცვის მხარის უუფლებობა, კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობით მიემართა სასამართლოსთვის. ამ ხარვეზის დაძლევა მხოლოდ 2017 წლიდან საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილებით გახდა შესაძლებელი.[7]

ყურადღებას იმსახურებს აგრეთვე, 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტიც, [8] რომლის შედეგადაც გაუქმდა ფარული საგამოძიებო მოქმედების დებულებების სსსკ-ის 136-ე მუხლზე გავრცელება და მისი რეგულირება ამავე კოდექსის 112-ე მუხლის, სასამართლოს განჩინებით ჩასატარებელ საგამოძიებო მოქმედებათა წესის მიხედვით განისაზღვრა. ამ ძალზედ მნიშვნელოვანი

[4] იხ. განმარტებითი ბარათი „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის თაობაზე“ საქართველოს კანონის პროექტი, N2634-რს, 31.07.14.

[5] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 24 თებერვლის N1გ/272-16 განჩინება. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 4 ოქტომბრის N1გ/1537-16 განჩინება.

[6] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2014 წლის 9 დეკემბრის განჩინება N1გ/1245, 2.

[7] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“.

[8] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24/05/2022.

გადაწყვეტილებით როგორც ბრალდების, ისე დაცვის მხარეს, ნებისმიერი კატეგორიის დანაშაულზე მიმდინარე გამოძიებისას, შენახული კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობით სასამართლოსთვის მიმართვის უფლებამოსილება მიენიჭა. თუმცა, არსებული რეგულაცია პრივილეგირებული ინფორმაციის დაცვისა და თანხმობის საფუძველზე მონაცემთა გადაცემის მხრივ კვლავ არ არის სრულყოფილი და სიღრმისეულ კვლევას საჭიროებს.

ამდენად, 2010 წლიდან დღემდე კომპიუტერული მონაცემის გამოთხოვის საპროცესო სამართლებრივ რეგულირებას არაერთი მნიშვნელოვანი საკანონმდებლო ცვლილება შეეხო და თითოეული მათგანი მათივე თანმდევი შედეგების გათვალისწინებით კვლევის მნიშვნელოვან ნაწილს წარმოადგენს. ყოველივე ზემოაღნიშნულთან ერთად, კვლევის საგანია აგრეთვე კომპიუტერული მონაცემის შინარსობრივი მხარე, მისთვის დამახასიათებელი ნიშან-თვისებები, ეროვნული კანონმდებლობის როგორც ევროპის საბჭოს მიერ შემუშავებული „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირებით აღებულ ვალდებულებებთან, ისე ადამიანის უფლებათა საერთაშორისო სამართლით უზრუნველყოფილი პირადი ცხოვრების ხელშეუხებლობის შეზღუდვის მართლზომიერ საფუძვლებთან შესაბამისობის საკითხი.

წინამდებარე კვლევის მიზანი:

კომპიუტერული მონაცემის გამოთხოვის საქართველოს სისხლის სამართლის საპროცესო კოდექსში დამოუკიდებელი საგამოძიებო მოქმედების სახით გათვალისწინებიდან დღემდე განხორციელებული საკანონმდებლო ცვლილებები ერთმნიშვნელოვნად მიუთითებს საკითხის აქტუალურობაზე. ამას ემატება ისიც, რომ განხორციელებული საკანონმდებლო ცვლილება თუ სასამართლოს განმარტება განსხვავებული სასამართლო პრაქტიკის საფუძველი ხშირად გამხდარა, რაც ყოველ ჯერზე გვარწმუნებს, რომ საკითხი ღრმა მეცნიერულ კვლევას, ანალიზს საჭიროებს.

სწორედ აღნიშნულის გათვალისწინებით, სადისერტაციო კვლევის მიზანია, შეძლებისდაგვარად სრულყოფილად და საფუძვლიანად შეისწავლოს კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედების არსი და თავისებურებანი, მიმოიხილოს ეროვნულ კანონმდებლობაში განხორციელებული ცვლილებები და სასამართლო პრაქტიკისა და „კიბერდანაშაულის შესახებ“

კონვენციის ანალიზის საფუძველზე გამოკვეთოს ამა თუ იმ საკანონმდებლო ცვლილების ნაკლოვანებანი. ადამიანის უფლებათა საერთაშორისო სამართლით უზრუნველყოფილი სტანდარტების გათვალისწინებით, დაადგინოს ეროვნული კანონმდებლობით რამდენად გათვალისწინებულია ძირითად უფლებაში თვითნებურად ჩარევისგან დაცვის მყარი გარანტიები და დაცულია თუ არა პრივილეგირებული ინფორმაცია გამჟღავნებისგან. საზღვარგარეთის კანონმდებლობის შესწავლის ფონზე წარმოაჩინოს საკვლევი საკითხისადმი განსხვავებული მიდგომები და დისერტაციაში განხილულ სხვადასხვა საკითხებთან თანხვედრაში შეიმუშაოს რეკომენდაციები შენახული კომპიუტერული მონაცემის გამოთხოვის მარეგულირებელი დებულებების შემდგომი სრულყოფის მიზნით.

კვლევის მეთოდები: ძირითადად კვლევის მიზნებისთვის გამოყენებულია ისტორიული, ანალიტიკური, სისტემური, დოგმატური, ფორმალურ-ლოგიკური და შედარებით-სამართლებრივი მეთოდები.

დისერტაციის თეორული და პრაქტიკული მნიშვნელობა: ნიშანდობლივია, რომ სამეცნიერო თვალსაზრისით კვლევა წარმოადგენს ნოვაციას. მასში განხილულია საკითხები, რომლებიც საქართველოში მეცნიერულად არ არის დამუშავებული. განსაკუთრებით მნიშვნელოვანია თავად საგამოძიებო მოქმედების ბუნება და არსი, ელექტრონული მტკიცებულებების მახასიათებლები, „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნები და ეროვნული კანონმდებლობის მასთან შესაბამისობის საკითხი, წლების მანძილზე დაგროვილი საერთო სასამართლოების პრაქტიკა დოკუმენტის ან ინფორმაციის გამოთხოვის კუთხით და სხვა. აღნიშნულის გათვალისწინებით, ნაშრომში მოყვანილი მოსაზრებები სასარგებლო უნდა იყოს როგორც პრაქტიკოსი, ისე მეცნიერი იურისტებისთვის.

დისერტაციის სტრუქტურა და მოცულობა: სადისერტაციო ნაშრომი შედგება შესავლისგან, 7 თავისაგან და დასკვნისგან. დისერტაციას თან ერთვის ბიბლიოგრაფია და 3 დანართი.

თავი I. კომპიუტერული მონაცემის ზოგადი მიმოხილვა

1. კომპიუტერული მონაცემის არსი

1.1 ტერმინთა განმარტების მნიშვნელობა

თუ წინათ კომპიუტერული მოწყობილობის ან კომპიუტერული მონაცემის გამოძიების ინტერესებისთვის გამოყენება განსაკუთრებულ მოვლენად განიხილებოდა, დღეს, ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ინტენსიური განვითარების გათვალისწინებით, ისინი მის განუყოფელ ნაწილს წარმოადგენენ.[9]

როგორც სხვა ქვეყნების, ისე საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში სისხლის სამართლის საქმისათვის მნიშვნელობის მქონე ელექტრონული ინფორმაციის მოპოვებისა და მტკიცების პროცესში მისი გამოყენების ხელშეწყობის მიზნით გათვალისწინებულ იქნა „კიბერდანაშაულის შესახებ“ კონვენციით განსაზღვრული კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებები. სწორედ, მათი ეროვნულ კანონმდებლობაში დანერგვის თანმხლები შედეგი იყო სპეციფიკური და ტექნიკური მახასიათებლების მქონე ტერმინების, როგორებიცაა კომპიუტერული სისტემა, კომპიუტერული მონაცემი და სხვა გამოჩენა, რაც შეიძლება ითქვას, მნიშვნელოვან გამოწვევად იქცა იურიდიული საზოგადოებისათვის.

სირთულეს წარმოადგენს მათი შინაარსობრივი მხარის ზუსტი გაგება, მატერიალურ და ელექტრონულ დოკუმენტს შორის არსებული სხვაობის წარმოჩენა. ამას ემატება ისიც, რომ ქართულ იურიდიულ ლიტერატურაში მწირია კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების შესახებ ინფორმაცია. ამასთან, საერთო სასამართლოებს საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით დადგენილი წესით დაყენებული შუამდგომლობების განხილვისას გამუდმებით უწევთ შეფასება, შუამდგომლობით მოთხოვნილი ინფორმაცია მიეკუთვნება თუ არა კომპიუტერულ მონაცემს და ინახება თუ არა ის კომპიუტერულ სისტემაში ან მონაცემთა შესანახ მოწყობილობაში.[10]

---

[9] *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006, 1.

[10] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2014 წლის 9 დეკემბრის განჩინება №1გ/1245, 3-4. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 4 ოქტომბრის განჩინება №1537-16, 6;ზესტაფონის რაიონული სასამართლოს 2020 წლის 8 იანვრის

შესაბამისად, კომპიუტერული სისტემისა და მონაცემის შინაარსობრივი კვლევა ერთის მხრივ ხელს შეუწყობს ინფორმაციული სიმწირის შევსებას, ხოლო მეორეს მხრივ საკითხით დაინტერესებულ პირებსა და იურისტებს დაეხმარება პრაქტიკული საქმიანობის განხორციელებაში.

1.2. კომპიუტერული სისტემა

კომპიუტერული მონაცემის შინაარსისა და არსის გაგება უპირველესად კომპიუტერული სისტემის შინაარსის და მისი ფუნქციის გაცნობიერებით უნდა დავიწყოთ.

კომპიუტერული სისტემა, „კიბერდანაშაულის შესახებ“ კონვენციის 1-ლი მუხლის „ა“ ქვეპუნქტით განიმარტება, როგორც „ნებისმიერი მექანიზმი ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელთაგან ერთი ან მეტი, პროგრამის მეშვეობით ავტომატურად ამუშავებს მონაცემებს“. ნიშანდობლივია, რომ იდენტური შინაარსის მატარებელია საქართველოს სისხლის სამართლის საპროცესო კოდექსში მოცემული კომპიუტერული სისტემის განმარტებაც (სსსკ-ის მე-3 მუხლის 27-ე ნაწილი), თუმცა მათ უკან ბევრი სხვა საკითხია, რისი ცოდნაც აუცილებელია კომპიუტერული სისტემის უკეთ გასაცნობიერებლად.

კომპიუტერული სისტემა კომპიუტერული მოწყობილობისა და პროგრამული უზრუნველყოფის ერთიანობას წარმოადგენს.[11] კომპიუტერული სისტემა სხვადასხვა მოწყობილობებისგან შედგება, თუმცა შესაძლოა ითქვას, რომ მონაცემთა შესატან[12] და გამოსატან მოწყობილობებთან[13] ერთად მის განუყოფელ ნაწილებს ცენტრალური პროცესორი, ინფორმაციის შემნახველი მოწყობილობა და პროგრამული უზრუნველყოფა წარმოადგენენ.[14]

განჩინება №11/1-20, 4; ზესტაფონის რაიონული სასამართლოს 2021 წლის 6 იანვრის განჩინება №11/1-2021, 4.

[11] *Stanfield R. A.*, The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 61 <https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf> [23.05.2023].

[12] მოწყობილობათა ძირითადი ფუნქცია მონაცემთა კომპიუტერულ სისტემაში გადატანაა. მათ რიცხვს მიეკუთვნება კლავიატურა, მაუსი, სენსორული ეკრანი, ქსელური კავშირი და სხვა.

[13] დამუშავების შემდეგ მონაცემები გარდაიქმნება იმდაგვარად, რომ მისი გაგება და აღქმა შესაძლებელი ხდება ადამიანებისათვის. ინფორმაციათა გამოსატან მოწყობილობებს განეკუთვნება მონიტორი, ეკრანი, დინამიკი, პრინტერი და სხვა.

[14] *Stanfield R. A.,* "The Authentification of Electronic Evidence" Queensland University of Technology, 2016, 61

ცენტრალური პროცესორი - როგორც კომპიუტერის ფუნქციონალური ნაწილი ლოგიკურ-არითმეტიკული ოპერაციების დახმარებით ამუშავებს მონაცემებს [15] და მიღებული შედეგი გამოაქვს მონიტორზე, ინახავს მეხსიერებაში ან ინტერნეტის მეშვეობით გადასცემს სხვა მოწყობილობას.[16]

პროგრამული უზრუნველყოფა - კომპიუტერის მართვისათვის გამოყენებად პროგრამათა ერთობლიობაა, რომელთაგან შესაძლოა გამოვყოთ როგორც სისტემური (ოპერაციული), ისე აპლიკაციური (გამოყენებითი) უზრუნველყოფა. [17] სისტემური პროგრამული უზრუნველყოფა კომპიუტერული მოწყობილობის ფუნქციონირების განუყოფელ ნაწილს წარმოადგენს. იგი აკონტროლებს მონაცემთა მიმოქცევას, კავშირს ამყარებს მოწყობილობებთან და ამასთან, მართავს გამოყენებით პროგრამებს. [18] ხოლო აპლიკაციური (გამოყენებითი) უზრუნველყოფა - ეს არის „განსაკუთრებული დანიშნულების“ პროგრამა, რომელიც მომხმარებელს ვებ ბრაუზერის, ელექტრონული ფოსტის ან სხვა პროგრამების დახმარებით საშუალებას აძლევს განსაკუთრებული სახის დავალებები შეასრულოს კომპიუტერზე.

ინფორმაციის შემნახველი მოწყობილობები - უმეტესად ინფორმაციის შესანახ საშუალებებს მყარი დისკი და ოპერატიული მეხსიერება მიეკუთვნებიან. [19] ნებისმიერი პროგრამა ან მონაცემი, რომელიც პროცესორის მიერ მუშავდება ოპერატიულ მეხსიერებაში ინახება და მოწყობილობის გამორთვის ან გადატვირთვის შემთხვევაში როგორც წესი იკარგება. შესაბამისად მისი დროებითი და არასტაბილური ხასიათიდან გამომდინარე, [20] სამართალდამცავი ორგანოები მონაცემების დროებითი მეხსიერებიდან ამოღებას რეალურ დროში (Live), მოწყობილობის გამორთვამდე ცდილობენ. [21] ოპერატიული მეხსიერებისგან განსხვავებით, მყარი დისკი მუდმივ მეხსიერებას წარმოადგენს და სისტემის

---

[15] *Casey E,* Digital Evidence and Computer Crime, 3rd Edition, USA, Academic Press, 2011, 439.

[16] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 119.

[17] *Mason S., Weir R.S. G.,* The sources of electronic evidence, Electronic Evidence, Mason. S., Seng D., (eds.), 4th edition, London, 2017, 2-4.

[18] *ოთხოზორია ვ., ცირამუა ზ.,* ინფორმაციული ტექნოლოგიები, თბილისი, 2015, 226, < https://drive.google.com/file/d/1LyzJT-xOLJAlGNUyONrUvhhC_tOnppPu/view> [20.05.2023].

[19] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 120.

[20] იქვე.

[21] მოსამართლეთა ტრენინგი ქსელურ დანაშაულში, ევროპის საბჭო, 2010, 35. <https://rm.coe.int/16802fa3c1> [20.05.23].

გათიშვის შემთხვევაშიც მასში განთავსებული ინფორმაცია არ ნადგურდება. [22] შესაბამისად, იგი ელექტრონული ინფორმაციის ერთ-ერთ ძირითად წყაროს წარმოადგენს. საგულისხმოა, რომ მონაცემთა მატარებელი შეიძლება აგრეთვე მონაცემთა ისეთი დამგროვებლები იყოს როგორებიცაა მეხსიერების ბარათი, კომპაქტური დისკი და სხვა.[23]

ნათელია, რომ კომპიუტერული სისტემა თავის მხრივ კომპლექსურ მოწყობილობას წარმოადგენს, რომელსაც წინასწარ შედგენილი ინსტრუქციების, ე.წ. ალგორითმების მეშვეობით მონაცემთა შენახვის, ძებნისა და დამუშავების შესაძლებლობა გააჩნია.

კომპიუტერულ სისტემასთან დაკავშირებით საინტერესო შეფასებებს ვხვდებით ქართულ იურიდიულ ლიტერატურაშიც. ბატონი ლევან ბოძაშვილი და ნიკოლოზ კოხრეიძე სახელმძღვანელოში „კიბერსივრცის სამართალი“, კომპიუტერულ სისტემას განმარტავენ როგორც „ნებისმიერ მოწყობილობას ან ურთიერთდაკავშირებულ ხელსაწყოთა ჯგუფს, რომელთაგან ერთ-ერთი მაინც ასრულებს მონაცემების ავტომატურ გადაცემას პროგრამის მეშვეობით“ [24] აღნიშნულ განმარტებას გამოეხმაურა ბატონი უჩა ზაქაშვილი მის სადისერტაციო ნაშრომში „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“[25] და ავტორთა მიერ ჩამოყალიბებულ განმარტებას მოქმედ სისხლის სამართლის საპროცესო კანონმდებლობაში მოცემულ განმარტებასთან შედარებით მეტად ზუსტი უწოდა. [26] ნამდვილად აღნიშვნის ღირსია მათ მიერ მოცემული განსაზღვრება, თუმცა ყურადღება უნდა გავამახვილოთ მათ მიერ კომპიუტერული სისტემის ცნების განსაზღვრისას გამოყენებულ ტერმინზე „გადაცემა“. მართალია „გადაცემა“ დამუშავების შემადგენელი ნაწილია, თუმცა იგი ამ პროცესის მხოლოდ ერთი კონკრეტული გამოვლინებაა. შესაბამისად „დამუშავების“ ნაცვლად

---

[22] *Mason S., Weir R.S. G.,* The sources of electronic evidence, Electronic Evidence, Mason. S., Seng D., (eds.), 4th edition, London, 2017, 8.

[23] იქვე.

[24] *ბოძაშვილი ლ., კოხრეიძე ნ.,* კიბერსივრცის სამართალი 2012. <https://www.lit.ge/book/643-kibersivrcis-samartali-levan-bodzashvili,-nikoloz-koxreidze> [20.05.2023].

[25] *ზაქაშვილი უ.,* სადისერტაციო ნაშრომში „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“, 2013, 28-29 >http://press.tsu.ge/data/image_db_innova/disertaciebi_samartali/ucha_zaqarashvilii.pdf> [20.05.2023].

[26] ბატონი უჩა ზაქაშვილი სადისერტაციო ნაშრომში ეჭვს გამოთქვამს მექანიზმის ნაცვლად სიტყვა „ხელსაწყოს“ გამოყენების გამო და თვლის, რომ „მექანიზმი“ ბევრად უკეთ გამოხატავს კომპიუტერული სისტემის შემადგენელ ნაწილს, რაც სავსებით მისაღებია.

„გადაცემის“ გამოყენება შეიძლება ითქვას სრულყოფილად ვერ აღწერს კომპიუტერული სისტემის ფუნქციონირებისა და მის მიერ მონაცემთა დამუშავების პროცესს. ყოველივეს გათვალისწინებით კი, ვფიქრობთ, რომ ფართო ტერმინის გამოყენება მეტი სიზუსტით წარმოაჩენდა კომპიუტერული სისტემის ფუნქციონირებას. შესაბამისად, შეგვიძლია ვთქვათ, რომ კომპიუტერული სისტემა არის მექანიზმი ან მექანიზმთა ჯგუფი, რომელიც ავტომატურად, ადამიანის უშუალო ჩარევის გარეშე,[27] პროგრამის მეშვეობით[28] ამუშავებს მონაცემებს.

1.3. კომპიუტერული მონაცემი

ოფიციალური განმარტების თანახმად კომპიუტერულ მონაცემს კომპიუტერულ სისტემაში დამუშავებისთვის ხელსაყრელი ფორმით გამოსახული ინფორმაცია და კომპიუტერული სისტემის ფუნქციონირებისთვის აუცილებელი პროგრამა განეკუთვნება.[29] სიტყვა „მონაცემი“ ელექტრონული ფორმით არსებულ ნებისმიერ ინფორმაციას, ტექსტურ დოკუმენტს, სურათს, აუდიო-ვიდეო რგოლს, პროგრამას აერთიანებს, ხოლო კომპიუტერი კი თავისი ფართო გაგებით მიანიშნებს მოწყობილობაზე, რომელიც ინფორმაციას ელექტრონული ფორმით ინახავს, ამუშავებს ან/და გადასცემს.[30]

ნიშანდობლივია, რომ უცხოურ იურიდიულ ლიტერატურაში კომპიუტერული მონაცემის ნაცვლად უმეტესწილად „ციფრული ან ელექტრონული მტკიცებულების“ ცნებას ვხვდებით.[31] მაგალითისთვის, ციფრული მტკიცებულებების სამეცნიერო-სამუშაო ჯგუფის (SWDGE) მიერ შემოთავაზებული განმარტების მიხედვით ციფრულ მტკიცებულებას ელექტრონული ფორმით შენახული ან გადაცემული მტკიცებულებითი ღირებულების მქონე ინფორმაცია წარმოადგენს.[32]

---

[27] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 5.

[28] იქვე.

[29] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 20.12.2019, მუხ. 3(28). კიბერდანაშაულის შესახებ კონვენცია, ბუდაოეშტი, 23.11.2001. მუხ. 1(ბ).

[30] *Murdoch J.S., Seng D., Schafer B., Mason S.,* The sources and characteristics of electronic evidence and artificial intelligence, Electronic Evidence and Electronic Signature, *Mason. S., Seng D.*, (eds.) 5th edition, London, 2021, 40.

[31] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 122.

[32] Scientific Working Group on Digital Evidence (SWDGE), SWDGE Digital and Multimedia Evidence Glossary, 2016, 7 <https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Digital-Multimedia-Evidence-Glossary-062316.pdf> [21.05.2023].

კომპიუტერული მტკიცებულებების საერთაშორისო ორგანიზაციის (IOCE) ხედვით კი ელექტრონულ მტკიცებულებას ბინარული ფორმით შენახული ან გადაცემული ინფორმაცია მიეკუთვნება, რომლის გამოყენებაც სასამართლოშია შესაძლებელი. [33] საყურადღებოა, რომ აღნიშნული ორგანიზაციები ცნების განმარტებისას ყურადღებას ელექტრონული ინფორმაციის სასამართლოში გამოყენების მნიშვნელობაზე ამახვილებენ და არაფერს ამბობენ გამოძიების პროცესში მის მნიშვნელობაზე. [34] თუმცა, მისგან განსხვავებით, უფროს პოლიციელთა ასოციაცია (ACPO) ელექტრონულ მტკიცებულებას განმარტავს როგორც გამოძიებისთვის ღირებულ ინფორმაციას ან მონაცემს, რომელიც შენახული ან გადაცემულია კომპიუტერული მოწყობილობის მიერ.[35] საგულისხმოა, რომ ამგვარი ხედვა აქვს მართლმსაჯულების ეროვნულ ინსტიტუტსაც (NIJ). [36]

ცხადია, რომ კომპიუტერული მონაცემის შინაარსის მკაფიოდ განსაზღვრა არ არის ადვილი საქმე. განსაკუთრებით ისეთ პირობებში, როდესაც უცხოურ იურიდიულ ლიტერატურაში მის ნაცვლად ციფრული ან ელექტრონული მტკიცებულების ცნება გამოიყენება. საქმეს კიდევ უფრო ართულებს საინფორმაციო ტექნოლოგიების მუდმივი განვითარება, რაც მოძველების რისკის ქვეშ აყენებს კომპიუტერული მონაცემის არსებულ გაგებას. ამიტომ, არსებული რისკის შესამცირებლად მისი შინაარსის მაქსიმალურად ფართოდ წარმოჩენაა საჭირო. ყოველივეს მხვედველობაში მიღებით კი შეგვიძლია ვთქვათ, რომ კომპიუტერული მონაცემი ეს არის კომპიუტერულ სისტემაში შეყვანილი, ხოლო შემდგომ კომპიუტერული მოწყობილობის მიერ ავტომატურად დამუშავებული, შენახული ან გადაცემული ინფორმაცია. ხოლო ელექტრონული/ციფრული მტკიცებულება - კომპიუტერულ სისტემაში ან მასთან დაკავშირებულ მოწყობილობაში არსებული კომპიუტერული მონაცემი, რომელიც ღირებულია გამოძიებისთვის ან პროცესის მონაწილე მხარისათვის, სასამართლოში მნიშვნელოვანი გარემოებების დასადასტურებლად.[37]

---

[33] *Casey E.,* "Digital Evidence and Computer Crime", 3rd Edition, USA, Academic Press, 2011, 7.

[34] იქვე, 7.

[35] იქვე.

[36] *Mukasey B. M., Sedgwick L. J., Hagy W. D.*, Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, IX.

[37] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 122.

2. კომპიუტერული მონაცემის მახასიათებლები

ნიშანდობლივია, რომ ელექტრონული მტკიცებულების მიმართ განსხვავებული დამოკიდებულება არა მარტო პროფესიონალ იურისტებს, არამედ სამართლებრივ სისტემებს შორისაც გამოიკვეთა. [38] ერთი მხრივ ახალი კანონმდებლობა იქნა შემუშავებული უშუალოდ ელექტრონული მტკიცებულებისთვის, ხოლო რიგ შემთხვევებში არსებული ნორმები გავრცელდა ელექტრონული ფორმით შენახული მონაცემების გამოძიების მიზნებისთვის შეგროვება-გამოყენებაზე.[39]

განსხვავებული მიდგომის საფუძველი ძირითადად მაინც ელექტრონულ და ტრადიციულ მტკიცებულებებს შორის არსებული საერთო თუ განმასხვავებელი ნიშნები ხდებოდა. [40] შესაბამისად, ივარაუდება, რომ საქართველოს სისხლის სამართლის საპროცესო კოდექსში კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების ცალკე თავად გამოყოფა არა მარტო „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირების, არამედ მათ შორის არსებული ფუნდამენტური სხვაობის, შედეგიცაა.[41]

წესისამებრ, ელექტრონული მტკიცებულების მახასიათებლების სათანადოდ წარმოსაჩენად მის მატერიალურ მტკიცებულებასთან შედარების გზას მიმართავენ. შესაბამისად, იურიდიულ ლიტერატურაში გავრცელებულია ხედვა, რომ ელექტრონული მტკიცებულება თითის ანაბეჭდის ან დნმ-ის მსგავსად ლატენტურია, მარტივად და სწრაფად კვეთს ფიზიკურ-გეოგრაფიულ საზღვარს, [42] ადვილად ზიანდება [43] და ტრადიციულ მტკიცებულებასთან შედარებით განსხვავებულ მოპყრობას საჭიროებს.[44] თუმცა, გადამწყვეტი სიტყვა ელექტრონული დოკუმენტის ან მტკიცებულების მახასიათებლებზე მსჯელობისას მაინც სედონას საკონფერენციო

[38] *Schafer B., Mason S.,* The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 18.

[39] იქვე.

[40] იქვე.

[41] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 123.

[42] *Mukasey B. M., Sedgwick L. J., Hagy W. D*., Electronic Crime Scene Investigation: A Guide for First Responders, National Institute of Justice, USA, 2008, 9.

[43] *Gonzales R. A., Schofield B. R., Hagy W. D*., Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007, 2. იხ. *Casey E*, Digital Evidence and Computer Crime, 3rd edition., USA, Academic Press, 2011, 26.

[44] *Goodison E. S., Davis C. R., Jackson A.B.,* Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 3.

სამუშაო ჯგუფს[45] ეკუთვნის.[46] მათი შეფასებით ელექტრონული დოკუმენტისთვის დამახასიათებელია მეტამონაცემების, იგივე მაიდენტიფიცირებელი მონაცემების არსებობა; მოცულობა და გამრავლების შესაძლებლობა; ხანგრძლივუნარიანობა; დინამიურობა და ცვალებადობა; გარემოზე დამოკიდებულება და დისპერსია.[47]

2.1. მეტამონაცემები

მეტამონაცემები, როგორც კომპიუტერული მონაცემის შესახებ დამატებითი ინფორმაცია გავრცელებულია საინფორმაციო სისტემებში[48] და იმის გათვალისწინებით, რომ იგი როგორც უშუალოდ მომხმარებლის, ისე ავტომატურად, პროგრამული საშუალების მიერ იქმნება, არის მრავალგვარი.[49]

მეტამონაცემი საშუალებას გვაძლევს მივიღოთ დამატებითი ინფორმაცია დოკუმენტის სახელწოდების, შექმნის თარიღის, ადგილმდებარეობის, მისი ფორმატის, მახასიათებლებისა თუ სხვა მნიშვნელოვანი მონაცემების შესახებ. საგულისხმოა, რომ ხშირად მეტამონაცემები მომხმარებელთა ყურადღების მიღმა რჩება. წარმოვიდგინოთ შემთხვევა, როდესაც მომხმარებელი სოციალურ ქსელში ათავსებს განცხადებას ან მიმოწერას ახორციელებს მეგობართან, ნებისმიერ სხვა პირთან (პირებთან), ასეთ დროს პროგრამული საშუალება ავტომატურად განსაზღვრავს მეტამონაცემს განცხადების განთავსების ან აქტივობის დაწყებისა და დასრულების დროსთან დაკავშირებით, ავტორის ვინაობისა და ადგილმდებარეობის შესახებ.[50] შესაბამისად, ალბათობა იმისა, რომ მომხმარებელს წარმოდგენა არ

---

[45] *The Sedona Conference* – „სედონას კონფერენცია“, როგორც არაკომერციული, კვლევითი და საგანმანათლებლო ინსტიტუტი დაარსდა 1997 წელს *რიჩარდ ბრეიმანის* მიერ. სედონას კონფერენცია აერთიანებს რამდენიმე სამუშაო ჯგუფს, მათ შორის, სამუშაო ჯგუფს ელექტრონული დოკუმენტების შენახვისა და წარმოების შესახებ, რომლის მიზანს ელექტრონული დოკუმენტის მართვისა და ელექტრონული აღმოჩენის შესახებ სახელმძღვანელო პრინციპებისა და რეკომენდაციების შემუშავება წარმოადგენს. <https://thesedonaconference.org/> [23.05.2023]

[46] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 123-124.

[47] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, №1, 2018, 207.

[48] *Riley J.*, Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017, 1-3 < https://groups.niso.org/higherlogic/ws/public/download/17446/Understanding%20Metadata.pdf> [23/05.2023].

[49] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 27.

[50] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 125.

ჰქონდეს მისი შეცვლის ან განადგურების შესაძლებლობის თაობაზე საკმაოდ მაღალია.[51]

ყურადსაღებია უშუალოდ მეტამონაცემის უტყუარობის საკითხიც. [52] მისი ნამდვილობა დამოკიდებულია არა მარტო კომპიუტერული სისტემის გამართულად ფუნქციონირებაზე, არამედ სხვადასხვა გარე ფაქტორებზე, როგორიცაა მაგალითად კომპიუტერული მოწყობილობის დროის სარტყელი. [53] თუ ელექტრონული მოწყობილობის დროის სარტყელი არასწორია ან მისი საათი შეფერხებით მუშაობს, არაზუსტი იქნება მის მიერ შემქნილი მეტამონაცემიც.[54]

შეჯამების სახით კი უნდა ითქვას, რომ მეტამონაცემი წერილობითი დოკუმენტისგან განსხვავებით მხოლოდ ელექტრონულ დოკუმენტს გააჩნია და მისი განუყოფელი ნაწილია. [55] ამასთან, ძალზედ მნიშვნელოვანი ნაწილი, რომლის შეგროვებამ და ანალიზმა შესაძლოა გამოძიებისთვის მეტად სასარგებლო ინფორმაცია მოგვცეს. მეტიც, ხშირ შემთხვევაში ის, გადამწყვეტ როლს თამაშობს ელექტრონული დოკუმენტის ავთენტურობის დადგენის პროცესში.[56]

2.2. მოცულობა და გამრავლების შესაძლებლობა

თანამედროვე ტექნოლოგიებისა და ელექტრონული კომუნიკაციის საშუალებების განვითარების შედეგად, მსოფლიო მასშტაბით ინფორმაციის სწრაფი გაცვლა ყველასთვის ხელმისაწვდომი გახდა.[57] დედამიწის ნებისმიერი წერტილიდან დროის უმოკლეს მონაკვეთში ნებისმიერი მოცულობის ინფორმაციის გადაცემაა შესაძლებელი და ამის თვალსაჩინო მაგალითს ინტერნეტი, სოციალური ქსელი და ელექტრონული ფოსტა წარმოადგენენ. გარდა იმისა, რომ ზემოთხსენებული

---

[51] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 27.

[52] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,,,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, №1, 2018, 211.

[53] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 28.

[54] იქვე.

[55] *Stanfield R. A.*, The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 64 <https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf> [23.05.2023].

[56] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 125.

[57] იქვე.

საშუალებები ინფორმაციის მყისიერად გადაცემაში გვეხმარება, ელექტრონული ინფორმაციის გამრავლებასაც უწყობენ ხელს.[58]

ელექტრონული ფოსტის მაგალითზე თუ ვიმსჯელებთ, მომხმარებლები ხშირად ერთსა და იმავე შეტყობინებას ერთდროულად რამდენიმე ადრესატს უგზავნიან, ხოლო შეტყობინების მიმღებნი როგორც წესი ავტორს პასუხს უბრუნებენ ან სულაც მიღებულ წერილს მესამე პირებზე გადაამისამართებენ. ეს კი ცხადია ელექტრონული წერილის გამრავლებას, მისი არაერთი ეგზემპლარის შექმნას უწყობს ხელს.[59]

ელექტრონული დოკუმენტის ადვილად გავრცელებისა და გამრავლების თვალსაჩინო მაგალითია ასევე ინგლისისა და უელსის უმაღლესი სასამართლოს მიერ გახილული საქმე „ამპ უცნობთა წინააღმდეგ“.[60] კერძოდ, საქმეში არსებული მასალების მიხედვით დაზარალებულის მიერ ტელეფონის დაკარგვიდან სულ მცირე დროში, მასში განთავსებული სექსუალური ხასიათის ფოტომასალა ინტერნეტსივრცეში განთავსდა და ნებისმიერ მსურველს მათი გადმოწერისა და გაზიარების შესაძლებლობა მიეცა.

ელექტრონული დოკუმენტის დუბლირებასთან ერთად, ყურადღება უნდა გავამხვილოთ მის მოცულობაზეც. ხაზი გვინდა გავუსვათ იმ გარემოებას, რომ თუ დიდი მოცულობის წერილობით მასალას ფართობიც დიდი სჭირდება შესანახად, იგივე ან გაცილებით მეტი მოცულობის ელექტრონული ინფორმაციის განთავსება სულ პატარა ზომის მოწყობილობაში, განუსაზღვრელი ვადით არის შესაძლებელი.[61]

ინფორმაციის შემნახველ ფიზიკურ მოწყობილობებთან ერთად, ფართოდაა გავრცელებული ინფორმაციის ღრუბლოვან საცავში განთავსების მეთოდი. თუმცა, გარკვეული უპირატესობის მიუხედავად, ასეთ შემთხვევებში გასათვალისწინებელია როგორც იურისდიქციასთან დაკავშირებული საკითხები, ისე ინფორმაციაზე კონტროლის დაკარგვის საფრთხე.[62] მხედველობაში გვაქვს ის ფაქტი თუ რამდენად არის დაცული კონფიდენციალურობის პრინციპი, ვინ არის პასუხისმგებელი მის დაცვაზე, ხომ არ კარგავს მომხმარებელი კონტროლს მონაცემებზე, კერძოდ კი მისი

---

[58] იქვე.

[59] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,,,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, № 1, 2018, 208.

[60] *AMP v. Persons Unknown*, [2011] England and Wales High Court (EWHC) 3454 (TCC).

[61] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 126.

[62] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 26.

განკარგვის შესაძლებლობას. იმის გათვალისწინებით, რომ ელექტრონულ სივრცეში მონაცემთა წაშლა არ ნიშნავს მის განადგურებას,[63] მომხმარებლის მიერ ინფორმაციის წაშლის შემთხვევაში, ხომ არ რჩება მომსახურების მომწოდებლის მიერ მომხმარებლის კუთვნილი ინფორმაციის არამიზნობრივად და უკანონოდ გამოყენების საფრთხე.[64]

ამდენად კიდევ ერთხელ თვალსაჩინო გახდა, რომ ელექტრონული დოკუმენტის მოცულობისა და გამრავლების შესაძლებლობები აშკარად მიგვანიშნებენ მასსა და მატერიალურ დოკუმენტს შორის არსებულ სხვაობაზე. ეს კი გარდა იმისა, რომ საგამომძიებო ორგანოებს ელექტრონულ ინფორმაციაზე სხვადასხვა გზით წვდომის ახალ შესაძლებლობებს უხსნის, იმავდროულად მათი მხრიდან ელექტრონული მტკიცებულებისადმი განსხვავებული და ფრთხილი მოპყრობის საჭიროებაზე მიგვანიშნებენ.

2.3. ხანგრძლივუნარიანობა

კომპიუტერული მონაცემის დამახასიათებელი თვისებებიდან ერთ-ერთი გამორჩეულია მისი ხანგრძლივუნარიანობა.

წერილობითი დოკუმენტისგან განსხვავებით ელექტრონული ინფორმაციის წაშლა და განადგურება გარკვეულ სირთულეებთან არის დაკავშირებული. თუ მატერიალურ დოკუმენტს დაქუცმაცებით ან ცეცხლის მოკიდებით ადვილად გავანადგურებთ, ელექტრონული მონაცემების შემთხვევაში ეს არ კმარა.[65]

ელექტრონული სახით არსებულ ინფორმაციაზე საუბრისას ხშირად სიტყვა „წაშლას“ დაინტერესებული პირები და მათ შორის მომხმარებლები შეცდომაში შეყავს. [66] კომპიუტერული სისტემის მიერ ელექტრონული ინფორმაციის შენახვის პრინციპის მიხედვით დოკუმენტებს ენიჭებათ პირობითი აღმნიშვნელი, ხოლო მომხმარებლის მიერ დოკუმენტით სარგებლობის მოთხოვნის შემთხვევაში, კომპიუტერული სისტემა პირობითი აღმნიშვნელის მეშვეობით ადგენს ინფორმაციის განთავსების ადგილს. თუ

---

[63] იქვე, 25.

[64] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021,

[65] *Stanfield R. A.*, The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65 <https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf> [23.05.2023].

[66] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, № 1, 2018, 209.

მომხმარებელი ინფორმაციის „წაშლას“ გადაწყვეტს, კომპიუტერული სისტემა ინფორმაციის განადგურების ნაცვლად მხოლოდ ათავისუფლებს კონკრეტულ სექტორს ახალი ინფორმაციის ჩასაწერად. შესაბამისად, თუ გათავისუფლებულ ადგილზე არ მოხდება ახალი ინფორმაციის ჩაწერა, კომპიუტერული ექსპერტიზის დახმარებით ძველი ინფორმაციის აღდგენა და გამოყენება სავსებით შესაძლებელი იქნება.[67]

კომპიუტერული მონაცემის ეფექტური განადგურების საშუალებას ძველი ინფორმაციის ახლით შეცვლასთან ერთად, მისი ფიზიკური ან მაგნიტური დაზიანება წარმოადგენს. [68] შესაბამისად ეჭვგარეშეა, რომ ელექტრონული დოკუმენტი წერილობით დოკუმენტთან შედარებით უფრო ხანგრძლივუნარიანია. ეს კი გარდა იმისა, რომ კიდევ ერთხელ ცხადყოფს მათ შორის არსებულ სხვაობას, იმავდროულად სამართალდამცავი ორგანოების მხრიდან მათდამი განსხვავებული მოპყრობის აუცილებლობაზე მიგვანიშნებს.[69]

2.4. დინამიურობა და ცვალებადობა

დინამიურობა და ცვალებადობა ელექტრონული ინფორმაციის ძირითად მახასიათებლებს წარმოადგენენ. [70] ადამიანური რესურსის ჩარევის გარეშე შესაძლებელია მისი შინაარსის შეცვლა და ამის უტყუარ დადასტურებად კომპიუტერული სისტემის მიერ მონაცემთა ავტომატური განახლება შეგვიძლია დავასახელოთ.[71] პერიოდულად და ავტომატურად ხდება ელექტრონული ფოსტის მიერ მიღებული თუ გაგზავნილი შეტყობინებების შესახებ მონაცემების განახლება და ძველი წერილების განადგურება.[72]

ყურადსაღებია, რომ ელექტრონული ფორმით შენახული ინფორმაციის შეცვლის ფაქტი ხშირად მომხმარებლის ყურადღების მიღმა რჩება და განხორციელებული

---

[67] *Stanfield R. A.*, The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016, 65-66 <https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf> [23.05.2023].

[68] იქვე.

[69] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 127-128.

[70] იქვე.

[71] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, №1, 2018, 209.

[72] იქვე.

ცვლილების დადგენა მაიდენტიფიცირებელი მონაცემების გამოკვლევისა და კომპიუტერულ-ტექნიკური ექსპერტიზის გარეშე შეუძლებელია. [73] ეფექტური კვლევისთვის კი მნიშვნელოვანია დროულად მოხდეს მონაცემთა დაცვა და მათი რაც შეიძლება უსაფრთხოდ შენახვა.

სწორედ ამიტომ, კომპიუტერული მონაცემის დინამიური და ცვალებადი ხასიათის საპასუხოდ „კიბერდანაშაულის შესახებ“ კონვენცია გვთავაზობს როგორც შენახული კომპიუტერული მონაცემის სწრაფად დაცვის, ისე ინტერნეტ-ტრაფიკის მონაცემთა დაჩქარებული დაცვისა და ნაწილობრივ გამჟღავნების საგამოძიებო მოქმედებებს,[74] რაც ეროვნულ კანონმდებლობაში დამოუკიდებელი საგამოძიებო მოქმედების სახით დღემდე გათვალისწინებული არ არის.[75] ამდენად ყოველივე ზემოაღნიშნული კიდევ ერთხელ გვარწმუნებს, რომ ელექტრონულ მტკიცებულებებთან დაკავშირებულ გამოწვევებს მხოლოდ ეროვნული კანონმდებლობის მუდმივი განახლების, მისი სრულყოფის გზით შეიძლება გაეცეს პასუხი.

2.5. გარემოზე დამოკიდებულება

თუ ენის სრულყოფილად ცოდნა და კარგი მხედველობა წერილობითი დოკუმენტის გასაცნობად სრულებით საკმარისია, ელექტრონული დოკუმენტის შემთხვევაში ეს საკმარისად ვერ ჩაითვლება. მიზეზს, მისი მოწყობილობისა და პროგრამული უზრუნველყოფისადმი დამოკიდებულება წარმოადგენს. მათი დახმარების გარეშე მომხმარებელს არა თუ დოკუმენტის გაცნობა, არამედ მისი შექმნა, მასში ცვლილების შეტანა და მეტიც, მისი დაზიანებაც კი არ შეუძლია.[76]

გარემოზე დამოკიდებულების წარმოსაჩენად შეგვიძლია მესამე პირისთვის ელექტრონული დოკუმენტის გაგზავნის მაგალითი მოვიშველიოთ. ხშირია შემთხვევები, როდესაც ჩვენ მიერ სხვისთვის გაზიარებული დოკუმენტი ადრესატის

[73] იქვე.

[74] Convention on Cybercrime, Budapest, 23.11.2001, Art. 16-17.

[75] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 128.

[76] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 21.

კომპიუტერულ სისტემაში სათანადოდ ან საერთოდ არ ფუნქციონირებს. გამომწვევი მიზეზი კი განხვავებული პროგრამული უზრუნველყოფაა.[77]

სამართლებრივი კუთხით, მათ შორის გამოძიების თვალსაზრისით დამატებით სირთულეებს ქმნის ტექნიკური და პროგრამული უზრუნველყოფის განვითარების ტემპიც. ტექნოლოგიის განვითარების შესაბამისად სულ უფრო ჭირს გამოძიებისთვის რელევანტური მტკიცებულებების მოპოვებაც. აღნიშნულის უმთავრეს მიზეზს კომპიუტერული მონაცემის მოპოვებისთვის საჭირო ხელსაწყოების არ არსებობა ან მათზე წვდომის შეუძლებლობა წარმოადგენს. [78] შესაბამისად, ელექტრონული მტკიცებულების მოპოვების თვალსაზრისით იურისტებისა და ექსპერტების პრაქტიკულ გამოცდილებაზე არანაკლებ მათ სისტემატიურ გადამზადებაზე ზრუნვაა საჭირო.[79]

ფაქტია, ელექტრონული ინფორმაცია, კომპიუტერული სისტემა და პროგრამული უზრუნველყოფა ერთმანეთთან მჭიდროდ დაკავშირებული ცნებებია. მათი ერთმანეთის გარეშე არსებობა შეუძლებელია. [80] მეტიც, იმისათვის რომ კომპიუტერული მონაცემი ადამიანისთვის აღქმადი გახდეს, ხშირად სხვადასხვა ტექნოლოგიათა ერთობლივად გამოყენების საჭიროებაც კი დგება დღის წესრიგში.

2.6. დისპერსია

დისპერსიულობა მჭიდრო კავშირშია ელექტრონული ინფორმაციის გამრავლების შესაძლებლობასთან. კომპიუტრული მონაცემის გამრავლებისა და დისპერსიულობის გათვალისწინებით შესაძლოა ელექტრონული დოკუმენტი სხვადასხვა ადგილას, ოპერატიულ მეხსიერებაში, მყარ დისკზე ან მონაცემთა ისეთ შემნახველებში განთავსდეს, როგორებიცაა მეხსიერების ბარათი, მყარი დისკი ან ღრუბლოვანი საცავი. ამასთან, მონაცემთა განთავსების ადგილის მიუხედევად, თითოეული დოკუმენტი როგორც წესი იდენტურად გამოიყურება, რაც დედანის ასლისგან გამიჯვნას მნიშვნელოვნად ართულებს.

---

[77] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 129.

[78] *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 24.

[79] იქვე, 23.

[80] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 129.

ცხადია, მარტივი არც მოცულობით ელექტრონულ ინფორმაციაზე მუშაობაა. თუმცა, ასეთ შემთხვევაში იდენტური მოცულობის წერილობით დოკუმენტთან შედარებით, ელექტრონული დოკუმენტების მოძიებასა და გამოყენებას მონაცემთა ავტომატური ძებნის ფუნქცია ამარტივებს.[81]

3. კომპიუტერული მონაცემის მტკიცებულებითი ძალა

თანამედროვე ეპოქაში რთული წარმოსადგენია დანაშაული, რომელსაც კავშირი არ აქვს ციფრულ განზომილებასთან. დღითიდღე მატულობს კრიმინალების მიერ დანაშაულის ჩადენის პროცესში თანამედროვე ტექნოლოგიების გამოყენების ფაქტები, რაც თავის მხრივ ახალი გამოწვევის წინაშე აყენებს, როგორც რიგით მოქალაქეებს, ისე სამართალწარმოების პროცესში ჩართულ პირებს. [82] უწინ თუ იურიდიული საზოგადოება ელექტრონულ მტკიცებულებას კომპიუტერულ დანაშაულთან კავშირში განიხილავდა, ახლა მის მნიშვნელობაზე ყურადღებას სხვა სახის დანაშაულის გამოძიების პროცესშიც ამახვილებენ.

კომპიუტერული მონაცემის სიუხვიდან გამომდინარე, მისი მოპოვება და გამოყენება თითქმის ნებისმიერი სახის დანაშაულის გამოძიების პროცესშია შესაძლებელი. ხელს უწყობს მომხდარის შესახებ დეტალური ინფორმაციის მიღებას. კერძოდ, სად და როდის მოხდა დანაშაულის ჩადენა, რა სახის ურთიერთობა ჰქონდა დაზარალებულსა და სავარაუდო დამნაშავეს ერთმანეთთან. მეტიც, ციფრული მტკიცებულების მეშვეობით „განზრახვის“ დადგენაც კია შესაძლებელი. [83]

ლოკარდის „გაცვლითი პრინციპის“[84] მიხედვით, ყოველი კონტაქტი ტოვებს კვალს. მაგალითისთვის, მკვლელობის საქმეში დამნაშავემ, მსხვერპლის კუთვნილ

---

[81] *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, № 1, 2018, 213.

[82] *Casey E.,* Digital Evidence and Computer Crime, Forensic Science Computers and the Internet, 3rd edition, USA, Academic Press, 2011, 3.

[83] იქვე, 6.

[84] *ედმონდ ლოკარდი* - მედიცინის მეცნიერებათა დოქტორი, რომელიც ცნობილია სასამართლო აქსიომის გამო, რომელიც მის სახელს ატარებს: „ლოკარდის გაცვლითი პრინციპი“. ეს დოქტრინა გაცხადდა ედმონდ ლოკარდის მიერ მე-20 საუკუნის დასაწყისში ლიონში, საფრანგეთში. მოცემული პრინციპის მიხედვით, ორი ელემენტის კონტაქტისას ხდება მიკროსკოპული მასალის ცვლა. შესაბამისად, ინდივიდის ნებისმიერმა ქმედებამ და განსაკუთრებით ძალადობრივმა ქმედებამ, შეუძლებელია არ დატოვოს კვალი. საუცხოო კი - ამ კვალის მრავალფეროვნებაა: ზოგჯერ ეს ანაბეჭდებია, ზოგჯერ მარტივი კვალი, ზოგჯერ ლაქები. ***იხ. უეინ. ა. პეტერიკი, ბრენტ ე. ტიორვი., ფერგუსონი კ.,*** „სასამართლო კრიმინოლოგიის შესავალი“, 2013, 23-26;

კომპიუტერულ სისტემაში თვითმკვლელობის შესახებ ჩანაწერის დატოვებით, შესაძლოა თავგზა აუბნიოს გამოძიებას. თუმცა, დამნაშავე დაზარალებულის მიერ თითქოსდა თვითმკველელობის ინსცენირების პროცესში, კომპიუტერულ მოწყობილობაში კონკრეტული ჩანაწერის შექმნით საბეჭდ მოწყობილობაზე ტოვებს კვალს. საბეჭდ მოწყობილობაზე დატოვებული თითის ანაბეჭდების საშუალებით კი სამართალდამცავ ორგანოებს საშუალება ეძლევათ დაადასტურონ ამა თუ იმ პირის დანაშაულის ადგილზე ყოფნის ფაქტი. ნიშანდობლივია, რომ მსგავსი პრინციპი მოქმედებს ციფრულ სივრცეშიც. [85] ციფრულ სამყაროში ლოკარდის გაცვლითი პრინციპის ნათლად წარმოსაჩენად წარმოვიდგინოთ შემთხვევა როდესაც ინდივიდი მუქარის შემცველ შეტყობინებას ელექტრონული ფოსტის მეშვეობით აგზავნის, შეტყობინებასთან დაკავშირებულ ინფორმაციას კი მისი კომპიუტერული სისტემა მყარ დისკზე ინახავს. შესაბამისად, აღნიშნული შესაძლოა წარმატებით გამოიყენონ გამომძიებლებმა და სათანადო საგამოძიებო მოქმედებებისა და ექსპერტიზის ჩატარების მეშვეობით ზემოთხსენებულ ინფორმაციასთან ერთად სხვა, გამოძიებისთვის სასიცოცხლო მნიშვნელობის მქონე ელექტრონული მტკიცებულებაც მოიპოვონ. [86] ცხადია, რომ დამნაშავე მატერიალურ საგნებთან ურთიერთობის მსგავსად ციფრულ სამყაროშიც ტოვებს კვალს და ციფრული ინფორმაცია შესაძლოა ისეთივე მტკიცებულებითი ღირებულების მატარებელი იყოს სისხლის სამართლის საქმეში, როგორც ფიზიკური მტკიცებულება ან მოწმის ჩვენება. შესაბამისად, ციფრული მტკიცებულების მნიშვნელობის საილუსტრაციოდ მიზანშეწონილად მიგვაჩნია რამდენიმე გახმაურებული საქმის მიმოხილვა.

მაშასადამე, კომპიუტერული მონაცემის მტკიცებულებით ღირებულებას უკავშირდება პედრო ბრავოს საქმე. [87] საქმის მასალების მიხედვით ფლორიდის უნივერსიტეტის პირველკურსელი კრისტიან აგილარი 2012 წლის სექტემბერში უგზოუკვლოდ დაიკარგა. გაუჩინარებამდე კი, ის მის მეგობარ, პედრო ბრავოსთან ერთად ადგილობრივ მაღაზიაში შენიშნეს. სამ კვირიანი ძებნის შემდეგ მის ნეშტს, ლენტში გახვეულს მაღაზიიდან 60 მილის დაშორებით მიაკვლიეს. ჩატარებული საგამოძიებო მოქმედებების შედეგად პოლიციამ აგილარის სისხლის კვალი ბრავოს

[85] *Casey E.,* Digital Evidence and Computer Crime, 2nd edition, USA, Academic Press, 2004, 96-97.
[86] იქვე, 98.
[87] *The State of Florida v. Pedro Andres Bravo*, Alachua County Courthouse, case No.CF003821A, 2014.

ავტომობილში აღმოაჩინა, ხოლო დაზარალებულის ზურგჩანთა კი ეჭვმიტანილის სახლში. ასევე, გამომძიებლებმა გამოძიების შედეგად მოიპოვეს ქვითარი, რომლის მიხედვითაც დანაშაულის ჩადენამდე ბრავომ ლენტი და ნიჩაბი შეიძინა. ექსპერტების მიერ ბრავოს კუთვნილი მობილური ტელეფონის გამოკვლევის შედეგად კი აღმოჩნდა, რომ გარდაცვლილის გაუჩინარებიდან მალევე, ბრავო ერთ-ერთი პროგრამის გამოყენებით მეგობრის გადამალვის ხერხის შესახებ ინფორმაციის მოძიებას ცდილობდა. ამასთან, დაზარალებულის გაუჩინარების დროს ბრავოს მობილურ ტელეფონში არსებული ელექტროფანარი საათზე მეტ ხანს იყო ჩართული. ხოლო სატელეფონო ანძების კვლევამ აჩვენა, რომ აგილარის გაუჩინარებიდან ბრავო დასავლეთით გაემგზავრა, სადაც მოგვიანებით გარდაცვლილის გვამი აღმოაჩინეს. მტკიცებულებების გათვალისწინებით კი პედრო ბრავოს მსჯავრი პირველი ხარისხის მკვლელობისთვის დაედო.[88]

გადაწყვეტილება, რომელშიც შეიძლება ითქვას გადამწყვეტი როლი კომპიუტერულმა მონაცემებმა ითამაშეს, დაკავშირებულია კეისი ენტონის საქმესთან. [89] კეისიმ პოლიციას განუცხადა, რომ მან ორი წლის ქალიშვილი დაკარგა, რომელიც ბოლოს ძიძასთან ერთად დატოვა. თუმცა, მან ამის შესახებ პოლიციას მცირეწლოვნის დაკარგვიდან ერთი თვის შემდეგ აცნობა. ნაფიც მსაჯულთა გადაწყვეტილებით კეისის მსჯავრი ცრუ ინფორმაციის მიწოდებისათვის დაედო, ხოლო ქალიშვილის მკვლელობის ნაწილში გამართლდა.

საქმეში არსებული მასალების მიხედვით, მცირეწლოვნის, კელის გვამი, სახლთან ახლოს, ტყეში იპოვეს. ბრალდების მხარის პოზიცია, რომ შვილის მკვლელობაში ბრალი დედას, კეისის მიუძღვოდა, მნიშვნელოვანწილად ციფრულ მტკიცებულებებს ეფუძნებოდა. კერძოდ, სასამართლოში წარმოდგენილი იყო ენტონის კომპიუტერული სისტემიდან ამოღებული ინტერნეტ-ბრაუზერის ისტორია, რომლის მიხედვითაც ენტონი მკვლელობის მეთოდებთან და აგრეთვე, ქლოროფორმის სითხესთან (რომელიც მოგვიანებით მის ავტომობილში აღმოაჩინეს) დაკავშირებით ინფორმაციას ეძებდა. თუმცა, მოგვიანებით დადგინდა, რომ ექსპერტ-გამომძიებლების მიერ გამოყენებული საშუალება ციფრული მტკიცებულებების მოსაპოვებლად არაზუსტი

[88] *Goodison E.S., Davis C.R., Jackson A.B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 2.
[89] *Casey Marie Anthony v. State of Florida,* Case No. 5D11-2357, 2013.

იყო. კერძოდ, ხელსაწყო, რომელიც ექსპერტ-გამომძიებლებმა ციფრული მტკიცებულების მოსაპოვებლად გამოიყენეს, მხოლოდ ერთ კონკრეტულ ინტერნეტ-ბრაუზერზე მოქმედებდა, ხოლო საქმის მასალების მიხედვით კეისი უპირატესობას სხვა საძიებო პროგრამას ანიჭებდა. შესაბამისად, არასათანადო გამოძიების შედეგად ენტონის მიერ „უსაფრთხო ასფიქსიასთან“ დაკავშირებით მოძიებული ინფორმაცია სასამართლოსთვის ხელმიუწვდომელი აღმოჩნდა,[90] რამაც მკვლელობის საქმეში კეისის გამართლებას შეუწყო ხელი.

ციფრული მტკიცებულების ნაკლებობით გამოწვეულ დაბრკოლებას ეხება ასევე ფილიპ ველშის მკვლელობის საქმე.[91] გარდაცვლილი ტაქსის ექსპედიტორად მუშაობდა. მართალია გარდაცვლილი სამსახურეობრივი მოვალეობის შესრულების დროს აქტიურად სარგებლობდა კომპიუტერული მოწყობილობით, თუმცა პირად ცხოვრებაში იგი ერიდებოდა მათ გამოყენებას. მეტიც, მობილური ტელეფონიც კი არ გააჩნდა. როგორც გამომძიებისთვის გახდა ცნობილი, იგი მარტო ცხოვრობდა და სახლის კარს ტაქსის მძღოლებისთვის მუდამ ღიას ტოვებდა, რათა მათ ცვლებს შორის გამოეძინათ. ერთ დღესაც, მას საკუთარ სახლში მოკლულს მიაკვლიეს, თუმცა გამომძიებამ ვერ შეძლო დაედგინა თუ ვისთან ჰქონდა გარდაცვლილს ურთიერთობა, რით იყო დაზარალებული დაკავებული თავისუფალ დროს, რა წარმოადგენდა მისი ინტერესის სფეროს და ა.შ. პოლიციის წარმომადგენლების განცხადებით, ის ფაქტი, რომ დაზარალებული არ სარგებლობდა ელექტრონული მოწყობილობებით, ართულებდა საქმის გამოძიებას და სწორედ ამიტომ, აღნიშნული საქმე დღემდე გამოუძიებელი რჩება.[92]

ნიშანდობლივია, რომ ქართულ რეალობაშიც მოიძებნება საქმეები, სადაც კომპიუტერულმა მონაცემებმა თუ გადამწყვეტი არა, გარკვეული სახის წვლილი შეიტანეს როგორც გამოძიების, ისე სასამართლო განხილვის პროცესში. საქმე, რომელშიც ელექტრონული სახის ინფორმაციამ მნიშვნელოვანწილად განსაზღვრა გამოძიების მიმართულება უკავშირდებოდა თამარ ბაჩალიაშვილის მკვლელობას.[93]

---

[90] *Goodison E.S., Davis C.R., Jackson A.B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015, 2.

[91] იქვე, 2.

[92] იქვე, 3.

[93] *იხ.* პროკურატურის ოფიციალური განცხადება <https://pog.gov.ge/news/saqarTvelos-prokuraturis-gancxadeba-Tamar-bachaliashvilis-saqmeze> [24.05.2023]

საგამოძიებო უწყების განცხადებით, გამოძიების მსვლელობისას სხვადასხვა ობიექტებიდან მოპოვებული მოცულობითი ზომის ვიდეოჩანაწერები და სატელეფონო აქტივობის შესახებ საკომუნიკაციო ოპერატორებისგან გამოთხოვილი ინფორმაცია დამუშავდა. აღდგენილ და შესწავლილ იქნა ტელეფონსა თუ კომპიუტერში არსებული ინფორმაცია, გამოთხოვილ იქნა სოციალური ქსელებთან დაკავშირებული მონაცემები და ინფორმაცია მათში განხორციელებული აქტივობების შესახებ. აგრეთვე, შესწავლილ იქნა გარდაცვლილის მიერ საძიებო სისტემაში განხორციელებული აქტივობებიც, რომლის კვლევის შედეგადაც დადგინდა, რომ გარდაცვლილი ხშირად ეძებდა ინფორმაციას თვითმკვლელობის გზების და ასევე ურეცეპტო საძილე აბების შესახებ, რომლის ცარიელი ფირფიტებიც მოგვიანებით აღმოჩენილ იქნას მის ავტომობილში. ასევე, გამოძიების პროცესში დადგინდა, რომ სოციალური ქსელის „Facebook"-ის დახმარების განყოფილებაში გარდაცვლილი ეცნობოდა ინფორმაციის იმის შესახებ თუ რა ბედი ეწეოდა მის ანგარიშს მისი გარდაცვალების შემთხვევაში. სოციალურ ქსელში არსებული აქტივობის უშუალოდ გარდაცვლილის მიერ განხორციელების ფაქტი კი თავად სოციალური ქსელიდან გამოთხოვილი ინფორმაციითა და ანგარიშზე წვდომის დროს გამოყენებული IP მისამართების დეტალური შესწავლით დადასტურდა, რამაც სრულად გამოირიცხა გარეშე პირთა მხრიდან ანგარიშზე წვდომის ან ინფორმაციის შესწორების ან წაშლის შესახებ არსებული ვერსია. [94] საყურადღებოა, რომ მიმდინარე საქმეზე, გარდაცვლილის „Google"-ის ანგარიშზე დაფიქსირებული გადაადგილებისა და ადგილმდებარეობის ამსახველი ინფორმაციის შესწავლით გამოიკვეთა რომ ვიდეოკამერების მიერ დაფიქსირებული ავტომობილის გადაადგილების მარშრუტი, ანგარიშზე დაფიქსირებული მონაცემების იდენტური იყო. აღნიშნული და სხვა დამატებითი მტკიცებულებებით კი დადგინდა, რომ არა თუ მკვლელობას, არამედ თვითმკვლელობას ჰქონდა ადგილი.

კიდევ ერთი ცნობილი საქმე, სადაც კომპიუტერული მონაცემები მნიშვნელოვან მტკიცებულებას წარმოადგენდნენ ე.წ. „ციანიდის საქმეს"უკავშირდება. პირს ბრალად მკვლელობის მომზადება და ცეცხლსასროლი იარაღის მართლსაწინააღმდეგოდ

[94] *იხ.* პროკურატურის ოფიციალური განცხადება <https://pog.gov.ge/news/saqa-1> [24.05.2023].

შეძენა-შენახვა ედებოდა.[95] მოცემულ საქმეზე მიმდინარე გამოძიების პროცესში ჩატარდა არაერთი საგამოძიებო თუ საპროცესო მოქმედება, დათვალიერდა და ამოღებულ იქნა როგორც მობილური ტელეფონები, ისე კომპიუტერები და ელექტრონული ინფორმაციის მატარებლები და დადგინდა, რომ ბრალდებული დაზარალებულის მოკვლას მომწამვლელი ნივთიერების „ციანიდის“ გამოყენებით გეგმავდა. გამოიკვეთა, რომ ბრალდებული ინტერნეტ ქსელის მეშვეობით აქტიურად ეძებდა და ეცნობოდა ინფორმაციას კალიუმ ციანიდის ნიშან-თვისებების, გამოყენების წესისა და ადამიანის ორგანიზმზე მისი ზემოქმედების შესახებ, ასევე მისი შეძენის შესაძლებლობის შესახებ. აგრეთვე, საქმეში მოიპოვებოდა საუბრის აუდიო და ვიდეო ჩანაწერები, სადაც ჩანდა, რომ ბრალდებული აქტიურად ითხოვდა ციანიდის მოპოვებაში დახმარებას.[96] შესაბამისად, საქმეზე შეკრებილმა ელექტრონულმა და სხვა სახის მტკიცებულებებმა ერთობლიობაში ხელი შეუწყეს მის მიმართ გამამტყუნებელი განაჩენის დადგენას.

განხილულმა საქმეებმა გვიჩვენა თუ რა მტკიცებულებითი ღირებულების მატარებელი შეიძლება იყოს ელექტრონული ინფორმაცია. ერთის მხრივ, დავინახეთ თუ რამდენად გადამწყვეტი როლი ითამაშა ელექტრონულმა მტკიცებულებებმა პირის მსჯავრდების პროცესში, მეორეს მხრივ კი ნათელი გახდა თუ რა შედეგამდე შეიძლება მიიყვანოს სასამართლო გამომძიებლების მიერ ელექტრონული ინფორმაციის მოსაპოვებლად არასწორად შერჩეულმა მეთოდმა ან საშუალებამ. ფილიპ ველშის მკვლელობისა და თამარ ბაჩალეიშვილის საქმემ კი კვლავ გვიჩვენა თუ რაოდენ მნიშვნელოვანი შეიძლება იყოს ელექტრონული ინფორმაცია არა მარტო სასამართლოს ან ნაფიც მსაჯულთა მიერ გადაწყვეტილების მიღების პროცესში, არამედ უშუალოდ გამოძიების სრულფასოვნად წარმართვის კუთხით.

3.1 კომპიუტერული მონაცემი, როგორც გამამართლებელი მტკიცებულება

სისხლის სამართლის პროცესში კომპიუტერული მონაცემის მტკიცებულებითი მნიშვნელობა დიდია. გარდა იმისა, რომ შესაძლოა მან გამოძიების სწორად წარმათვას ან სასამართლოს მიერ დასაბუთებული გადაწყვეტილების მიღებას შეუწყოს ხელი,

[95] *იხ.* პროკურატურის ოფიციალური განცხადება <https://pog.gov.ge/news/mTavari-prokuratura-braldebul-giorgi-mamalaZis-saqmeze-gamoZiebis-shualedur-shedegebs-asajaroebs> [24.05.2023]

[96] Mamaladze v. Georgia, N9487/19, [2023] ECHR.

შესაძლებელია იგი ბრალდებულისთვის გამამართლებელ მტკიცებულებას წარმოადგენდეს.

მოგეხსენებათ, საქართველოს სისხლის სამართლის საპროცესო კოდექსი არ იცნობს ალიბის ცნებას, თუმცა თუ იურიდიულ ლიტერატურას გადავხედავთ, ვნახავთ, რომ ალიბი განმარტებულია, როგორც „ფაქტი ან ცნობა დანაშაულის ჩადენის დროს პირის გარკვეულ ადგილას ყოფნის შესახებ“. [97] ალიბი ეს არის, ბრალდებულის უდანაშაულობის დასაბუთების ერთ-ერთი საშუალება, რომლის მიხედვითაც პირს არ შეეძლო მართლსაწინააღმდეგო და ბრალეული ქმედების ჩადენა, ვინაიდან დანაშაულის ჩადენის მომენტში იგი სხვაგან იმყოფებოდა.[98] შესაბამისად, დროსა და ადგილმდებარეობას გადამწყვეტი მნიშვნელობა აქვს ალიბზე საუბრისას.[99] დროისა და ადგილმდებარეობის შესახებ ზუსტი მონაცემების მიწოდებით ბრალდებულმა შესაძლოა მისი უდანაშაულობის დადასტურება შეძლოს [100] და მტკიცების პროცესში მას კომპიუტერულმა მონაცემმა ფასდაუდებელი სამსახური გაუწიოს.

როდესაც ციფრულ სამყაროში დროის შესახებ ვსაუბრობთ, მხედველობაში გვაქვს კომპიუტერული სისტემის მიერ დაფიქსირებული მონაცემები. კომპიუტერული სისტემის საათს გადამწყვეტი მნიშვნელობა აქვს მოვლენათა დათარიღებისა და თანმიმდევრულად დახარისხებაში. [101] ჩვენთვის კარგად ნაცნობი თანამედროვე მოწყობილობები ინახავენ ინფორმაციას მომხმარებელთა აქტივოვების შესახებ. მაგალითისთვის, მობილურ ტელეფონში შენახულია მონაცემები განხორციელებული ზარის დროისა და ხანგრძლივობის შესახებ. მოწყობილობაში დაფიქსირებული ზარის განხორციელების დრო კი მობილური ტელეფონის სისტემის დროის იდენტურია. მართალია, თანამედროვე მოწყობილობები ინტერნეტ სივრცესთან არის დაკავშირებული, რაც საშუალებას იძლევა კომპიუტერული სისტემის ადგილმდებარეობის მიხედვით განსაზღვროს ზუსტი დროის სარტყელი, თუმცა მისი

[97] *Dysart E. J., Strange D.*, Beliefs about alibis and alibi investigations: A Survey of Law Enforecement, Psychology, Crime & Law, Vol. 18, Issue 1, 2012, 11.

[98] Criminal Procedure and Investigations Act 1996, Part I, Section 6A(3).

[99] *Casey E.,* Digital Evidence and Computer Crime, 3rd edition, USA, Academic Press, 2011, 323.

[100] *Burchill J.,* Alibi Evidence: Responsibility for disclosure and investigation, Manitoba Law Journal, 2018, Vol. 41, Issue 3, 121.

[101] *Mason S., Weir R.S. G.,* The sources of electronic evidence, Electronic Evidence, Mason. S., Seng D., (eds.), 4th edition, London, 2017, 3.

შეცვლა მექანიკურადაც არის შესაძლებელი.[102] შესაბამისად, როდესაც გამოძიების ინტერესის სფეროს კომპიუტერულ სისტემაში დაფიქსირებული დროისა და ადგილმდებარეობის ნამდვილობის დადგენა წარმოადგენს, ამისთვის სათანადო კვლევის ჩატარებაა აუცილებელი.

საყურადღებოა, რომ კომპიუტერული სისტემის მიერ დაფიქსირებული დრო და ადგილმდებარეობა ხშირად გამხდარა ბრალდებულის ბრალეულობის უარყოფის საშუალება. ამ მხრივ საინტერესოა როდნი ბრედფორდის საქმე.[103] ცხრამეტი წლის ნიუორკელს ბრალად 2009 წლის 17 ოქტომბრის ღამეს ბრუკლინში მომხდარ ძარცვაში მონაწილეობა ედებოდა. თუმცა ბრალდებული ამტკიცებდა, რომ დანაშაულის ჩადენის დროს იგი ბრუკლინიდან მოშორებით ჰარლემში, მამამისის სახლში იყო. მის განცხადებას ადასტურებდნენ მამა და დედინაცვალი. ამასთან, დაცვის მხარემ მტკიცებულებად ბრუკლინში დანაშაულის ჩადენამდე რამდენიმე წუთით ადრე ბრალდებულის მიერ სოციალურ ქსელში გამოქვეყნებული განცხადება წარადგინა. აღნიშნული განცხადების ნამდვილობა დადასტურდა სოციალური ქსელის ადმინისტრაციის მიერ. აგრეთვე, დადასტურდა, რომ კომპიუტერული სისტემის მისამართი, საიდანაც განაცხადი გაკეთდა, ბრალდებულის მამის სახელზე იყო დარეგისტრირებული. ყოველივემ კი ერთობლიობაში, როდნი ბრედფორდის მიმართ ბრალდების უარყოფას დაუდო საფუძველი.

ელექტრონული ალიბის გამოყენების მხრივ არანაკლებ საინტერესოა ალბერტო სტაზის საქმე, რომლის მიხედვითაც მას მეგობარი გოგონას მკვლელობა ედებოდა ბრალად.[104] ბრალდებულმა გამოძიებას განუცხადა, რომ მკვლელობის დროს სახლში იმყოფებოდა და სადისერტაციო ნაშრომზე მუშაობდა. ამასთან, მან კუთვნილი კომპიუტერი გამოკვლევის მიზნით პოლიციას მკვლელობიდან მეორე დღესვე გადასცა, თუმცა ექსპერტებმა მისი გამოკვლევის დროს არსებითი შეცდომები დაუშვეს და ელექტრონული ინფორმაციის გარკვეული ნაწილი დააზიანეს. მიუხედავად ამგვარი დაუდევრობისა, კვლევის შედეგად დადგინდა, რომ დაზარალებულის მკვლელობის დროს ბრალდებულის საკუთრებაში არსებული

---

[102] *Casey E.,* Digital Evidence and Computer Crime, 3rd edition, USA, Academic Press, 2011, 324.

[103] *Hoffmeister A. T.,* Social Media in the Courtroom: A New Era for Criminal Justice?, USA, Praeger, 2014, 99-100.

[104] *Colombo E.*, The Garlasco case and the digital alibi evidence: A difficult relationship between law and informatics, Digital Evidence and Electronic Signature Law Review, vol. 14, 2017.

მოწყობილობა ჩართული იყო და იგი ნამდვილად მუშაობდა ნაშრომზე. ექსპერტების მიერ დაშვებული შეცდომების მიუხედავად, პირველი და მეორე ინსტანციის სასამართლოებმა კვლევის შედეგად დადგენილი ფაქტები სარწმუნოდ მიიჩნიეს და საქმეში არსებულ სხვა მტკიცებულებებთან ერთობლიობაში ალბერტო სტაზის მიმართ გამამართლებელი განაჩენი გამოიტანეს. განსხვავებული იყო უზენაესი სასამართლოს მიდგომა, რომელმაც შეცვალა ქვემდგომი სასამართლოს გადაწყვეტილება და ალბერტო სტაზი მეგობარი გოგონას მკვლელობის საქმეში დამნაშავედ ცნო. ძირითად არგუმენტს კი ქვემდგომი ინსტანციის სასამართლოების მიერ ელექტრონული მტკიცებულების სრულყოფილად შეუსწავლელობა წარმოადგენდა. კერძოდ, საკასაციო სასამართლოს შეხედულებით, ქვემდგომი ინსტანციის სასამართლოებმა ბრალდებულის კომპიუტერული სისტემიდან მოპოვებული მონაცემები ყოველმხრივ სრულყოფილად არ გამოიკვლის და ამასთან, არ გაითვალისწინეს გამოძიების პროცესში ექსპერტთა და გამომძიებელთა მიერ მოვალეობის შესრულებისას გამოჩენილი დაუდევრობა, რასაც შედეგად კომპიუტერული მონაცემის, შემდგომში კი ელექტრონული მტკიცებულების დაზიანება მოყვა. შესაბამისად, უზენაესმა სასამართლომ ელექტრონული მტკიცებულების ერთიანობა დარღვეულად, ხოლო მისი შინაარსი არასარწმუნოდ მიიჩნია.[105]

კომპიუტერული მონაცემი ალიბის დადასტურების ნაცვლად შესაძლოა მისი უარყოფის საშუალებაც იყოს. ამ მოსაზრების ნათელი მაგალითია ჯოუ რაილის საქმე. [106] მას მეუღლის მკვლელობა ედებოდა ბრალად, თუმცა სამართალდამცავ ორგანოებს განუცხადა, რომ მაშინ როდესაც მისი მეუღლე მოკლეს, სახლიდან რამდენიმე მილის დაშორებით იმყოფებოდა. ამ განცხადებით ბრალდებული ცდილობდა ალიბის შექმნას, თუმცა საავტომობილო გზებზე არსებული ვიდეო კამერებისა და ბრალდებულის მობილური ტელეფონის კვლევამ აჩვენა, რომ დანაშაულის ჩადენის დროს იგი სახლთან ახლოს იყო. შესაბამისად, გამოძიების შედეგად მოპოვებულმა კომპიუტერულმა მონაცემმა ბრალდებულის ალიბი უარყო

[105] იქვე, 35.
[106] DPP v. Joseph O'Reilly, The Court of Criminal Appeal, [2009] IECCA 18.

და საბოლოო ჯამში სხვა მტკიცებულებებთან ერთობლიობაში მის მიმართ გამამტყუნებელი განაჩენის დადგენის საფუძველიც გახდა.

მსგავსი მოცემულობის იყო საქართველოს უზენაესი სასამართლოს განსახილველი საქმე,[107] რომლის მიხედვითაც რ.შ-ს მსჯავრი უმწეო მდგომარეობაში მყოფი დ.ც-ის განზრახ მკვლელობასა და თავისუფლების უკანონო აღკვეთაში, სხვა დანაშაულის ჩადენის გაადვილების მიზნით დაედო, ასევე უმწეო მდგომარეობაში მყოფი პ.ქ-ას განზრახ მკვლელობასა და თავისუფლების უკანონო აღკვეთაში, ჩადენილი ორგანიზებული ჯგუფის მიერ. მსჯავრდებულის ადვოკატის განცხადებით მისი დაცვის ქვეშ მყოფი დანაშაულის ჩადენის დროს სხვა ქალაქში იმყოფებოდა. შესაბამისად, იგი ვერ შეძლებდა მისთვის ბრალად შერაცხული დანაშაულის ჩადენას. დაცვის მხარის მიერ წარმოდგენილი ვერსიისგან განსხვავებულ გარემოებებზე მიუთითებდა გამოძიების შედეგად მოპოვებული მონაცემები. კერძოდ, მსჯავრდებულის მობილური ტელეფონის სიმბარათებზე დაფიქსირებული შემავალი და გამავალი ზარების ნუსხა. საკომუნიკაციო ანძების კვლევით დადგინდა, რომ მსჯავრდებული არამარტო იმ ქალაქში იმყოფებოდა სადაც დანაშაულს ჰქონდა ადგილი, არამედ უშუალოდ დანაშაულის ადგილის სიახლოვეს. [108] შესაბამისად, საქართველოს უზენაესმა სასამართლომ არ გაიზიარა როგორც მსჯავრდებულის განცხადება ალიბის შესახებ, ისე იმ მოწმეთა ჩვენებები, რომლებიც მის ალიბს ადასტურებდნენ.

აღნიშნულ საქმეთა განხილვა კვლავ გვარწმუნებს, თუ რაოდენ ღირებული შეიძლება იყოს კომპიუტერული მონაცემი როგორც გამოძიების მიზნებისთვის, ისე სასამართლოს მიერ ჭეშმარიტების დადგენის კუთხით. თუმცა, როდესაც კომპიუტერულ მონაცემს ალიბის კუთხით განვიხილავთ, უნდა გავითვალისწინოთ, რომ იგი, როგორც დამოუკიდებელი მტკიცებულება ვერ იქნება უდანაშაულობის დასაბუთებისთვის საკმარისი, ვინაიდან დრო, ადგილმდებარეობა, IP მისამართი და სხვა მაიდენტიფიცირებლები დაკავშირებულია არა ინდივიდთან არამედ კომპიუტერულ მოწყობილობასთან. [109] შესაბამისად, აუცილებელია დამატებითი მტკიცებულებების არსებობა, რომლებიც მაგალითისთვის, დროის კონკრეტულ

[107] საქართველოს უზენაესი სასამართლოს 2018 წლის 18 სექტემბრის განაჩენი საქმეზე N138ა3-18.
[108] იქვე, II-17.
[109] *Casey E,* "Digital Evidence and Computer Crime", 3rd Edition, USA, Academic Press, 2011, 328.

მონაკვეთში მოწყობილობის კომუნიკაციისთვის ან სხვა აქტივობისთვის გამოყენებას დაადასტურებს. აღნიშნული ხელს შეუწყობს ალიბის დადასტურებას და გამორიცხავს ხელოვნურად მისი შექმნის მცდელობას.[110]

3.2. კომპიუტერული მონაცემის ავთენტურობა

იურიდიულ ლიტერატურაში კომპიუტერული მონაცემების მახასიათებლების მსგავსად, ელექტრონული დოკუმენტის ავთენტურობის საკითხზე მათი წერილობით დოკუმენტთან შედარების გზით მსჯელობენ.[111]

მეცნიერთა ერთი ნაწილის აზრით ელექტრონული დოკუმენტის ავთენტურობის დასადგენად მიზანშეწონილია წერილობითი დოკუმენტისთვის გათვალისწინებული ნორმების გამოყენება, [112] ხოლო მეორე ნაწილის ხედვით ელექტრონული დოკუმენტის მახასიათებლებიდან გამომდინარე აუცილებელია საკითხის ახლებურად გადაწყვეტა.[113]

მეცნიერთა შეხედულებებს შორის არსებული სხვაობის უკეთ გააზრებაში მიგვაჩნია თავად კომპიუტერული მონაცემის ავთენტურობასთან დაკავშირებული საკვანძო საკითხების ყურადღებით განხილვა და უცხოური საკანონმდებლო მიდგომების გაცნობა-წარმოჩენა დაგვეხმარება. ნიშანდობლივია, რომ ავთენტურობის მხრივ ამერიკის შეერთებული შტატებისა და კანადის კანონმდებლობა მსგავსია. [114] მათი კანონმდებლობით ავთენტურობის დადგენის საშუალებებს მოწმეთა ჩვენება, [115] არაპირდაპირი მტკიცებულება და ნებისმიერი ის მტკიცებულება მიეკუთვნება, რომელიც დოკუმენტის ან ინფორმაციის უტყუარობაზე მიგვითითებს. [116] ამასთან,

---

[110] იქვე.

[111] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 130.

[112] *Mason S.*, *Stanfield A.,* Authenticating electronic evidence, Mason S., Seng D., (eds.), 4th edition, London, 2017, 193.

[113]*Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017, 18.. *იხ. Johnson A.M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, vol. 75, 1992, 445.

[114] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 131.

[115] *R. v. Morgan,* [2002], N.J., 15 (NLPC). იხ. *R. v. Nichols*, [2004], No 6186, CarswellOnt 8225, (Ont. C.J.)

[116] Federal Rules of Evidence, USA, Rule 901(b)(1,4,9), As amended to December 1, 2019; იხ. Canada Evidence Act (RSC, 1985, c. C-5), Section 31.1-31.7.

მხარემ სასამართლოს ამომწურავად უნდა მიაწოდოს ინფორმაცია ჩანაწერის ბუნების, მისი წყაროსა და ერთიანობის შესახებ.[117]

ხაზი უნდა გაესვას იმ გარემოებას, რომ ელექტრონული დოკუმენტის წყარო ავთენტურობისა და სანდოობის დადგენის კუთხით გადამწყვეტ როლს თამაშობს.[118] იმის გათვალისწინებით, რომ როგორც თავად ელექტრუნული ინფორმაცია, ისე მისი შემნახველი საშუალებები ბუნებით არამყარია, მეტიც, დროთა განმავლობაში მათი შეცვლის ან დაზიანების საფრთე არსებობს,[119] მხარემ სასამართლო პირველ რიგში ელექტრონული მტკიცებულებისა და მისი წყაროს სანდოობაში უნდა დაარწმუნოს.[120] მონაცემთა წყაროსთან ერთად, განსაკუთრებული ყურადღება ენიჭება თავად ინფორმაციის მიღების ფორმას. მნიშვნელოვანია შეფასდეს ელექტრონული დოკუმენტი კომპიუტერული სისტემის ან პროგრამული უზრუნველყოფის ფუნქციონირების შედეგია თუ მისი ავტორი უშუალოდ მომხმარებელია. [121] გასათვალისწინებელია, აგრეთვე, სასამართლოში წარდგენილი ინფორმაციის უცვლელობის საკითხი, რომლის დადგენაც საგამოძიებო მოქმედების ამსახველი ოქმის მეშვეობით არის შესაძლებელი. კერძოდ, ოქმი დეტალურად უნდა ასახავდეს ინფორმაციას კომპიუტერული მონაცემის სახის, მოპოვების ფორმის, მეთოდების, დროის, იმ პირების შესახებ, რომელთაც წვდომა ჰქონდათ ამოღებულ მონაცემებზე.[122] შესაბამისად, დეტალური და თანმიმდევრული საგამოძიებო მოქმედების ოქმისა და საგამოძიებო მოქმედებაში მონაწილე პირების ჩვენებებით სრულებით შესაძლებელია ელექტრონული მტკიცებულების ერთიანობის დადგენა.[123]

ავთენტურობის თვალსაზრისით ყურადსაღებია უშუალოდ კომპიუტერული მოწყობილობის გამართულად ფუნქციონირების საკითხიც. თუმცა, ნიშანდობლივია, რომ მისი გამართულად ფუნქციონირება ვერ ჩაითვლება ელექტრონული ჩანაწერის

---

[117] *Gregory D.J,,* Authentication rules and electronic evidence, The Canadian Bar Review, vol.81(3), 2002, 531.

[118] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 131.

[119] *Gregory D.J,,* Authentication rules and electronic evidence, The Canadian Bar Review, vol.81(3), 2002, 537.

[120] *Capra D.,* Authenticating Digital Evidence, Baylor Law Review, vol.69(1), 2017, 3.

[121] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 131.

[122] *Gonzales R. A., Schofield B. R., Hagy W. D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 28.

[123] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 132.

უტყუარობის გარანტად.[124] ისევე, როგორც შესაძლებელია კომპიუტერული სისტემის გაუმართავად ფუნქციონირებამ ზეგავლენა ვერ იქონიოს სისხლის სამართლის საქმისთვის მნიშვნელოვანი დოკუმენტის სანდოობაზე. შესაბისად, აუცილებელია საქმეში მოიპოვებოდეს მტკიცებულება, რომელიც გამორიცხავს კომპიუტერული სისტემის ფუნქციონირების ზეგავლენას ელექტრონული ჩანაწერის ნამდვილობაზე.[125]

ავთენტურობაზე საუბრისას ასევე საყურადღებოა ბეჭდური სახით არსებული ელექტრონული დოკუმენტის ნამდვილობის საკითხი. მით უფრო, რომ ავთენტურობის დადგენის თვალსაზრისით შესაძლოა დამატებით სირთულეებს წავაწყდეთ არაოფიციალური დოკუმენტის შემთხვევაში, ვინაიდან ოფიციალური დოკუმენტისგან განსხვავებით მისი ნამდვილობის დადგენა რეკვიზიტების მიხედვით შეუძლებელია.[126] ასეთ შემთხვევაში ბეჭდური დოკუმენტის (რომელსაც არ გააჩნია კონკრეტული მაიდენტიფიცირებელი ნიშნები), უტყუარობისა და დედანთან შესაბამისობის დასამტკიცებლად, ავტორის ჩვენებასთან ერთად საჭიროა გამოვიყენოთ ექსპერტიზის დასკვნა, რომელიც კომპიუტერული მოწყობილობის გამართულად ფუნქციონირებასა და ინფორმაციის დედანთან შესაბამისობას დაადასტურებს.[127]

თუ საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობით დოკუმენტის ავთენტურობასთან დაკავშირებულ ნორმატიულ საფუძვლებს გადავხედავთ, დავრწმუნდებით, რომ უშუალოდ დოკუმენტის ავთენტურობასთან დაკავშირებული ნორმები კანონმდებლობით გათვალისწინებული არ არის, თუმცა განსაზღვრულია დოკუმენტის მტკიცებულებითი ძალისა და დასაშვებობის კუმულაციური წინაპირობები. [128] კერძოდ, თუ ცნობილია დოკუმენტის წარმომავლობა და ის ავთენტიკურია, მას სისხლის სამართლის პროცესის მიზნებისთვის მტკიცებულებითი

---

[124] *Johnson A.M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, vol. 75, 1992, 443-444.

[125] *Gonzales R.A., Schofield B.R., Hagy W.D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007, 44.

[126] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 133.

[127] იქვე.

[128] *ავტორთა კოლექტივი,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბილისი, ამერიკის იურისტთა ასოციაცია, 2015, 275.

ძალა გააჩნია. აგრეთვე, თუ მხარეს შეუძლია მოწმედ დაკითხოს პირი, რომელმაც მოიპოვა/შექმნა ან/და რომელთანაც სასამართლოსთვის წარდგენამდე ინახებოდა დოკუმენტი, ის სისხლის სამართლის საქმეზე დასაშვებ მტკიცებულებად მიიჩნევა. (სსსკ-ის 78-ე მუხლის 1-ლი ნაწილი).

საყურადღებოა, რომ დოკუმენტის წარმომავლობას არა მარტო მტკიცებულებითი ძალის განსაზღვრისთვის, არამედ მისი ავთენტურობის დადგენისთვისაც განსაკუთრებული მნიშვნელობა ენიჭება, ვინაიდან წარმომავლობის გამოკვლევით ცნობილი ხდება მისი შედგენის დრო, ადგილი, ავტორი და სხვა. [129] გასათვალისწინებელია ისიც, რომ დოკუმენტთან უშუალო კავშირში მყოფი პირების მიერ მოწოდებული ინფორმაციის გარდა, მისი ნამდვილობის დადგენა სხვა ხერხითაც არის შესაძლებელი. თუმცა, მათი ამომწურავი ჩამონათვალის მოტანა პრაქტიკულად შეუძლებელია.[130]

დასკვნის სახით კი შეიძლება ითქვას, რომ მიუხედავად განსხვავებული სამართლებრივი სისტემებისა, მსგავსება დოკუმენტის ავთენტურობის დადგენის საშუალებებს შორის მართლაც დიდია. [131] ცხადია დოკუმენტის ნამდვილობის განსაზღვრისას უპირატესობა ძირითადად მოწმის ჩვენებას, ექსპერტიზის დასკვნასა და სხვა პირდაპირ თუ არაპირდაპირ მტკიცებულებებს ენიჭება. ამასთან, კომპიუტერული მონაცემისთვის დამახასიათებელი ნიშან-თვისებებისა და მის ერთიანობაზე მოქმედი გარემოებებების მხედველობაში მიღებით, შესაძლებელია წერილობითი დოკუმენტის ავთენტურობის დასადგენად მოქმედი ნორმები წარმატებით იქნას გამოყენებული ელექტრონულ დოკუმენტებთან მიმართებაშიც.[132]

4. შეჯამება

არსებული რეალობის გათვალისწინებით კომპიუტერული მონაცემი გამოძიების განუყოფელ ნაწილს წარმოადგენს, [133] თუმცა მისთვის დამახასიათებელი სპეციფიკური თუ ტექნიკური ნიშან-თვისებებიდან გამომდინარე მისი

[129] იქვე, 276.
[130] იქვე, 277.
[131] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 134.
[132] იქვე.
[133] *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006, 1.

შინაარსობრივი მხარის ზუსტი გაგება საზოგადოებასთან ერთად იურისტებისთვისაც სირთულეს წარმოადგენს. შესაბამისად, აღნიშნულ თავში ყურადღება კომპიუტერული სისტემისა და მონაცემის არსის, მახასიათებელი ნიშნების, მტკიცებულებითი ძალისა და მის ავთენტურობასთან დაკავშირებული საკითხების კვლევას დაეთმო.

სამეცნიერო ლიტერატურის, საერთაშორისო ორგანიზაციების გამოცდილების შესწავლამ და შედარებითსამართლებრივმა ანალიზმა ცხადყო, რომ მიუხედავად კომპიუტერული მონაცემისა და ელექტრონული მტკიცებულების ფართო შინაარსისა, მათი დეფინიცია მეტნაკლებად ერთიანია და შესაძლოა ისინი შემდეგნაირად ჩამოყალიბდეს - „კომპიუტერული მონაცემი, ეს მომხმარებლის მიერ კომპიუტერულ სისტემაში შეყვანილი, ხოლო შემდგომ კომპიუტერული მოწყობილობის მიერ ავტომატურად დამუშავებული, შენახული ან გადაცემული ნებისმიერი სახის ინფორმაციაა“. რაც შეეხება ელექტრონულ მტკიცებულებას, აღნიშნული, „კომპიუტერულ სისტემაში არსებული კომპიუტერული მონაცემია, რომელიც ღირებულია გამოძიებისთვის ან პროცესის მონაწილე მხარისათვის, სასამართლოში მნიშვნელოვანი გარემოებების დასადასტურებლად“.[134]

კომპიუტერული მონაცემების მახასიათებლების კვლევამ ელექტრონულ და მატერიალურ მტკიცებულებებს შორის არსებული განსხვავება მკაფიოდ წარმოაჩინა და დაგვანახა, რომ საპროცესო კანონმდებლობაში, უშუალოდ ელექტრონული მტკიცებულების მოპოვებასთან დაკავშირებული საპროცესო ინსტრუმენტების არსებობა აუცილებელია. ასეთად შესაძლოა კომპიუტერული მონაცემის დინამიურობისა და ცვალებადი ბუნების საპასუხოდ „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული საგამოძიებო მოქმედებების, „მონაცემთა დაჩქარებული დაცვის ბრძანება“ ან თუნდაც, „კომპიუტერული მონაცემის გადაცემის ბრძანება“ მივიჩნიოთ.

კომპიუტერული მონაცემის მახასიათებლები [135] აგრეთვე, მნიშვნელოვან როლს თამაშობენ უშუალოდ მისი ავთენტურობის დადგენის პროცესშიც, თუმცა მასთან ერთად საყურადღებოა თავად ინფორმაციის მიღების ფორმის საკითხიც. კერძოდ,

---

[134] *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021, 122.

[135] იქვე, 128.

მნიშვნელოვანია დადგინდეს ელექტრონული დოკუმენტი უშუალოდ კომპიუტერული სისტემის ან პროგრამის ფუნქციონირების შედეგია თუ ინფორმაცია კომპიუტერულ სისტემაში მომხმარებელმა განათავსა. ასევე, ყურადსაღებია ბეჭდური სახით წარდგენილი ელექტრონული მონაცემის ნამდვილობის საკითხიც. უმეტესწილად, სირთულეს ბეჭდური სახით არსებული არაოფიციალური დოკუმენტის ავთენტურობის დადგენა წარმოადგენს, ვინაიდან ოფიციალური დოკუმენტისგან განსხვავებით მას რეკვიზიტები არ გააჩნია და მისი ნამდვილობის განსაზღვრა შედარებით მეტ ძალისხმევას მოითხოვს. მაგალითისთვის, მხარეს, მისი სასამართლოში წარდგენის შემთხვევაში, მისი უტყუარობისა და დედანთან შესაბამისობის წარმოსაჩენად, შესაძლოა ექსპერტიზის დასკვნის წარდგენაც კი დასჭირდეს, რომელიც სასამართლოს ინფორმაციის წყაროს, შემქმნელი მოწყობილობის გამართულობისა და დედანთან, ელექტრონული ფორმით არსებულ ინფორმაციასთან შესაბამისობას დაუდასტურებს. თუმცა, საკითხის სირთულის მიუხედავად უნდა აღინიშნოს, რომ კომპიუტერული მონაცემის ნამდვილობის დასადასტურებლად ტრადიციული მტკიცებულების ავთენტურობის დადგენისთვის გათვალისწინებული ნორმების გამოყენება სავსებით მიზანშეწონილია.[136]

გარდა ზემოთხსენებულისა, მოცემულ თავზე მუშაობის პროცესში შესწავლილმა სისხლის სამართლის საქმეებმა ნათლად დაგვანახა თუ თანამედროვე სამყაროში რაოდენ მჭიდრო კავშირი არსებობს ნებისმიერი სახის დანაშაულსა და ტექნოლოგიებს შორის.[137] აღნიშნულმა კი კიდევ ერთხელ გაუსვა ხაზი გამოძიებისა და სასამართლო განხილვის პროცესში ელექტრონული მტკიცებულების მნიშვნელობას.

[136] იქვე, 131-133.

[137] *Casey E.*, Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, Academic Press, 2011, 3.

თავი II. კომპიუტერული მონაცემის გამოთხოვის საერთაშორისო სამართლებრივი საფუძველი

1. კომპიუტერული დანაშაულის შესახებ 2001 წლის 23 ნოემბრის (ბუდაპეშტის) კონვენცია

კომპიუტერულ-ტექნოლოგიურმა რევოლუციამ ახალ, სასიკეთო შესაძლებლობებთან ერთად დანაშაულის ჩადენის განსხვავებულ ფორმასაც დაუდო საფუძველი. ტრანსნაციონალური ხასიათიდან გამომდინარე, იგი თანამედროვე მსოფლიოს გამოწვევად იქცა და სახელმწიფოები ევროპის საბჭოს მიერ შემუშავებული „კიბერდანაშაულის შესახებ“ კონვენციის გარშემო გააერთიანა. გამონაკლისი არც საქართველო ყოფილა.[138] ევროპის საბჭოს კონვენცია, რომელიც ევროპის საბჭოს ექსპერტებისა და სხვა არაწევრი სახელმწიფოების ოთხწლიანი შრომის შედეგია,[139] 2001 წლის 8 ნოემბერს იქნა მიღებული, ხოლო ამავე წლის 23 ნოემბერს, ხელმოსაწერად ქალაქ ბუდაპეშტში გაიხსნა და ძალაში 2004 წლის პირველ ივლისს შევიდა.[140] კონვენცია საქართველოსთვის განსაკუთრებით მნიშვნელოვანი მას შემდეგ გახდა, რაც 2009 წლის პირველი ივნისიდან 2010 წლის 31 მაისამდე, ევროსაბჭოს ორგანიზებით საქართველოში „კიბერდანაშაულის პროექტი საქართველოში“ განხორციელდა. მის ფარგლებში მომზადდა საკანონმდებლო ცვლილებათა პროექტი, რომელმაც მოგვიანებით საქართველოს სისხლის სამართლისა და საპროცესო კოდექსში პოვა ასახვა.[141]

უშუალოდ, კონვენციის მიზანს სისხლის სამართლის საერთო პოლიტიკის შემუშავება და დამკვიდრება წარმოადგენს, რომელიც კომპიუტერული დანაშაულისგან საზოგადოების დაცვისკენ იქნება მიმართული. აღნიშნული კი, მხოლოდ სწრაფი და ეფექტური საერთაშორისო თანამშრომლობით, საკანონმდებლო ბაზის დახვეწითა და

---

[138] საყურადღებოა, რომ 2012 წლის 1 ივნისს საქართველოს პრეზიდენტის N450 ბრძანებულებით დამტკიცდა „კიბერდანაშაულის შესახებ“ 2001 წლის კონვენცია, რაც საქართველოს ეროვნული კანონმდებლობის კონვენციასთან შესაბამისობაში მოყვანის ვალდებულებას გულისხმობს.

[139] 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, 6. < https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [27.05.2023].

[140] *კვათუაშვილი ე.,* კიბერდანაშაული და კიბერუსაფრთხოების პრობლემატიკა, ჟურნალი „მართლმსაჯულება და კანონი“ N1, 2013, 126.

[141] *იხ.* ოფიციალური განცხადება <https://www.coe.int/en/web/cybercrime/cybercrime-project-georgia >[27.05.2023].

ჰარმონიზაციით მიიღწევა.[142] სწორედ ამ სულისკვეთებით, სსსკ-ში ცალკე თავით განისაზღვრა კომპიუტერული მონაცემის მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებები.

სამი ძირითადი საკითხის გამოყოფაა შესაძლებელი კონვენციიდან. კერძოდ, დოკუმენტი ყურადღებას სისხლის სამართლის მატერიალურ კანონმდებლობაზე ამახვილებს, განსაზღვრავს ელექტრონული მტკიცებულების შეგროვების პროცედურულ მექანიზმებსა და საერთაშორისო თანამშრომლობისთვის აუცილებელ დებულებებს. მატერიალურ სამართლებრივი კუთხით, უშუალოდ კონვენციასთან ერთად მნიშვნელოვანია მისი დამატებითი ოქმი „კომპიუტერული სისტემის მეშვეობით ჩადენილი რასისტული და ქსენოფობიური ხასიათის ქმედებათა კრიმინალიზაციის შესახებ“, [143] ხოლო საერთაშორისო თანამშრომლობის თვალსაზრისით კონვენციის მეორე დამატებითი ოქმი „გაძლიერებული ურთიერთანამშრომლობისა და ელექტრონულ მტკიცებულებათა გადაცემის შესახებ“. საყურადღებოა აგრეთვე ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის საკითხი. ელექტრონული მტკიცებულების შეგროვებასთან დაკავშირებული საგამოძიებო მოქმედებები, იძულებით ღონისძიებებს განეკუთვნებიან. [144] შესაბამისად, აუცილებელია გამოირიცხოს სახელმწიფოს შესაძლებლობა თვითნებურად ჩაერიოს ძირითად უფლებებში. ამ მიზნით კონვენცია, ხელშემკვრელ მხარეებს ეროვნულ კანონმდებლობაში სათანადო გარანტიების გათვალისწინებისკენ მოუწოდებს. თუმცა, მსოფლიოში მოქმედი განსხვავებული სამართლებრივი სისტემების ფონზე,[145] კონკრეტული პირობებისა და გარანტიების შეთავაზებისგან თავს იკავებს და სანაცვლოდ, ზოგადი შინაარსის ნორმით, ძირითადი უფლებების საერთაშორისო სტანდარტით დაცვის ვალდებულებას აკისრებს.[146] საერთაშორისო სტანდარტი კი იურიდიული საზოგადოებისათვის კარგად ნაცნობ, ადამიანის უფლებების დაცვის კუთხით არსებულ დოკუმენტებს და ამ დოკუმენტების

[142] Convention on Cybercrime, Budapest, 23.11.2001.

[143] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), Strasbourg, 28/01/2003 < https://rm.coe.int/168008160f> [27.05.2023].

[144] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 54.

[145] მოსამართლეთა ტრენინგი ქსელურ დანაშაულში, ევროპის საბჭო, 2010, 88 <https://rm.coe.int/16802fa3c1> [28.05.23].

[146] Convention on Cybercrime, Budapest, 23.11.2001, Art. 15.

საფუძველზე ნაკისრ ვალდებულებებს აერთიანებს. ეს შეიძლება იყოს, როგორც 1950 წლის ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია და ამავე დოკუმენტის საფუძველზე შექმნილი სასამართლოს გადაწყვეტილებები, საერთაშორისო პაქტი სამოქალაქო და პოლიტიკურ უფლებათა შესახებ და სხვა. მოთხოვნის ფარგლებში სამართალწარმოების პროცესში უშუალოდ ჩართულ პირებთან ერთად, მესამე მხარეთა, მომსახურების მიმწოდებელთა უფლებებისა და კანონიერი ინტერესების დაცვის საკითხიც ექცევა,[147] რაც სახელმწიფოს პოზიტიური ვალდებულების ნაწილია.

დღეისათვის, „კიბერდანაშაულის შესახებ“ კონვენცია ერთადერთი სავალდებულო ძალის მქონე საერთაშორისო დოკუმენტია, რომელიც ერთგვარ სახელმძღვანელოსა და ორიენტირს წარმოადგენს კიბერდანაშაულის წინააღმდეგ ეროვნული კანონმდებლობისა და საერთო სისხლის სამართლის პოლიტიკის შემუშავებისთვის.[148] მისი აქტუალობა კი ტექნოლოგიურად ნეიტრალური მიდგომისა და თანამედროვე გამოწვევებისადმი მუდმივი ადაპტირების დამსახურებაა. იგი ადგენს კომპიუტერული სისტემის წინააღმდეგ ან მათი მეშვეობით განხორციელებული ქმედების კრიმინალიზაციის ვალდებულებას, ითვალისწინებს ელექტრონული მტკიცებულების მოპოვებისთვის აუცილებელ საგამოძიებო მოქმედებებს და განსაზღვრავს საერთაშორისო თანამშრომლობის წინაპირობებს.

2. მონაცემთა ტიპები და ტერმინთა განმარტება

„კიბერდანაშაულის შესახებ“ კონვენცია ერთმანეთისგან რამდენიმე ტიპის მონაცემს განასხვავებს, რომლებიც შესაძლოა დანაშაულის გამოძიებისა და საქმის სასამართლოში განხილვის დროს ელექტრონულ მტკიცებულად იყოს გამოყენებული. ამგვარ მონაცემებს მომხმარებლის შესახებ ინფორმაცია, შინაარსობრივი და ტრაფიკის შესახებ მონაცემები განეკუთვნება. თუმცა, მათ განმარტებასთან ერთად მნიშვნელოვანია სხვა ისეთი ტერმინების მნიშვნელობის ცოდნა, როგორებიცაა „მფლობელობა ან ზედამხედველობა“ და „მომსახურების მიმწოდებელი“.

---

[147] იქვე.

[148] 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, 6. < https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [28.05.2023].

უდაოა, რომ საგამოძიებო მოქმედებისთვის და კონვენციის მიზნებისთვის ზემოხსენებულ სიტყვებს განსაკუთრებული დატვირთვა აქვს და შესაბამისად მათი შინაარსობრივი მხარის ზუსტი გაგება არსებითია პრაქტიკული გამოყენებისათვის. განვიხილოთ თითოეული მათგანი. ტერმინ **„მომსახურების მიმწოდებლის“** განმარტებას კონვენციის პირველ მუხლში ვხვდებით და ის პირთა ფართო წრეს აერთიანებს. მასში მოიაზრებიან, როგორც კერძო და საჯარო სამართლის პირები, რომლებიც მომხმარებლებს კომპიუტერული სისტემის გამოყენებით ურთიერთობის შესაძლებლობით უზრუნველყოფენ, აგრეთვე, ის პირები, რომლებიც მომსახურების ან მომხმარებელთა სახელით კომპიუტერულ მონაცემს ამუშავებენ ან ინახავენ.[149] მნიშვნელობა არ ენიჭება სერვისი ხელმისაწვდომია ყველასთვის თუ მხოლოდ შეზღუდულ პირთა წრისათვის, ფასიანია თუ უფასო. მეტიც, სერვისის მომწოდებელთა ცნებაში ექცევა დახურული საკომუნიკაციო ქსელიც, როდესაც ორგანიზაციის თანამშრომლები ერთმანეთთან კორპორატიული ქსელის გამოყენებით ამყარებენ კომუნიკაციას.[150]

რაც შეეხება **მომხმარებლის შესახებ ინფორმაციას**, კიბერდანაშაულის შესახებ კონვენციის მე-18 მუხლის მე-3 ნაწილის მიხედვით იგი, 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 შესახებ ინფორმაციის, დამონტაჟებული საკომუნიკაციო აღჭურვილობის ადგილმდებარეობისა და სხვა ინფორმაციის დადგენა.[151] ფაქტია, რომ მომხმარებლის შესახებ ინფორმაცია მხოლოდ და მხოლოდ კომუნიკაციით არ არის შეზღუდული. მასში მოიაზრება, როგორც პიროვნების ვინაობა და მისი გეოგრაფიული ადგილმდებარეობა, აგრეთვე ინფორმაცია გადასახადებისა და იმ ინფორმაციის შესახებ, რომელსაც მომხმარებელსა და სერვისის

[149] Convention on Cybercrime, Budapest, 23.11.2001.
[150] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 5.
[151] Convention on Cybercrime, Budapest, 23.11.2001.

მომწოდებელს შორის დადებული ხელშეკრულება ითვალისწინებს. [152] თუმცა, პროვაიდერთა მხრიდან მომხმარებლის შესახებ ამგვარი ინფორმაციის გაცემის სავალდებულობა თავისთავად არ გულისხმობს ამავე ტიპის ინფორმაციის შეგროვებისა და შენახვის ვალდებულებას, არც პასუხისმგებლობას მის სიზუსტეზე.[153] **ტრაფიკის მონაცემი,** კონვენციის მიზნებისთვის, 1-ლი მუხლის „დ“ ქვეპუნქტის მიხედვით განიმარტება, როგორც „კომუნიკაციებთან დაკავშირებული და კომპიუტერული სისტემის მიერ გენერირებული ნებისმიერი კომპიუტერული მონაცემი, რომელიც კომუნიკაციათა ჯაჭვის ნაწილია, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს“. [154] უფრო დეტალურად, **კომუნიკაციის წყარო** მოიცავს ტელეფონის ნომერს, IP მისამართს და ნებისმიერი სხვა მოწყობილობის მაიდენტიფიცირებელ მონაცემს, რომელთან დაკავშირებითაც ე.წ. პროვაიდერი სთავაზობს სერვისს მომხმარებელს. **დანიშნულების ადგილი** - იმ მოწყობილობაზე და მაიდენტიფიცირებელ მონაცემებზე მიგვანიშნებს, რომელთანაც მყარდება კომუნიკაცია. ხოლო **მომსახურების ტიპი** უშუალოდ გამოყენებულ სერვისზე მიუთითებს. ნიშანდობლივია, რომ კონვენცია ეროვნულ საკანონმდებლო ორგანოებს ტრაფიკის მონაცემის დიფერენცირებისა და მათი სენსიტიურობის გათვალისწინებით განსხვავებული სამართლებრივი მოწესრიგების შესაძლებლობას უტოვებს.[155]

რაც შეეხება, **შინაარსობრივი მონაცემის** ცნებას, მას, კონვენცია არ განმარტავს, თუმცა თავად ტერმინიდანაც კი ნათელია, რომ უშუალოდ კომპიუტერული სისტემით გადაცემული კომუნიკაციის, შეტყობინების, ინფორმაციის შინაარსთან გვაქვს საქმე.[156] როგორიცაა, ელექტრონული ფოსტა, ხმოვანი შეტყობინება, აუდიო-ვიდეო მასალა, ფოტოსურათი და სხვა.

ელექტრონული მტკიცებულების **„მფლობელობას ან ზედამხედველობას“** განსაკუთრებული დატვირთვა კონვენციის მე-18 მუხლის „კომპიუტერული

[152] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 30-31.
[153] იქვე, 31.
[154] Understanding Cybercrime: Phenomena, challenges and legal response, 2012, 177. <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> [28.05.2023].
[155] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 6.
[156] იქვე, 40.

მონაცემის წარმოდგენის ბრძანებისთვის“ აქვს. განხილვისას შეიძლება გამოიყოს ორი მოცემულობა. ერთი, როდესაც ელექტრონული მონაცემის წარმოდგენის ბრძანების ადრესატი ზოგადად ფიზიკური ან იურიდიული პირია, ხოლო მეორე შემთხვევაში, სპეციალური სუბიექტი - მომსახურების მომწოდებელი. თითოეული ადრესატის შემთხვევაში იგულისხმება კომპიუტერული სისტემის, მონაცემის ან შემნახველი მოწყობილობის როგორც ფიზიკური ფლობა, ისე მოცემულობა, როდესაც პირი ინფორმაციას საკუთარი ანგარიშით ქვეყნის ფარგლებს გარეთ, ვირტუალურ სერვერზე ინახავს და მასზე სრული კონტროლი გააჩნია.[157] პროვაიდერების მხრიდან გავრცელებული მიდგომაა, როდესაც მათი კომპანია რეგისტრირებულია ერთ ქვეყანაში, ინფრასტრუქტურა განთავსებული აქვთ სხვა ქვეყანაში, ხოლო თავად მომსახურების მიწოდებას სხვა იურისდიქციაში ახორციელებენ.[158] შედეგად, ხშირია შემთხვევა, როდესაც ინფორმაცია ქვეყნის ფარგლებს გარეთ ონლაინ საცავშია მოთავსებული. თუმცა, ელექტრონული ინფორმაციის ქვეყნის ფარგლებს გარეთ განთავსება არ გამორიცხავს სამართალდამცავი უწყების წარმომადგენელთა მხრიდან ინფორმაციის მოთხოვნის უფლებას, ხოლო მომსახურების მომწოდებლის მიერ მოთხოვნილი ინფორმაციის მათთვის გადაცემის ვალდებულებას. მთავარია, ბრძანების ადრესატი მომსახურებას, მომთხოვნი სახელმწიფოს ტერიტორიაზე ახორციელებდეს. დაზუსტებას საჭიროებს თუ რა განიხილება სახელმწიფოს ტერიტორიაზე მომსახურების გაწევად. მართალია, შეფასების მხრივ, ღრუბლოვანი სერვისების განვითარებამ და ინფორმაციის ვირტუალურ სერვერზე განთავსების შესაძლებლობამ კითხვის ნიშნები დაბადა, თუმცა მომსახურების გაწევად ფასდება, როდესაც პროვაიდერი კომპანია ქვეყნის ტერიტორიაზე მყოფ ადამიანებს საკუთარი სერვისით სარგებლობის შესაძლებლობას აძლევს, ადგილობრივ ენაზე ეწევა სარეკლამო საქმიანობას, საკუთარი საქმიანობის მიზნებისთვის ამუშავებს მომხმარებელთა მონაცემებს, კავშირს ამყარებს მათთან და ა.შ.[159] შესაბამისად, ამგვარ მოცემულობაში პირი ან ორგანიზაცია, რომლის მიმართაც გაცემულია ბრძანება

[157] იქვე, 29.

[158] Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime: Towards Common Guidelines, Council of Europe, 2020, 5. < https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [01.06. 2023].

[159] Production Orders for Subscriber Information (Article 18 Budapest Convention), Cybercrime Convention Committee (T-CY), Council of Europe, 2017, 8.

ინფორმაციის გადაცემასთან დაკავშირებით, ვალდებულია ითანამშრომლოს და ინფორმაცია მიაწოდოს საგამოძიებო უწყებებს.

ცხადია, რომ თითოეული ტერმინი სპეციფიური და ამავდროულად, ფართო შინაარსის მატარებელია. მათ სიღრმისეულ და თანმიმდევრულ გააზრებას, გადამწყვეტი მნიშვნელობა აქვს როგორც კონვენციით გათვალისწინებული საგამოძიებო მოქმედებების პრაქტიკული გამოყენებისათვის, ისე მონაცემთა სენსიტიურობის გათვალისწინებით, ძირითად უფლებათა თვითნებური შეზღუდვისგან დამცავი სათანადო პროცესუალური გარანტიების შემუშავებისთვის.

3. პროცედურული მექანიზმები

3.1 შენახული კომპიუტერული მონაცემის დაჩქარებული დაცვა

კომპიუტერული მონაცემის დაჩქარებული დაცვა „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებულ იმ საგამოძიებო მოქმედებათა რიგს მიეკუთვნება, რომლებიც საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში დამოუკიდებელი სახით ჯერ იმპლემენტირებული არ არის.

საგამოძიებო მოქმედების მიზანი მარტივი და ამავდროულად, გამოძიებისთვის მეტად ეფექტურია. არსებობს შემთხვევები, როდესაც მონაცემთა დაცვის შესახებ კანონმდებლობა, სერვის პროვაიდერებს გარკვეული სახის ინფორმაციის დაუყოვნებლივ ან გარკვეული პერიოდის გასვლის შემდეგ მათ განადგურებას ავალდებულებს, ან თუნდაც შესაძლოა, აღარ არსებობს მონაცემთა დამუშავებისა და შენახვის კანონით გათვალისწინებული საფუძველი[160] და მონაცემთა მფლობელი მის განადგურებას გეგმავს. ასეთ ვითარებაში შესაძლოა ინფორმაციას განსაკუთრებული მნიშვნელობა ჰქონდეს გამოძიების მიზნებისთვის. შესაბამისად, მონაცემთა დაჩქარებული დაცვის ბრძანების საფუძველზე, მონაცემთა კანონიერი მფლობელი ან/და ზედამხედველი ვალდებულია ინფორმაცია დაუზიანებლად და სახეუცვლელად მაქსიმუმ 90 დღის განმავლობაში შეინახოს.[161] აღსანიშნავია, რომ დასაშვებია, ბრძანების შემდგომი განახლება და ვადის გახანგრძლივებაც.[162]

[160] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 25.
[161] იქვე, 27.
[162] იქვე.

ვინაიდან, მონაცემთა დაჩქარებულად დაცვის ბრძანების გაცემას წინ „ინფორმაციის დაკარგვის ან შეცვლის საფუძვლიანი საფრთხე“ უნდა უძღოდეს, ზოგადი მითითება ელექტრონული ინფორმაციის ცვალებად ბუნებაზე, არასაკმარისია.[163] დასაბუთებისას, დეტალურად უნდა განისაზღვროს მოსალოდნელი საფრთხე, რაც შეიძლება მონაცემთა დაცვის ეროვნული კანონმდებლობითა და ინფორმაციის გარკვეული პერიოდიულობით განადგურების ვალდებულებით დასაბუთდეს.[164] ბრძანებით გათვალისწინებულ უნდა იქნას საგამოძიებო მოქმედების კონფიდენციალურად შენახვის ვალდებულება და მისი ხანგრძლივობა.

საყურადღებოა, რომ საგამოძიებო ორგანოთა უფლებამოსილება, დაჩქარებული წესით მოითხოვონ მონაცემთა დაცვა და ამასთან, სავალდებულო მითითება გასცენ მონაცემთა მფლობელთა მიმართ კონფიდენციალურად შეინახონ აღნიშნული საკითხი, ისე არ უნდა იქნას გაგებული თითქოს მათ უფლება აქვთ „უსაფრთხოდ დაცულ“ ინფორმაციაზე წვდომის. მასზე წვდომისთვის აუცილებელია დამატებითი სამართლებრივი საფუძველი და დამოუკიდებელი საგამოძიებო მოქმედების ჩატარება, რაც შეიძლება დოკუმენტის ან ინფორმაციის გამოთხოვა, დათვალიერება, ჩხრეკა ან ამოღებაც კი იყოს.[165]

კონვენციის მე-16 მუხლით გათვალისწინებული „შენახულ კომპიუტერულ მონაცემთა დაჩქარებული დაცვის“ საგამოძიებო მოქმედება ადრესატებს ორმაგ ვალდებულებას აკისრებს. ერთი, უსაფრთხოდ შეინახონ ბრძანებით განსაზღვრული ინფორმაცია და მეორე, დაიცვან პირის მიმართ გამოყენებული პროცედურის კონფიდენციალურობა.

მიუხედავად იმისა, რომ მონაცემთა დაჩქარებულ დაცვას გარკვეული დროის მანძილზე მაინც ფარულობა ახასიათებს, იგი ყველაზე მსუბუქ საგამოძიებო ღონისძიებად ითვლება, ვინაიდან მონაცემთა დაცვის ბრძანების გაცემა სრულებით არ გულისხმობს ინფორმაციის შემდგომ გაცნობას.[166] ხოლო, თუ დაცული ინფორმაცია ღირებულია გამოძიებისთვის, მასზე წვდომა ახალი საფუძვლითა და

---

[163] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 107.

[164] იქვე.

[165] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 26.

[166] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 49. <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [02.06.23].

დამოუკიდებელი საგამოძიებო მოქმედების შედეგად მოხდება. შესაბამისად, ეროვნული კანონმდებლობით, მის ალტერნატიულ მექანიზმად სსსკ-ის 136-ე მუხლის გამოყენებამ შესაძლოა ადამიანთა პირად ცხოვრებაში მეტი დოზით ჩარევა გამოიწვიოს. ამრიგად, დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების მსგავსად მისი ეროვნულ კანონმდებლობაში გათვალისწინება მნიშვნელოვნად შეუწყობს ხელს როგორც ინდივიდთა ძირითადი უფლებების დაცვას, ისე გამოძიებისთვის შესაძლო მნიშვნელობის ინფორმაციის უსაფრთხოდ შენახვას.

3.2. ინტერნეტტრაფიკის დაჩქარებული დაცვა და ნაწილობრივ გადაცემა

არსებითად, ტრაფიკის მონაცემთა დაჩქარებული დაცვისა და ნაწილობრივ გამჟღავნების საგამოძიებო მოქმედება, მონაცემთა დაჩქარებული დაცვის ღონისძიების სახეცვლილ ვერსიას წარმოადგენს. კონვენციის მე-17 მუხლი კომუნიკაციის პროცესში მონაწილე რამდენიმე პროვაიდერის არსებობის პირობებში ტრაფიკის მონაცემთა დაჩქარებული წესით დაცვისა და გამოძიებისთვის მისი „ნაწილობრივ“ გამჟღავნების შესაძლებლობას იძლევა, რაც თავის მხრივ კომუნიკაციის მარშრუტის იდენტიფიცირებას უწყობს ხელს.[167]

გავრცელებული პრაქტიკაა, როდესაც კომპიუტერული სისტემის მეშვეობით განხორციელებულ კომუნიკაციაში რამდენიმე სერვის პროვაიდერი მონაწილეობს და ხშირად გამოძიებისთვის ხელსაყრელი ინფორმაცია, რომლის დახმარებითაც კომუნიკაციის წყაროს ან მისი დანიშნულების ადგილის იდენტიფიცირებაა შესაძლებელი, თითოეულ მათგანს ეკუთვნის. ერთიანი სურათის მისაღებად კი მათ მფლობელობაში თუ ზედამხედველობის ქვეშ არსებული მონაცემების შეჯამებაა საჭირო.[168] სწორედ ასეთ ვითარებაშია ეფექტური მე-17 მუხლით ხელმძღვანელობა. ტრაფიკის მონაცემთა დაჩქარებული წესით დაცვისა და ნაწილობრივ გამჟღავნების მნიშვნელობა მით უფრო აშკარა ხდება, როდესაც შემდგარი კომუნიკაციის შესახებ მონაცემები საშუალებას იძლევა იმ პირთა იდენტიფიცირების, რომლებიც ქსელის მეშვეობით ბავშვთა პორნოგრაფიის ამსახველი ფოტო-ვიდეო მასალას ავრცელებენ,

[167] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd , 2018, 107.
[168] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 28.

პირების, რომლებიც უკანონოდ აღწევენ სხვის კომპიუტერულ სისტემაში ან თუნდაც კომპიუტერული სისტემის დახმარებით ჩადიან დანაშაულს.[169]

ვინაიდან სხვადასხვა პროვაიდერთან არსებული ტრაფიკის მონაცემების უსაფრთხოდ შენახვა და ნაწილობრივ გამოძიებისთვის გამჟღავნება მნიშვნელოვანი მახასიათებელია კონვენციის მე-17 მუხლის მიზნებისთვის, პრაქტიკული კუთხით შეიძლება დაიბადოს კითხვა, თუ რა პროცედურების დაცვით უნდა იმოქმედოს უფლებამოსილმა პირმა? თითოეულ პროვაიდერს დამოუკიდებლად უნდა მიმართოს მონაცემთა დაცვისა და ნაწილობრივ გამჟღავნების მოთხოვნით თუ შესაძლოა მიმართვა ერთობლივ ხასიათს ატარებდეს? იმის გათვალისწინებით, რომ საგამოძიებო ღონისძიების მიზანი ინფორმაციის მაქსიმალურად სწრაფად დაცვა და მოპოვებაა, ხოლო ინდივიდუალური ბრძანების გაცემა შესაძლოა ხანგრძლივ პროცედურებთან იყოს დაკავშირებული, ერთიანი ბრძანების გაცემა, რომელიც კომუნიკაციაში მონაწილე პროვაიდერებს თანაბრად დაავალდებულებს, მიზანშეწონილია. მეტიც, ევროპის საბჭოს მიერ გაცხადებული რეკომენდაციით, ალტერნატიული სახით შესაძლოა, ერთიან ბრძანებაში მოხსენიებულ რომელიმე პროვაიდერს, ბრძანებისა და სამართლებრივი ვალდებულების არსებობის შესახებ სხვა პროვაიდერი კომპანიებისთვის ინფორმაციის მიწოდების ვალდებულება დაეკისროს.[170]

არსობრივად, კონვენციის მე-17 მუხლი ეფექტურ პროცესუალურ მექანიზმს წარმოადგენს ინტერნეტ ტრაფიკის მოპოვების კუთხით. განსაკუთრებით ისეთ პირობებში, როდესაც არსებობს მონაცემთა დაკარგვის საფრთხე და ამასთან, მისი დროული ანალიზი კომუნიკაციის წყაროსა და მისი დანიშნულების ადგილის განსასაზღვრად აუცილებელია. საგამოძიებო ორგანოთა მხრიდან მისი გამოყენებისა და ამავდროულად ბრძანების საფუძველზე პროვაიდერთა მიერ მონაცემთა დამუშავების პროცესში მნიშვნლოვანია პირადი ცხოვრების უფლების დაცვის საკითხი, რა დროსაც პროპორციულობის პრინციპი გადამწყვეტ როლს თამაშობს. სწორედ ამიტომ, კომპეტენტურმა ორგანოებმა მკაფიოდ უნდა განსაზღვრონ ტრაფიკის მონაცემთა ტიპი, რომლის გამჟღავნებაც აუცილებელია კომუნიკაციაში

[169] იქვე.
[170] იქვე.

მონაწილე სხვა შესაძლო პროვაიდერების დასადგენად და მათ მიმართ შესაბამისი ღონისძიებების გასატარებლად. დღეის მდგომარეობით აღნიშნულ ღონისძიებას ეროვნულ კანონმდებლობაში დამოუკიდებელი სახით არ ვხვდებით, თუმცა მის ნაცვლად „დოკუმენტის ან ინფორმაციის გამოთხოვის“ საგამოძიებო ღონისძიება გამოიყენება.[171] მიუხედავად სათადარიგო მექანიზმის არსებობისა, კონვენციის მე-17 მუხლის სრულყოფილი იპლემენტირება საგამოძიებო ორგანოებსა და პროვაიდერებს შორის სწრაფი და ეფექტური თანამშრომლობისთვის რეკომენდირებულია.

3.3. შენახულ კომპიუტერულ მონაცემთა ჩხრეკა - ამოღება

კომპიუტერული მონაცემის ჩხრეკა-ამოღების საკითხი „კიბერდანაშაულის შესახებ“ კონვენციის მე-19 მუხლით არის მოწესრიგებული, რომლის 1-ლი ნაწილის „ა“ და „ბ“ ქვეპუნქტები კომპეტენტურ ორგანოებს, ქვეყნის ტერიტორიაზე არსებული კომპიუტერული სისტემისა და მისი ნაწილის, მასში შენახული კომპიუტერული მონაცემისა და იმ მონაცემთა შესანახი საშუალების ჩხრეკის უფლებამოსილებით აღჭურავენ, რომელშიც გამოძიებისთვის მნიშვნელოვანი ინფორმაცია შეიძლება ინახებოდეს.[172] ნიშანდობლივია, რომ კომპიუტერულ სისტემებთან და მონაცემებთან სიტყვა „ჩხრეკა“ ძებნის, შემოწმების, წაკითხვისა და დათვალიერების შესაძლებლობას გულისხმობს.[173] თუ ჩხრეკის დროს გაჩნდება საფუძვლიანი ეჭვი, რომ კომპიუტერულ სისტემასთან დაკავშირებულ სხვა მოწყობილობაში შესაძლოა დანაშაულთან დაკავშირებული ინფორმაცია ინახებოდეს, მე-19 მუხლის მე-2 ნაწილზე დაყრდნობით ჩხრეკის არეალის გაფართოება და კომპიუტერულ სისტემასა თუ მასში განთავსებულ ინფორმაციაზე წვდომა დასაშვებია. თუმცა, რა პროცედურების დაცვით უნდა მოხდეს ეს, რომ მისი განხორციელების პროცესში ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვა უზრუნველყოფილი იყოს, მთლიანად შიდასახელმწიფოებრივი მოწესრიგების საგანს წარმოადგენს.

საგამოძიებო მოქმედების ჩატარებაზე უფლებამოსილი ორგანოები, ჩხრეკის შედეგად აღმოჩენილი კომპიუტერული სისტემისა თუ დოკუმენტის უსაფრთხოდ დაცვის

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

[172] Convention on Cybercrime, Budapest, 23.11.2001.

[173] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 33.

მიზნით, უფლებამოსილნი არიან უშუალოდ კომპიუტერული სისტემა ან მისი ნაწილი, ან მონაცემთა შემნახავი საშუალება ამოიღონ, შექმნან მონაცემთა ასლი, დაშიფვრის ან წვდომის უფლების სხვაგვარი შეზღუდვით უზრუნველყონ მონაცემთა უსაფრთხოება.[174]

საკითხის კომპლექსურობიდან გამომდინარე, კონვენცია კიდევ უფრო ფართო უფლებამოსილებით აღჭურავს საგამოძიებო უწყებებს, ვიდრე ეს უბრალოდ მონაცემთა ჩხრეკა, ამოღება ან მასზე წვდომის შეზღუდვაა. კერძოდ, მე-19 მუხლის მე-4 ნაწილი კომპიუტერული სისტემის ფუნქციონირების მცოდნე ნებისმიერი პირის დავალდებულების შესაძლებლობას ითვალისწინებს, გასცეს ჩხრეკა-ამოღების სრულყოფილად განხორციელებისთვის საჭირო ინფორმაცია. იქნება ეს სისტემის, ანგარიშის პაროლი თუ მონაცემთა განშიფრისთვისთვის აუცილებელი ინფორმაცია, რა დროსაც წყარო შესაძლოა სისტემის ადმინისტრატორი[175] ან მესაკუთრეც კი იყოს, ხოლო კომპიუტერულ მოწყობილობაზე ან ინფორმაციაზე წვდომისთვის საჭირო მონაცემი ბიომეტრული ხასიათის.[176] ჩხრეკის ნებართვის არსებობის მიუხედავად, სისტემის ადმინისტრტორისგან ამგვარი ხასიათის ინფორმაციის გადაცემის მოთხოვნას სჭირდება დამოუკიდებელი სამართლებრივი საფუძველი და სასამართლო ნებართვა, რაზეც კონვენცია ყურადღებას არ ამახვილებს. ხოლო კომპიუტერული სისტემის ან მონაცემთა შემნახველი მოწყობილობის მფლობელისადმი მსგავსი მონაცემების გადაცემის ვალდებულების დაკისრებით, შესაძლოა სათანადოდ ვერ იქნას გარანტირებული ისეთი კონსტიტუციური უფლება, როგორიცაა თვითინკრიმინაციისგან დაცვის პრივილეგია.[177]

უნდა ითქვას, რომ კონვენციის მე-19 მუხლის მიზანი, ელექტრონული ინფორმაციის მოპოვებისთვის, კლასიკური ჩხრეკა-ამოღების თანაბარღირებული საგამოძიებო მოქმედების დანერგვაა, რაც მთლიანობაში ეროვნული კანონმდებლობის თანამედროვე ტექნოლოგიებთან ჰარმონიზაციას შეუწყობს ხელს. მისი მოქმედების ფარგლები სახელმწიფო ტერიტორიით არის შეზღუდული, თუმცა საყურადღებოა, რომ როდესაც კომპიუტერულ სისტემაზე და მასში არსებულ ანგარიშებსა თუ

[174] იქვე, 34.
[175] იქვე.
[176] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 106.
[177] *United States v. Spencer*, WL 1400401, N.D. Cal., [2018], 3.

მონაცემებზე ხდება წვდომა, რთული დასადგენია თუ სად იკვეთება გეოგრაფიული საზღვარი. ნორმის ზოგადი ხასიათიდან გამომდინარე, პროპორციულობის პრინციპის საფუძველზე განსასაზღვრია თუ რა მოცულობის ინფორმაციის ამოღება უნდა მოხდეს ჩხრეკის დროს, რა დროს არის მიზანშეწონილი მხოლოდ მონაცემთა კოპირება და რა დროს მთლიანად მოწყობილობის ამოღება, როგორ უნდა მოწესრიგდეს მესამე პირთაგან კომპიუტერულ მოწყობილობასა თუ მასში არსებულ ანგარიშებზე წვდომისთვის და ჩხრეკისთვის საჭირო მონაცემების მოპოვება.

3.4. კომპიუტერული მონაცემის მიმდინარე რეჟიმში შეგროვება

3.4.1. ინტერნეტტრაფიკის მონაცემის მიმდინარე შეგროვება

კერძო კომუნიკაციის საიდუმლოების დარღვევა, კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა, ბავშვთა პორნოგრაფიის წარმოება და გავრცელება, ეს იმ დანაშაულთა მცირე ჩამონათვალია, რომელთა გამოძიების პროცესში ტრაფიკის მონაცემთა მიმდინარე რეჟიმში შეგროვებას გადამწყვეტი მნიშვნელობა აქვს დამნაშავესა და დაზარალებულს შორის არსებული საკომუნიკაციო კვალის გამოსაკვლევად. [178] შესაბამისად, „კიბერდანაშაულის შესახებ“ კონვენციის მე-20 მუხლი სახელმწიფო ორგანოებს თავიანთ ტერიტორიაზე, ტექნიკურ საშუალებათა გამოყენებით ან სერვის პროვაიდერი კომპანიების დახმარებით ინტერნეტტრაფიკის მონაცემთა მიმდინარე რეჟიმში შეგროვებისა და ჩაწერის უფლებამოსილებით აღჭურავს. საგამოძიებო მოქმედების ფარგლები ტერიტორიულობის პრინციპითაა შეზღუდული და მისი გამოყენების აუცილებელ წინაპირობას კომუნიკაციის ერთი მხარის (პირი/კომპიუტერი) საქართველოს ტერიტორიაზე არსებობა ან კომუნიკაციის გამტარი კომპიუტერული ან სხვა სახის მოწყობილობის ქვეყნის ტერიტორიაზე განთავსება წარმოადგენს.[179]

მსგავსად შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვებისა, ინტერნეტტრაფიკის მონაცემთა შეგროვებაც, ფარულ ხასიათს ატარებს. იგი ქმედითია, როდესაც კომუნიკაციაში მონაწილე მხარეებისთვის უცნობია მათ მიმართ განხორციელებული საგამოძიებო მოქმედების შესახებ. სწორედ ამიტომ,

[178] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 37.
[179] იქვე, 38.

მომსახურების მომწოდებელ კომპანიებს მიმდინარე ფარული საგამოძიებო მოქმედების შესახებ ინფორმაციის გაუმჟღავნებლობის ვალდებულება აკისრიათ. მეტიც, ისინი კონვენციის მე-20 მუხლით, კანონისა [180] და მომხმარებელთან დადებული ხელშეკრულების საფუძველზე ნაკისრი ვალდებულების, კერძოდ კი საკომუნიკაციო ქსელით გადაცემული ინფორმაციისა და მის გამოყენებასთან დაკავშირებული მონაცემების კონფიდენციალურად შენახვისგანაც კი თავისუფლდებიან. [181] თუმცა, მომხმარებელთა და მესამე პირთა კანონიერი ინტერესების დაცვის მიზნით, დაუშვებელია საგამოძიებო მოქმედება უკონტროლო ხასიათს ატარებდეს. მიზანშეუწონელია განუსაზღვრელად დიდი მოცულობის ინფორმაციის მონიტორინგი, მოპოვება და დამუშავება. შესაბამისად, ეს რომ არ დაემსგავსოს მაკომპრომეტირებელი მასალების ძებნას (Fishing Expedition), მნიშვნელოვანია საგამოძიებო მოქმედების ჩატარებაზე გაცემული სასამართლო ნებართვა ან გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის დადგენილება, კონკრეტული კომუნიკაციისა და მასთან დაკავშირებული ტრაფიკის მონაცემების მონიტორინგისა და შეგროვების ხანგრძლივობის შესახებ მითითებას ითვალისწინებდეს.

ინტერნეტტრაფიკის მიმდინარე რეჟიმში შეგროვება არსობრივად ფარულ საგამოძიებო მოქმედებას წარმოადგენს. იგი ფარულად, უწყვეტად, დროის გარკვეულ მონაკვეთში მიმდინარეობს და კომუნიკაციის დროის, წყაროს, მიმართულების, ხანგრძლივობის, ადგილმდებარეობის შესახებ მონაცემების შეგროვების შესაძლებლობას იძლევა. ხოლო მათი მიმდინარე რეჟიმში შეგროვება და დამუშავება, პირად ცხოვრებაში მაღალი ინტენსივობით ჩარევას გარდაუვალს ხდის. სწორედ ამიტომ, უფლების შეზღუდვისას სახელმწიფოს მოქმედების ფარგლების მკაფიოდ განსაზღვრა და პირადი ცხოვრების უფლების დაცვისთვის სხვა ქმედითი პროცესუალური გარანტიების გათვალისწინება მნიშვნელოვანია.

3.4.2. შინაარსობრივი მონაცემების მოპოვება

წლების მანძილზე ტრადიციული კომუნიკაციის ფარული მიყურადება სამართალდამცავი უწყების წარმომადგენელთათვის განსაკუთრებულ საგამოძიებო

[180] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი, სსმ.,26/06/2005, მუხლი 8.
[181] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 39.

ღონისძიებას წარმოადგენდა. განსაკუთრებით ეროვნული უსაფრთხოების დაცვისა და მძიმე კატეგორიის დანაშაულთა გამოძიების კუთხით. თანამედროვე ტექნოლოგიების, ქსელური კომუნიკაციის ელვისებური სისწრაფით განვითარების ფონზე კი იდენტური ფუნქცია შინაარსობრივი მონაცემების მიმდინარე რეჟიმში, ფარულად მოპოვებამ შეიძინა.

შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვების შესაძლებლობით, კონვენცია საგამოძიებო ორგანოებს საშუალებას აძლევს დამოუკიდებელი ძალებით ან სერვისის პროვაიდერი კომპანიის დახმარებით [182] თვალყური ადევნონ კომპიუტერული სისტემისა და ქსელის მეშვეობით განხორციელებულ კომუნიკაციას, შეიტყონ მისი შინაარსი და განსაზღვრონ კომუნიკაციის მიზანი.[183] განსხვავებით სხვა საგამოძიებო მოქმედებებისგან, ცხადია, რომ კომუნიკაციის შინაარსის შეგროვებისას და ჩაწერისას, პირადი ცხოვრების უფლების ხელშეუხებლობის შეზღუდვის ინტენსივობა ბევრად მაღალია. შესაბამისად, მისი გამოყენებისთვის შედარებით მკაცრი სამართლებრივი მოწესრიგებაა საჭირო, რაც პირველ რიგში მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვას გულისხმობს.[184] მოქმედების ფარგლები იზღუდება აგრეთვე „კონკრეტული კომუნიკაციით“, რომელიც შესაძლოა მობილური აბონენტის საერთაშორისო იდენტიფიკატორის (IMSI), მობილური აღჭურვილობის სადგურის საერთაშორისო იდენტიფიკატორის (IMEI), სიმ ბარათის ან IP-მისამართის მეშვეობით განისაზღვროს.[185]

დამატებით, პირთა პირად ცხოვრებაში თვითნებური ჩარევის თავიდან აცილების მიზნით მიზანშეწონილია საგამოძიებო მოქმედების ადრესატთა შერჩევა, ჩარევის ხანგრძლივობის დადგენა, მოპოვებული მტკიცებულების გამოკვლევის, გამოყენების, შენახვისა და განადგურების წესის გათვალისწინება.[186]

„კიბერდანაშაულის შესახებ“ კონვენცია ინტერნეტტრაფიკისა და შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვებას თითქმის იდენტურად აწესრიგებს. იდენტურია საგამოძიებო ორგანოთა უფლებამოსილება ინფორმაციის მოპოვების შესაძლებლობის მხრივ, თუმცა სხვაობას მოსაპოვებელი მონაცემის ტიპსა და

[182] Convention on Cybercrime, Budapest, 23.11.2001, Art. 21.
[183] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 40.
[184] Convention on Cybercrime, Budapest, 23.11.2001, Art. 21 (1).
[185] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 109.
[186] *Zakharov v. Russia,* [2015], ECHR, 230-231.

საგამოძიებო მოქმედების ფარგლების კუთხით ვხვდებით. შინაარსობრივი მონაცემის მიმდინარე რეჟიმში შეგროვება დანაშაულთა წრით იმპერატიულად იზღუდება, ხოლო ტრაფიკის მონაცემებთან მიმართებით სავალდებულო მოთხოვნა კონვენციაში არ იკითხება.

3.5. კომპიუტერული მონაცემის წარმოდგენის ბრძანების ინტერპრეტაცია

3.5.1. კომპიუტერული მონაცემის წარმოდგენის ბრძანება

პროპორციულობის პრინციპიდან გამომდინარე მნიშვნელოვანია ეროვნული კანონმდებლობა ლეგიტიმური მიზნის მიღწევის ალტერნატიულ ღონისძიებებს ითვალისწინებდეს. სისხლის სამართლის საქმისათვის ღირებული ელექტრონული მტკიცებულების მოპოვებისთვის გამუდმებით ჩხრეკა-ამოღების ან სხვა მძიმე ღონისძიების გამოყენება გაუმართლებელია, მაშინ როდესაც იგივე ინფორმაციის მიღება უფლების ნაკლებ მზღუდავი საგამოძიებო მოქმედების შედეგად არის შესაძლებელი. [187] მსგავს ვითარებაში კი ალტერნატიულ ღონისძიებას „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული „კომპიუტერული მონაცემის წარმოდგენის ბრძანება“ წარმოადგენს. გარდა უფლების შედარებით დაბალი ინტენსივობით მზღუდავი ბუნებით გამოწვეული უპირატესობისა, მისი ეროვნულ კანონმდებლობაში დანერგვა მესამე პირებზე, განსაკუთრებით კი ინტერნეტ-პროვაიდერებზეც დადებითად აისახება, რაც საგამოძიებო უწყების წარმომადგენლებისთვის მომხმარებელთა პერსონალური მონაცემების კეთილი ნების და არა სამართლებრივი საფუძვლის ან ვალდებულების გარეშე გადაცემის ფაქტს გამორიცხავს. [188] განსაკუთრებით მაშინ, როდესაც ელექტრონული საკომუნიკაციო ქსელების მომხმარებლების შესახებ და აგრეთვე მათ მიერ ქსელის მეშვეობით გადაცემული ინფორმაცია საიდუმლოა.[189]

შინაარსობრივად საგამოძიებო მოქმედება ორ დამოუკიდებელ შემთხვევას აწესრიგებს. კონვენციის მე-18 მუხლის პირველი ნაწილის „ა“ ქვეპუქნტის მიხედვით „კომპეტენტური პირები უფლებამოსილნი არიან ქვეყნის ტერიტორიაზე მყოფი პირის მფლობელობაში ან ზედამხველობის ქვეშ არსებული კომპიუტერული სისტემიდან ან

[187] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.
[188] იქვე.
[189] საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, სსმ., 26/06/2005, მუხლი 8(1).

ინფორმაციის შემნახველი მოწყობილობიდან ნებისმიერი სახის ინფორმაცია მოიპოვონ“, ხოლო „ბ“ ქვეპუნქტის თანახმად გამოითხოვონ მომხმარებლის შესახებ ინფორმაცია მომსახურების მომწოდებლისგან, რომელიც მომსახურებას სახელმწიფოს ტერიტორიაზე ახორციელებს და ეს ინფორმაცია მის მფლობელობაში ან ზედამხედველობის ქვეშ არის.[190]

საგამოძიებო მოქმედების პირველი ნაწილი ფართო შინაარსისაა და კომპეტენტურ ორგანოებს აძლევს შესაძლებლობას ქვეყნის ტერიტორიაზე მყოფი ნებისმიერი პირისგან, მათ შორის მომსახურების მომწოდებლისგან მოითხოვონ ნებისმიერი სახის კომპიუტერული მონაცემი იქნება ეს მომხმარებლის შესახებ ინფორმაცია, ტრაფიკის თუ შინაარსობრივი მონაცემი. აუცილებელია ინფორმაცია მოთავსებული იყოს კომპიუტერულ სისტემაში ან სხვა შემნახველ მოწყობილობაში, მათ შორის ვირტუალურ სერვერზე და პირი ფიზიკურად ფლობდეს ან თავისუფალ კონტროლს ახორციელებდეს მასზე.[191]

ნორმის მეორე ნაწილის მოქმედების ფარგლები კი „მომსახურების მომწოდებლითა“ და „მომხმარებლის შესახებ ინფორმაციით“ არის შეზღუდული,[192] თუმცა აუცილებელ მოთხოვნას არ წარმოადგენს პროვაიდერის იურიდიული რეგისტრაცია ან მისი ფიზიკური არსებობა უშუალოდ ქვეყნის ტერიორიაზე. მომხმარებლის შესახებ ინფორმაციის გამოთხოვის უფლებამოსილებით სარგებლობისთვის საკმარისია ის, რომ ფიზიკური პირი ან ორგანიზაცია საკუთარ მომსახურებას დაინტერესებული სახელმწიფოს მოქალაქეებს სთავაზობდეს, ხოლო უწყებას გააჩნდეს იურისდიქცია გამოსაძიებელ დანაშაულზე.[193]

თავად კომპიუტერული მონაცემის წარმოდგენის ბრძანების საგამოძიებო მოქმედება შიდასახელმწიფოებრივი ღონისძიებაა. [194] ერთი შეხედვით მისი მოქმედების ფარგლები საკმაოდ ფართოა, თუმცა გარკვეული შეზღუდვები მაინც არსებობს. კერძოდ, კონვენციის მე-18 მუხლის 1-ლი ნაწილის „ა“ ქვეპუნქტის მიხედვით შესაძლებელია მომხმარებლის შესახებ ინფორმაციის, ტრაფიკისა და შინაარსობრივი

[190] Convention on Cybercrime, Budapest, 23.11.2001, Art. 18.
[191] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.
[192] Production Orders for Subscriber Information (Article 18 Budapest Convention), Cybercrime Convention Committee (T-CY), Council of Europe, 2017, 6.
[193] იქვე.
[194] იქვე, 3.

მონაცემის გამოთხოვა მხოლოდ ქვეყნის ტერიტორიაზე მყოფი ფიზიკური თუ იურიდიული პირისგან, ხოლო მართალია „ბ“ ქვეპუნქტი არაფერს ამბობს საგამოძიებო მოქმედების „ტერიტორიით“ შეზღუდვაზე, თუმცა მხოლოდ მომხმარებლის შესახებ ინფორმაციის მოპოვების შესაძლებლობას იძლევა, ისიც ქვეყნის ფარგლებს გარეთ მყოფი პროვაიდერებისაგან, რომლებიც საკუთარ სერვისს საქართველოს მოქალაქეებს სთავაზობენ.

რაც შეეხება საგამოძიებო მოქმედების აღსრულებას და ბრძანების გაცემას, უფლებამოსილი პირების მიერ წინასწარ უნდა განისაზღვროს ინფორმაციის სახე და მოცულობა, ის თუ რა ფორმით (ელ. მოწყობილობა, ამონაბეჭდი და ა.შ.) უნდა მიეწოდოს ელექტრონული ინფორმაცია კომპეტენტურ ორგანოებს. დაუშვებელია ეს დაემსგავსოს მაკომპრომეტირებელი მასალების ძებნას (Fishing Expedition). კომპიუტერული მონაცემის გამოთხოვის ბრძანებით დასაშვებია პირთან დაკავშირებული კონკრეტული ელექტრონული წერილის შინაარსის ან მაიდენტიფიცირებელი მონაცემების გამოთხოვა, თუმცა დაუშვებელია წლების განმავლობაში დაგროვებული ყველა შეტყობინების მოპოვება. შეზღუდვის მიზანს საგამოძიებო მოქმედების განხორციელების პროცესში ადამიანის უფლებათა და თავისუფლებათა დაცვის ხელშეწყობა წარმოადგენს. ყოველივე კი მას, ჩხრეკა-ამოღებასთან შედარებით უფლების ნაკლებ მზღუდავ საგამოძიებო მოქმედებად აქცევს, რომელიც ამავდროულად ნაკლებ ძალისხმევას მოითხოვს ელექტრონული მტკიცებულების მოსაპოვებლად.

დასკვნის სახით, საგამოძიებო მოქმედებით შესაძლებელია ნებისმიერი სახის შენახული კომპიუტერული მონაცემის მოპოვება, იქნება ეს მომხმარებლის შესახებ ინფორმაცია, ტრაფიკის თუ შინაარსობრივი. გადაცემის ბრძანება შესასრულებლად სავალდებულოა ყველა იმ ფიზიკური თუ იურიდიული პირისათვის, რომელთაც მფლობელობაში ან კონტროლს ქვეშ აქვთ ელექტრონული ინფორმაცია. იმ შემთხვევაში თუ ისინი, განსაკუთრებით კი პროვაიდერები, თავიანთი საქმიანობის ფარგლებში, არ აგროვებენ ან ინახავენ ინფორმაციას კომუნიკაციისა და მომხმარებლის შესახებ, ცხადია საგამოძიებო მოქმედებით გათვალისწინებული ვალდებულება მათზე ვერ გავრცელდება.

3.5.2. ნებართვის გაცემაზე უფლებამოსილი პირი

თავიდანვე უნდა ითქვას, რომ არ არსებობს ერთიანი პოზიცია იმასთან დაკავშირებით თუ ვინ უნდა იყოს უფლებამოსილი პირი საგამოძიებო მოქმედების გამოყენებაზე. თავისი შინაარსით კომპიუტერული მონაცემის წარმოდგენის ბრძანება ყველა სახის ელექტრონულ ინფორმაციას მოიცავს და ერთიანი ხედვის არ არსებობის ძირითადი მიზეზიც სწორედ ესაა. მონაცემის სახის და მახასიათებლის გათვალისწინებით ავტორიზაციაზე უფლებამოსილი პირის თუ ორგანოს განსაზღვრის პრეროგატივა მთლიანად ხელშემკვრელი მხარის ხელშია.

სახელმწიფოს შეუძლია წესები, უფლებამოსილი ორგანოები და უფლების დაცვის გარანტიები ელექტრონულ მონაცემთა სახის მიხედვით განსაზღვროს. საჯაროდ ხელმისაწვდომი მომხმარებლის შესახებ ინფორმაციის გამოთხოვის უფლებამოსილება შესაძლოა პროკურორს, გამომძიებელს ან პოლიციელს მიენიჭოს, მაშინ როდესაც განსხვავებულ მოცემულობაში სასამართლოს ნებართვა იყოს საჭირო. [195] მაგალითისთვის, პერსონალურ მონაცემთა და პირადი ცხოვრების უფლების დაცვის ინტერესებიდან გამომდინარე ტრაფიკისა და შინაარსობრივი მონაცემების გადაცემა შესაძლოა სასამართლო ნებართვით შეიზღუდოს. შესაბამისად, რთულია კონკრეტული უფლებამოსილი პირის ან ორგანოს განსაზღვრა. ნათელი მაგალითია სხვადასხვა ქვეყნის კანონმდებლობის განსხვავებული მოწესრიგება, სადაც ზოგადად კომპიუტერული მონაცემის წარმოდგენის ბრძანებაზე უფლებამოსილ პირებად შეიძლება პროკურორი, გამომძიებელი, პოლიციელი ან სასამართლო მოგვევლინონ.[196]

3.5.3. ნორმის იმპლემენტაცია

კომპიუტერული მონაცემის გადაცემის ბრძანება იძულებით ღონისძიებებს შორის ალტერნატიულ მექანიზმს წარმოადგენს, რომელიც სამართალდამცავ ორგანოებს ნებისმიერი კატეგორიის ელექტრონული ინფორმაციის მოპოვების უფლებამოსილებას ანიჭებს.[197]

---

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

[196] Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, 2014, 15-28. <https://rm.coe.int/16802e7ad1> [03.06.2023].

[197] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 227.

„კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნების გათვალისწინებით, კომპიუტერული მონაცემის წარმოდგენის ბრძანების ეროვნულ კანონმდებლობაში სათანადოდ იმპლემენტირებისათვის შემდეგი ძირითადი მოთხოვნების დაკმაყოფილებაა აუცილებელი: კერძოდ, **ა) კომპიუტერული მონაცემის წარმოდგენის ბრძანება ეროვნულ კანონმდებლობაში დამოუკიდებელი საგამოძიებო მოქმედების სახით უნდა იყოს გათვალისწინებული ბ) ეროვნული კანონმდებლობა უნდა აკმაყოფილებდეს სიზუსტისა და განჭვრეტადობის მოთხოვნებს; და გ) გათვალისწინებული უნდა იქნას უფლებაში თვითნებური ჩარევისგან დაცვის ქმედითი პროცესუალური გარანტიები.**[198]

ხაზი უნდა გაესვას იმ გარემოებასაც, რომ ძირითად მოთხოვნებთან ერთად შესაძლოა ეროვნული კანონმდებლობით პრივილეგირებული ინფორმაციის დაცვის [199] და საგამოძიებო მოქმედების ჩატარებისთვის სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობის განხორციელების ვალდებულებაც იყოს განსაზღვრული.[200]

3.5.4. პროცედურული ღონისძიებების მოქმედების ფარგლები

კომპიუტერული მონაცემის წარმოდგენის ბრძანების ეფექტური გამოყენებისთვის არსებითი მნიშვნელობა აქვს საგამოძიებო მოქმედების ფარგლებსა და მიზნებთან დაკავშირებით „კიბერდანაშაულის შესახებ“ კონვენციის მე-14 მუხლით განსაზღვრულ დათქმებს.

მოცემული ნორმის თანახმად, საგამოძიებო ღონისძიების გამოყენება დასაშვებია კონვენციით გათვალისწინებული დანაშაულის, კომპიუტერული სისტემის გამოყენებით ჩადენილი დანაშაულისა და ნებისმიერი დანაშაულის გამოძიების მიზნებისთვის, რომლის ფარგლებშიც შესაძლოა ელექტრონული მტკიცებულების მოპოვება.[201]

---

[198] 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> [03.06.23].

[199] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 30. იხ. *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 227-228.

[200] იქვე.

[201] 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>

საგამოძიებო მოქმედების ფარგლების ასე ფართოდ განსაზღვრის მიუხედავად, კონვენცია შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შესაგროვლად საგამოძიებო ღონისძიების გატარებისას, მისი მოქმედების ფარგლების „მძიმე დანაშაულთა“ (Serious Offence) კატეგორიით [202] შეზღუდვის ვალდებულებას ითვალისწინებს. რაც შეეხება ტრაფიკის მონაცემების მიმდინარე რეჟიმში შეგროვების საგამოძიებო მოქმედების დანაშაულთა წრით შეზღუდვას, ხელშემკვრელი მხარე უფლებამოსილია ამ საკითხთან დაკავშირებით დამოუკიდებლად მიიღოს გადაწყვეტილება, თუმცა შეზღუდვის დაწესების შემთხვევაში ვალდებულია დაიცვას კონვენციის მოთხოვნა და შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვების საგამოძიებო მოქმედებაზე მეტად არ შეზღუდოს მისი მოქმედების ფარგლები.[203]

ამდენად შეიძლება ითქვას, რომ მართალია „კიბერდანაშაულის შესახებ“ კონვენციის მე-14 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი საგამოძიებო მოქმედების ფარგლების ამავე დოკუმენტით განსაზღვრული დანაშაულებით შეზღუდვას ითვალისწინებს, თუმცა „ბ“ და „გ“ ქვეპუნქტების ფორმულირება პროცედურული მექანიზმების ნებისმიერი დანაშაულის გამოძიების დროს გამოყენების შესაძლებლობას მაინც იძლევა. [204] შინაარსობრივი მონაცემების მიმდინარე რეჟიმში შეგროვების საგამოძიებო მოქმედების ფარული ბუნება და პირადი ცხოვრების უფლების შეზღუდვის ხასიათი აუცილებელს ხდის მისი მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვას. შესაძლოა იგივე ითქვას ტრაფიკის მონაცემთა მიმდინარე რეჟიმში შეგროვებაზე, თუმცა კომპიუტერული მონაცემის წარმოდგენის ბრძანების შემთხვევაში,

[03.06.2023]. იხ. *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 229.

[202] „მძიმე დანაშაულთა“ განმარტებისას კონვენციას ნეიტრალური პოზიცია უკავია. მის განმარტებას სრულებით ხელშემკვრელ მხარეს ანდობს. შესაძლოა საკითხის იმის მიხედვით გადაწყვეტა თუ რომელი დანაშაული ითვლება მძიმედ ეროვნული კანონმდებლობით. ამასთან, დასაშვებია სახელმწიფომ თავად განსაზღვროს დანაშაულთა ჩამონათვალი და ღონისძიების მოქმედების ფარგლები.

[203] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 23.

[204] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 100.

მიზანშეწონილად მიგვაჩნია მოქმედების ფარგლებთან დაკავშირებული დებულებები უფრო ვრცლად იქნას განმარტებული.[205]

3.5.5. პირობები და გარანტიები

კომპიუტერული მონაცემის გადაცემის ბრძანება „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებულ სხვა საგამოძიებო მოქმედებებთან ერთად იძულებითი ხასიათის ღონისძიებათა რიგს მიეკუთვნება.[206] იმის გათვალისწინებით, რომ იძულებითი საგამოძიებო ღონისძიება მნიშვნელოვნად ზღუდავს ადამიანის ძირითად უფლებებსა და თავისუფლებებს, განსაკუთრებით კი პირადი ცხოვრების ხელშეუხებლობის უფლებას, [207] კონვენციის მე-15 მუხლი პროცესუალური ღონისძიებების გამოყენების პროცესში უფლებათა ადეკვატური დაცვის მიზნით ხელშემკვრელ მხარეებს გარკვეულ ვალდებულებებს აკისრებს, რაც ა) ადამიანის უფლებათა დაცვის საერთაშორისო ინსტრუმენტებით ნაკისრი ვალდებულებების პატივისცემით; ბ) უფლებაში ჩარევის გამამართლებელი საფუძვლის არსებობით; გ) პროპორციულობის პრინციპის დაცვით; დ) უფლებამოსილების ხანგრძლივობისა და ფარგლების შეზღუდვით; ე) სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობის განხორციელებათა [208] და ვ) მესამე მხარის უფლებების, ვალდებულებებისა და კანონიერი ინტერესების პატივისცემით უნდა გამოიხატოს.[209]

ა) ადამიანის უფლებათა დაცვის საერთაშორისო ინსტრუმენტებით ნაკისრი ვალდებულების პატივისცემა - საერთაშორისო ხელშეკრულება, როგორც წესი ხელმომწერი სახელმწიფოსთვის გარკვეულ უფლებებსა და მოვალეობებს წარმოშობს. ადამიანის ძირითად უფლებათა და თავისუფლებათა დაცვის კუთხით საქართველოსთვის როგორც მისი კანონმდებლობის ნაწილი განსაკუთრებით

---

[205] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 229-230.

[206] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 230.

[207] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 61.

[208] 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> [04.06.23].

[209] Convention on Cybercrime, Budapest, 23.11.2001, Article 15(3).

მნიშვნელოვანია 1950 წლის ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია და მის საფუძველზე შექმნილი სასამართლოს მიერ მიღებული გადაწყვეტილებები. აღნიშნულის გათვალისწინებით სახელმწიფო ვალდებულია მის იურისდიქციაში უზრუნველყოს კონვენციით გათვალისწინებული უფლებების, მათ შორის საქმის სამართლიანი განხილვის უფლების, პირადი და ოჯახური ცხოვრებისა თუ სხვა უფლებების დაცვა.[210]

ბ) ჩარევის გამამართლებელი საფუძვლის არსებობა - „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული საგამოძიებო ღონისძიებები კერძო საკუთრების, მფლობელობის ან პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვას ითვალისწინებენ. [211] შესაბამისად, მნიშვნელოვანია დასაბუთებული იყოს მათი გამოყენების აუცილებლობა. როგორც წესი დასაბუთება ვარგის ცნობებსა და დასკვნებს უნდა ეფუძნებოდეს, რომელიც საგამოძიებო მოქმედების ჩატარებამდე იქნება წარმოდგენილი. [212] საგულისხმოა, რომ კონვენციის მოთხოვნებიდან გამომდინარე, საგამოძიებო ღონისძიების გამოყენების ერთ-ერთ მნიშვნელოვან წინაპირობას სისხლის სამართლის საქმეზე ოფიციალური გამოძიების მიმდინარეობა წარმოადგენს. ყოველივე ზემოაღნიშნული კი, ერთობლიობაში სახელმწიფოს მხრიდან ძირითად უფლებებში თვითნებური ჩარევის რისკის შემცირებას ემსახურება.[213]

გ) პროპორციულობის პრინციპი - ნიშანდობლივია, რომ „კიბერდანაშაულის შესახებ“ კონვენცია პროპორციულობის პრინციპზე დაყრდნობით როგორც უფლების ნაკლებ, ისე მაღალი ინტენსივობით მზღუდავ საგამოძიებო მოქმედებებს ითვალისწინებს.[214] აღნიშნული საშუალებას აძლევს და იმავდროულად ავალდებულებს

---

[210] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 11<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [04.06.23].

[211] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 231.

[212] 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> [04.06.23].

[213] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway,John Wiley & Sons Ltd, 2018, 99.

[214] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 231.

სამართალდამცავ ორგანოებს დანაშაულის ბუნებისა და საქმის გარემოებების გათვალისწინებით არსებული ღონისძიებებიდან ნაკლებად მზღუდავი საგამოძიებო მოქმედება შეარჩიონ. [215] საგულისხმოა, რომ კონვენციით გათვალისწინებული იმპერატიული მოთხოვნა შინაარსობრივი მონაცემების შეგროვების საგამოძიებო მოქმედების დანაშაულთა წრით შეზღუდვასთან დაკავშირებით, სწორედ პროპორციულობის პრინციპის დაცვას ემსახურება.[216]

დ) უფლებამოსილების ხანგრძლივობისა და ფარგლების შეზღუდვა - აღნიშნულ მოთხოვნას განსაკუთრებული მნიშვნელობა აქვს ისეთი საგამოძიებო მოქმედების განხორციელებისას, რომელიც ბუნებით ფარულ საგამოძიებო მოქმედებათა კატეგორიას მიეკუთვნება და ხანგრძლივად, გარკვეული დროის განმავლობაში მაღალი ინტენსივობით ზღუდავს პირადი ცხოვრების ხელშეუხებლობის უფლებას. მაგალითისთვის, კომპიუტერულ მონაცემთა მიმდინარე რეჟიმში შეგროვების საგამოძიებო მოქმედება „მძიმე დანაშაულთა“ წრით შეზღუდვასთან ერთად, აუცილებელია გამოყენების ხანგრძლივობის შეზღუდვასაც დაექვემდებაროს. საყურადღებოა, რომ აღნიშნული არ გამორიცხავს ნებართვის პერიოდულად გადახედვას და საჭიროების შემთხვევაში მისი გონივრული ვადით გახანგრძლივებას.[217]

ე) სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობა[218] - პირადი ცხოვრების ხელშეუხებლობის უფლების არამართლზომიერი შეზღუდვის თავიდან ასაცილებლად საგამოძიებო მოქმედებებზე სასამართლო ზედამხედველობის განხორციელება ეფექტურ საშუალებად მიიჩნევა. [219] მნიშვნელოვანია უფლებაში

---

[215] 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> [04.05.23].

[216] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [04.06.23].

[217] 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> [04.06.23].

[218] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 101.

[219] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 232.

ჩარევა ნეიტრალური ორგანოს ან პირის გადაწყვეტილების საფუძველზე მოხდეს, რომელიც მხარეებისგან ფუნქციურად იქნება დამოუკიდებელი და უფლებაში ჩარევის აუცილებლობის შემოწმებას ობიექტურად უზრუნველყოფს. საგულისხმოა, რომ სასამართლოსთან ერთად, ასეთ ორგანოებად შესაძლოა მიჩნეულ იქნას პარლამენტი, პერსონალურ მონაცემთა დაცვის სამსახური და სხვა.[220]

ვ) მესამე მხარის უფლებების, ვალდებულებებისა და კანონიერი ინტერესების პატივისცემა - ნებისმიერი საგამოძიებო მოქმედება, განსაკუთრებით კი კომპიუტერულ მონაცემებთან დაკავშირებული ღონისძიებები გარკვეულწილად ზეგავლენას ახდენენ იმ პირთა უფლებრივ მდგომარეობაზე, რომელთაც კავშირი არ აქვთ დანაშაულთან.[221] მათი უფლებრივი მდგომარეობის დაცვის უზრუნველყოფის მიზნით „კიბერდანაშაულის შესახებ“ კონვენციის მე-15 მუხლის მე-3 ნაწილი მართალია ხელშემკვრელ მხარეებს კონკრეტულ მექანიზმებს არ სთავაზობს, თუმცა ელექტრონული მტკიცებულებების შეგროვების პროცესში მესამე პირთა კანონიერი ინტერესების გათვალისწინებისა და დაცვის ზოგადი ვალდებულებისკენ მოწოდებას მაინც შეიცავს.[222]

კომპიუტერულ მონაცემთან დაკავშირებული საგამოძიებო მოქმედების მესამე პირთა უფლებრივი მდგომარეობაზე ზეგავლენის საილუსტრაციოდ წარმოვიდგინოთ მოცემულობა, როდესაც მომსახურების მომწოდებლისგან ბრალდებულის სატელეფონო ნომერზე შემავალი და გამავალი ზარების შესახებ ინფორმაციის გამოთხოვა ან გარკვეული დროის განმავლობაში მისი კომუნიკაციის შინაარსობრივი მონაცემების შეგროვება ხდება.[223] ასეთ დროს გარდაუვალია მესამე პირთა პირად ცხოვრებასთან დაკავშირებული ინფორმაციის შეგროვება. შესაბამისად მნიშვნელოვანია ეროვნული კანონმდებლობა უფლებაში თვითნებური ჩარევისგან

---

[220] 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> [04.06.23].

[221] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 232-233.

[222] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 102.

[223] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 233. იხ. *United States of America v. Kim Dotcom,* US, №1:12CR3, [2012].

დაცვის მექანიზმებთან ერთად, მონაცემთა განსაზღვრული მიზნითა და მოცულობით შეგროვების კონტროლის შესაძლებლობასაც ითვალისწინებდეს.

შეჯამების სახით კი უნდა ითქვას, რომ „კიბერდანაშაულის შესახებ“ კონვენციის საფუძველზე განხილული პირობებისა და გარანტიების დაცვა წარმოადგენს მინიმალურ და აუცილებელ მოთხოვნას კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების ეროვნულ კანონმდებლობაში დასანერგად. [224] გარდა აღნიშნულისა, მნიშვნელოვანია სამართალწარმოების პროცესში უზრუნველყოფილი იყოს სხვა ისეთი ძირითადი უფლებებისა და თავისუფლებების დაცვა, როგორებიცაა უდანაშაულობის პრეზუმფცია, სამართლიანი სასამართლო განხილვის უფლება და სხვა.[225]

4. შეჯამება

შეიძლება ითქვას, რომ „კიბერდანაშაულის შესახებ“ კონვენცია ერთადერთ სავალდებულო ძალის მქონე საერთაშორისო დოკუმენტს წარმოადგენს, რომელიც ელექტრონული მტკიცებულების მოპოვებისთვის აუცილებელ და ქმედით საგამოძიებო მოქმედებებს ითვალისწინებს. ჩვენთვის განსაკუთრებით საინტერესო საგამოძიებო მოქმედებასთან, „კომპიუტერული მონაცემის გადაცემის ბრძანებასთან“ ერთად, მასში თავმოყრილია ისეთი ქმედითი მექანიზმები, როგორიცაა შენახულ კომპიუტერულ მონაცემთა დაჩქარებული დაცვა, ინტერნეტ ტრაფიკის დაჩქარებული დაცვა და ნაწილობრივ გადაცემა, შენახულ კომპიუტერულ მონაცემთა ჩხრეკა-ამოღება და კომპიუტერულ მონაცემთა მიმდინარე რეჟიმში შეგროვება. მართალია თითოეული მათგანი იძულებით საგამოძიებო ღონისძიებას მიეკუთვნება,[226] თუმცა, ხელშემკვრელ მხარეებს მათი ეროვნულ კანონმდებლობაში დანერგვის პარალელურად, ძირითად უფლებებში თვითნებურად ჩარევისგან დაცვის უზრუნველსაყოფად, სათანადო გარანტიების გათვალისწინების ვალდებულება

[224] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 233.

[225] 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> [04.06.23].

[226] *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 54.

აკისრიათ. აღნიშნული ვალდებულება თანაბრად ვრცელდება კონვენციით გათვალისწინებულ ყველა საგამოძიებო მოქმედებაზე, თუმცა მათი განსხვავებული ბუნებისა და უფლებაში ჩარევის ინტენსივობიდან გამომდინარე, დაცვის მექანიზმებიც შესაძლოა სხვადასხვა იყოს.

უშუალოდ „კომპიუტერული მონაცემის გადაცემის ბრძანებაზე“ რომ გავამახვილოთ ყურადღება, მისი ეროვნულ კანონმდებლობაში სრულყოფილად დანერგვისთვის როგორც თავად „კიბერდანაშაულის შესახებ“ კონვენცია, ისე მისი განმარტებითი ანგარიში ამომწურავ ინფორმაციას გვაწვდის საგამოძიებო მოქმედების შინაარსისა და მიზნის, მოქმედების ფარგლების შესახებ. აგრეთვე, ადამიანის ძირითადი უფლებებისა და თავისუფლებების სათანადოდ დაცვის უზრუნველყოფისთვის გასატარებელი ღონისძიებების თაობაზე.

„კომპიუტერული მონაცემის გადაცემის ბრძანების“ ეროვნულ კანონმდებლობაში სათანადო დანერგვისთვის აუცილებელია მისი დამოუკიდებელ საგამოძიებო მოქმედებად გათვალისწინება, ნორმის მიერ სიზუსტისა და განჭვრეტადობის მოთხოვნის დაკმაყოფილება და ძირითად უფლებაში თვითნებურად ჩარევისგან დამცავი პროცესუალური გარანტიების არსებობა,[227] რაც თავის მხრივ სულ მცირე ადამიანის უფლებათა დაცვის საერთაშორისო ინსტრუმენტებით ნაკისრი ვალდებულების პატივისცემას, უფლებაში ჩარევის გამამართლებელი საფუძვლის არსებობას, მისი გამოყენებისას პროპორციულობის პრინციპის დაცვას, უფლებამოსილების ფარგლებისა და ხანგრძლივობის შეზღუდვასა და საგამოძიებო მოქმედების განხორციელებისას სასამართლო ან სხვა დამოუკიდებელი ზედამხედველობის განხორციელებას გულისხმობს.[228] ხოლო, რაც შეეხება მისი მოქმედების ფარგლებს, პროპორციულობის პრინციპისა და აგრეთვე, სხვა საგამოძიებო მოქმედებებისგან განსხვავებით ძირითადი უფლების დაბალი ინტენსივობით მზღუდავი ბუნების გათვალისწინებით, მისი გამოყენება დასაშვებია როგორც თავად კონვენციით გათვალისწინებული დანაშაულის გამოსაძიებლად,

[227] 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> [04.06.23].

[228] 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> [04.06.23].

ასევე ნებისმიერი დანაშაულის გამოძიებისას, სადაც შესაძლოა მტკიცებულება ელექტრონული სახით არსებობდეს.[229]

[229] იქვე, 7.

თავი III. ადამიანის უფლებათა საერთაშორისო სამართლით უზრუნველყოფილი სტანდარტები კომპიუტერული მონაცემის გამოთხოვა-მოპოვების პროცესში

1. პირადი ცხოვრების პატივისცემისა და პერსონალურ მონაცემთა დაცვის უფლების ურთიერთკავშირი

პერსონალურ მონაცემთა დაცვა ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით გარანტირებული პირადი და ოჯახური ცხოვრების დაცვის უფლების განუყოფელი ნაწილია, თუმცა ევროკავშირის კანონმდებლობის თანახმად იგი დამოუკიდებელ უფლებად არის აღიარებული.[230]

დღეს, როდესაც კომპიუტერული სისტემისა და ინტერნეტის განვითარების შედეგად ინდუსტრიული საზოგადოება ინფორმაციულ საზოგადოებად ტრანსფორმირდა,[231] პერსონალური მონაცემის დაცვამ განსაკუთრებული ადგილი დაიკავა პირადი ცხოვრების ხელშეუხებლობის უზრუნველყოფის პროცესში.

კომპიუტერული მოწყობილობების საყოველთაობამ, გლობალური ქსელით ურთიერთდაკავშირებულობამ,[232] რთული ამოცანების შესრულების ფუნქციამ, დიდი ოდენობით ინფორმაციის შენახვის, გარკვეულ კატეგორიებად დაჯგუფების, დამუშავების, გადაცემის და მათზე სხვადასხვა ლოკაციიდან წვდომის შესაძლებლობამ [233] დიდი მოცულობის მონაცემების, მათ შორის პერსონალური მონაცემების დამუშავებას დაუდო საფუძველი.

მსოფლიოში არსებული უმსხვილესი კომპანიების და უკვე არამარტო მათ, ძირითად აქტივს არამატერიალური სახის ინფორმაცია წარმოადგენს. სწორედ მომხმარებელთა შესახებ მონაცემები განაპირობებს მათ წარმატებას. მათი დამუშავებისა და ანალიზის საფუძველზე გვთავაზობენ სხვადასხვა სერვისს, რომელიც ჩვენზე, მომხმარებლების მოთხოვნებზეა მორგებული.[234]

მომსახურების სფეროში არსებული კომპანიები აგროვებენ და ამუშავებენ ინფორმაციას სახელის, გვარის, დაბადების თარიღის, სქესის, ოჯახური

---

[230] Charter of Fundamental Rights of The European Union, 2012/C 326/02.

[231] *Schermer W. B.,* Surveillance and Privacy in the Ubiquitous Network Society*,* Amsterdam Law Forum, vol. 1, No. 4, 2009, 1.

[232] *Wooldridge M.,* An Introduction to Multi-agent Systems, West Sussex: John Wiley & Sons Ltd., 2001, 2-9.

[233] *Walden I.*, Privacy and Data Protection, Computer Law –The Law and Regulation of Information Technology, 6th edition, *Reed C., Angel J.* (eds.), Oxford University Press, 2007, 470.

[234] იქვე, 459.

მდგომარეობის, საქმიანობის, საცხოვრებელი მისამართის, ელექტრონული ფოსტის, მობილური ნომრის, განათლების, ადგილმდებარეობის, საბანკო ანგარიშებისა და შესაბამისი აქტივობების, ონლაინ ვაჭრობის, გამოყენებული ვებ გვერდების, მასზე დაყოფილი დროის და ხანგრძლივობის, პაროლებისა და სხვადასხვა ინტერესების შესახებ. მაგალითისთვის ისეთი კომპანია, როგორიც არის "Google" - საკუთარ ანგარიშზე პერსონალურ მონაცემთა ფართო სპექტრს ინახავს. კერძოდ, ინფორმაციას აპლიკაციების, მოწყობილობების, ოპერაციული სისტემის, კავშირგაბმულობის არხის, მათ შორის სახელისა და ნომრის, IP მისამართის, საძიებო სიტყვების, ნანახი ვიდეოს, გაგზავნილი ან მიღებული ხმოვანი და აუდიო შეტყობინების, თქვენთან დაკავშირებული ადამიანების, ბრაუზერის ისტორიის, ადგილმდებარეობის შესახებ და ა.შ. საყურადღებოა, რომ ეს ინფორმაციათა ძალიან მცირე ჩამონათვალია, რომელსაც კომპანია ინახავს და ამუშავებს. თუ მათი კონფიდენციუალობის პოლიტიკას გავეცნობით, ვნახავთ, რომ Google - მა შესაძლოა ჩვენი პერსონალური მონაცემები **ჩვენი თანხმობით, სამართლებრივი საფუძვლით** ან **გარე დამუშავების** მიზნით გასცეს და გაამჟღავნოს.

აგრეთვე, თავადვე გავცემთ საკუთარ მონაცემებს და წვდომის საშუალებას ვაძლევთ კომპანიას, როდესაც მაღაზიათა ქსელში „ლოიალობის" ბარათს ვიღებთ. მფლობელმა იცის არამარტო ის თუ ვინ არის ამ ბარათის მფლობელი, არამედ რა იყიდა და გადახდის რა მეთოდი გამოიყენა. ამის მეშვეობით იგი სწავლობს ინდივიდის ცხოვრების წესს, მის მოთხოვნილებებს და შემდეგ მას პირდაპირი მარკეტინგის მიზნებისთვის იყენებს.[235]

ალან ვესტინმა საკუთარ ნაშრომში „საინფორმაციო ტექნოლოგია დემოკრატიულ სახელმწიფოში" კონტროლის ერთ-ერთ მექანიზმად მონაცემებზე დაკვირვება დაასახელა. [236] დაკვირვების ეს პასიური ფორმა პიროვნების შესახებ მრავალ ინფორმაციას გვაწვდის. სწორედ მომხმარებელთა პერსონალურ ინფორმაციაზე დაკვირვებით იქმნება ციფრული პორტრეტი, რომელსაც კომპანიები საკუთარი მიზნების მისაღწევად იყენებენ. ანალოგიურად, სამართალდამცავი ორგანოების მიერ

[235] *Lloyd J. I.,* Privacy, technology and the law, Information Technology Law, 4th edition, Oxford University Press, 2004, 45.

[236] *Westin F. A.,* Information technology in a democracy, USA, Harvard University Press, 1971, 68.

ინდივიდთა შესახებ მონაცემების დამუშავებით შესაძლებელი ხდება მათი ციფრული პორტრეტის შედგენაც.

ცხადია, რომ საინფორმაციო ეპოქაში პერსონალური ინფორმაცია და მონაცემთა დამუშავება მჭიდროდ არის დაკავშირებული პირადი ცხოვრების ხელშეუხბლობის ძირითად უფლებასთან. განსაკუთრებით ისეთ გარემოში, სადაც ყოველდღიური მოხმარებისთვის აუცილებელი ნივთები იქნება ეს პერსონალური კომპიუტერი, მობილური ტელეფონი, ავტომობილი [237] თუ სხვა, ინტერნეტთან არის დაკავშირებული. ინდივიდის მონაცემებთან დაკავშირებული ნებისმიერი აქტივობა პირად ცხოვრებაში ჩარევას გულისხმობს, რამაც შეიძლება მისი დარღვევაც კი გამოიწვიოს. შესაბამისად, მნიშვნელოვანია მონაცემთან დაკავშირებული ნებისმიერი საქმიანობა, განსაკუთრებით კი საპოლიციო და საგამოძიები საქმიანობის პროცესში კანონის სრული დაცვით განხორციელდეს.

2. პირადი ცხოვრების ხელშეუხებლობის უფლება და კომუნიკაციის კონფიდენციალურობა

პირადი ცხოვრების ხელშეუხებლობა, როგორც ადამიანის ფუნდამენტური უფლება არაერთი საერთაშორისო სამართლებრივ აქტით არის განმტკიცებული. იგი მეტია ვიდრე უბრალოდ „მარტოდ დარჩენის“ და განცალკევების შესაძლებლობა. მათ შორის ის მოიცავს პიროვნების იდენტობას, მის პიროვნულ სივრცეს, საკუთარი პერსონალური მონაცემების შენახვისა და გავრცელების საკითხს, [238] სექსუალურ ცხოვრებასა და პიროვნების სოციალურ კავშირებს და ა.შ. [239] უფლების ფართო ხასიათის მიუხედავად, მეცნიერთა გარკვეულმა ნაწილმა სცადა მისი ცნების

[237] თანამედროვე ავტომობილი მუდმივ რეჟიმში უგზავნის მწარმოებელს ინფორმაციას ავტომობილისა და მისი ძირითადი კომპონენტების ფუნქციონირების, მძღოლის მართვის სტილის შესახებ. ავტომობილში დამონტაჟებული გასართობი მოწყობილობა, რომელიც ხშირად დაკავშირებულია ინტერნეტთან ან მობილურ ტელეფონთან, ნავიგაციის ფუნქციით არის აღჭურვილი, ინახავს და გადასცემს მონაცემებს ჩვენი კომუნიკაციის, შემავალი და გამავალი ზარების, შეტყობინებების, ადგილმდებარეობის შესახებ. მონაცემთა ასეთმა ნაკადმა კი შეიძლება არაერთი სამართლებრივი საკითხი წამოჭრას პირადი ცხოვრების უფლების დაცვის ჭრილში. იხ. *Kronke C.,* Data Regulation in the Internet of Things, Paradigms of Internet Regulation in the European Union and China, *Kronke, Muller, Yu, Tian,* (eds.), 2018, 84-86.

[238] *Leander v. Sweden,* [1987], ECHR, 116. იხ. *Murray v. United Kingdom*, [1994] ECHR, 84-86.

[239] *Harris D.J., O'Boyle M., Warbrick C., Buckley C., Kamber K.,* Law of the European Convention on Human Rights, London, Oxford University Press, 2018, 303.

განსაზღვრა და ასე მაგალითად, ტომას ქულის,[240] სამუელ უორენისა და ლუის ბრანდეისის[241] მიერ შემოთავაზებული განმარტებით იგი „მარტოდ დარჩენის“ უფლებას გულისხმობს. სხვა ავტორების ხედვით კი პირადი ცხოვრება ინფორმაციის კონფიდენციალურობასთან არის დაკავშირებული[242] და ადამიანთან და მის პერსონალურ ინფორმაციასთან საზოგადოების მხრიდან წვდომის შეზღუდვას გულისხმობს.[243]

განსხვავებული გზა აირჩია ადამიანის უფლებათა ევროპულმა სასამართლომ. მას წარმოუდგენლად და მათ შორის მიზანშეუწონლად მიაჩნია „პირადი ცხოვრების“ ცნების ამომწურავად განსაზღვრა, ვინაიდან ეს ინდივიდთა გარკვეულ საზღვრებში მოქცევას გამოიწვევდა.[244] ამიტომ, პირადი ცხოვრების უფლების კონცეფცია სასამართლო პრაქტიკით ფართოდ განიმარტება. მოცემული უფლების და კერძოდ, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის ძირითად მიზანს, სახელმწიფოს მხრიდან ინდივიდის პირად ცხოვრებაში თვითნებური ჩარევისგან დაცვა წარმოადგენს.[245] ეს სახელმწიფოს ნეგატიური ვალდებულების კლასიკური გამოხატულებაა,[246] თუმცა, ნეგატიურ ვალდებულებასთან ერთად სახელმწიფოს პოზიტიური ვალდებულებაც გააჩნია, რაც სათანადო ზომების მიღებითა და აქტიური მოქმედებით უფლების პატივისცემისა და დაცვის უზრუნველყოფას გულისხმობს.[247] მიუხედავად იმისა, რომ ადამიანის უფლებათა ევროპული სასამართლო არ იძლევა პირადი ცხოვრების ერთიან განმარტებას,[248] სასამართლომ მისი პრაქტიკის მანძილზე მეტნაკლებად განსაზღვრა საკითხები, რომლებიც პირადი ცხოვრების დაცვის ფარგლებში ექცევა. პირადი ცხოვრების კონცეფცია მოიცავს ფიზიკურ და მორალურ

---

[240] *Lloyd J. I.,* Privacy, technology and the law, Information Technology Law, 4th edition, Oxford University Press, 2004, 46.

[241] *Warren S., Brandeis D. L.,* The Right to Privacy, Harvard Law Review 4, 1890, 193–220.

[242] *Moore D. A.,* Privacy Rights – Moral and Legal Foundations, USA, The Pennsylvania State University Press, 2021, 12.

[243] იქვე, 25.

[244] *Niemietz v. Germany,* [1992] ECHR (Ser. A), 29. იხ. *Costello-Roberts v. The United Kingdom,* [1993] ECHR (Ser. A), 36.

[245] *Liber v. France,* [2018] ECHR, 40-42.

[246] *Kroon and Others v. the Netherlands*, [1994] ECHR, 31.

[247] *Barbulescu v. Romania*, [2017] ECHR, 108-110.

[248] *Niemietz v. Germany,* [1992] ECHR, 29. იხ. *Pretty v. The United Kingdom,* [2002] ECHR, 61.

ხელშეუხებლობას, [249] სქესობრივი ცხოვრების საიდუმლოებას, [250] ოჯახურ ცხოვრებას, [251] მიმოწერას, [252] პროფესიულ და კომერციულ საქმიანობას, [253] პერსონალურ მონაცემთა დაცვას [254] და სხვა მნიშვნელოვან საკითხებს, რომლებიც პიროვნების თავისუფალი განვითარებისთვისაა საჭირო. იგი არ არის შეზღუდული ე.წ. „შიდა წრით“ და არ გამორიცხავს პიროვნების გარე სამყაროსთან ურთიერთობას.[255] “პირადი სოციალური ცხოვრების“ უფლება ინდივიდს სხვებთან ურთიერთობის ქონის და მათთან ერთად მისი განავითარების უფლებას ანიჭებს.[256] მეტიც, პირადი სოციალური ცხოვრება დაცულია სამუშაო ადგილზეც და პირადი ცხოვრებებისა და მათ შორის მიმოწერის კონფიდენციალურობის პატივისცემა გარანტირებულია.[257]

თანამედროვე მსოფლიოში ტექნოლოგიური განვითარების ფონზე მიმოწერის და ზოგადად კომუნიკაციის კონფიდენციალურობამ გარდამტეხი მნიშვნელობა შეიძინა პირადი ცხოვრების პატივისცემის თვალსაზრისით. შესაბამისად არაერთი განმარტება გააკეთა ადამიანის უფლებათა ევროპულმა სასამართლომ იმის შესახებ თუ რას გულისხმობს კომუნიკაციის კონფიდენციალურობის დაცვა. იგი მოიცავს როგორც ოჯახის წევრებს შორის[258], ისე სხვებთან[259] არსებულ სატელეფონო საუბრებს, სატელეფონო ზარებს კერძო თუ სამსახურეობრივი დაწესებულებიდან [260] , ინფორმაციას კომუნიკაციის განხორციელების თარიღის, ხანგრძლივობისა და აბონენტების ნომრების შესახებ, [261] მონაცემებს მობილური თუ სხვა ნებისმიერი

[249] *X and Y v. The Netherlands,* [1985] ECHR, 22. იხ. *Osman v. The United Kindgom*, [1998] ECHR, 128-130. *Dordevic v. Croatia*, [2012] ECHR, 141-143.

[250] *B v. France,* [1992] ECHR, 63. იხ. *P.G and J.H v. The United kingdom*, [2001] ECHR, 56. *Orlandi and Others v. Italy*, [2017] ECHR, 143. *Beizaras and Levickas v. Lithuania*, [2020], ECHR, 109.

[251] *Marckx v. Belgium,* [1979] ECHR, 31.

[252] *Halford v. The United Kingdom,* [1997] ECHR, 44.

[253] *Fernandez Martinez v. Spain,* [2014] ECHR, 110. იხ. *Barbulescu v. Romania,* [2017] ECHR, 71. *Antovic and Mirkovic v. Montenego*, [2017] ECHR, 42. *Denisov v. Ukraine,* [2018] ECHR, 100. *Lopez Ribalda and Others v. Spain*, [2019] ECHR, 92-95. *Satakunnan Markkinaporssi OY and Satamedia OY v. Finland,* [2017] ECHR, 130.

[254] *Yonchev v. Bulgaria,* [2018] ECHR, 49-54. იხ. *Z v. Finland,* [1997] ECHR, 95. *Klass and Others v. Germany*, [1978] ECHR, 36. *Bykov v. Russia,* [2009] ECHR, 81-83.

[255] Denisov v. Ukraine, [2018] ECHR, 96.

[256] Botta v. Italy, [1998] ECHR, 32.

[257] *Barbulescu v. Romania*, [2017] ECHR, 80.

[258] *Margareta and Roger Andersson v. Sweden*, [1992] ECHR, 72.

[259] *Klass and Others v. Germany*, [1978] ECHR, 21. *Malone v. The United Kingdom*, [1984] ECHR, 64.

[260] *Halford v. The United Kigdom*, [1997] ECHR,44. *Copland v. The United Kingdom*, [2007] ECHR, 41.

[261] *P.G and J.H v. The United Kingdom*, [2001] ECHR, 42.

კომპიუტერული მოწყობილობიდან,[262] ელექტრონულ შეტყობინობას,[263] მონაცემებს ინტერნეტის გამოყენების შესახებ [264] და მონაცემებს, რომელიც განთავსებულია სერვერებსა[265] თუ კომპიუტერულ მონაცემთა შემნახველ მოწყობილობებში.[266]

ცხადია, პირადი ცხოვრების ხელშეუხებლობის უფლება ინდივიდის ცხოვრების ყველა ასპექტთან მჭიდროდ არის დაკავშირებული. დიდია თანამედროვე ტექნოლოგიათა ზეგავლენაც ადამიანთა ყოველდღიურობაზე, განსაკუთრებით კი მათ მიერ განხორციელებულ კომუნიკაციაზე, რაც პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის საკითხს გამუდმებით ახალი გამოწვევების წინაშე აყენებს. შესაბამისად, ადამიანის უფლებათა ევროპულმა სასამართლომ კომუნიკაციის საიდუმლოების განმარტებისას, მისი განხორციელების ყველა შესაძლო საშუალება თუ მოვლენა გაითვალისწინა და მათში ტრადიციულთან ერთად, კომუნიკაციის თანამედროვე საშუალებებით გადაცემული, დამუშავებული თუ შენახული ინფორმაციაც მოაქცია.

2.1. უფლების მართლზომიერი შეზღუდვის საფუძვლები

ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვის საფუძვლებს ზუსტად და ამომწურავად განსაზღვრავს. შეიძლება ითქვას, რომ სხვა გამონაკლისების გათვალისწინება დაუშვებელია (numerus clausus).[267] მიზანს, სახელმწიფოს მხრიდან ინდივიდთა ძირითად უფლებაში თვითნებურად ჩარევის შესაძლებლობის აღმოფხვრა წარმოადგენს. აგრეთვე, სამოქალაქო და პოლიტიკური უფლებების შესახებ პაქტის მე-17 მუხლის მიხედვით დაუშვებელია პირის პირად თუ ოჯახურ ცხოვრებასა და კორესპონდენციაში თვითნებური ან უკანონო ჩარევა. ასევე მისი ღირსებისა და რეპუტაციის უკანონო ხელყოფა.[268] ჩარევა შეიძლება მხოლოდ კანონის საფუძველზე განხორციელდეს, ხოლო ჩარევისას თვითნებობისგან დაცვის მიზნით,

[262] *Saber v. Norway,* [2020] ECHR, 48.
[263] *Copland v. The United Kingdom*, [2007] ECHR, 41.
[264] იქვე.
[265] *Wieser and Bicos Beteiligungen GmbH v. Austria*, [2008] ECHR, 45.
[266] *Petri Sallinen and Others v. Finland*, [2005] ECHR,71. *Iliya Stefanov v. Bulgaria*, [2008] ECHR, 42.
[267] *Corstens G., Pradel J.*, European Criminal Law, The Hague, The Netherlands Kluwer Law International, 2002, 449.
[268] International Covenant on Civil and Political Rights (ICCPR), 1966.

მათ შორის თუ ის კანონის საფუძველზე ხორციელდება, გამოყენებული ღონისძიება პაქტის მიზნებისა და დებულებების შესაბამისი და ამავდროულად მოცემულ სიტუაციაში გონივრული უნდა იყოს. ჩარევა კი გონივრულია თუ ღონისძიება განპირობებულია ობიექტური კრიტერიუმებითა და ის დასახული მიზნის პროპორციულია. [269] ამ მხრივ იდენტურია ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაც.[270]

შესაბამისად, პირადი და ოჯახური ცხოვრების უფლების შეზღუდვის მართლზომიერების დადგენისთვის საყურადღებოა სამი ასპექტის შეფასება. კერძოდ, შეზღუდვა არის თუ არა კანონის შესაბამისი, ემსახურება თუ არა ის სოციალური ღირებულებების დაცვას ანუ ლეგიტიმურ მიზანს და მესამე, არსებობს თუ არა დემოკრატიულ საზოგადოებაში მისი გამოყენების აუცილებლობა.

2.2. კანონის შესაბამისი

ადამიანის უფლებათა ევროპული სასამართლო გამუდმებით მიუთითებს, რომ საჯარო ხელისფლების მხრიდან ნებისმიერი ჩარევა პიროვნების პირად და ოჯახურ ცხორებაში, სახლსა თუ მიმოწერაში კანონის შესაბამისად უნდა განხორციელდეს.[271] საწყის ეტაპზევე მნიშვნელოვანია განისაზღვროს თუ როგორია ადამიანის უფლებათა ევროპული სასამართლოს „კანონის“ კონცეფცია. ყურადსაღებია, რომ კანონის გაგება მხოლოდ ფორმალური სამართლით არ არის შეზღუდული და მასში მატერიალური და პრეცენდენტული სამართალიც მოიაზრება. [272] აგრეთვე, შეცდომა იქნება რაიმე სახის მითითება კონტინენტური ევროპის ან ანგლო-ამერიკული სამართლის სისტემაზე. შესაბამისად კონცეფციაში ექცევა როგორც დაწერილი, ისე დაუწერელი სამართალი.

„კანონის შესაბამისად“ გულისხმობს შეზღუდვის არა მარტო შიდა, ეროვნულულ კანონმდებლობასთან შესაბამისობას, არამედ მის „კანონის ხარისხთანაც“ თანხვედრას. [273] თავის მხრივ „კანონის ხარისხის“ მოთხოვნებიდან გამომდინარე

[269] *Toonen v. Australia,* Communication No. 488/1992, Human Rights Committee, 6.4.
[270] Golder v. United Kindgom, [1975] ECHR, 44.
[271] *Vavricka and Others v. The Czech Republic*, [2021] ECHR, 267-269.
[272] *Chappell v. United Kindgom,* [1989] ECHR, 52.
[273] Big Brother Watch and Others v. The United Kingdom, [2021] ECHR, 332.

მნიშვნელოვანია ორი ელემენტის არსებობა, როგორიც არის ხელმისაწვდომობა და განჭვრეტადობა.

ა) ხელმისაწვდომობა - ხელმისაწვდომობის მოთხოვნის მიხედვით მოქალაქეს, მოპასუხეს ან ბრალდებულს კონკრეტული გარემოებების მიხედვით უნდა შეეძლოს იმის გარკვევა თუ მოცემულ შემთხვევაში, რომელი სამართლებრივი ნორმა გამოიყენება. მოცემული მოთხოვნა დაკმაყოფილებად ითვლება, როდესაც კანონი გამოქვეყნებულია. [274] მკაცრია მიდგომა, როდესაც საქმე ფარულ საგამოძიებო მოქმედებებს ეხება. ვინაიდან აღნიშნული ფარულად ხორციელდება და თვითნებობის რისკი მაღალია, აუცილებელია ხელისუფლებისთვის მინიჭებული დისკრეციის გამოყენების ფარგლების, ხერხის საკმარისი სიცხადით განსაზღვრა, რათა ინდივიდს თვითნებური ჩარევისგან დაცვის ადეკვატური დაცვის საშუალება მიეცეს.[275]

ბ) განჭვრეტადობა - აღნიშნული მოთხოვნა დაკავშირებულია კანონის განსაზღვრულობის მოთხოვნასთან. (Lex Certa პრინციპი). პრინციპის მიხედვით ნორმა მკაფიოდ, საკმარისი სიზუსტით უნდა იყოს ფორმილურებული, რომ ადრესატმა შეძლოს საკუთარი ქმედების მასთან შესატყვისება.[276] ნათლად უნდა იყოს განსაზღვრული ხელისუფლების დისკრეციის ფარგლები და როგორც ევროპული სასამართლოს პრაქტიკით არის ჩამოყალიბებული, მართალია კანონის განჭვრეტადობის მოთხოვნა ფარული საგამოძიებო მოქმედებების მხრივ განსხვავებულია ვიდრე სხვა სფეროში, [277] თუმცა აუცილებელია ადეკვატური გარემოებებისა და პირობების მკაფიოდ გათვალისწინება ეროვნული კანონმდებლობით, რათა ინდივიდს ჰქონდეს წარმოდგენა სახელმწიფო ორგანოთა მიერ ფარული ღონისძიებების გამოყენების შესახებ. [278] მეტიც, პრეცენდენტული სამართლით, სასამართლომ უფლებამოსილების ბოროტად გამოყენების თავიდან

[274] *Silver v. United Kingdom,* [1983] ECHR, 87. *Leander v. Sweden*, [1987] ECHR,50-54. *Rotaru v. Romania*, [2000] ECHR, 52-54.
[275] *Malone v. The United Kingdom*, [1984] ECHR, 67.
[276] *Lebois v. Bulgaria*, [2017] ECHR, 66.
[277] *Leander v. Sweden,* [1987] ECHR, 51.
[278] Roman Zakharov v. Russia, [2015] ECHR, 229.

ასაცილებლად ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით დამატებითი მინიმალური გარანტიები შეიმუშავა. კერძოდ, კანონით უნდა განისაზღვროს დანაშაულთა წრე, რომელთა შემთხვევაშიც დასაშვები იქნება ღონისძიების გამოყენება, პირთა წრე, რომელთა მიმართაც შეიძლება გამოყენებულ იქნას საგამოძიებო მოქმედება, მისი ხანგრძლივობა, შეგროვებული მონაცემების გამოკვლევის, გამოყენების, შენახვის, გადაცემის უსაფრთხოების, წაშლის და განადგურების პროცედურები.[279]

კანონის განჭვრეტადობისას ყურადღება გამახვილებულია **„საკმარის“** და არა **„აბსოლუტურ“** სიზუსტეზე, ვინაიდან უკანასკნელის მიღწევა შეუძლებელია, ხოლო კანონის სხვადასხვა გარემოებებთან თანხვედრის აუცილებლობიდან გამომდინარე გარკვეული ბუნდოვანება გამართლებულია.[280]

ერთობლიობაში კანონის ხელმისაწვდომობისა და განჭვრეტადობის კრიტერიუმები მნიშვნელოვან როლს თამაშობენ პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის მხრივ და არამარტო.[281] რაც უფრო ბუნდოვანია უფლების მზღუდავი ნორმა, მით უფრო დიდია რისკი უფლების დარღვევის. ამასთან, აღნიშნული მოთხოვნა ეფექტური სასამართლო კონტროლის წინაპირობასაც წარმოადგენს. როდესაც ნორმა მკაფიო და ზუსტია, ნათელია მისი მოქმედების ფარგლები, ადვილია უფლების დარღვევის ფაქტის მტკიცება და შესაბამისად, მიყენებული ზიანის ანაზღაურების მოთხოვნა. თუმცა, ღია ტიპის საგამოძიებო მოქმედებებთან შედარებით, როგორც ზემოთ ითქვა, ფარული საგამოძიებო მოქმედების მხრივ დამატებითი გარანტიებია საჭირო.

2.3. ლეგიტიმური მიზანი

ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მე-2 ნაწილი ამომწურავად განსაზღვრავს უფლებაში ჩარევის ლეგიტიმურ მიზნებს. საჯარო ხელისუფლების მხრიდან უფლებაში ჩარევა გამართლებულია თუ იგი ხორციელდება კანონის შესაბამისად და აუცილებელია ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების, ქვეყნის ეკონომიკური კეთილდღეობის, უწესრიგობისა თუ

[279] იქვე, 231.
[280] *Sunday Times v. United Kingdom*, [1979] ECHR, 49.
[281] *Olsson v. Sweden,* [1988[ECHR, 61.

დანაშაულის თავიდან ასაცილებლად, ჯანმრთელობისა ან მორალის, ანდა სხვათა უფლებებისა და თავისუფლებების დასაცავად.[282]

ლეგიტიმური მიზნის ტესტი არ არის გარდამტეხი მნიშვნელობის ევროპული სასამართლო მიერ გადაწყვეტილების მიღების პროცესში, თუმცა როგორც სასამართლო პრაქტიკამ აჩვენა მას თანამედროვე ტექნოლოგიების განთავსების და გამოყენების ზღვრის დასადგენად იყენებენ. [283] მაგალითისთვის, ევროპული სასამართლო დაეთანხმა მთავრობის პოზიციას, რომ თითის ანაბეჭდის და დნმ-ის ინფორმაციის შენახვა დანაშაულის გამოვლენის და პრევენციის ლეგიტიმურ მიზანს ემსახურება მიუხედავად იმისა, რომ ამ ინფორმაციის თავდაპირველად მოპოვების მიზანი კონკრეტული პირის დანაშაულთან კავშირის დადგენა წარმოადგენდა, ხოლო მისი გარკვეული დროით შენახვა უფრო ფართო მიზანს ემსახურება, როგორიცაა სამომავლოდ დამნაშავეების იდენტიფიცირებაში დახმარება. [284] ანალოგიურად, სატელეფონო საუბრის ფარული მიყურადება, ინფორმაციის შენახვა და გამჟღავნება სასამართლომ უწესრიგობის ან დანაშაულის პრევენციისა და სხვათა უფლებების დაცვის მიზნით ლეგიტიმურად მიიჩნია. [285] ასევე, დანაშაულის გამოვლენისა და პრევენციის პროცესში სასამართლომ სამეთვალყურეო კამერის როლს გაუსვა ხაზი, თუმცა მსჯელობისას ლეგიტიმურ მიზანზე მეტად ყურადღება უფლებაში ჩარევის პროპორციულობას მიაპყრო.[286]

ცხადია, რომ ადამიანის უფლებათა ევროპული სასამართლო დადგენილი პრაქტიკით სამართალწარმოების პროცესში თანამედროვე ტექნოლოგიების გამოყენების და მათი დახმარებით ლეგიტიმური მიზნის მიღწევის მომხრეა, თუმცა აღნიშნული აუცილებლად თანაზომიერების პრინციპის დაცვით უნდა განხორციელდეს.

2.4. აუცილებელი დემოკრატიულ საზოგადოებაში

ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მე-2 ნაწილით გათვალისწინებული საფუძვლის „აუცილებელი დემოკრატიულ საზოგადოებაში“

[282] *Vavricka and Others v. The Czech Republic*, [2021] ECHR, 272.
[283] *Murphy T., Cuinn O. G.,* Works In Progress: New Technologies and the European Court of Human Rights, Human Rights Law Review 10(4), 2010, 618.
[284] *S. and Marper v. The United Kingdom,* [2008], ECHR, 100.
[285] *Adomaitis v. Lithuania,* [2022] ECHR, 84.
[286] Peck v. The United Kingdom, [2003] ECHR, 79, 87.

ფარგლებში მოიაზრება როგორც შეზღუდვის საფუძველიანობა, ისე სუბსიდიარულობა და თანაზომიერება. [287] ადამიანის უფლებათა ევროპული სასამართლოს მიერ დადგენილი პრაქტიკის მიხედვით გამოყენებული ღონისძიება მიზნის მიღწევის გამოსადეგი საშუალება უნდა იყოს, თუმცა სუბსიდიარულობის პრინციპიდან გამომდინარე თუ პროცედურულ სამართალში მიზნის მიღწევის სხვა, უფლების ნაკლებ მზღუდავი საშუალება მოიპოვება, პრიორიტეტი მას უნდა მიენიჭოს. პროპორციულობის თანახმად კი გამოყენებული ღონისძიების მოცულობასა და ლეგიტიმურ მიზანს შორის სათანადო ბალანსი უნდა არსებობდეს.[288] მნიშვნელოვანია, ყურადღება გავამახვილოთ სიტყვა „აუცილებელის“ ფუნქციურ დატვირთვაზე. ადამიანის უფლებათა ევროპული სასამართლოს მიდგომით იგი არ იძლევა ლავირების საშუალებას და მისი ჩანაცვლება ისეთი ტერმინებით როგორებიცაა გამოსადეგი, გონივრული, სასურველი და სხვა, მიუღებელია. შესაბამისად, იგი მხოლოდ და მხოლოდ აუცილებელი უნდა იყოს „მწვავე სოციალური საჭიროების“ დასაცავად.[289]

დასადგენად, არის თუ არა ღონისძიების გამოყენება „აუცილებელი“, მთლიანი სამართალწარმოების გათვალისწინებით სასამართლო აფასებს სახელმწიფოს დისკრეციის შესაძლებლობას.[290] შეფასების ზღვრის მოცულობა დამოკიდებულია რიგ ფაქტორებზე, მათ შორის, კონვენციით დაცული უფლების შინაარსზე, ადრესატისთვის მის მნიშვნელობაზე, ჩარევის ინტენსივობასა და დაცვის ობიექტზე. ზღვარი მით უფრო იზღუდება როდესაც სასწორზე ინდივიდის ისეთი უფლება დევს, რომელიც აუცილებელია „ინტიმური“ ან ძირითადი უფლებებით სარგებლობისთვის. [291] შესაბამისად, შეზღუდული უფლების მართლზომიერების შესაფასებლად პროპორციულობის (თანაზომიერების) პრინციპს გარდამტეხი მნიშვნელობა ენიჭება. თანაზომიერების მოთხოვნის თანახმად სახელმწიფოს მიერ გატარებული ღონისძიება, რომელიც უფლების შეზღუდვას იწვევს, მწვავე საზოგადოებრივი საჭიროების პროპორციული უნდა იყოს. პროპორციულობის

[287] *Corstens G., Pradel J.*, European Criminal Law, The Hague, The Netherlands, Kluwer Law International, 2002, 453.

[288] *Observer and Guardian v. United Kingdom*, [1991] ECHR, 59.

[289] *Handyside v. United Kingdom*, [1976] ECHR, 48.

[290] *Paradiso and Campanelli v. Italy,* [2017] ECHR, 179-184. იხ. *Klaus Muller v. Germany,* [2020] ECHR, 66.

[291] იქვე.

მოთხოვნა კი დაკმაყოფილებულია, როდესაც საჯარო და პირის კერძო ინტერესს შორის ბალანსი დაცულია. ბალანსის დაცვის მნიშვნელობა კი გამოძიების პროცესში თანამედროვე ტექნოლოგიების გამოყენების ფონზე უფრო მეტად იზრდება, ვინაიდან როგორც ევროპულმა სასამართლომ განმარტა კონკურენტულ ინტერესებს შორის სათანადო ბალანსის დაცვის გარეშე თანამედროვე სათვალთვალო ტექნოლოგიების გამოძიების მიზნებისთვის გამოყენება მნიშვნელოვნად შეასუსტებს პირადი ცხოვრების უფლებით დაცულ ინტერესებს.[292]

3. მართლზომიერი შეზღუდვის პირობები ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მიხედვით

ნიშანდობლივია, რომ ევროკავშირის ფუნდამენტურ უფლებათა ქარტია განსხვავებით ადამიანის უფლებათა ევროპული კონვენციისგან დამოუკიდებელი სახით იცავს როგორც პირადი და ოჯახური ცხოვრების, ისე პერსონალურ მონაცემთა დაცვის უფლებას.[293] თუმცა, იმის გათვალისწინებით, რომ ისინი არ მიეკუთვნებიან აბსოლუტურ უფლებათა კატეგორიას, ქარტიის 52-ე მუხლის პირველი პუნქტი უშვებს მათი შეზღუდვის შესაძლებლობას, თუ ის გათვალისწინებულია კანონით, შეზღუდვით არ ილახება ამ უფლებებისა და თავისუფლებების არსი, შეზღუდვა აუცილებელი და პროპორციულია, იგი ემსახურება ევროკავშირის მიერ აღიარებულ საჯარო ინტერესის მიზნებს, ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად. [294] შესაბამისად, უფლებაში ჩარევის გამართლებისთვის აუცილებელია დაკმაყოფილებულ იქნას ქარტიით გათვალისწინებული მართლზომიერი შეზღუდვის წინაპირობები.

3.1. შესაბამისობა კანონთან

ადამიანის უფლებათა ევროპული კონვენციით დადგენილი მოთხოვნის მსგავსად ქარტიის მიზნებისთვისაც კანონთან შესაბამისობის კრიტერიუმი უფლებაზე დაწესებული შეზღუდვის კანონით მოწესრიგებას მოითხოვს, რომელიც ხელმისაწვდომი, განჭვრეტადი და საკმარისი სიცხადით იქნება ფორმულირებული.

[292] *S. and Marper v. The United Kingdom,* [2008] ECHR, 112.
[293] Charter of Fundamental Rights of The European Union, 2012, article 7-8.
[294] *Volker unda Markus Schecke GbR and Hartmunt Eifert v. Land Hessen,* [2010] CJEU, 50.

კანონით მკაფიოდ უნდა განიმარტოს უფლებამოსილი ორგანოს საქმიანობის ფარგლები და ფორმა, რათა უზრუნველყოფილ იქნას ინდივიდთა დაცვა უფლებაში თვითნებური ჩარევისგან.

როდესაც ქარტიის მიზნებისთვის „კანონთან შესაბამისობის“ კრიტერიუმზე ვმსჯელობთ უნდა გვახსოვდეს, რომ „კანონის ხარისხის“ მოთხოვნასთან დაკავშირებული ადამიანის უფლებათა ევროპული სასამართლოს განმარტებები აქტუალური და რელევანტურია.[295] შესაბამისად, მსჯელობისას მხედველობაში უნდა იქნას მიღებული საკითხისადმი სტრასბურგის სასამართლოს მიერ დამკვიდრებული განმარტებანი.

3.2. ძირითადი უფლების არსის პატივისცემა

მიუხედავად იმისა, რომ ქარტიით დაცული უფლების შეზღუდვა დასაშვებია, ამან უფლების არსის ხელყოფა არ უნდა გამოიწვიოს. თუ უფლების შეზღუდვის შედეგად ილახება მისი არსი, შეზღუდვა უკანონოდ უნდა ჩაითვალოს.[296]

ამ მხრივ საინტერესოა მართლმსაჯულების ევროპული სასამართლოს მსჯელობა “Facebook”-ის მიერ შვილობილი კომპანიისთვის ავსტრიის მოქალაქის პერსონალური მონაცემების გადაცემის ფაქტის კანონიერებასთან დაკავშირებით. [297] ფაქტობრივი გარემოებების მიხედვით, განმცხადებლის მონაცემები სოციალური ქსელის „Facebook”-ის ირლანდიურმა შვილობილმა კომპანიამ კომისიის გადაწყვეტილების[298] საფუძველზე „Facebook” inc.-ს და აშშ-ში მდებარე სერვერებს გადასცა. მოქალაქის მტკიცებით აშშ-ში არსებული კანონმდებლობა ვერ უზრუნველყოფდა პერსონალური მონაცემების სათანადო დაცვას, რომლის არგუმენტაციასაც წინ ედვარდ სნოუდენის 2013 წლის სკანდალი უძღოდა. პირის, რომელმაც აშშ-ს ეროვნული უსაფრთხოების

---

[295] *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* Opinion of Advocate General Cruz Villalon, [2011] CJEU, 100.

[296] Handbook on European Data Protection Law, 2018, 44. <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].

[297] Maximillian Schrems v. Data Protection Commissioner, [2015] CJEU.

[298] Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000. იხ. Communication from The Commission to The European Parliament and The Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 2013. < https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF> [05.06.23].

სააგენტო ისეთი ორგანიზაციების პირდაპირი წვდომით მიყურადებაში ამხილა, როგორიცაა „Facebook".

სასამართლომ, ქარტიის გათვალისწინებით კომისიის გადაწყვეტილების მართებულობის შეფასებისას განმარტა, რომ ფუნდამენტური უფლების დაცვა მის შეზღუდვას მხოლოდ მკაცრი აუცილებლობის პირობებში გულისხმობს, ხოლო კანონმდებლობა, რომელიც ხელისუფლებას აძლევს ზოგადი წვდომის საშუალებას კომუნიკაციის შინაარსზე, ზიანს აყენებს ქარტიის მე-7 მუხლით გარანტირებულ უფლებას. თუ აშშ-ს ხელისუფლებას ყოველგვარი ობიექტური გამართლების გარეშე წვდომა ექნება ელექტრონული კომუნიკაციის შინაარსზე, ხოლო არ იარსებებს უფლებამოსილების ბოროტად გამოყენებისგან დაცვის სათანადო მექანიზმები, უფლება დაკარგავს მის მნიშვნელობას. შესაბამისად, სასამართლოს შეფასებით ამერიკის შეერთებული შტატები ვერ შეასრულებდა „უსაფრთხო ნავსადგურის როლს" და ქარტიასთან ერთობლიობაში ვერ დაიცავდა ევროკავშირის დირექტივით განატირებულ უფლებებს.

აგრეთვე, უფლების არსის პატივისცემას ეხმიანება ევროკავშირის მართლმსაჯულების სასამართლო შპს ირლანდიის ციფრული უფლებების საქმეში.[299] კერძოდ, სასამართლომ მონაცემთა შენახვის დირექტივის[300] შესაბამისობის საკითხი ქარტიის მე-7 და მე-8 მუხლებთან მიმართებით განიხილა. დირექტივის თანახმად ელექტრონული კომუნიკაციის პროვაიდერ კომპანიებს მომხმარებელთა გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების 6 თვიდან 24 თვემდე შენახვის ვალდებულება ჰქონდათ,[301] რაც საგამოძიებო ორგანოებს მძიმე დანაშაულის პრევენციის, გამოძიების, დამნაშავის გამოვლენისა და დასჯის მიზნით მათზე წვდომის შესაძლებლობას აძლევდა. შესანახი მონაცემები ეხებოდა ინფორმაციას კომუნიკაციის წყაროს, დანიშნულების ადგილის, თარიღის, დროის,

[299] *Digital Rights Ireland Ltd* (C-293/12) *v. Minister of Communications, Marine and Natural Resources and Others and Kartner Landesregierung and Others* (C-594/12), GC, 2014. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=511178> [05.06.23].

[300] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC >https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32006L0024> [05.06.23].

[301] იქვე, მუხლი 6.

ხანგრძლივობის, სატელეფონო ნომრების, ინტერნეტ პროტოკოლისა (IP) და ადგილმდებარეობის, შესახებ.[302] მიუხედავად იმისა, რომ დირექტივა კომუნიკაციის შინაარსის შენახვის არც უფლებას და არც ვალდებულებას ითვალისწინებდა, ზემოთ ჩამოთვლილი მონაცემები ერთობლიობაში განხილვისას ადამიანთა პირად ცხოვრებაზე იმდენად ზუსტი დასკვნების გაკეთების შესაძლებლობას იძლეოდა, რომ ადვილი მისახვედრი იყო ინდივიდთა ყოველღიური ჩვევები, აქტივობები, სოციალური კავშირები და ა.შ. მართალია, აღნიშნული მძიმე ჩარევას წარმოადგენდა პირადი ცხოვრებისა და მონაცემების დაცვის უფლებაში, თუმცა ვინაიდან დირექტივა გამორიცხავდა ელექტრონული კომუნიკაციის შინაარსის მოპოვების შესაძლებლობას და ამასთან, იგი პროვაიდერ კომპანიებს ავალდებულებდა მონაცემთა დაცვისა და უსაფრთხოების გარკვეული პრინციპებით მოქმედებას, სასამართლოს განმარტებით პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა დაცვის უფლების არსის ხელყოფას ადგილი არ ჰქონია.

3.3. პროპორციულობა

პროპორციულობის მოთხოვნის თანახმად შეზღუდვის შედეგად უფლებისთვის მიყენებული ზიანი მიღებულმა სარგებელმა უნდა გადაწონოს. [303] ამასთან, გამოყენებული ღონისძიება დასახული მიზნის მიღწევის შესაფერისი და აუცილებელი საშუალება უნდა იყოს, რაც გარკვეულწილად ხელისუფლებას უფლებამოსილების განხორციელებისას ზღუდავს და გამოყენებულ საშუალებასა და დასახულ მიზანს შორის ბალანსის დაცვისკენ უბიძგებს. პროპორციულობა აუცილებლობის კრიტერიუმსაც მოიცავს, რაც გულისხმობს გამოსაყენებელი საშუალების ეფექტურობისა და ინტრუზიულობის შეფასებას. კერძოდ, შერჩეული ღონისძიება მიზნის მიღწევის სხვა საშუალებებთან შედარებით ნაკლებ ინტრუზიული უნდა იყოს. [304] როგორც წესი, ევროპული მართლმსაჯულების სასამართლო პირადი ცხოვრების ხელშეუხბელობისა და პერსონალურ მონაცემთა დაცვის უფლებების შეზღუდვის მართლზომიერების დადგენისას „მკაცრ ტესტს“

[302] იქვე, მუხლი 5.
[303] Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, EDPS, 2017, 5-6. https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf [05.06.23].
[304] იქვე.

მიმართავს და აცხადებს, რომ „შეზღუდვა გამოყენებულ უნდა იყოს იმდენად, რამდენად მკაცრადაც ეს აუცილებელია“. ხოლო თუ შეზღუდვა მკაცრად აუცილებელია, მაშინ ასევე საჭიროა მისი პროპორციულობის შეფასებაც.[305]

სწორედ შპს ირლანდიის ციფრული უფლებების [306] საქმეში ევროპის მართლმსაჯულების სასამართლომ დაადგინა, რომ მიუხედავად იმ გარემოებისა, რომ დირექტივის საფუძველზე პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევა არ ხელყოფდა უფლების არსს, დირექტივა მაინც არ შეესაბამებოდა ქარტიის მე-7 და მე-8 მუხლის მოთხოვნებს. დირექტივის საფუძველზე მაიდენტიფიცირებელი მონაცემების, გადაადგილებისა და ადგილმდებარეობის განმსაზღვრელი მონაცემების შენახვა ევროპის მთლიან მოსახლეობაზე ახდენდა ზეგავლენას, ხოლო დოკუმენტი არ ითვალისწინებდა ობიექტურ კრიტერიუმს, რომლითაც მკაცრი აუცილებლობის შესაბამისად შეიზღუდებოდა ადგილობრივი ორგანოების წვდომა მონაცემებზე. ამასთან კომპეტენტური ორგანოების წვდომა შენახულ მონაცემებზე დამოკიდებული არ იყო სასამართლოს ან სხვა დამოუკიდებელი ორაგანოს მიერ წინასწარ გაცემულ ნებართვაზე, რომელიც მონაცემებზე წვდომას მკაცრი საჭიროებით შეზღუდავდა.[307]

იდენტური ხედვა ჰქონდა ევროპული მართლმსაჯულების სასამართლოს გაერთიანებულ საქმეებში Tele2 Sverige AB, Tom Watson and Others *[308]*, რომლებიც ელექტრონული საკომუნიკაციო სერვისის მომხმარებელთა შესახებ გადაადგილების, ადგილმდებარეობის განმსაზღვრელი და მაინდენტიფიცირებელი მონაცემების ყოველგვარი დიფერენციაციის, შეზღუდვისა და გამონაკლისების გარეშე შენახვას ეხებოდა.[309] მონაცემთა შენახვისას არ იკვეთებოდა კავშირი შენახულ მონაცემებსა და ეროვნულ უსაფრთხოებას შორის. აგრეთვე, შენახვა არ იყო შეზღუდული პიროვნების პირდაპირი ან ირიბი კავშირით დანაშაულთან, ან ეროვნული უსაფრთხოებისთვის

---

[305] Handbook on European Data Protection Law, 2018, 46. <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].

[306] *Digital Rights Ireland Ltd* (C-293/12) *v. Minister of Communications, Marine and Natural Resources and Others and Kartner Landesregierung and Others* (C-594/12), GC, 2014. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=511178> [05.06.23].

[307] იქვე, 62.

[308] *Tele2 Sverige AB* (C-203/15) *v Post- och telestyrelsen and Secretary of State for the Home Department (*C-698/15) *v Tom Watson and Others.* GC, [2016] CJEU, 105-107.

[309] იქვე.

რელევანტური კომუნიკაციით, დროით ან თუნდაც გეოგრაფიული არეალით. შესაბამისად, სასამართლომ დაადგინა, რომ ეროვნული კანონმდებლობა აჭარბებდა მკაცრი აუცილებლობის ზღვარს.[310]

თუმცა, მართლმსაჯულების ევროპულმა სასამართლომ საქმეში La Quadrature Du Net and Others v. Premier Ministre and Others[311] განმარტა, რომ ეროვნული უსაფრთხოების დაცვის, მძიმე დანაშაულთან ბრძოლისა და საზოგადოებრივ უსაფრთხოებასთან დაკავშირებული საფრთხეების პრევენციის მიზნით, ინტერნეტ კავშირის წყაროსთვის მინიჭებული IP მისამართების ბლანკეტური და განურჩეველი შენახვა მკაცრად აუცილებელი განსაზღვრული ვადით, ხოლო ელექტრონული საკომუნიკაციო სისტემების მომხმარებლების ვინაობის შესახებ ინფორმაციის ბლანკეტური და განურჩეველი შენახვა, დასაშვებია.[312]

სასამართლოს განმარტებით, მართალია IP მისამართები მომხმარებელთა ონლაინ აქტივობების აღსარიცხად გამოიყენება და პირთა დეტალური პროფილის შექმნის შესაძლებლობას იძლევა, თუმცა დანაშაულის ონლაინ ჩადენის შემთხვევაში იგი შესაძლოა ერთადერთი საშუალება იყოს დამნაშავის იდენტიფიცირებისათვის. აღნიშნული განსაკუთრებით მნიშვნელოვანია, როდესაც საქმე ბავშვთა პორნოგრაფიას ეხება. საყურადღებოა ის გარემოებაც, რომ პროვაიდერი კომპანიების მიერ IP მისამართის შესახებ მონაცემების შეგროვება დროებით, მხოლოდ მომსახურების ანგარიშსწორების მიზნით ხდება, ხოლო აღნიშნული ღონისძიების გარეშე ონლაინ ჩადენილი დანაშაულის გამოვლენა ფაქტობრივად შეუძლებელი იქნებოდა.[313]

რაც შეეხება პირთა ვინაობასთან დაკავშირებული მონაცემების შეგროვებას, სასამართლოს განმარტებით იგი პირადი ცხოვრების შესახებ ინფორმაციას არ ამჟღავნებს. შესაბამისად, ამ მონაცემების შენახვით გამოწვეული ჩარევა უფლებაში სერიოზულად ვერ შეფასდება.[314] ამრიგად, დანაშაულის პრევენციის, გამოძიების, გამოვლენისა და სისხლისსამართლებრივი დევნის დაწყების მიზნებით და იმ

[310] იქვე, 107.
[311] *La Quadrature Du Net and Others v. Premier Ministre and Others,* C-511/18, C-512/18 and C-520/18, [GC], [2020], CJEU.
[312] იქვე, 154-158.
[313] იქვე, 153-154.
[314] იქვე,§157.

შემთხვევაშიც კი, თუ მისაღწევ მიზანსა და მომხმარებელთა მონაცემებს შორის კავშირი არ აკვეთება, დირექტივის მე-15 მუხლის 1-ლი პუნქტი[315] არ გამორიცხავს ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლების დავალდებულებას, შეუზღუდავი დროით შეინახონ ამ სახის მონაცემები.[316]

3.4. საჯარო ინტერესის სტანდარტი

უფლების შეზღუდვის გასამართლებლად საჯარო ინტერესის სტანდარტის დაკმაყოფილება მნიშვნელოვანია. იგი მოიცავს ევროკავშირის შესახებ ხელშეკრულების მე-3 მუხლით გარანტირებულ მშვიდობისა და კეთილდღეობის ხელშეწყობას, სოციალურ სამართლიანობას, უსაფრთხოებასა და მის დაცვას, დანაშაულის პრევენციას და მასთან ბრძოლას. ასევე, სხვათა უფლებებისა და თავისუფლებების,[317] საზოგადოებრივი უსაფრთხოების დაცვას და სხვა.[318]

აღსანიშნავია, რომ საჯარო ინტერესის საკმარისი სიცხადით განსაზღვრას განსაკუთრებული მნიშვნელობა ენიჭება უფლების შეზღუდვის აუცილებლობის დადგენისას. [319] საყურადღებოა ისიც, რომ შერჩეული ღონისძიების შედეგად გადასაჭრელი პრობლემა არა თუ ჰიპოთეტური, არამედ რეალური უნდა იყოს, რაც შესაბამისი მტკიცებულებით იქნება დადასტურებული. თუმცა ადამიანის უფლებათა ევროპული სასამართლოს მიდგომით, გადასაჭრელი პრობლემა არა მარტო რეალური ან გარდაუვალი, არამედ საზოგადოების ფუნქციონირებისათვის კრიტიკული მნიშვნელობის უნდა იყოს. [320] გასათვალისწინებელია, რომ თუ ღონისძიების

---

[315] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058> [05.06.23].

[316] *La Quadrature Du Net and Others v. Premier Ministre and Others,* C-511/18, C-512/18 and C-520/18, [GC], [2020] CJEU, 158.

[317] Charter of Fundamental Rights of The European Union, 2012, Article 52.

[318] Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 23. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [05.06.23].

[319] Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, EDPS, 2017, 4. <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> [05.06.23].

[320] იქვე, 14-15.

გამოყენება ერთზე მეტ მიზანს ემსახურება, აუცილებელია თითოეული მათგანის სათანადოდ დასაბუთება.[321]

4. მონაცემთა დაცვა პოლიციისა და სისხლის სამართლის მართლმსაჯულების კონტექსტში

4.1. 108-ე მოდერნიზებული კონვენცია

„პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის“ შესახებ 108-ე კონვენციას საქართველომ ხელი 2005 წელს მოაწერა, ხოლო ძალაში 2006 წლიდან შევიდა. უნდა ითქვას, რომ დოკუმენტი მიღების დღიდან მონაცემთა დაცვის სფეროში მნიშვნელოვან საერთაშორისო სამართლებრივ ინსტრუმენტს წარმოადგენს, თუმცა თანამედროვე ტექნოლოგიებისა და გლობალიზაციის პროცესის ფონზე და მათგან მომდინარე გამოწვევებზე საპასუხოდ მისი განახლება გახდა საჭირო. განახლების შემდეგ კი კონვენცია ხელმოსაწერად 2018 წლის 10 ოქტომბერს გაიხსნა. კონვენციის მიზანს გლობალურ დონეზე კონფიდენციალურობის, პირადი ცხოვრების, პერსონალურ მონაცემთა დაცვისა და ადამიანებს შორის ინფორმაციის თავისუფალი გაცვლის ხელშეწყობა წარმოადგენს.

კონვენცია ვრცელდება როგორც კერძო და საჯარო სფეროში, ისე მართლმსაჯულებისა და სამართალდამცველი ორგანოების მიერ მონაცემთა ავტომატიზირებულ და არაავტომატიზირებულ დამუშავებაზე, თუმცა მისი მოქმედების ფარგლებში არ ექცევა ინდივიდის მიერ პირადი ან საყოფაცხოვრებო მიზნით დამუშავებულ ინფორმაცია.[322]

დოკუმენტით გათვალისწინებულია მონაცემთა დამუშავების პრინციპები, რომლებიც უზრუნველყოფენ მის კანონიერ და სამართლიან შეგროვებას, ლეგიტიმური მიზნით დამუშავებას, რაც თავის მხრივ დაუშვებელს ხდის მონაცემების სხვა მიზნით გამოყენებას და იმაზე ხანგრძლივი დროით შენახვას ვიდრე ეს კანონიერი მიზნის მისაღწევად არის საჭირო.[323] ამასთან, მონაცემთა დამუშავების ლეგიტიმურობისა და მონაცემთა ხარისხის მოთხოვნიდან გამომდინარე, მონაცემთა დამუშავების პროცესი დასახული მიზნის პროპორციული უნდა იყოს და ეს დამუშავების ნებისმიერ ეტაპზე

---

[321] იქვე.

[322] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018, article 3.

[323] *S. and Marper v. The United Kingdom,* [2008] ECHR, 119, 125.

კერძო და საჯარო ინტერესს შორის სამართლიანი ბალანსის დაცვით უნდა გამოიხატებოდეს.[324]

კონვენციით გარანტირებულია ნებისმიერი კატეგორიის პერსონალურ მონაცემთა დაცვა, თუმცა ზოგადიდან გამოყოფილია „განსაკუთრებული კატეგორიის მონაცემები“. კერძოდ, გენეტიკური და ბიომეტრული მონაცემები, პიროვნების რასობრივი თუ ეთნიკური კუთვნილება, ჯანმრთელობა, რელიგიური ან ფილოსოფიური მრწამსი, სქესობრივი ცხოვრება, სისხლის სასამართალწარმოებასთან დაკავშირებული საკითხები, ნასამართლობა და ა.შ. ხოლო მათი დამუშავება დაცვის სათანადო სამართლებრივი მექანიზმის გარეშე დაუშვებელია. დამატებითი მექანიზმი შესაძლოა იყოს როგორც ტექნიკური, ისე ორგანიზაციული სახის. მაგალითისთვის, დაშიფვრა, შენახვის მოკლე პერიოდი და ა.შ.[325]

გასათვალისწინებელია, რომ პოლიციის სფეროში პერსონალური მონაცემების შეგროვება იზღუდება იმ მოცულობით რაც აუცილებელი და პროპორციულია საფრთხის ან დანაშაულის პრევენციის, გამოძიების ან სისხლისსამართლებრივი დევნის განხორციელების მიზნებისთვის. [326] ამასთან, აუცილებელია აშკარა და პირდაპირი კავშირის არსებობა პოლიციის მიერ მონაცემის შეგროვებასა და ლეგიტიმურ მიზანს შორის. [327] ყურადსაღებია ინდივიდების მიხედვით პერსონალური მონაცემების დიფერენცირების საკითხიც. პერსონალური მონაცემები დაკავშირებულია ბრალდებულთან, მსჯავრდებულთან, გამართლებულთან, დაზარალებულთან, მოწმესთან თუ მესამე პირთან.

ყოველივესთან ერთად და ამასთან, მიზნის შეზღუდვის პრინციპის მოთხოვნებიდან გამომდინარე, მონაცემთა დამუშავების დაწყებამდე მნიშვნელოვანია დამუშავების მიზნის წინასწარ და მკაფიოდ განსაზღვრა. დაუშვებელია მისი ხელახალი დამუშავება განსხვავებული მიზნით. [328] ასეთ შემთხვევაში საჭიროა დამოუკიდებელი

[324] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018, article 5.

[325] Practical Guide on the Use of Personal Data in the Police Sector, Strasbourg, 2018, 5. <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> [05.06.23].

[326] იქვე, 3.

[327] Recommendation No. R (87) 15, Regulating the use of personal data in the police sector, 1987, 2(1).

[328] Practical Guide on the Use of Personal Data in the Police Sector, Strasbourg, 2018, 4. <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> [05.06.23].

სამართლებრივი საფუძველი. შესაბამისად, მონაცემის დამუშავება განუსაზღვრელი მიზნით კანონდარღვევას წარმოადგენს.[329]

საყურადღებოა შენახვის ვადის შეზღუდვის პრინციპი, რომელიც პერსონალური მონაცემების წაშლას ან ანონიმიზაციას გულისხმობს, როგორც კი დასახული მიზანი მიღწეულ იქნება.[330]

გარდა იმისა, რომ კონვენცია აწესრიგებს პერსონალური მონაცემების დამუშავების საკითხს და გარკვეულ სამართლებრივ ჩარჩოში აქცევს მას, იგი არაერთ უფლებრივ გარანტიას ანიჭებს მონაცემთა დაცვის სუბიექტს უფლებათა დასაცავად. კერძოდ, ინფორმაციის მიღების უფლება, რომლის ფარგლებშიც დამმუშავებელი ვალდებულია სუბიექტს აცნობოს მისი ვინაობა, მისამართი, დამუშავების სამართლებრივი საფუძველი, მონაცემთა კატეგორია, მიმღები, მონაცემთან წვდომის, შესწორებისა და სამართლებრივი დაცვის უფლების რეალიზების გზები.[331] ამასთან, ნებისმიერი დამატებითი ინფორმაცია, რომელიც პერსონალური მონაცემების სამართლიანი და გამჭვირვალე დამუშავებისთვის იქნება აუცილებელი. აღნიშნული ინფორმაცია კი ხელმისაწვდომი, გარკვევით შედგენილი, გასაგები და მონაცემთა სუბიექტზე მორგებული უნდა იყოს (მაგ. არასრულწლოვანისთვის).[332]

პერსონალური ინფორმაციის მაღალ დონეზე დასაცავად მნიშვნელოვანია მონაცემთა სიზუსტე, შესაბამისად კონვენციის მე-9 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტის თანახმად მონაცემთა სუბიექტს შეუძლია მოითხოვოს მათი გასწორება. ამასთან, პირს უფლება აქვს არ დაექვემდებაროს მისი მოსაზრებების გაუთვალისწინებლად, მონაცემთა ავტომატური დამუშავების შედეგად მიღებულ გადაწყვეტილებას, თუ იგი მნიშვნელოვან გავლენას ახდენს მასზე. აღნიშნული კი ამგვარი გადაწყვეტილების გასაჩივრების შესაძლებლობას გულისხმობს.[333]

კიდევ ერთი მნიშვნელოვანი საკითხი, რომელსაც მოდერნიზებული კონვენცია აწესრიგებს პერსონალური მონაცემების საერთაშორისო გადაცემა და მიმოცვლაა.

---

[329] *Karabeyoglu v. Turkey,* [2016], ECHR.

[330] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018, Article 5.

[331] Handbook on European Data Protection Law, 2018, 210. <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].

[332] Explanatory Report of Modernised Convention 108, 2018, 68.

[333] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018, Article 9.

როგორც წესი ხელშემკვრელ მხარეებს შორის პერსონალური მონაცემები თავისუფლად იცვლება, თუმცა შესაძლოა მისი შეზღუდვაც, როდესაც არსებობს „რეალური და სერიოზული საფრთხე“, რომ მათი გადაცემა კონვენციის დებულებების უგულვებელყოფას გამოიწვევს ან აკრძალვა განპირობებულია რეგიონალური საერთაშორისო ორგანიზაციების მიერ დადგენილი წესების მიხედვით. [334] არახელშემკვრელი სახელმწიფოსთვის ან საერთაშორისო ორგანიზაციისთვის კი მონაცემის გადაცემა დასაშვებია თუ მათი მხრიდან მონაცემთა დაცვა სათანადო დონეზეა აყვანილი.[335]

უფლების არააბსოლუტური ხასიათიდან გამომდინარე 108-ე კონვენციით გათვალისწინებულია პერსონალურ მონაცემთა დაცვის უფლების მართლზომიერი შეზღუდვის საფუძვლები, რომლებიც ადამიანის უფლებათა ევროპული კონვენციით გარანტირებული პირადი ცხოვრების უფლების შეზღუდვის საფუძვლების იდენტურია. მიუხედავად ამისა, კონვენცია არ ექვემდებარება ადამიანის უფლებათა ევროპული სასამართლოს კონტროლს, თუმცა თავად სასამართლო მსჯელობისას ხშირად ხელმძღვანელობს 108-კონვენციის პრინციპებით.[336]

4.2. მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოებისათვის

ევროკავშირის დონეზე პოლიციისა და სისხლის სამართლის მართლმსაჯულების სფეროში მონაცემთა დაცვის დირექტივით [337] დაცულია ის პერსონალური მონაცემები, რომლებიც გროვდება და მუშავდება სისხლის სამართლის დანაშაულის პრევენციის, გამოძიების, სისხლის სამართლებრივი დევნის, სასჯელის აღსრულების, საზოგადოებრივი უსაფრთხოების დაცვის, პოლიციის ან სხვა სამართალდამცავი ორგანოს მიერ კანონის, საზოგადოების უსაფრთხოებისა თუ ფუნდამენტური

[334] იქვე, მუხ. 14.
[335] იქვე.
[336] *Z v. Finland,* [1997] ECHR.
[337] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [05.06.23].

უფლებების დაცვის მიზნით.[338] მისი მოქმედების ფარგლების მხრივ აღსანიშნავია, რომ იგი ვრცელდება როგორც შიდასახელმწიფოებრივ, ისე სახელმწიფოთაშორის დონეზე. აგრეთვე სამართალდამცავი ორგანოებისა თუ ხელისუფლების წარმომადგენელთა მხრიდან პერსონალურ მონაცემთა საერთაშორისო გადაცემაზე, თუმცა არ ვრცელდება ისეთ საქმიანობაზე, რომელიც სცილდება ევროკავშირის კანონმდებლობის იურისდიქციის ფარგლებს, ეროვნული უსაფრთხოების სფეროში, ევროკავშირის ინსტიტუტების, უწყებების, ორგანოებისა და სააგანტოების მიერ მონაცემთა დამუშავებაზე.[339]

მოცემული დირექტივა ძირითადად აგებულია მონაცემთა დაცვის ზოგად რეგულაციაზე (GDPR),[340] თუმცა გათვალისწინებულია პოლიციისა და სისხლის სამართლის მართლმსაჯულების ორგანოთა და ზოგადად, სამართალწარმოების თავისებურებანი.[341] მაგალითისთვის, დირექტივის დებულებების მიხედვით აუცილებელია მონაცემთა სუბიექტების დიფერენცირება. კერძოდ, მონაცემთა დამმუშავებელმა შეძლებისდაგვარად მკაფიოდ უნდა განასხვავოს ერთმანეთისგან ბრალდებულის, მსჯავრდებულის, ასევე მათთან კავშირში მყოფი პირების, მოწმის, დაზარალებულის და სხვა პირთა პერსონალური მონაცემები.[342] ამასთან, სამართალწარმოების სპეციფიკურობის გათვალისწინებით წარმოუდგენელია მონაცემთა სუბიექტის ინფორმირების, პერსონალურ მონაცემზე წვდომის და წაშლის უფლების იმავე დოზით დაცვა ვიდრე ეს „მონაცემთა დაცვის ზოგადი რეგულაციით“ არის გათვალისწინებული. აუცილებელია მეტი მოქნილობა.[343] წინააღმდეგ

[338] იქვე, მუხ. 1.
[339] იქვე, მუხ. 2.
[340] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC < https://eur-lex.europa.eu/eli/reg/2016/679/oj> [05.06.23].
[341] Handbook on European Data Protection Law, 2018, 283 <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].
[342] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities), Article 6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [05.06.23].
[343] Handbook on European Data Protection Law, 2018, 283 <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].

შემთხვევაში სამართალდამცავი ორგანოების რიგი ღონისძიებები შესაძლოა არაეფექტური იყოს.

სწორედ ამიტომ დირექტივა არ ითვალისწინებს „გამჭვირვალობის“ პრინციპს, [344] თუმცა განსაკუთრებული ყურადღება ექცევა „მონაცემთა მინიმიზაციისა“ და „მიზნის შეზღუდვის“ პრინციპებს, რომ პერსონალურ მონაცემეთა დამუშავებას მხოლოდ მკაფიოდ განსაზღვრული მიზნითა და დასახული მიზნის მიღწევისთვის აუცილებელი მოცულობით ჰქონდეს ადგილი. [345] მონაცემთა სათანადოდ დაცვა აგრეთვე უზრუნველყოფილია მონაცემთა დამუშავების კანონიერების, სამართლიანობის, რელევანტურობისა და პროპორციულობის, სიზუსტის, განახლების, განსაზღვრული დროით შენახვისა და მონაცემთა დაკარგვის, განადგურების ან დაზიანებისგან დაცვის მოთხოვნებით.[346]

დამატებით, პერსონალურ მონაცემთა სათანადოდ დაცვის მიზნით გათვალისწინებულია დამმუშავებლის მიერ ავტომატიზებული სისტემების მეშვეობით მონაცემთა დამუშავების ოპერაციების აღრიცხვის ვალდებულება. [347] მიმართვისა და გამჟღავნების ჩანაწერებში ოპერაციის განხორციელების დროის, თარიღის, საფუძვლის და იმ პირის პერსონალური მონაცემების მითითების ვალდებულება, რომელმაც მიიღო, გაეცნო ან გაამჟღავნა ისინი. [348] აგრეთვე, დამუშავების პროცესში ფიზიკური პირის უფლებებისა და თავისუფლებების ხელყოფის საშიშროების არსებობისას, ოპერაციის დაწყებამდე მონაცემთა დაცვის რისკების შეფასების [349] , ხოლო საჭიროების შემთხვევაში საზედამხედველო ორგანოსთან წინასწარი კონსულტაციის გავლის ვალდებულება.[350]

გარკვეული უფლებებით სარგებლობს თავად მონაცემთა სუბიექტიც. კერძოდ, მონაცემზე წვდომის, საზედამხედველო ორგანოში საჩივრის შეტანის, მონაცემთა

---

[344] იქვე.
[345] იქვე.
[346] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities), Article 4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [05.06.23].
[347] იქვე, მუხლი 25.
[348] იქვე.
[349] იქვე. მუხლი 27.
[350] იქვე, მუხლი 28.

წაშლის, გასწორებისა და დამუშავების შეზღუდვის მოთხოვნის უფლებით. აგრეთვე, კონკრეტულ შემთხვევებში დამმუშავებელს აკისრია ვალდებულება სუბიექტს მიაწოდოს ინფორმაცია დამუშავების სამართლებრივი საფუძვლის, მონაცემთა შენახვის ვადის, ან თუ ასეთი ვადის განსაზღვრა შეუძლებელია, კრიტერიუმის შესახებ, რომელიც გამოიყენება ვადის დასადგენად, მონაცემების მიმღებთა ვინაობის შესახებ, მათ შორის მესამე სახელმწიფოებსა და საერთაშორისო ორგანიზაციებში.[351] თუმცა, დასაშვებია წვდომის უფლების შეზღუდვა, თუ ეს აუცილებელ და პროპორციულ ზომას წარმოადგენს დემოკრატიულ საზოგადოებაში, სათანადოდ არის დაცული პირის ძირითადი უფლებები და ლეგიტიმური ინტერესები და ამასთან, მონაცემთა დამუშავება ერთ-ერთი ან რამდენიმე მიზნის მისაღწევად ხორციელდება. კერძოდ, ა) ოფიციალური ან სამართლებრივი ღონისძიებების ხელის შეშლის თავიდან ასაცილებლად ბ) დანაშაულის პრევენციის, დადგენის, გამოძიების, სს დევნის ან სასჯელის აღსრულებისთვის გ) საზოგადოებრივი წესრიგის დაცვის მიზნით დ) ეროვნული უსაფრთხოების ან ე) სხვათა უფლებების და თავისუფლებების დასაცავად.[352]

შეჯამებისთვის ევროკავშირის მონაცემთა დაცვის დირექტივა პოლიციისა და სისხლის სამართლის მართლმსაჯულების სფეროში მოითხოვს, რომ სამართალდამცავი ორგანოების მიერ მონაცემები კანონიერად და სამართლიანად დამუშავდეს, შეგროვდეს კონკრეტული, ნათელი და ლეგიტიმური მიზნისთვის თავსებადი ფორმით, ადეკვატურად და პროპორციულად, დაცულ იქნას არაავტორიზირებული და უკანონო დამუშავებისგან, ხოლო საჭიროების შემთხვევაში მოხდეს მისი შესწორება, განახლება. დაწესდეს პერსონალურ მონაცემთა წაშლისა და შენახვის საჭიროების პერიოდული გადასინჯვის ვადები, რომლის სათანადო დაცვა უზრუნველყოფილ იქნება შესაბამისი პროცედურული წესებით. აგრეთვე, დირექტივის მიზნებისთვის არსებითი მნიშვნელობისაა, როგორც დამუშავების მიზნის შეზღუდვის და მონაცემთა მინიმიზაციის მოთხოვნები, ისე მონაცემთა სუბიექტისთვის მინიჭებული უფლებები და მონაცემთა დამმუშავებლისთვის დაკისრებული ვალდებულებები.

[351] იქვე, მუხლები 13-14.
[352] იქვე, მუხლები 14-15.

5. საერთაშორისო სტანდარტით გათვალისწინებული მართლზომიერი შეზღუდვის საფუძვლები ქართულ კანონმდებლობაში

5.1. პირადი ცხოვრებისა და პირადი კომუნიკაციის შეზღუდვის საფუძვლები საქართველოს კონსტიტუციის მიხედვით

პირადი სივრცე, კომუნიკაცია, ოჯახური ცხოვრება, საცხოვრებელი ბინისა და სხვა მფლობელობის ხელშეუხებლობის უფლება, პირადი ცხოვრების ხელშეუხებლობის უფლების მნიშვნელოვან კომპონენტებს წარმოადგენს. [353] პირადი ცხოვრების ხელშეუხებლობის უფლების ფარგლებში პირები დაცულნი არიან სახელის, პირადი მონაცემების, მიმოწერისა თუ სატელეფონო საუბრის საიდუმლოების ხელშეუხებლობის უფლებებით.[354]თუმცა, უფლების არა აბსოლუტური ხასიათი, მათი შეზღუდვის შესაძლებლობას მაინც იძლევა.[355]

საყურადღებოა, რომ საქართველოს კონსტიტუციის მე-15 მუხლის პირველი ნაწილი, რომელიც მხოლოდ პირადი და ოჯახური ცხოვრების ხელშეუხებლობას ეხება, შეზღუდვას მხოლოდ კანონის შესაბამისად და დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით ითვალისწინებს, მაშინ როდესაც ამავე მუხლის მე-2 ნაწილით დაცული ადამიანის პირადი სივრცის, კომუნიკაციისა და საცხოვრებელი ან სხვა მფლობელობის ხელშეუხებლობის შეზღუდვისთვის დამატებით სასამართლოს გადაწყვეტილების არსებობაა საჭირო. მართალია, ძირითადი უფლების შეზღუდვა დასაშვებია წინასწარი სასამართლო ნებართვის გარეშეც, გადაუდებელი აუცილებლობისას, თუმცა მისი კანონიერების კონტროლსა და შეფასებას სასამართლო post factum მაინც ახორციელებს.[356] ამასთან, გადაუდელი აუცილებლობის შემთხვევა უშუალოდ კანონით უნდა იყოს გათვალისწინებული. წინააღმდეგ შემთხვევაში, უფლებაში ჩარევა დაუშვებელი იქნება.[357]

---

[353] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება საქმეზე N1/1/625,640 „საქართველოს სახალხო დამცველი და მოქალაქეები პარლამენტის წინააღმდეგ“, II-20.

[354] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის გადაწყვეტილება საქმეზე N1/3/407 „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე - ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ“, II-4.

[355] *კუბლაშვილი კ.,* ადამიანის ძირითადი უფლებები და თავისუფლებები, მე-5 გამოცემა, თბილისი, იურისტების სამყარო, 2019, 149.

[356] საქართველოს კონსტიტუცია, სპუ, 24.08.1995, მუხლი 15(2).

[357] საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 29 თებერვლის გადაწყვეტილება საქმეზე N2/1/484 „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ჩუგოშვილი საქართველოს პარლამენტის წინააღმდეგ“, II-22.

ზოგადად, სასამართლო გადაწყვეტილების არსებობა, როგორც უფლებაში ჩარევის წინაპირობა აღმასრულებელი ხელისუფლების მიერ კანონის სწორად გამოყენების კონტროლის ეფექტურ მექანიზმს წარმოადგენს და ამასთან უფლებაში ჩარევის აუცილებლობის შემოწმებას უზრუნველყოფს.[358] შესაბამისად, პირადი და ოჯახური ცხოვრების შეზღუდვის ნაწილში სასამართლო ნებართვის მოთხოვნის არარსებობა სახელმწიფოს მხრიდან თვითნებურად მოქმედების რისკს ზრდის.[359]

მნიშვნელოვანია, პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვა თანაზომიერების პრინციპის დაცვით ხორციელდებოდეს. კერძოდ, უფლების მზღუდავი საკანონმდებლო მოწესრიგება ღირებული ლეგიტიმური მიზნის მიღწევის გამოსადეგ და აუცილებელ საშუალებას წარმოადგენდეს და იმავდროულად, უფლების შეზღუდვის ინტენსივობა მისაღწევი მიზნის პროპორციული იყოს. [360] ნიშანდობლივია, რომ საქართველოს კონსტიტუციის მიზნებისთვის კანონის შესაბამისობას, ლეგიტიმურ მიზანს, გამოსადეგ და აუცილებელ საშუალებას და პროპორციულობის პრინციპს იდენტური შინაარსი და დატვირთვა აქვს როგორც ეს ადამიანის უფლებათა ევროპული კონვენციისა და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის შემთხვევაშია.

შესაბამისად, დარწმუნებით შეიძლება ითქვას, რომ საქართველოს კონსტიტუციით გათვალისწინებული პირადი ცხოვრებისა და კომუნიკაციის მართლზომიერი შეზღუდვისთვის გათვალისწინებული როგორც ფორმალური, ისე მატერიალური წინაპირობები მჭიდრო კავშირშია საერთაშორისო სტანდარტებთან და მოთხოვნებთან.

5.2. საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობის მიხედვით

სისხლის საპროცესო სამართალი მჭიდრო კავშირშია საქართველოს კონსტიტუციასთან. [361] გარდა იმისა, რომ სისხლის საპროცესო სამართლის რიგი

---

[358] საქართველოს საკონსტიტუციო სასამართლოს 2018 წლის 26 ივლისის გადაწყვეტილება საქმეზე N2/4/665, 683, „საქართველოს მოქალაქე ნანა ფარჩუკაშვილი საქართველოს სასჯელაღსრულებისა და პრობაციის მინისტრის წინააღმდეგ“, II-111.

[359] *კუბლაშვილი კ.,* ადამიანის ძირითადი უფლებები და თავისუფლებები, მე-5 გამოცემა, თბილისი, იურისტების სამყარო, 2019, 149.

[360] საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 26 ივნისის გადაწყვეტილება საქმეზე N3/1/512 „დანიის მოქალაქე ჰეიკე ქრონქვისტი საქართველოს პარლამენტის წინააღმდეგ“, II-60.

[361] *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი - ზოგადი ნაწილის მიმოხილვა, თბილისი, იურისტების სახლი, 2014, 49-50.

დებულებები პირდაპირ გამომდინარეობენ კონსტიტუციიდან, საქართველოს სისხლის სამართლის საპროცესო კოდექსი ასევე კონსტიტუციით გარანტირებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების შეზღუდვის საფუძვლებსა და პროცესუალურ წესებს ითვალისწინებს. [362] შესაბამისად კონსტიტუცია განსაზღვრავს იმ სამართლებრივ ჩარჩოებს, რომლის ფარგლებშიც სსსკ-ის ნორმების ინტერპრეტირება უნდა ხდებოდეს.[363]

ზოგადად, დაცულ სფეროში ნებისმიერი ჩარევა მხოლოდ სავალდებულო მოთხოვნების დაცვით უნდა განხორციელდეს. მაგალითისთვის, სსსკ-ის მე-6 მუხლის პირველი ნაწილის მიხედვით, „სისხლის სამართლის პროცესის მონაწილის კონსტიტუციურ უფლებათა და თავისუფლებათა შეზღუდვა მხოლოდ საქართველოს კონსტიტუციითა და ამავე კოდექსით გათვალისწინებული სპეციალური ნორმების საფუძველზეა დასაშვები“. მეტიც, ამავე კოდექსის მე-7 მუხლის 1-ლი ნაწილით „გამოძიების პროცესში მხარეს არ აქვს უფლება, თვითნებურად და უკანონოდ ჩაერიოს სხვის პირად ცხოვრებაში. კანონით გარანტირებულია კერძო საკუთრების, მფლობელობისა თუ ნებისმიერი საშუალებით განხორციელებული კერძო კომუნიკაციის ხელშეუხებლობა“. ხოლო საგამოძიებო მოქმედება, რომელიც იწვევს კერძო საკუთრების, მფლობელობის ან პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვას, სასამართლო განჩინების საფუძველზე უნდა ჩატარდეს (სსსკ-ის 112-ე მუხლის 1-ლი ნაწილის პირველი წინადადება).

დოკუმენტის ან ინფორმაციის გამოთხოვის მაგალითზე რომ ვიმსჯელოთ, კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის ან დოკუმენტის მოპოვების ნებართვის მისაღებად, მხარემ, სასამართლოს დასაბუთებული ვარაუდის სტანდარტით შედგენილი შუამდგომლობით უნდა მიმართოს. საყურადღებოა, რომ ნებართვის მისაღებად, შუამდგომლობასთან ერთად წარდგენილი მასალების საკმარისობა, ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად, საქმის ფაქტობრივი გარემოებების გათვალისწინებით ფასდება, თუმცა დარწმუნებით შეიძლება ითქვას, რომ შენახული კომპიუტერული მონაცემის გამოთხოვის

[362] იქვე.
[363] იქვე.

განჩინების მისაღებად, აუცილებელია სულ მცირე დასაბუთებული იყოს ინფორმაციის სისხლის სამართლის საქმესთან რელევანტურობა და ის, თუ რა გარემოებების დადგენას შეუწყობს ხელს მათი მოპოვება, [364] დადგენილი იყოს კომპიუტერული სისტემის ან მონაცემის მესაკუთრე ან მფლობელი [365] და შუამდგომლობით ზუსტად იყოს განსაზღვრული გამოსათხოვი ინფორმაციის სახე და მოცულობა.[366]

თუ სსსკ-ის 136-ე მუხლს საქართველოს კონსტიტუციით გარანტირებული პირადი ცხოვრების ხელშეუხებლობის უფლების შეზღუდვისთვის გათვალისწინებულ მოთხოვნებთან კავშირში განვიხილავთ, დავინახავთ, რომ შენახული კომპიუტერული მონაცემის გამოთხოვისათვის გათვალისწინებული დებულებები თანხვედრაშია კონსტიტუციით გათვალისწინებული მართლზომიერი შეზღუდვის საფუძვლებთან. კერძოდ, სსსკ-ის 136-ე მუხლი აკმაყოფილებს კანონთან შესაბამისობის, მათ შორის ხელმისაწვდომობისა და განჭვრეტადობის მოთხოვნებს. მის საფუძველზე პირადი ცხოვრების შეზღუდვის ლეგიტიმური მიზანიც სახეზეა, რაც მეტწილად უწესრიგობის თუ დანაშაულის თავიდან აცილებაში ან მის გამოძიებაში გამოიხატება. გამოსადეგობისა და აუცილებლობის კრიტერიუმების თვალსაზრისით მისთვის დამახასიათებელი, უფლების დაბალი ინტენსივობით მზღუდავი ბუნება, [367] ლეგიტიმური მიზნის, ჩხრეკა-ამოღებასთან შედარებით ნაკლებად მზღუდავი საშუალებით მიღწევის შესაძლებლობას იძლევა. ხოლო მისი გამოყენების ნებართვის მისაღებად დასაბუთებული შუამდგომლობის წარდგენის, იმავე შუამდგომლობით გამოსათხოვი ინფორმაციის მოცულობის განსაზღვრის ვალდებულება და ყოველივეზე სასამართლოს მიერ კონტროლის განხორციელება, თანაზომიერების პრინციპის დაცვას უზრუნველყოფს.

[364] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 14 სექტემბრის განჩინება N1გ/1553-21.

[365] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 12 ოქტომბრის განჩინება N1გ/1709-21.

[366] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 2 თებერვლის განჩინება N1გ/152-22.

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

6. შეჯამება

ცხადია, რომ ინფორმაციულ საზოგადოებაში ინდივიდთა პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის საკითხი მუდამ ახალი გამოწვევების წინაშე დგას. აღნიშნული კი როგორც ადამიანის უფლებათა ევროპულ სასამართლოს, ისე მართლმსაჯულების ევროპულ სასამართლოს აიძულებს პრეცენდენტული სამართლით დადგენილი განმარტებებით, სამომავლოდ, ხელი შეუწყოს სათანადო ბალანსის დაცვას საჯარო, ლეგიტიმურ მიზანსა და ინდივიდის ფუნდამენტურ უფლებებს შორის.

შეიძლება ითქვას, რომ ევროკავშირის ფუნდამენტურ უფლებათა ქარტიითა და ადამიანის უფლებათა ევროპული კონვენციით გათვალისწინებული უფლების მართლზომიერი შეზღუდვის საფუძვლები იდენტურია, გარდა იმისა, რომ ქარტიით გათვალისწინებულ ერთ-ერთ წინაპირობას ძირითადი უფლების არსის პატივისცემა წარმოადგენს. თუმცა, ორივე შემთხვევაში პირადი და ოჯახური ცხოვრების დაცულობის, ასევე პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვის მართლზომიერების გამოსარკვევად არსებითია დადგინდეს 1. შეზღუდვა გათვალისწინებულია თუ არა შიდასახელმწიფოებრივი კანონმდებლობით და აკმაყოფილებს თუ არა ის განჭვრეტადობისა და ხელმისაწვდომობის კრიტერიუმებს; 2. არსებობს თუ არა მწვავე სოციალური საჭიროება შეზღუდვის გამოსაყენებლად და 3. აუცილებელი და პროპორციულია თუ არა გამოყენებული ღონისძიება დასახული მიზნის მისაღწევად. დამატებით, ქარტიის მიზნებისთვის კი დაცულია თუ არა ძირითადი უფლების არსი.

საყურადღებოა, რომ სამართალდამცავი ორგანოების მხრიდან მონაცემთა კანონიერად და სამართლიანად, ასევე კონკრეტული ლეგიტიმური მიზნებისთვის პროპორციულობის მოთხოვნით შეგროვებისა და დამუშავების წესები, რაც გარკვეულწილად შეუძლებელს ხდის მონაცემთა ხანრგძლივი დროით და აბსტრაქტული მიზეზით დამუშავებას,[368] აგრეთვე გარანტირებულია ევროპის საბჭოს „108-ე კონვენციით“ და ევროკავშირის მონაცემთა დაცვის დირექტივით „პოლიციისა და სისხლის სამართლის

[368] *S. and Marper v. The United Kingdom,* [2008] ECHR, 119, 125. იხ. Practical Guide on the Use of Personal Data in the Police Sector, Strasbourg, 2018, 5. <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> [08.06.23].

მართლმსაჯულების ორგანოებისათვის“. თითოეული დოკუმენტით გათვალისწინებულია დამუშავების მიზნის შეზღუდვისა და მონაცემთა მინიმიზაციის მოთხოვნები. დიფერენცირებულია პერსონალურ მონაცემთა სუბიექტები. დადგენილია მონაცემთა შენახვის ვადის შეზღუდვის პრინციპი, რაც დასახული მიზნის მიღწევის შემდეგ მის წაშლას ან ანონიმიზაციას გულისხმობს.[369] შესაბამისად, თუ სამართალდამცავ ორგანოთა მხრიდან გათვალისწინებული იქნება ადამიანის უფლებათა ევროპული კონვენციის, ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის, 108-ე კონვენციის, საპოლიციო და სამართალდამცავ სფეროში მონაცემთა დაცვის დირექტივის, საქართველოს კონსტიტუციის, საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობის მოთხოვნები და ამასთან მხედველობაში მიიღებენ ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული სასამართლოს მიერ დამკვიდრებულ განმარტებებს, დარწმუნებით შეიძლება ითქვას, რომ სისხლის სამართლის მართლმსაჯულების კონტექსტში დაცული იქნება როგორც ძირითადი უფლების მართლზომიერი შეზღუდვის ფარგლები, ისე ბალანსი საჯარო და კერძო ინტერესებს შორის.

[369] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018, Article 5. იხ. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [08.06.23].

თავი IV. კომპიუტერული მონაცემის წარმოდგენის საკითხი აღმოსავლეთ პარტნიორობის რეგიონში

1. აღმოსავლეთ პარტნიორობის შესახებ

აღმოსავლეთ პარტნიორობა - ევროკავშირისა და ევროპის საბჭოს ერთობლივი პოლიტიკური ინიციატივაა, რომელსაც საფუძველი 2009 წელს ჩაეყარა. იცინიატივის მიზანი ევროკავშირის, მის წევრ სახელმწიფოებსა და მის ექვს აღმოსავლეთ მეზობელს შორის ურთიერთობების გაღრმავება და გაძლიერება გახლავთ. პარტნიორობის მიერ განსაზღვრულ პრიორიტეტულ მიმართულებებს შორის კიბერუსაფრთხოება (Cybereast) ერთ-ერთი ძირითად გამოწვევად ითვლება. შესაბამისად კიბერუსაფრთხოების პროექტის ფარგლებში მონაწილე ქვეყნებისთვის, როგორებიცაა სომხეთი, აზერბაიჯანი, ბელორუსია, საქართველო, მოლდოვასა და უკრაინისთვის საკანონმდებლო ბაზის „კიბერდანაშაულის“ შესახებ კონვენციასთან შესაბამისობაში მოყვანისთვის, სამართალდამცავი ორგანოებისა და სასამართლო ხელისუფლების გაძლიერებისათვის, მომსახურების მომწოდებლებსა და სამართალდამცავ უწყებებს შორის ნდობის გაღრმავებისთვისა და ეფექტური საერთაშორისო თანამშრომლობის ჩამოყალიბებისთვის დღემდე ინტენსიური მუშაობა მიმდინარეობს.[370] ვინაიდან სისხლის სამართლის მართლმსაჯულების, კიბერსაფრთხეების მიმართ მდგრადობისა და საერთო უსაფრთხოების გაძლიერების უზრუნველსაყოფად კონვენციით გათვალისწინებული მატერიალური და პროცესუალური დებულებების ეროვნულ კანონმდებლობაში სათანადოდ იმპლემენტირებას გადამწყვეტი მნიშვნელობა აქვს, ელექტრონული ინფორმაციის გამოთხოვის კუთხით პარტნიორი ქვეყნების საკანონმდებლო ბაზისა და მათ წინაშე არსებული გამოწვევების გაცნობა რეგიონში არსებული საერთო ვითარების წარმოდგენასა და აგრეთვე, ქართული, ეროვნული კანონმდებლობის სიძლიერისა თუ სისუსტის წარმოჩენაში დაგვეხმარება. ამასთან, აღნიშნული შესაძლებლობას მოგვცემს, ურთიერთშედარების საფუძველზე ვიმსჯელოთ ნორმატიული ბაზის დახვეწისა და სამომავლო განვითარების გზებზე.

[370] იხ. ოფიციალური განცხადება <https://www.coe.int/en/web/cybercrime/cybereast> [08.06.23].

2. სომხეთი

„კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებიდან გამომდინარე ხელშემკვრელი სახელმწიფოების ეროვნული კანონმდებლობა სრულად უნდა ასახავდეს მასში გათვალისწინებულ საგამოძიებო მოქმედებებს. იმპერატიული დათქმის მიზანი ელექტრონული მტკიცებულების მოპოვებისთვის აუცილებელი პროცესუალური მექანიზმების ეროვნულ კანონმდებლობაში დანერგვის გარდა, გამოძიების პროცესში ადამიანის ძირითადი უფლებებისა და თავისუფლებების სათანადო დაცვის უზრუნველყოფა წარმოადგენს.

ნიშანდობლივია, რომ კომპიუტერული მონაცემის წარმოდგენის ბრძანება, როგორც დამოუკიდებელი საგამოძიებო მოქმედება, სომხეთის სისხლის სამართლის საპროცესო კანონმდებლობაში არ არის იმპლემენტირებული. მის ნაცვლად, გამოძიებაზე უფლებამოსილი პირები კომპიუტერულ სისტემაში ან ელექტრონულ მატარებელში შენახულ კომპიუტერულ მონაცემს, ჩხრეკა-ამოღებისათვის დადგენილი წესის მიხედვით მოიპოვებენ.[371]

სომხეთის სისხლის სამართლის საპროცესო კოდექსის 228-ე მუხლის მე-6 ნაწილის თანახმად „ნებართვის გაცნობის შემდეგ, გამომძიებელი სთავაზობს პირს ნებაყოფლობით გადასცეს საქმისათვის მნიშვნელოვანი ინფორმაცია. წინააღმდეგ შემთხვევაში ჩამორთმევა იძულებითი წესით განხორციელდება“. ამასთან, ამავე კოდექსის 226-ე მუხლის მე-3 ნაწილით დაწესებულებებს, ორგანიზაციებს, თანამდებობის პირებს, მოქალაქეებს არ აქვთ უფლება უარი განუცხადონ გამომძიებელს, მის მიერ მოთხოვნილი ნივთების, დოკუმენტების ან ასლების გადაცემაზე“. იმის გათვალისწინებით, რომ სომხეთის საპროცესო კანონმდებლობა არ იცნობს კომპიუტერულ მონაცემთა სახეებს, როგორებიცაა მომხმარებლის შესახებ ინფორმაცია, ტრაფიკისა და შინაარსობრივი მონაცემები, კომპიუტერული მონაცემის მოპოვებისთვის ნებართვის გაცემისას ჩხრეკა-ამოღების წესთან ერთად, ხელმძღვანელობენ საპროცესო კოდექსის 122-ე მუხლის 1-ლი ნაწილით განსაზღვრული დოკუმენტის ცნებით, რომელიც საკმაოდ ფართო შინაარსის მატარებელია და აერთიანებს ქაღალდზე, მაგნიტურ, ელექტრონულ და სხვა

[371] Criminal Procedure Code of the Republic of Armenia, 01/09/1998, Article 228(6),

საშუალებებზე გაკეთებულ სიტყვიერ, რიცხვით, გრაფიკულ ან სხვა სიმბოლური ფორმით გამოსახულ ინფორმაციას.

დასკვნითვის, მიუხედავად იმისა, რომ სომხეთის საპროცესო კანონმდებლობა შენახული კომპიუტერული მონაცემის მოპოვების შესაძლებლობას იძლევა, იგი ვერ აკმაყოფილებს კონვენციით გათვალისწინებულ მოთხოვნებს.[372] კონვენციის მე-18 მუხლის ძირითად მიზანს ელექტრონული მტკიცებულების, უფლების ნაკლები შეზღუდვის ხარჯზე მოპოვება წარმოადგენს. შესაბამისად, სისხლის სამართლის საქმისთვის რელევანტური ელექტრონული მტკიცებულების შეგროვებისთვის გამუდმებით ჩხრეკა-ამოღების ჩატარება მიზანშეუწონელია.[373]

3. აზერბაიჯანი

მსგავსად სომხეთისა, აზერბაიჯანის სისხლის სამართლის საპროცესო კოდექსი შენახული კომპიუტერული მონაცემის, მათ შორის მომხმარებლის შესახებ ინფორმაციის მოპოვებას, დამოუკიდებელი საგამოძიებო მოქმედების სახით არ აწესრიგებს.[374] ისეთ ვითარებაში, როდესაც სისხლის სამართლის საქმისათვის რელევანტური კომპიუტერული მონაცემის მოპოვებაა აუცილებელი, მხარეები სისხლის სამართლის საპროცესო კოდექსის 143-ე მუხლის მე-2 ნაწილისა და 135-ე მუხლის პირველი ნაწილის მიხედვით მოქმედებენ. საპროცესო კოდექსის 143-ე მუხლის მე-2 ნაწილის მიხედვით „გამომძიებელი და პროკურორი უფლებამოსილნი არიან ფიზიკური თუ იურიდიული პირისგან მოითხოვონ გამოძიებისათვის მნიშვნელოვანი საგნებისა და დოკუმენტების წარმოდგენა“. მართალია ჩამონათვალში კომპიუტერულ მონაცემს ან ელექტრონულ მტკიცებულებას არ ვხვდებით, თუმცა ამავე კოდექსის 135-ე მუხლის 1-ლი ნაწილით დოკუმენტი, რომლის მოპოვებაც 143-ე მუხლის თანახმად შესაძლებელია, ელექტრონულ ინფორმაციასაც მოიაზრებს. ამრიგად, ამ ორი ნორმის ურთიერთშეჯერებით გამოძიებისათვის სასარგებლო ელექტრონული ინფორმაციის მოპოვება ხელმისაწვდომი ხდება, თუმცა საყურადღებოა, რომ მოთხოვნა შესასრულებლად სავალდებულო ძალის მქონე არაა

[372] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 17 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.06.23].

[373] იქვე.

[374] Code of Criminal Procedure of the Azerbaijan Republic, 14/07/2000.

და მოცემული მუხლის საფუძველზე ინფორმაციის გადაცემა ნებაყოფლობით ხასიათს ატარებს. იმის გათვალისწინებით რომ თანამშრომლობის ნებაყოფლობითობამ შესაძლოა მესამე პირთა მხრიდან გამოძიებისთვის რელევანტური მტკიცებულების გადაუცემლობა გამოიწვიოს, აზერბაიჯანის საპროცესო კოდექსის მიხედვით, მოთხოვნის შეუსრულებლობის შემთხვევაში, გამომძიებელი და პროკურორი ელექტრონულ ინფორმაციას ჩხრეკა-ამოღებისათვის დადგენილი წესის მიხედვით მოიპოვებენ, [375] თუმცა, ჩხრეკა-ამოღების ჩატარებისთვის, სისხლის სამართლის საქმეზე ოფიციალური გამოძიების მიმდინარეობა და სასამართლო ნებართვის არსებობა აუცილებელ წინაპირობას წარმოადგენს.[376]

მართალია, ყოველივე ერთობლიობაში პროცესუალურ მექანიზმს ქმნის სისხლის სამართლის საქმისთვის ღირებული ელექტრონული მტკიცებულების შეგროვებისთვის, თუმცა აზერბაიჯანის ეროვნულ კანონმდებლობაში კონვენციით დადგენილი კონკრეტული და მკაფიო ნორმების არარსებობა მნიშვნელოვან გამოწვევად რჩება და მიუხედავად ალტერნატიული ღონისძიების გამოყენებით კომპიუტერული მონაცემის მოპოვების შესაძლებლობისა, ეს კონვენციის მე-18 მუხლის მოთხოვნების დაკმაყოფილებად ვერ ჩაითვლება.

4. ბელარუსი

ბელარუსის სისხლის სამართლის საპროცესო კოდექსით „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული „კომპიუტერული მონაცემის წარმოდგენის ბრძანება“, როგორც დამოუკიდებელი საგამოძიებო მოქმედება განსაზღვრული არ არის, თუმცა ცალკე გამოყოფს „კომპიუტერული მონაცემის დათვალიერების“ საგამოძიებო მოქმედებას. [377] ბელარუსის სისხლის სამართლის საპროცესო კოდექსის 203-ე მუხლის მიხედვით, ზოგადად დათვალიერების და მათ შორის კომპიუტერული მონაცემის დათვალიერების საფუძველია საკმარისი მონაცემების არსებობა, რომ საგამოძიებო მოქმედების შედეგად მიკვლეულ იქნება

[375] Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, 2017, 11 <https://rm.coe.int/3271-3608-report-on-eap-state-may2017/1680728bca> [08.06.23].

[376] იქვე.

[377] Criminal Procedure Code of Republic of Belarus, 16/07/1999, Art. 204[1].

დანაშაულის კვალი ან აღმოჩენილ იქნება სისხლის სამართლის საქმისთვის რელევანტური გარემოება.[378]

ამავე კოდექსის 204[1]-ე მუხლის მე-2 ნაწილის მიხედვით თუ კომპიუტერული მონაცემის დასათვალიერებლად წვდომისთვის აუცილებელია მომხმარებლის მიერ ავტორიზაციის გავლა, ან თუ იგი შეიცავს ინფორმაციას პირადი ცხოვრების შესახებ, ან კანონით დაცულ საიდუმლო ინფორმაციას, ან ინფორმაციას, რომლის გავრცელება ან მიწოდება შეზღუდულია, დათვალიერება დასაშვებია მხოლოდ ინფორმაციის მფლობელის თანხმობმობითა და მისი თანდასწრებით ან გამომძიებლის ან საგამოძიებო ორგანოს გადაწყვეტილებით, რომელიც დადასტურებულია პროკურორის ან მისი მოადგილის თანხმობით. გადაუდებელი აუცილებლობის შეთხვევაში დათვალიერება შეიძლება პროკურორის ან მისი მოადგილის ნებართვის გარეშე, მხოლოდ გამომძიებლის ან საგამოძიებო უწყების გადაწყვეტილების საფუძველზე ჩატარდეს, თუმცა მათ საგამოძიებო მოქმედების ჩატარების შესახებ 24 საათის განმავლობაში უნდა ეცნობოთ.

კომპიუტერული მონაცემის დათვალიერების დროს ბელარუსის სისხლის სამართლის საპროცესო კოდექსი იცნობს აგრეთვე კომპიუტერული სისტემის ან ინფორმაციის მატარებლის ამოღების შესაძლებლობასაც, თუმცა თუ მათი ამოღება შემდგომი დათვალიერების მიზნით შეუძლებელია, გამომძიებელი უფლებამოსილია გააკეთოს კომპიუტერული მონაცემის ასლი, რა დროსაც უნდა გამოირიცხოს მისი დაკარგვის ან დაზიანების საფრთხე და შენარჩუნებულ იქნას მისი ვარგისიანობა.[379] საყურადღებოა, რომ დათვალიერების ოქმში უნდა აღინიშნოს კომპიუტერული მონაცემის დათვალიერებისთვის გამოყენებული სამეცნიერო და ტექნიკური საშუალებების, ხელსაწყოების და კომპიუტერული პროგრამების შესახებ. ამასთან, უნდა აღიწეროს წვდომის პროცედურა, შემოწმების დროს განხორციელებული ქმედებები და მიღებული შედეგები.[380]

დათვალიერების გარდა, ბელარუსიის სისხლის სამართლის საპროცესო კანონმდებლობით კომპიუტერული მონაცემის მოპოვებისთვის შესაძლოა გამოყენებულ იქნას ჩხრეკა-ამოღებისთვის დადგენილი წესები, რაც დათვალიერების

[378] იქვე, მუხლი 203.
[379] იქვე, მუხლი 204[1] (3).
[380] იქვე, მუხლი 204[1] (4).

მსგავსად გამომძიებლის დადგენილებასთან ერთად პროკურორის თანხმობის არსებობასაც მოითხოვს.[381] დამატებით დებულებებს ვხვდებით „შინაგან საქმეთა სამინისტროს შესახებ“ ბელარუსიის რესპუბლიკის კანონშიც, რომლის 24-ე მუხლის მიხედვით „უწყება უფლებამოსილია ჩაატაროს ოპერატიულ-სამძებრო ღონისძიებები, ორგანიზაციებისაგან და მოქალაქეებისაგან მოითხოვოს და მიიღოს გამოძიებისათვის საჭირო ინფორმაცია და დოკუმენტი, ხოლო აუცილებლობის შემთხვევაში იძულებითი წესით ამოიღოს ისინი“.[382]

მომხმარებლის შესახებ ინფორმაციის მოპოვებასთან დაკავშირებით ნიშანდობლივია ბელარუსიის რესპუბლიკის პრეზიდენტის №60 ბრძანება, რომელიც განსაზღვრავს მომსახურების მომწოდებელთა მიერ მომხმარებელთა ინფორმაციის შენახვისა და დამუშავების წესებს,[383] რომელზე დაყრდნობითაც გამოძიებას ხელი მიუწვდება ისეთ ინფორმაციაზე, როგორიცაა მომხმარებლის მოწყობილებების მაიდენტიფიცირებელი მონაცემები, მის მიერ გამოყენებული ინტერნეტ სერვისები, ვებ-გვერდების მისამართები და ა.შ.[384]

შეიძლება ითქვას, რომ არსებული მდგომარეობით ბელარუსიის საკანონმდებლო ბაზა სრულყოფილად ვერ ასახავს ე.წ. „ბუდაპეშტის“ კონვენციით გათვალისწინებულ მოთხოვნებს და საჭიროებს საკითხის მეტად ზუსტ მოწესრიგებას.[385] საყურადღებოა ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის საკითხიც, ვინაიდან ნებისმიერი სახის, მათ შორის შინაარსობრივი მონაცემების დათვალიერება და ამოღებაც გამომძიებლისა და პროკურორის გადაწყვეტილების საფუძველზე ხორციელდება. საგამოძიებო მოქმედების გადაუდებელი აუცილებლობის საფუძვლით ჩატარების შემთხვევაში კი პროკურორის ნებართვაც არ არის საჭირო, რომ აღარაფერი ვთქვათ შემდგომ მისი კანონიერების სასამართლო გზით შემოწმების სავალდებულოობაზე. არც ერთ საგამოძიებო მოქმედებაზე, იქნება ეს კომპიუტერული მონაცემის დათვალიერება თუ ჩხრეკა-ამოღება, სასამართლო,

---

[381] იქვე, მუხლი 210.

[382] Law on the Internal Affairs Bodies of the Republic of Belarus, 17/07/2007.

[383] Decree of The President of The Republic of Belarus on measures to improve the use of the national segment of the internet, №60, 01/02/2010.

[384] იქვე.

[385] Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, 2017, 14 <https://rm.coe.int/3271-3608-report-on-eap-state-may2017/1680728bca> [08.06.23].

ზედამხედველობას არ ახორციელებს, ხოლო პროკურორი ან მისი მოადგილე, რომელთა თანხმობაც გამომძიებლის დადგენილებასთან ერთად საგამოძიებო მოქმედების ჩასატარებლად აუცილებელია, ვერ ჩაითვლება ეფექტურ მექანიზმად პირთა პირად ცხოვრებაში არამართლზომიერი ჩარევის თავიდან ასაცილებლად, ვინაიდან ისინი ერთმანეთისგან ფუნქციურად დამოუკიდებლები არ არიან, რაც გადამწყვეტი ფაქტორია ეფექტური ზედამხედველობის განხორციელებისათვის. შესაბამისად, საკითხის ურთიერთშეჯერების საფუძველზე, დარწმუნებით შეგვიძლია ვთქვათ, რომ ბელარუსიის ეროვნული კანონმდებლობა ვერ პასუხობს კონვენციის მე-18 მუხლის მოთხოვნებს.[386]

5. მოლდოვა

შეიძლება ითქვას, რომ „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული კომპიუტერული მონაცემის გადაცემის ბრძანება, მოლდოვის ეროვნულ კანონმდებლობაში ნაწილობრივ არის იმპლემენტირებული. როგორც ჩვენთვის ცნობილია, კომპიუტერული მონაცემის გადაცემის ბრძანება ფართო შინაარსისაა და ერთის მხრივ კომპეტენტურ ორგანოებს საშუალებას აძლევს მოიპოვონ ქვეყნის ტერიტორიაზე მყოფ პირთაგან ნებისმიერი კატეგორიის კომპიუტერული მონაცემი, ხოლო მეორეს მხრივ პროვაიდერისგან მომხმარებლის შესახებ ინფორმაცია. ნაცვლად ნორმის სრულყოფილად იმპლემენტირებისა, მოლდოვის კანონმდებლობით, ყურადღება მხოლოდ მომხმარებლის შესახებ ინფორმაციის მოპოვებაზეა გამახვილებული. კერძოდ კი „კიბერდანაშაულის პრევენციისა და მასთან ბრძოლის შესახებ“ კანონის მე-7 მუხლის 1-ლი ნაწილის „დ“ ქვეპუნქტის მიხედვით მომსახურების მომწოდებელნი, კომპეტენტური ორგანოს კანონიერი მოთხოვნის საფუძველზე ვალდებულნი არიან მიაწოდონ მათ ინფორმაცია მომხმარებლის, მის მიერ გამოყენებული კომუნიკაციის ტიპის და სერვისების შესახებ. [387] ანალოგიურად, საპროცესო კოდექსის 134^5-ე მუხლის თანახმად შესაძლებელია მომხმარებლის იდენტიფიცირება, რაც ასევე პროვაიდერს

[386] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 41 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.06.23].

[387] Law on the prevention and fight agains crime in the field of computer information, №20, 03/02/2009.

ავალდებულებს მიაწოდოს ინფორმაცია გამოძიებას მომხმარებლის შესახებ, თუმცა უნდა ითქვას, რომ აღნიშნული საგამოძიებო მოქმედება ფარულ საგამოძიებო მოქმედებათა თავშია მოქცეული და მის განხორციელებაზე უფლებამოსილ პირს პროკურორი წარმოადგენს.[388]

რაც შეეხება კომპიუტერულ სისტემაში ან ელექტრონულ მონაცემთა მატარებელში არსებული შინაარსობრივი მონაცემის მოპოვებას, აღნიშნული, მოლდოვის საპროცესო კანონმდებლობის მიხედვით ჩხრეკა-ამოღებისათვის დადგენილი წესის მიხედვით ხორციელდება. სისხლის სამართლის საპროცესო კოდექსის 126-ე მუხლის მიხედვით საგამოძიებო უწყება, დასაბუთებული შუამდგომლობისა და სასამართლო ნებართვის საფუძველზე უფლებამოსილია მოიპოს სისხლის სამართლის საქმისათვის მნიშვნელოვანი, მათ შორის კომუნიკაციის შინაარსისა და სახელმწიფო, კომერციული თუ საბანკო საიდუმლოების შემცველი დოკუმენტები. [389] რა თქმა უნდა, კანონმდებლობით დოკუმენტი ფართოდ განიმარტება და მასში წერილობითი, აუდიო-ვიდეო, ელექტრონული თუ სხვა ნებისმიერი ფორმით გამოსახული ინფორმაცია მოიაზრება. [390] შესაბამისად, მათი ურთიერთშეჯერებით ნებისმიერი სახის შენახული კომპიუტერული მონაცემის მოპოვება ხელმისაწვდომი ხდება.

ცხადია, რომ მოლდოვის კანონმდებლობა არაერთ სამართლებრივ მექანიზმს აერთიანებს ელექტრონული მონაცემის მოსაპოვებლად. დავინახეთ, რომ საპროცესო კოდექსი „„მომხმარებლის იდენტიფიცირების“ საგამოძიებო მოქმედებას ითვალისწინებს, რომელიც ფარულ საგამოძიებო მოქმედებად ითვლება, თუმცა მისი გამოყენება არ საჭიროებს სასამართლო ნებართვას და პროკურორის დადგენილების საფუძველზეც შესაძლებელია. ამასთან, „კიბერდანაშაულის პრევენციისა და მასთან ბრძოლის შესახებ“ კანონის მიხედვით ხელმისაწვდომია პროვაიდერისგან მომხმარებლის შესახებ ინფორმაციის გამოთხოვა და ნიშანდობლივია, რომ შინაარსობრივად, იგი ახლოს დგას კონვენციის მე-18 მუხლის იმ ნორმატიულ შინაარსთან, რომელიც მომხმარებლის შესახებ ინფორმაციის შეგროვებას გულისხმობს. სწორედ ამიტომ შეგვიძლია ვთქვათ, რომ მოლდოვის ეროვნული კანონმდებლობა მხოლოდ ნაწილობრივ აკმაყოფილებს ხელშეკრულების

[388] Criminal Procedure Code of The Republic of Moldova, №122, 14/03/2003.
[389] იქვე, მუხლი 126.
[390] იქვე, მუხლი 157.

მოთხოვნებს. მართალია, სხვა სახის კომპიუტერულ მონაცემზე წვდომა გამოძიებას ჩხრეკა-ამოღებისათვის დადგენილი წესის მიხედვით აქვს, თუმცა, როგორც უკვე არაერთხელ ვახსენეთ, კომპიუტერული მონაცემის გადაცემის ბრძანებასთან შედარებით იგი ვერ აკმაყოფილებს პროპორციულობის პრინციპს და შესაბამისად, არ განიხილება კონვენციის მე-18 მუხლის ალტერნატიულ ღონისძიებად.[391]

6. უკრაინა

კომპიუტერული მონაცემის წარმოდგენის ბრძანება, როგორც დამოუკიდებელი საგამოძიებო მოქმედება უკრაინის ეროვნულ კანონმდებლობაში იმპლემენტირებული არ არის. თუმცა, უკრაინის სისხლის სამართლის საპროცესო კოდექსის მე-15 თავში, 159-ე მუხლით გათვალისწინებულია „ნივთებსა და დოკუმენტებზე დროებითი წვდომის“ საგამოძიებო მოქმედება. [392] ამავე მუხლის პირველი ნაწილის მიხედვით, მხარე უფლებამოსილია დაათვალიეროს, გაეცნოს, ასლი გააკეთოს და ამოიღოს პირის მფლობელობაში არსებული საგანი ან დოკუმენტი, ხოლო ელექტრონულ საინფორმაციო და საკომუნიკაციო სისტემაზე დროებითი წვდომის შემთხვევაში კი მოწყობილობის ფიზიკური ამოღების გარეშე, მასში დაცული ინფორმაციის კოპირება მოახდინოს. რასაკვირველია, აღნიშნულ საგამოძიებო მოქმედებაზე ნებართვის გაცემის უფლებამოსილება მხოლოდ სასამართლოს გააჩნია, [393] ხოლო საგამოძიებო მოქმედების ჩატარების შუამდგომლობით სასამართლოსთვის მიმართვის უფლებამოსილება კი მხარეებს. თუმცა, კანონის დათქმის თანახმად, სასამართლოს წინაშე შუამდგომლობის დაყენება გამომძიებელს მხოლოდ პროკურორის თანხმობითა და დავალებით შეუძლია. [394] არსებობს აკრძალვაც, როდესაც დაუშვებელია ინფორმაციაზე წვდომის საშუალება მიეცეთ მხარეებს. კერძოდ, საპროცესო კოდექსის 161-ე მუხლის მიხედვით აკრძალულია ადვოკატსა და კლიენტს შორის არსებულ კომუნიკაციასა და იმ

[391] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 67 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [08.06.23].

[392] Criminal Procedural Code of Ukraine, BVR, 20/11/2012, Art. 159.

[393] იქვე.

[394] იქვე, მუხლი 160(1).

ნივთებსა და დოკუმენტებზე წვდომა, რომლებიც თან ერთვის ან კავშირშია მათ ურთიერთობასთან.

რაც შეეხება პირს, ვის მიმართაც გაიცემა სასამართლო ნებართვა, იგი ვალდებულია გამოძიებას მასალებზე წვდომის საშუალება მისცეს, ხოლო თავად ადრესატი უფლებამოსილია მოითხოვოს მისგან ამოღებული დოკუმენტების ასლების მისთვის დატოვება. [395] საინტერესოა შუამდგომლობისთვის დადგენილი მოთხოვნების დაკმაყოფილების საკითხიც. კერძოდ, აუცილებელია შუამდგომლობაში მითითება გაკეთდეს დანაშაულთან დაკავშირებულ გარემოებებზე და იმ მუხლზე, რომელზეც გამოძიება მიმდინარეობს, განისაზღვროს ის საგანი ან დოკუმენტი, რომლის მოპოვებაც იგეგმება, დაკმაყოფილებული იყოს ვარაუდის საფუძველი, რომ კონკრეტულ მასალებს ესა თუ ის პირი ფლობს ან შეიძლება ფლობდეს და რომ მას სისხლის სამართლის საქმისათვის მტკიცებულებითი ღირებულება გააჩნია. კანონით დაცულ საიდუმლო ინფორმაციასთან წვდომის შემთხვევაში დასაბუთული უნდა იყოს, რომ სხვა გზით შეუძლებელია კონკრეტული გარემოებების მტკიცება და ამ მიზნით მასალებზე წვდომა აუცილებელია. [396] სწორედ კანონით დაცულ საიდუმლოთა ჩამონათვალში ექცევა მომხმარებლის შესახებ ინფორმაცია. მათ შორისაა პირის ჯანმრთელობასთან დაკავშირებული მონაცემები, კომერციული საიდუმლოება, საბანკო საიდუმლოება, სხვა პირადი ხასიათის ინფორმაცია და ა.შ.[397] შესაბამისად, ასეთი სახის ინფორმაციაზე წვდომის შუამდგომლობის დაყენებისას გამომძიებელი თუ ზოგად მოთხოვნებთან ერთად დაასაბუთებს, რომ ინფორმაციაზე წვდომა დაეხმარება კონკრეტული გარემოებების დამტკიცებაში და სხვა გზით შეუძლებელია მისი პოზიციის დასაბუთება, სასამართლო ვალდებულია დააკმაყოფილოს მისი შუამდგომლობა.[398]

შეჯამებისთვის, უკრაინის ეროვნული კანონმდებლობით, კომპიუტერული მონაცემის წარმოდგენის ბრძანების ალტერნატიულ ღონისძიებად, ნივთებსა და დოკუმენტებზე დროებითი წვდომის საგამოძიებო მოქმედება განიხილება. შინაარსობრივად იგი კომპიუტერული მონაცემის წარმოდგენის ბრძანებისა და

[395] იქვე, მუხლი 165.
[396] იქვე.
[397] იქვე, მუხლი 162.
[398] იქვე, მუხლი 163 (5-6).

ჩხრეკა-ამოღების ელემენტებს შეიცავს.[399] საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელია სასამართლო ნებართვა. ამასთან, დადგენილია მთელი რიგი მოთხოვნები შუამდგომლობის დაყენებისას, რაც ერთობლიობაში უფლებაში თვითნებური ჩარევისგან დაცვის მყარ გარანტიებს ქმნის. კონვენციის მე-18 მუხლიდან გამომდინარე მნიშვნელოვანია მომხმარებლის შესახებ ინფორმაცია სათანადო გარანტიების პირობებში ადვილად ხელმისაწვდომი იყოს გამოძიებისათვის. შესაბამისად, მისი საიდუმლო ინფორმაციისთვის მიკუთვნება და ამით დამატებითი ბარიერის შექმნა კონვენციის მიზნებიდან გამომდინარე გაუმართლებელია.[400]

7. შეჯამება

როგორც არაერთხელ გავამახვილეთ ყურადღება, „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული „კომპიუტერული მონაცემის წარმოდგენის ბრძანება“ ეფექტური საპროცესო მექანიზმია როდესაც სამართალდამცავ ორგანოს ქვეყნის ტერიტორიაზე მყოფი პირის, მათ შორის სერვის პროვაიდერის, მფლობელობაში ან ზედამხედველობის ქვეშ არსებული კომპიუტერული სისტემიდან ან შემნახველი მოწყობილობიდან ინფორმაციის გამოთხოვა ესაჭიროება და მეორე, როდესაც მომხმარებლის შესახებ არსებული ელექტრონული ინფორმაცია იმ პროვაიდერის მფლობელობაში ან კონტროლს ქვეშაა, რომელიც მართალია ადგილობრივი ქვეყნის ტერიტორიაზე არ არის რეგისტრირებული, თუმცა მომსახურებას ადგილობრივ მოსახლეობას სთავაზობს. შესაბამისად, როგორც ელექტრონული მტკიცებულების მოპოვების, ისე გამოძიების პროცესში ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის უზრუნველყოფის კუთხით, ნორმის ეროვნულ კანონმდებლობაში სრულყოფილ იმპლემენტირებას გარდამტეხი მნიშვნელობა აქვს. დასახული მიზნიდან გამომდინარე, აუცილებელია საგამოძიებო მოქმედება ეროვნულ კანონმდებლობაში

[399] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 80 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [09.06.23].

[400] Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, 2017, 11 <https://rm.coe.int/3271-3608-report-on-eap-state-may2017/1680728bca> [09.06.23].

დამოუკიდებელი სახით იყოს გათვალისწინებული, ხოლო საკითხის საკანონმდებლო მოწესრიგება უფლებაში თვითნებური ჩარევისგან დასაცავ სათანადო პროცესუალურ გარანტიებს მოიცავდეს.[401] შესაბამისად, კონვენციის მოთხოვნების შესასრულებლად მნიშვნელოვანია აღმოსავლეთ პარტნიორობის პროექტში შემავალი ქვეყნების კანონმდებლობა ზემოთდასახელებულ პირობებს აკმაყოფილებდეს.

ნორმატიული კანონმდებლობის შესწავლამ დაგვანახა, რომ კომპიუტერული მონაცემის გადაცემის საგამოძიებო მოქმედება სრულყოფილად არცერთი პარტნიორი ქვეყნის კანონმდებლობით არ არის მოწესრიგებული. კანონმდებლობაში ვერ ვხვდებით კონვენციასთან დაკავშირებულ ტერმინთა დეფინიციას და თავის მხრივ ელექტრონული მტკიცებულება, მტკიცებულების ან დოკუმენტის ფართო ცნების დახმარებით განიმარტება. შენახული კომპიუტერული მონაცემის მოპოვება ძირითადად ჩხრეკა-ამოღებისათვის დადგენილი წესით ხდება. „კომპიუტერული მონაცემის დათვალიერების“ საგამოძიებო მოქმედებას ვხვდებით ბელარუსიის კანონმდებლობაში, ხოლო უკრაინის შემთხვევაში კი „ნივთებსა და დოკუმენტებზე დროებითი წვდომის“ შესაძლებლობას, რომელიც შინაასრობრივად კომპიუტერული მონაცემის წარმოდგენის ბრძანებისა და ჩხრეკა-ამოღების ელემენტებს შეიცავს.[402]

დარწმუნებით შეიძლება ითქვას, რომ ზემოთ განხილულ ქვეყნებს შორის „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლის მოთხოვნებთან ახლოს მხოლოდ საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობა დგას. დამოუკიდებელი საგამოძიებო მოქმედების სახით არის გათვალისწინებული კომპიუტერული მონაცემის წარმოდგენის ბრძანება. საპროცესო კანონმდებლობით განმარტებულია კომპიუტერული სისტემის, კომპიუტერული მონაცემის, მომსახურების მომწოდებლის, ინტერნეტტრაფიკის მონაცემის შინაარსი და მომხმარებლის შესახებ ინფორმაცია. სსსკ-ის 136-ე მუხლის პირველი და მეორე ნაწილებით შესაძლებელია როგორც ქვეყნის ტერიტორიაზე მყოფი პირისგან ელექტრონული ინფორმაციის მოპოვება, ისე მომსახურების მიმწოდებლისგან

[401] 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> [09.06.23].

[402] Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018, 80 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [09.06.23].

მომხმარებლის შესახებ მონაცემების გამოთხოვა. ხოლო დაბრკოლება, რაც წლების განმავლობაში კონვენციის მოთხოვნების დაკმაყოფილებისგან ყველაზე მეტად გვაშორებდა, მხედველობაში გვაქვს, საგამოძიებო მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვა და მასზე ფარული საგამოძიებო მოქმედებებისათვის დადგენილი წესებით მოქმედების ვალდებულება, 2022 წელს განხორციელებული საკანონმდებლო ცვლილებით მოიხსნა[403]და კომპიუტერული მონაცემის გამოთხოვა, ინტერნეტ ტრაფიკისა და შინაარსობრივი მონაცემების მიმდინარე რეჟიმში მოპოვებასთან შედარებით, მსუბუქ მოწესრიგებას დაექვემდებარა.[404]

[403] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24/05/2022.

[404] Cybercrime Strategies, Procedural Powers and Specialized institutions in the Eastern Partnership Region – State of Play, Council of Europe, 2017, 18 <https://rm.coe.int/3271-3608-report-on-eap-state-may2017/1680728bca> [09.06.23].
იხ. *Dragicevic D., Juric M.,* Article 15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [09.06.23].

თავი V. კომპიუტერული მონაცემის გამოთხოვის საკითხი საზღვარგარეთის კანონმდებლობის მიხედვით

1. ამერიკის შეერთებული შტატების კანონმდებლობის მიხედვით

1.1. მომხმარებლის და მის მიერ განხორციელებული კომუნიკაციის შესახებ მონაცემთა გადაცემის ვალდებულება

მომსახურების მომწოდებლებისგან კომპიუტერული მონაცემის გამოთხოვა „შენახულ კომუნიკაციათა აქტის“ 18. U.S.C. § 2701-2712 (“SCA”) მუხლების საფუძველზე ხორციელდება. პროვაიდერი კომპანია მისი საქმიანობის ფარგლებში მომხმარებელთან დაკავშირებულ მნიშვნელოვანი მოცულობის ინფორმაციას აგროვებს. შესაძლოა ეს მომხმარებლის სახელი, გვარი, მისამართი, საბანკო ბარათის მონაცემები, ლოგირების მონაცემები, IP მისამართი, ელ. შეტყობინებები ან ნებისმიერი სხვა სახის ინფორმაციაც იყოს. შესაბამისად, გამომძიებელმა თუ პროკურორმა, რომელსაც პროვაიდერისგან მომხმარებელთან დაკავშირებული ინფორმაციის გამოთხოვა სურს, ყურადღება „შენახულ კომუნიკაციათა აქტით“ გათვალისწინებულ მონაცემთა სახეებს უნდა მიაპყროს. აღნიშნული აქტის თანახმად, მონაცემები სამ ძირითად სახედ არის დაყოფილი. კერძოდ, განსაზღვრულია ა) მომხმარებლის ძირითადი მონაცემები, ბ) მომხმარებელთან დაკავშირებული არაშინაარსობრივი ხასიათის ჩანაწერები და მონაცემები, და გ) შინაარსობრივი მონაცემები. მონაცემთა პირველი ორი სახე არაშინაარსობრივ მონაცემთა კატეგორიას განეკუთვნება, თუმცა მათი ცნების ქვეშ განსხვავებული ინფორმაცია ერთიანდება და მათი განხილვა, გააზრება და ერთმანეთისგან გამიჯვნა პროცესუალური კუთხით მნიშვნელოვანია, ვინაიდან სწორედ მონაცემის სახეზეა დამოკიდებული მისი მოპოვების სამართლებრივი გზა. ამრიგად, განვიხილოთ თითოეული მათგანი.

ა) მომხმარებლის ძირითადი მონაცემები

მომხმარებლის ძირითადი მონაცემის განმარტებას „შენახულ კომუნიკაციათა აქტის“ 2703(c)(2) მუხლში ვხვდებით. იგი მომხმარებლის სახელსა და გვარს, მის მისამართს, ადგილობრივი და საქალაქთაშორისო სატელეფონო კავშირის შესახებ ჩანაწერებს, კომუნიკაციის დაწყების, დამთავრებისა და ხანგრძლივობის შესახებ მონაცემებს, გამოყენებული სერვისის შესახებ ინფორმაციას, მოწყობილობისა და მომხმარებლის საიდენტიფიკაციო მონაცემებს, მათ შორის დროებით მინიჭებული ქსელის

მისამართს (IP) და ინფორმაციას მომსახურების გადახდის საშუალების შესახებ, მათ შორის საკრედიტო ბარათის ან საბანკო ანგარიშის მონაცემებს, აერთიანებს.

ნიშანდობლივია, რომ ძირითადად მონაცემები მომხმარებლის ვინაობასთან, პროვაიდერსა და მას შორის არსებულ საკონტრაქტო ურთიერთობასთან და აბონენტის მიერ განხორციელებულ კომუნიკაციასთან არის დაკავშირებული. [405] სწორედ ამიტომ გამოიყენება მათ მიმართ ტერმინი „ძირითადი მონაცემები“.

რაც შეეხება გამოძიების მიზნებისთვის მათ შეგროვებას, კანონი სახელისუფლებო ორგანოებს საშუალებას აძლევს პროვაიდერებისგან ინფორმაციის გადაცემა-გამჟღავნება ბრძანების ე.წ. „Subpoena”-ს[406] საფუძველზე მოითხოვონ, რომლის გაცემის დასაბუთების სამართლებრივი ბარიერი საკმაოდ დაბალია.[407]

ბ) მომხმარებელთან დაკავშირებული არა შინაარსობრივი ხასიათის ჩანაწერები და მონაცემები

აღნიშნულ მონაცემთა განმარტებას „შენახულ კომუნიკაციათა აქტის“ 2703 (c)(1) მუხლში ვხვდებით, რომელიც მომხმარებლის ძირითად მონაცემებთან ერთად სხვა არა-შინაარსობრივი სახის ინფორმაციასაც მოიცავს. ძირითადად, იგი ლოგირების,[408] ადგილმდებარეობის შესახებ, ფიჭური ქსელის მონაცემებს, ელექტრონული ფოსტის მისამართებს, მობილური ტელეფონის მიერ გამოყენებული ანძების შესახებ ინფორმაციას, აერთიანებს.

მომხმარებლის ძირითადი მონაცემების მსგავსად, აღნიშნული ინფორმაციაც არა შინაარსობრივი ხასიათისაა, თუმცა კანონმდებელმა მათი გამიჯვნა და მოპოვებისთვის განსხვებული პროცესუალური მოწესრიგება ამჯობინა. მიზეზი, პირადი ცხოვრების უფლების დაცვის საკითხია. მოცემული ინფორმაციის საფუძველზე პიროვნების მთლიანი „ონლაინ“ პროფილის შექმნაა შესაძლებელი, რაც

---

[405] *Goldfoot J.,* Compelling Online Providers to Produce Evidence under ECPA, Obtaining and Admitting Electronic Evidence, The United States Attorneys' Bulletin, Vol. 59, №6, 2011, 36.

[406] *Subpoena decus tecum* (ლათ. duces tecum - წარმოადგინე) - გულისხმობს მესამე პირის დავალდებულების შესაძლებლობას წარმოადგინოს მის ხელთ არსებული დოკუმენტები ან ჩანაწერები. მისი გამოყენება შეუძლია როგორც პროკურორს, ისე დაცვის მხარეს და შესაძლებელია ადრესატს მიეწოდოს როგორც ელექტრონული ფოსტის საშუალებით, ისე პირისპირ ბრძანების ხელზე გადაცემით.

[407] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 128.

[408] *United States v. Allen*, 53 M.J. 402, 409, 2000.

თავის მხრივ ინდივიდის პირადად ცხოვრებაში მეტი ინტენსივობით ჩარევას იწვევს. [409] შესაბამისად, მომხმარებელთან დაკავშირებული არა შინაარსობრივი ჩანაწერებისა და მონაცემების მოსაპოვებლად, სასამართლო ნებართვაა საჭირო. [410] ნიშანდობლივია, რომ იმავე სასამართლო ნებართვით გამომძიებლებს მომხმარებლის ძირითადი მონაცემების მოპოვებაც შეუძლიათ.

რაც შეეხება უშუალოდ სასამართლოს ნებართვას, მის გასაცემად აუცილებელია საგამოძიებო ორგანომ სასამართლოს „კონკრეტული და დასაბუთებული ფაქტები წარუდგინოს [411] , რომელიც დაარწმუნებს მოსამართლეს რომ შუამდგომლობით მოთხოვნილი ინფორმაცია რელევანტური და არსებითია მიმდინარე სისხლის სამართლის საქმისთვის". ნებართვის გაცემის უფლებამოსილება აქვს ფედერალური ან რაიონული სასამართლოს მოსამართლეს (მათ შორის მაგისტრი მოსამართლე), რომელსაც გააჩნია იურისდიქცია გამოსაძიებელ დანაშაულზე ან, თუ კომპანია ფუნქციონირებს ან კომპიუტერული მონაცემი ინახება მის სამოქმედო ტერიტორიაზე. [412] ნიშანდობლივია, რომ ნებართვის გაცემისთვის აუცილებელი სტანდარტი გარკვეულწილად გამორიცხავს შესაძლებლობას საგამოძიებო მოქმედების განხორციელება მაკომპრომიტირებელი მასალების ძებნას (Fishing Expedition) დაემსგავსოს,[413] თუმცა, უზენაესმა სასამართლომ, მოცემული სტანდარტი ადგილმდებარეობის შესახებ მოცულობითი ინფორმაციის გამოთხოვისთვის, რომელიც „თითქმის აბსოლუტური დაკვირვების" შესაძლებლობას იძლევა პიროვნების გადაადგილებაზე, არასაკმარისად მიიჩნია და განმარტა, რომ მათ მისაღებად „დასაბუთებული ვარაუდის სტანდარტით" გაცემული სასამართლო ნებართვის, კერძოდ კი ჩხრეკის განჩინების არსებობაა საჭირო, რაც საგამოძიებო მოქმედების გამოყენების დასაბუთებისთვის მეტად მაღალ სტანდარტს აწესებს. [414] საყურადღებოა, რომ სასამართლო ნებართვის გარდა, მომხმარებელთან

[409] *Goldfoot J.,* Compelling Online Providers to Produce Evidence under ECPA, Obtaining and Admitting Electronic Evidence, The United States Attorneys' Bulletin, Vol. 59, №6, 2011, 37.
[410] SCA, 18 U.S.C. § 2703 (c)(1)(b).
[411] *Terry v. Ohio,* 392 U.S. 1 (1968).
[412] ECPA, 18 U.S.C. § 2711 (3) (a).
[413] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 131.
[414] *Carpenter v. United States,* 2018.

დაკავშირებული არაშინაარსობრივი მონაცემების მოპოვება ჩხრეკის განჩინებითა[415] და თავად მომხმარებლის თანხმობის[416] საფუძველზეც შესაძლებელია. შესაბამისად, სასამართლომ აღნიშნული განმარტებით არა თუ ახალი სტანდარტი დაადგინა, არამედ კანონით გათვალისწინებულ მექანიზმებს შორის მონაცემთა მოცულობისა და პრივატულობის გათვალისწინებით უპირატესობა „ჩხრეკის განჩინებას“ მიანიჭა.

გ) შინაარსობრივი მონაცემები

შინაარსობრივ მონაცემებში ელექტრონული ფოსტა, ხმოვანი შეტყობინება, აუდიო-ვიდეო ჩანაწერი, დოკუმენტი და ნებისმიერი სხვა ინფორმაცია მოიაზრება, რომელიც კომუნიკაციის მიზანს და არსს უკავშირდება. [417] სასამართლოების მიერ „შინაარსობრივი მონაცემი“ კიდევ უფრო ფართოდ, არსებულ სინამდვილესთან კავშირში განიმარტება და ასე მაგალითად, სოციალური ქსელის „ინსტაგრამის ისტორიას“(Instagram Story) შინაარსობრივი ხასიათის მონაცემს მიაკუთვნებენ.[418]

ნიშანდობლივია, რომ „ელექტრონული კომუნიკაციების შესახებ კანონი“ შინაარსობრივ მონაცემებს ორ მოცემულობაში განიხილავს. ერთი, როდესაც იგი ელექტრონული კომუნიკაციის პროვაიდერთან შემდგომი კომუნიკაციის მიზნით ინახება (ECS)[419] და მეორე, როდესაც იგი ელექტრონული კომუნიკაციის მონაცემთა შენახვისა და დამუშავების სერვის პროვაიდერთან არის განთავსებული (RCS). [420] საყურადღებოა, რომ დღეის მდგომარეობით სატელეკომუნიკაციო კომპანიები ორივე ფუნქციას ითავსებენ. [421] მართალია პრაქტიკული კუთხით რთულია მათი ურთიერთგამიჯვნა, [422] თუმცა სამართლებრივი თვალსაზრისით, პრინციპული

---

[415] SCA, 18 U.S.C. § 2703 (c) (1) (a).

[416] იქვე, 18 U.S.C. § 2703 (c) (1) (c).

[417] იქვე, 18 U.S.C. § 2510(8).

[418] *Facebook, Inc. V. Pepe,* A.3d. WL 1870591, 2020. იხ. *C.f. Brown v. Waddell*, 50 F.3d 285, 292 (4th. Cir. 1995).

[419] *Freedman v. America Online Inc.,* 325 F. Supp. 2d 638, 634 n.4 (E.D. Va. 2004).

[420] *Steve Jackson Games, Inc. v. US Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993).

[421] *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008).

[422] გამიჯვნის დროს მნიშვნელოვანია ყურადღება მივაქციოთ პროვაიდერის კავშირს ინფორმაციასთან. მაგალითისთვის, ინდივიდი პროვაიდერის მეშვეობით იღებს ელექტრონულ შეტყობინებას. შესაბამისად, იგი სარგებლობს სატელეკომუნიკაციო სერვისით, ხოლო კომუნიკაციის დასრულებამდე ან შეტყობინების გაცნობამდე ან მასთან დაკავშირებულ შემდგომ გადაწყვეტილებამდე, ინფორმაცია პროვაიდერთან, სატელეკომუნიკაციო სისტემის მეხსიერებაში ინახება (ECS). ECS -ში არსებული ინფორმაცია არის დროებითი, შუალედური, გადაცემისთვის განკუთვნილი ან თუნდაც სარეზერვო მიზნებისთვის. საყურადღებოა, რომ ECS-ში 180 დღეზე მეტი დროით მოთავსებული ინფორმაციის მოპოვებაზე იგივე წესები მოქმედებს, რაც RCS-ში არსებულ მონაცემებზე.
იმ შემთხვევაში, თუ მომხმარებელი დაასრულებს კომუნიკაციას და გადაწყვეტს ინფორმაციის შენახვას, მაშინ პროვაიდერი კომპანია მონაცემთა შენახვის სერვის სთავაზობს მომხმარებელს (RCS).

მნიშვნელობისაა ინფორმაციის განთავსების ადგილი, ვინაიდან საგამოძიებო ორგანოს სატელეკომუნიკაციო სერვისის მიმწოდებლისგან, სატელეკომუნიკაციო სისტემაში 180 დღეზე ნაკლები დროით შენახული შინაარსობრივი მონაცემების გამოთხოვა მხოლოდ სასამართლო ნებართვის, კერძოდ კი ჩხრეკის განჩინების საფუძველზე შეუძლია,[423] ხოლო 180 დღეზე მეტი დროით შენახული ინფორმაციის მოსაპოვებლად ნაკლებ მკაცრი მოთხოვნების დაკმაყოფილება უწევს.

რაც შეეხება თავად მონაცემთა შემნახველ პროვაიდერს, მისგან შინაარსობრივი მონაცემის გამოთხოვა ა) ჩხრეკის განჩინებით, ბ) მტკიცებულების გადაცემის ბრძანებითა (Subpoena) და გ) სასამართლო ნებართვის საფუძველზე, ხელმისაწვდომია. თუმცა, ჩხრეკის განჩინებისგან განსხვავებით, "Subpoena"-სა და სასამართლო ნებართვის საფუძველზე ინფორმაციის მოპოვებისას, სავალდებულოა მომხმარებლის ინფორმირება საგამოძიებო მოქმედების ჩატარების თაობაზე.[424] რა თქმა უნდა, ობიექტური საფუძვლის არსებობის პირობებში, გათვალისწინებულია გამონაკლისი მომხმარებლის დროული ინფორმირების ვალდებულებიდან და შეტყობინების გადავადება მიზანშეწონილია თუ მომხმარებლისთვის ინფორმაციის მიწოდებით შესაძლოა საფრთხე შეექმნას პირის სიცოცხლეს ან ჯანმრთელობას, შეიძლება თავი აარიდოს გამოძიებას ან გაანადგუროს მტკიცებულებები, დააშინოს მოწმეები ან სხვაგვარად ხელი შეუშალოს გამოძიებისა და მართლმსაჯულების განხორციელების პროცესს.[425] აღსანიშნავია, რომ სასამართლო ნებართვის გაცემისას, შეტყობინების გადავადების შესახებ მითითება კეთდება იქვე, ხოლო თუ ინფორმაციის გამოთხოვა ბრძანების, „Subpoena"-ს საფუძველზე ხორციელდება, გადავადების შესახებ წერილობითი დოკუმენტი ზედამხედველი თანამდებობის პირის მიერ გაიცემა. ზედამხედველი თანამდებობის პირი კი შეიძლება იყოს საქმის გამოძიებაზე პასუხისმგებელი გამომძიებელი ან მისი თანაშემწე, საგამოძიებო უწყების შტაბ-ბინის ან რეგიონული ოფისის გამომძიებელი, მთავარი პროკურორი ან მისი პირველი მოადგილე, ან რაიონული პროკურორი.

გასათვალისწინებელია, რომ კანონის მიღების დროს, ტექნოლოგიური განვითარების ფონზე ფუნქციათა ამგვარ გამიჯვნას გადამწყვეტი მნიშვნელობა ჰქონდა, თუმცა, დღეს სატელეკომუნიკაციო პროვაიდერის მხრიდან აღნიშნული ფუნქციების შესრულება მისი საქმიანობის განუყოფელ ნაწილს წარმოადგენს.

[423] SCA, U.S.C. § 2703 (a).

[424] იქვე, § 2703 (b) (1) (a).

[425] იქვე, §2705 (b).

საყურადღებოა, რომ მონაცემთა შემნახველი პროვაიდერისგან ან სატელეკომუნიკაციო სისტემაში 180 დღეზე მეტი დროით შენახულ შინაარსობრივი მონაცემის, მტკიცებულების გადაცემის ბრძანების „Subpoena" საფუძველზე მოპოვება გარკვეულწილად საფრთხეს უქმნის პირადი ცხოვრების დაცვის უფლებას. თუ გავითვალისწინებთ, რომ შინაარსობრივი მონაცემების პრივატულობიდან გამომდინარე, მისი კონფიდენციალურობის დაცვის მოლოდინი მაღალია, უმჯობესი იქნებოდა, ადმინისტრაციული უწყების ნაცვლად შინაარსობრივ მონაცემებზე წვდომა მხოლოდ სასამართლო ბრძანებითა(მომხმარებლის ინფორმირების ვალდებულების დაცვით) და ჩხრეკის განჩინების საფუძველზე იყოს ნებადართული. სასამართლო ბრძანების, რომლის ფარგლებშიც საგამოძიებო ორგანო სასამართლოს „კონკრეტულ და დასაბუთებულ ფაქტებს წარუდგენს[426], რომელიც დაარწმუნებს მოსამართლეს რომ შუამდგომლობით მოთხოვნილი ინფორმაცია რელევანტური და არსებითია მიმდინარე სისხლის სამართლის საქმისთვის". ამასთან, სასამართლოს ზედამხედველობის ფარგლებში შეფასდება მომხმარებლისთვის შეტყობინების ვალდებულების გადავადების აუცილებლობის საკითხიც, რაც ერთობლიობაში მნიშვნელოვნად აამაღლებს პირადი ცხოვრების დაცვის ხარისხს.

პრობლემურია აგრეთვე ელექტრონული კომუნიკაციის პროვაიდერისა (ECS) და ელექტრონული კომუნიკაციის მონაცემთა შემნახველი პროვაიდერის (RCS) ხელოვნურად გამიჯვნის საკითხი. როგორც უკვე აღვნიშნეთ, არსებულ რეალობაში სატელეკომუნიკაციო კომპანიები მულტიფუნქციურად, ორივე სახის სერვისს სთავაზობენ მომხმარებლებს. ამრიგად, რთული დასადგენია თუ დროის კონკრეტულ მონაკვეთში, რომელი სერვისით სარგებლობს მომხმარებელი. შესაბამისად, ინფორმაციასთან პროვაიდერის დამოკიდებულების მიხედვით სამართლებრივი მოწესრიგების შერჩევა არახელსაყრელია.[427] უმჯობესი იქნება მათი ერთი ცნების ქვეშ გაერთიანება, როგორიცაა „ქსელის სერვის პროვაიდერი" (NSP), ხოლო ინფორმაციის მოპოვების განსხვავებული სამართლებრივი მოწესრიგების, მონაცემთა ტიპის მიხედვით გადაწყვეტა.[428] გარდა იმისა, რომ ამგვარი შესწორებით უცვლელი დარჩება

[426] *Terry v. Ohio,* 392 U.S. 1 (1968).

[427] *Kerr S. O.,* A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 The George Washington Law Review 1208, 2004, 1235.

[428] იქვე.

კანონის მიზანი, იგი უფრო განჭვრეტადი და თანამედროვე ტექნოლოგიებზე მორგებული გახდება.[429]

შეჯამებისთვის, მომხმარებელთან დაკავშირებული მონაცემების, მათ შორის მის მიერ განხორციელებული კომუნიკაციის შინაარსის შესახებ ინფორმაციის მოპოვება „შენახულ კომუნიკაციათა აქტის“ 2703 მუხლის საფუძველზე ხორციელდება და ამავე ნორმაზე დაყრდნობით საგამოძიებო მოქმედების ოთხი ეტაპის გამოყოფაა შესაძლებელი. პირველი ეტაპი, ეს მონაცემთა დაცვაა.[430] მიუხედავად იმისა, რომ იგი სავალდებულო მოქმედებას არ წარმოადგენს, სასამართლო ნებართვის მიღებამდე ან/და სხვა კანონით გათვალისწინებული პროცედურის განხორციელებამდე მტკიცებულების დაკარგვის/განადგურების თავიდან აცილების მიზნით მონაცემთა ე.წ. „გაყინვა“ და უსაფრთხოდ შენახვაა მიზანშეწონილი. [431] როგორც წესი, ინფორმაციის შენახვა 90 დღის ვადით არის შესაძლებელი, თუმცა, ვადის გახანგრძლივება როგორც პროკურორის, ისე გამომძიებლის მოთხოვნის საფუძველზე დასაშვებია და ადრესატი პროვაიდერისთვის მისი გაგზავნა ელექტრონული ფოსტით ან ონლაინ პორტალის მეშვეობით ხორციელდება.[432] საყურადღებოა, რომ მონაცეთა უსაფრთხოდ შენახვის მოთხოვნის გაგზავნისას, უფლებამოსილი პირები მოკლებულნი არიან შესაძლებლობას პროვაიდერი კომპანიისგან მოითხოვონ იმ ინფორმაციის შენახვა, რომელიც მოთხოვნის გაგზავნის დროისთვის არ იყო შექმნილი. [433] რაც შეეხება მეორე ეტაპს, მას მოსაპოვებელი მონაცემის სახეობის განსაზღვრა წარმოადგენს, რომელთანაც ავტომატურად არის დაკავშირებული შემდგომი, მესამე ეტაპი, რაც შესაბამისი სამართლებრივი პროცედურის შერჩევა/გამოყენებას გულისხმობს. ხოლო ბოლო და მეოთხე ეტაპად კი შესაძლოა პროვაიდერთა მიმართ ინფორმაციის გამჟღავნების აკრძალვის შესახებ ბრძანების გაცემა მივიჩნიოთ.[434]

---

[429] იქვე, 1237.

[430] SCA, U.S.C. § 2703 (f) (1).

[431] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 58.

[432] იქვე.

[433] ასეთ დროს მათ შემდეგი აქტებით უნდა იხელმძღვანელონ: Pen Register and Trap and Trace Act, 18 U.S.C. §§ 3121-3127; Wiretap Act, 18 U.S.C. §§ 2510-2522.

[434] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 59.

1.2. მომხმარებელთან დაკავშირებული მონაცემების ნებაყოფლობით გადაცემა

აშშ-ს კანონმდებლობა ტელეკომუნიკაციის პროვაიდერებისგან სავალდებულო წესით მონაცემთა გამოთხოვის გარდა, ინფორმაციის ნებაყოფლობით გადაცემის წესს ითვალისწინებს. [435] მომსახურების მიმწოდებლები უფლებამოსილნი არიან მომხმარებელთან დაკავშირებული როგორც შინაარსობრივი, ისე არა შინაარსობრივი ხასიათის ინფორმაცია და ჩანაწერები ნებაყოფლობით გადასცენ როგორც სახელმწიფო, ისე არასამთავრობო ორგანიზაციებს.[436] შესაბამისად, თუ პროვაიდერთა მხრიდან საგამოძიებო უწყებისთვის ინფორმაციის გადაცემა ნებაყოფლობით ხასიათს ატარებს, სასამართლო ნებართვა, ჩხრეკის განჩინება ან თუნდაც მტკიცებულების წარმოდგენის ბრძანება „Subpoena" საჭირო არ არის.[437]

როდესაც პროვაიდერთა მხრიდან მონაცემთა ნებაყოფლობით გამჟღავნებაზე ვსაუბრობთ, ყურადღება უნდა გავამახვილოთ მათი მომსახურება საზოგადოებისთვის ხელმისაწვდომია თუ არა, ვინაიდან „შენახულ კომუნიკაციათა აქტით" (SCA) მონაცემთა გამჟღავნებასთან დაკავშირებული შეზღუდვები კერძო კომპანიებზე არ ვრცელდება. [438] გამომდინარე აქიდან, თუ მომსახურების მიმწოდებლის მიერ შემოთავაზებული სერვისები საჯაროდ ხელმისაწვდომია, მაშინ SCA - ით განსაზღვრული გამონაკლისების გარდა, აკრძალულია როგორც შინაარსობრივი, ისე მომხმარებელთან დაკავშირებული სხვა ხასიათის ჩანაწერების გამჟღავნება.[439]

როგორც წესი ორივე სახის მონაცემთა ნებაყოფლობით გადაცემას ხშირ შემთხვევაში ადგილი აქვს, როდესაც პროვაიდერს კეთილსინდისიერად სჯერა, რომ არსებობს გადაუდებელი აუცილებლობა, საფრთხე ემუქრება პირის სიცოცხლეს ან ჯანმრთელობას და საგანგებო მდგომარეობასთან დაკავშირებული კომუნიკაციის შინაარსის გამჟღავნება აუცილებელია. [440] ასეთ დროს პროვაიდერთა მოთხოვნაა, სახელმწიფო უწყებებმა მიაწოდონ დეტალური ინფორმაცია საგანგებო

[435] SCA, 18 U.S.C. §2702.

[436] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 135.

[437] იქვე.

[438] SCA, 18 U.S.C. §2702(a).

[439] იქვე, §2702.

[440] იქვე, §2702 (b)(8), (c)(4).

მდგომარეობის შესახებ და ის თუ როგორ დაეხმარებათ მას მოთხოვნილი ინფორმაცია საკითხის მოგვარებაში.[441] მეტიც პროვაიდერთა გარკვეულმა ნაწილმა სპეციალური მიმართვის ფორმებიც კი შეიმუშავეს.[442]

მონაცემთა ნებაყოფლობით გამჟღავნება დასაშვებია აგრეთვე, როდესაც არსებობს: მომხმარებლის ან კომუნიკაციის მხარის თანხმობა; [443] ინფორმაციის გადაცემა პროვაიდერის უფლებებისა თუ საკუთრების დაცვისთვის არის აუცილებელი; [444] გადაცემა ხდება „დაკარგული და ექპლუატირებული ბავშვების ეროვნული ცენტრისთვის“ [445] ; კომუნიკაციის შინაარსი უნებლიედ იქნა მოპოვებული პროვაიდერის მიერ და იგი სავარაუდო დანაშაულის ჩადენის შესახებ შეიცავს ინფორმაციას[446].

ნიშანდობლივია, რომ მიუხედავად ნებაყოფლობით გადაცემის შესაძლებლობისა, პროვაიდერი უფლებამოსილია უარი განაცხადოს ინფორმაციის გამჟღავნებაზე, რა დროსაც საგამოძიებო ორგანომ ელექტრონული ინფორმაციის მოპოვების სურვილის შემთხვევაში „შენახულ კომუნიკაციათა აქტის“ 2703 პარაგრაფის მიხედვით უნდა იხელმძღვანელოს.

1.3. ელექტრონული ფორმით შენახული მონაცემების მოპოვება

ელექტრონული ფორმით შენახული ინფორმაციის მოპოვება როგორც პირის თანხმობით, ისე მტკიცებულების გადაცემის უწყებითა „Subpoena” [447] და ჩხრეკა-ამოღების განჩინებით არის შესაძლებელი. [448] როგორც წესი გამომძიებელი თავდაპირველად ადრესატს თხოვნით მიმართავს და მისი თანხმობის შემთხვევაში გამოძიებისთვის საინტერესო ელექტრონული ინფორმაციის ასლს აკეთებს. იმ შემთხვევაში კი თუ მონაცემთა მფლობელი ნებაყოფლობით თანამშრომლობაზე უარს აცხადებს, შედარებით მძიმე სამართლებრივი მექანიზმები ამოქმედდებიან.[449]

---

[441] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 61.

[442] იქვე.

[443] SCA, 18 U.S.C. §2702 (b)(3), (c)(2).

[444] იქვე, §2702 (b)(5), (c)(3).

[445] იქვე, §2702 (b)(5), (c)(6).

[446] იქვე, §2702 (b)(7).

[447] 18 U.S.C. Fed. R. Crim. P. Rule 17.

[448] 18 U.S.C. Fed. R. Crim. P. Rule 41.

[449] იქვე.

მეტი თვალსაჩინოებისთვის, თითქმის ყველა სისხლის სამართლის საქმეზე მოთხოვნადი მტკიცებულების, ვიდეო ჩანაწერის მაგალითზე რომ ვისაუბროთ, ამერიკის შეერთებულ შტატებში გავრცელებული პრაქტიკაა მოქალაქეთა მიერ, ნებაყოფლობით საკუთარი ვიდეო კამერების შესახებ ინფორმაციის ადგილობრივი პოლიციის ბაზებში რეგისტრაცია. გარდა იმისა, რომ რეგისტრაციის დროს მითითება ხდება თუ რა მისამართზეა განთავსებული სამეთვალყურეო კამერა და კონკრეტულად რა არეალის კონტროლი მიმდინარეობს, აგრეთვე მოქალაქე ბაზაში თავად კამერის მაიდენტიფიცირებელ მონაცემებსაც აფიქსირებს. რა თქმა უნდა, აღნიშნული, პოლიციის თანამშრომლებს კამერაზე პირდაპირი წვდომის საშუალებას არ აძლევს, თუმცა მოცემულ ტერიტორიაზე დანაშაულის ჩადენისას, დროული და ეფექტური გამოძიების მიზნით, მოქალაქისგან ნებართვის მიღების შეთხვევაში, დისტანციურად შეუძლიათ განახორციელონ წვდომა ჩანაწერებზე.

როდესაც ვიდეო კამერის მფლობელი უარს აცხადებს ნებაყოფლობით თანამშრომლობაზე, ინფორმაციის მოპოვება მტკიცებულების გადაცემის ბრძანებით ან ჩხრეკა-ამოღების სასამართლო ნებართვის საფუძველზე ხორციელდება. ნიშანდობლივია, რომ გამოძიების ხელთ არსებობს კიდევ ერთი მნიშვნელოვანი სამართლებრივი ბერკეტი. კერძოდ, შესაძლოა ჩანაწერი მისი მფლობელის გვერდის ავლით, თავად სამეთვალყურეო კამერის პროვაიდერი კომპანიისგან გამოითხოვონ, რაც აგრეთვე დასაბუთებული ვარაუდის საფუძველზე გაცემული ჩხრეკა-ამოღების სასამართლო ნებართვას საჭიროებს.

ა) მტკიცებულების გადაცემის ბრძანება (Subpoena)

პირველ რიგში განვიხილოთ მტკიცებულების გადაცემის ბრძანების „Subpoena"-ს საკითხი. სისხლის სამართლის პროცესის ფედერალური წესების მე-17 მუხლის მიხედვით პირს შესაძლოა ჩანაწერების, დოკუმენტების, მონაცემების ან ბრძანებით განსაზღვრული ნებისმიერი საგნის წარმოდგენის ვალდებულება დაეკისროს. [450] ამასთან, კანონი ბრძანების ადრესატს აღჭურავს შესაძლებლობით, სასამართლოს წინაშე დააყენოს შუამდგომლობა ბრძანებით გაცემული ვალდებულების შეცვლის ან

[450] 18 U.S.C. Fed. R. Crim. P. Rule 17(c)(1).

გაუქმების მოთხოვნით, თუ მისი შესრულება არაგონივრულია ან ზედმეტად დიდ ტვირთს აკისრებს მას.[451]

ბ) ჩხრეკა-ამოღების ნებართვა

რაც შეეხება შენახული კომპიუტერული მონაცემის ჩხრეკა-ამოღების ნებართვის საფუძველზე მოპოვებას, ფედერალური სამართალდამცავი ოფიცრის ან პროკურორის მიერ დასაბუთებული ვარაუდის სტანდარტით დაყენებული შუამდგომლობის საფუძველზე მაგისტრატი ან რაიონული/შტატის მოსამართლე უფლებამოსილია ჩხრეკა-ამოღების ნებართვა გასცეს. [452] ნიშანდობლივია, რომ ნებართვა უნდა ითვალისწინებდეს მითითებას, რომლის თანახმად შესაძლებელია როგორც უშუალოდ ელექტრონული მონაცემის მატარებლის ამოღება, ისე კონკრეტული ინფორმაციის ამოღება-კოპირება. გასათვალისწინებელია, რომ თუ დოკუმენტით სხვაგვარად არ განისაზღვრება, ამოღებული ინფორმაციის შემდგომი დათვალიერება და გამოკვლევა დამოუკიდებელ, ახალ ნებართვას არ საჭიროებს.[453]

გარდა იმისა, რომ შუამდგომლობა წარდგენილ უნდა იქნას დასაბუთებული ვარაუდის სტანდარტის დაცვით [454] , აუცილებელია დაცული იყოს განჩინების დეტალიზაციის მოთხოვნაც.[455] კერძოდ, უნდა განისაზღვროს ადგილი, სადაც ძებნა უნდა ჩატარდეს და ის საგნები და ნივთები, რომელთა ამოღებაც უნდა მოხდეს.[456] მნიშვნელოვანია, იმდენად დეტალურად და გასაგები ენით იყოს აღწერილი ამოსაღები ნივთები, რომ გამომძიებელმა შეძლოს მათი განცალკევება სხვა არსებული საგნებისგან. [457] ამასთან, საგნების განსაზღვრა იმის მიხედვით უნდა მოხდეს, დაკმაყოფილებულია თუ არა კონკრეტული ნივთების მიმართ დასაბუთებული ვარაუდის სტანდარტი. შესაბამისად, როდესაც გამოძიებისთვის მნიშვნელოვანია კონკრეტული სახის ინფორმაცია, შემნახველ მოწყობილობაზე მეტად მითითება, რელევანტური მონაცემების შინაარსზე უნდა გაკეთდეს. [458] გასათვალისწინებელია,

---

[451] იქვე, R.17 (c)(2).
[452] იქვე, R.41 (b).
[453] იქვე, R. 41 (e)(2)(b).
[454] *Illinois v. Gates*, 462, U.S. 213, 238, 1983.
[455] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 69.
[456] *United States v. Grubbs*, 547 U.S. 90, 97, 2006.
[457] *Marron v. United States,* 275, U.S. 192, 296, 1927.
[458] *United States v. Otero,* 563 F.3d 1127, 1132 (10th Cir. 2009).

რომ გამოძიებისთვის რელევანტური ინფორმაციის ნაცვლად მთლიანი ელექტრონული მატარებლის ან თუნდაც სრული მონაცემების ამოღება არღვევს კონსტიტუციის მე-4 შესწორებით დაცულ პირადი ცხოვრების უფლებას. [459] აღნიშნული მოთხოვნების დაცვის ვალდებულება აიძულებს გამომძიებლებს თავი შეიკავონ პირად ცხოვრებაში უკანონო და დაუსაბუთებელი ჩარევისგან.[460]

გარდა იმისა, რომ ჩხრეკა-ამოღების საგამოძიებო მოქმედება სასამარლო ნებართვას საჭიროებს, მისი ჩატარება სასამართლო ნებართვის არსებობის გარეშეც მიზანშეწონილია თუ არსებობს პირის ნებაყოფლობითი თანხმობა[461], გადაუდებელი აუცილებლობით გამოწვეული საჭიროება ან ე.წ. „ღია სივრცის" დოქტრინის შემთხვევა. მიზანშეწონილია, თითოეული სამართლებრივი საფუძველი განვიხილოთ თანმიმდევრულად.

გ) პირის ნებაყოფლობითი თანხმობა

იმის გათვალისწინებით, რომ ჩხრეკა-ამოღების საგამოძიებო მოქმედება პირად ცხოვრებაში მაღალი ინტენსივობით ჩარევას გულისხმობს, აუცილებელია პირის მიერ გაცემული თანხმობა ნებაყოფლობით ხასიათს ატარებდეს. შესაბამისად უზენაესმა სასამართლომ რამდენიმე მნიშვნელოვანი ფაქტორი გამოყო, რომლებიც მხედველობაში უნდა მიიღოს როგორც მის ჩატარებაზე უფლებამოსილმა პირმა, ისე სასამართლომ მისი კანონიერების შემოწმებისას. კერძოდ ეს გარემოებებია ასაკი, განათლება, ფიზიკური და გონებრივი მდგომარეობა, თანხმობის გაცემის მომენტში პირი დაკავებული იყო თუ არა და განემარტა თუ არა თანხმობის გაცემაზე უარის თქმის უფლება. [462] თანხმობის გაცემის მომენტში აუცილებელია აგრეთვე განისაზღვროს თანხმობის ფარგლები და ის თუ ვინ არის უფლებამოსილი პირი გასცეს თანხმობა კომპიუტერული სისტემის ან ინფორმაციის ჩხრეკაზე.

თანხმობის ფარგლები, როგორც წესი ჩხრეკის საგნითა თუ ობიექტით და თანხმობის მოცულობის მიხედვით განისაზღვრება.[463] თუმცა, უშუალოდ თანხმობის მოცულობა „ობიექტური გონივრულობის" სტანდარტით დგინდება. კერძოდ, თუ რა დასკვნას

---

[459] *United States v. Riccardi,* 405, F.3d 852, 862 (10th Cir. 2005).
[460] *Andresen v. Maryland,* 427 U.S. 463, 482, n.11, 1976.
[461] *Schneckloth v. Bustamonte,* 412 U.S. 218, 219 (1973).
[462] იქვე, 226-227.
[463] *United States v. Pena,* 143 F.3d 1363, 1368, (10th Cir. 1998).

გამოიტანდა ტიპიური გონიერი ადამიანი გამომძიებლისა და ინდივიდის კომუნიკაციის შედეგად. თუ პოლიციელს ობიექტურად სჯერა, რომ თანხმობა კონკრეტული საგნების ჩხრეკის უფლებას აძლევდა, კონსტიტუციის მე-4 შესწორების მოთხოვნები დაკმაყოფილებულად ჩაითვლება.[464] ხოლო ისეთ შემთხვევაში, როდესაც ჩხრეკის ფარგლები აშკარად განსაზღვრულია, გამომძიებელი ვალდებულია პატივი სცეს შეთანხმებას.

კომპიუტერულ სისტემებთან დაკავშირებით კითხვებს ბადებს, კონკრეტულ ლოკაციაზე გაცემული ჩხრეკის თანხმობა, პოტენციურად გულისხმობს თუ არა თანხმობას იქ არსებული ელექტრონული მოწყობილობის დათვალიერებაზე. აქვს თუ არა უფლება გამომძიებელს, ჩართოს და დაათვალიეროს კომპიუტერული მოწყობილობა და მასში არსებული ინფორმაცია. შემთხვევის შეფასების დროს, სასამართლო, ყურადღებას პირის თანხმობაზე ამახვილებს. კერძოდ, ინდივიდის მიერ გაცემული თანხმობა პირდაპირ ან ირიბად მაინც თუ გულისხმობდა მისი დათვალიერების შესაძლებლობას და ამასთან, გამომძიებელმა თუ ითხოვა თანხმობა მოწყობილობის განთავსების ადგილის, საგნის თუ ობიექტის ჩხრეკაზე, ვინაიდან პრეცედენტული სამართლის მიხედვით, ობიექტის ჩხრეკაზე გაცემული თანხმობა, მასზე არსებული საგნების დათვალიერებასაც გულისხმობს.[465]

აშკარაა, რომ თანხმობის საფუძველზე ჩხრეკა-ამოღების ჩატარება ბევრ სირთულესთან არის დაკავშირებული. რთულია თანხმობის ფარგლების განსაზღვრა და დიდია რისკი ჩატარებული საგამოძიებო მოქმედების არაკანონიერად ცნობის. ამრიგად, დასაბუთებული ვარაუდის არსებობის პირობებში, უმჯობესია ინფორმაციის მოპოვება სასამართლო ნებართვის საფუძველზე მოხდეს.[466]

დ) მესამე პირების თანხმობა

ხშირია შემთხვევა როდესაც ადამიანები საზიარო კომპიუტერულ ტექნიკას იყენებენ. შესაბამისად თუ რომელიმე მათგანს გააჩნია ზიარი ინტერესი ან უფლებამოსილება

---

[464] *Florida v. Jimeno,* 500 U.S. 248, 251, (1991).

[465] *ფაფიაშვილი ლ.,* „თანხმობის საფუძველზე ჩხრეკის წარმოების პრობლემური საკითხები“ ჟურ. საკონსტიტუციო სამართლის მიმოხივა, VII გამოცემა, 2014, 50.

[466] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 19.

მასზე, [467] პოლიციის თანამშრომლები უფლებამოსილნი არიან ჩხრეკა-ამოღების ჩატარებისას ერთ-ერთი მათგანის თანხმობას დაეყრდნონ. [468] როგორც წესი ერთობლივი უფლებამოსილება ქონების ერთობლივი გამოყენებით, უმეტესი მიზნებისთვის მასზე წვდომითა და კონტროლით განისაზღვრება, რა დროსაც გონივრულია იმის განსაზღვრა, რომ თანამფლობელიდან ერთ-ერთს გააჩნია ნებართვის გაცემის უფლებამოსილება და მეორე მხარე აცნობიერებს რისკს, რომ საერთო საკუთრებაში არსებული ქონების ჩხრეკა შესაძლოა თანამფლობელის თანხმობის საფუძველზე ჩატარდეს. [469] შესაბამისად, კომპიუტერული ტექნიკის თანამფლობელს შეუძლია თანხმობა ფაილთა ჩხრეკაზე გასცეს. მაგალითისთვის, შეყვარებული წყვილის სახლში არსებული კომპიუტერის ჩხრეკაზე ნებართვა შესაძლოა ერთ-ერთა მათგანმა განაცხადოს, თუმცა თუ პირი საკუთარ მონაცემებზე წვდომისთვის პაროლს იყენებს, რომელიც სხვისთვის არ გაუზიარებია, პარტნიორის თანხმობა ვერ გავრცელდება პაროლით დაცული ფაილების ჩხრეკაზე. [470] საქმეში *ამერიკის შეერთებული შტატები სმიტის* წინააღმდეგ, სასამართლომ განმარტა, რომ მიუხედავად იმისა, რომ საცხოვრებელ ფართში მეუღლის კომპიუტერული მოწყობილობა განცალკევებით იყო განთავსებული, იგი არ უკრძალავდა ცოლს მის გამოყენებას და ამასთან, მას არ ჰქონია საკუთარი ანგარიში და დოკუმენტები პაროლით დაცული. შესაბამისად, მეუღლე უფლებამოსილი იყო თანხმობა გაეცხადებინა ქმრის პერსონალური კომპიუტერის ჩხრეკაზე.[471]

პრაქტიკული კუთხით, რთული განსასაზღვრია თუ რა მოცულობის უფლებამოსილება გააჩნიათ მესამე პირებს ქონებაზე. მეტიც, შესაძლოა პირი ცრუობდეს უფლებამოსილების არსებობაზე, თუმცა უზენაესი სასამართლოს ხედვით, ამგვარი თანხმობის საფუძველზე მოპოვებული მტკიცებულების დაუშვებლად ცნობა სულაც არ გამომდინარეობს კონსტიტუციის მე-4

---

[467] *ფაფიაშვილი ლ.,* „თანხმობის საფუძველზე ჩხრეკის წარმოების პრობლემური საკითხები“ ჟურ. საკონსტიტუციო სამართლის მიმოხივა, VII გამოცემა, 2014, 52.

[468] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 19.

[469] *United States v. Matlock,* 415 U.S. 164 (1974).

[470] *Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir. 2001).

[471] *United States v. Smith,* 27 F. Supp. 2d 1111 (C.D. I11. 1998).

შესწორებიდან.[472] სასამართლოს განმარტებით, ოფიცრებს შეუძლიათ მესამე პირის თანხმობას დაეყრდნონ, თუ არსებული ფაქტების სიფრთხილით შეფასებამ, მათ საშუალება მისცა ეფიქრათ, რომ ამ პირს მართლაც ჰქონდა თანხმობის გაცემის უფლებამოსილება.[473] მაგალითისთვის, პოლიციის თანამშრომლებმა ბრალდებულის მეუღლის თანხმობის საფუძველზე სახლის საერთო სივრცეში არსებული კომპიუტერი გაჩხრიკეს. მეუღლის განცხადებით, კომპიუტერზე წვდომა როგორც მას, ისე მის მეუღლეს ჰქონდა და ამასთან, ისინი არა თუ დამოუკიდებელი ანგარიშით, არამედ საკუთარი მონაცემების პაროლის დაცვის ფუნქციითაც კი არ სარგებლობდნენ. მოგვიანებით აღმოჩნდა, რომ ყოველდღიურად იგი დამოუკიდებელი პერსონალური კომპიუტერით სარგებლობდა, [474] თუმცა სასამართლომ დაადგინა, რომ პოლიციელებს გონივრული ვარაუდის საფუძველი მართლაც ჰქონდათ, რომ ქალბატონს თანხმობის გაცემის უფლებამოსილება ნამდვილად გააჩნდა.

აგრეთვე, შეფასების საგანია მშობლების მიერ ნებართვის გაცემის საკითხი შვილების საკუთრებაში არსებულ კომპიუტერულ მოწყობილობაზე. როგორც წესი, მშობლების თანხმობა არასრულწლოვანი შვილების საკუთრების თუ საცხოვრებელი ფართის ჩხრეკის თაობაზე კანონიერია, თუმცა საქმე რთულადაა როდესაც შვილები სრულწლოვანები არიან. [475] თუ სრულწლოვანი შვილები იხდიან სახლის ქირას, ფინანსურ მონაწილეობას იღებენ ოჯახურ ყოველდღიურობაში ან აშკარად უზღუდავენ მშობლებს საკუთარ ნივთებზე ან საცხოვრებელ ფართზე წვდომას, მაშინ მშობლები არ არიან უფლებამოსილნი თანხმობა განუცხადონ გამოძიებას ჩხრეკის ჩატარებაზე.[476]

აგრეთვე, აშშ-ს პრეცედენტულ სამართლში დადგა საკითხი თუ რამდენად უფლებამოსილია ტექნიკოსი გასცეს ნებართვა შესაკეთებლად დატოვებული კომპიუტერული მოწყობილობის ჩხრეკაზე. ხშირია შემთხვევა, როდესაც მომხმარებლის მიერ შესაკეთებლად დატოვებული კომპიუტერული მოწყობილობის

---

[472] *Ilinois v. Rodriguez,* 497 U.S. 177 (1990).

[473] *Terry v. Ohio*, 392, U.S. 1, 21-22 (1968).

[474] *United States v. Morgan,* 435 F.3d 660 (6th Cir. 2006).

[475] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 23.

[476] *United States v. Whitfield,* 939 F.2D 1071, 1075 (D.C. Cir. 1991).

დათვალიერებისას სპეციალისტი დანაშაულის ამსახველ ინფორმაციას აწყდება. მაგალითად, ტექნიკოსთან ვირუსებისგან გასათავისუფლებლად დატოვებული მეხსიერების დათვალიერებისას, იგი შემთხვევით ბავშვთა პორნოგრაფიის ამსახველ მასალას წააწყდა, [477] რის შესახებაც მან დაუყოვნებლივ პოლიციას აცნობა. პოლიციელთა მითითებით მან ფაილები დააკოპირა და მომდევნო დღეს პოლიციის განყოფილებაში მიიტანა, სადაც პოლიციელებმა ისინი დაათვალიერეს. [478] სასამართლოს განმარტებით სპეციალისტს მეხსირების ბარათი შეზღუდული მიზნით, კერძოდ კი შესაკეთებლად ჰქონდა გადაცემული, რაც მას არ აძლევდა უფლებას თანხმობა გაეცა ან ნება დაერთო პოლიციელთათვის მასში არსებული ინფორმაციის დათვალიერებაზე. მესამე პირთა მხრიდან ნებართვის გაცემისთვის აუცილებელია ქონების ერთობლივი გამოყენება, წვდომა და კონტროლი ძირითადი მიზნებისთვის,[479] რაც მოცემულ შემთხვევაში სახეზე არ იყო.[480]

ე) გადაუდებელი აუცილებლობა

კომპიუტერულ მონაცემებთან დაკავშირებით ძირითადად გადაუდებელი აუცილებლობის შემთხვევა სახეზეა როდესაც არსებობს მტკიცებულებათა განადგურების საფრთხე.[481] როდესაც პოლიციელებმა დაინახეს თუ როგორ შლიდა სავარაუდო დამნაშავე ფაილებს, მათ დაუყოვნებლივ ამოიღეს კომპიუტერული მოწყობილობა. მოცემულ საქმეზე კი სასამართლომ განმარტა, რომ სამართალდამცავებს არ სჭირდებოდათ სასამართლო ნებართვა კომპიუტერის ამოსაღებად, ვინაიდან ბრალდებულის მოქმედებამ გადაუდებელი აუცილებლობის შემთხვევა განაპირობა.[482]

სხვადასხვა კომპიუტერული მოწყობილობის შემთხვევაში, გადაუდებელი აუცილებლობა შეიძლება წარმოშვას მისი კვების წყაროს დაზიანებამ, ან როდესაც ახალი ინფორმაციის განთავსებამ შესაძლოა ძველი ინფორმაციის წაშლა გამოიწვიოს.

---

[477] *United States v. Barth*, 26 F. Supp. 2d (1998).

[478] იქვე, 933.

[479] *ფაფიაშვილი ლ.,* „თანხმობის საფუძველზე ჩხრეკის წარმოების პრობლემური საკითხები“ ჟურ. საკონსტიტუციო სამართლის მიმოხივა, VII გამოცემა, 2014, 53.

[480] *United States v. Barth*, 26 F. Supp. 2d, 929, 938, (1998).

[481] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, , Office of Legal Education Executive Office for United States Attorneys, 2009, 28.

[482] *United States v. David,* 756 F. Supp. 1385 (1991).

მაგალითისთვის, სასამართლომ პოლიციელთა მიერ სასამართლო ნებართვის გარეშე პეიჯერში არსებულ ინფორმაციაზე წვდომა ზემოხსენებული საფუძვლებით კანონიერად მიიჩნია.[483] თუმცა, აღსანიშნავია, რომ გადაუდებელი აუცილებლობის დადგენა ყველა საქმეში ინდივიდუალურად უნდა მოხდეს. მაგალითისთვის, მობილურ ტელეფონთან დაკავშირებით სასამართლომ განმარტა, რომ მას საკმაოდ მოცულობითი მეხსიერება აქვს და მისი სასამართლო ნებართვის გარეშე, მტკიცებულების განადგურების თავიდან აცილების მოტივით ჩხრეკა მიზანშეუწონელია.[484] თუმცა, სხვა შემთხვევაში, როდესაც მობილური ტელეფონი 1 დღის შემდეგ ავტომატურად შლიდა შეტყობინებებს, გადაუდებელი აუცილებლობის საფუძვლით ინფორმაციაზე წვდომა სასამართლომ კანონიერად მიიჩნია.[485]

ზოგადი მიდგომის თანახმად გადაუდებელი აუცილებლობის საფუძვლით ამოღებული კომპიუტერული მოწყობილობის შემდგომი ჩხრეკა სასამართლო ნებართვის გარეშე დაუშვებელია. მტკიცებულებების განადგურების თავიდან აცილების საფუძვლით ელექტრონული მოწყობილობის ამოღება არ ამართლებს და ამავდროულად, არ მოიცავს უფლებას მასში დაცული ინფორმაციის ჩხრეკაზე.[486]

ვ) ღია სივრცის დოქტრინა

სასამართლო ნებართვის გარეშე, ღია სივრცის დოქტრინის საფუძველზე, მტკიცებულების ამოღებისთვის მნიშვნელოვანია გამომძიებელს კანონიერად ჰქონდეს წვდომა მტკიცებულებაზე და დაკვირვების შედეგად მისი დანაშაულებრივი ხასიათი აშკარად იკვეთებოდეს.[487] კომპიუტერულ სისტემებთან და ელექტრონულ მტკიცებულებებთან მიმართებით, ღია სივრცის დოქტრინის გამოყენების გავრცელებული შემთხვევაა, როდესაც გამომძიებელი სასამართლო ნებართვის საფუძველზე ჩხრეკის ჩატარებისას სხვა დანაშაულის შესახებ ინფორმაციას აღმოაჩენს, რომელზეც მითითება სასამართლო ნებართვაში გათვალისწინებული არ ყოფილა. მაგალითისთვის, პოლიციის თანამშრომელმა კომპიუტერულ მოწყობილობაში მკვლელობის შესახებ მტკიცებულებების ძებნისას შემთხვევით

---

[483] *United States v. Ortiz,* 84 F.3d 977, 984 (7th. Cir. 1996).
[484] *United States v. Park,* 2007 WL 1521573 (N.D. Cal. 2007).
[485] *United States v. Young,* WL 1302667, 13, (2006).
[486] *United States v. Doe,* 61 F.3d 107-111 (1st Cir. 1995).
[487] *Horton v. California*, 496 U.S. 128, 136, (1990).

ბავშვთა პორნოგრაფიის ამსახველი მასალა აღმოაჩინა, რომელიც ღია სივრცის დოქტრინის საფუძველზე დაუყოვნებლივ ამოიღო.[488]

იმის გათვალისწინებით, რომ ხშირად ელექტრონული ინფორმაცია სხვადასხვა გზით არის შენიღბული [489] და ჩხრეკისას გამომძიებელს ყველა ფაილის გახსნა და დათვალიერება უწევს, უმეტესწილად დეტალიზებული სასამართლო ნებართვა პრაქტიკაში ზოგადი ხასიათის დოკუმენტად გადაიქცევა ხოლმე. [490] შესაბამისად, ვინაიდან ამ დროს გამოძიებისთვის დიდი მოცულობის ინფორმაცია ხდება ხელმისაწვდომი, სასამართლოს მოსაზრებით „ღია სივრცის“ დოქტრინის ფარგლები შეზღუდვას უნდა დაექვემდებაროს. კერძოდ, სასამართლოს განმარტებით, დოქტრინა ვრცელდება თავდაპირველი მტკიცებულების მოულოდნელ აღმოჩენაზე, ხოლო თუ გამომძიებელს სურს ძებნა ამ მიმართულებით გააგრძელოს, მან დამატებითი, ხელახალი სასამართლო ნებართვა უნდა მოიპოვოს. [491] თუმცა ელექტრონული დოკუმენტის ბუნებიდან გამომდინარე, შეუძლებელია წინასწარ, მის გახსნამდე მისი სავარაუდო შინაარსის განსაზღვრა. შესაბამისად, სასამართლოს ხედვით „ღია სივრცის“ დოქტრინის საფუძველზე სხვა დანაშაულის ჩადენაში მამხილებელი მტკიცებულების მოპოვება დასაშვებია.[492]

1.4. შეჯამება

აღსანიშნავია, რომ აშშ-ს კანონმდებლობით მომხმარებელთან დაკავშირებული ნებისმიერი კატეგორიის ინფორმაციისა და ზოგადად ელექტრონული ფორმით შენახული მონაცემის მოპოვება სამართლებრივი თვალსაზრისით დეტალურად არის მოწესრიგებული. „შენახულ კომუნიკაციათა აქტით“ განსაზღვრულია მომხმარებელთან დაკავშირებული ინფორმაციის რამდენიმე სახე და პრივატულობის გათვალისწინებით, თითოეული მათგანის მოპოვებისთვის განსხვავებული წესები მოქმედებს. ნიშანდობლივია, რომ ტელეკომუნიკაციის პროვაიდერი კომპანიებისგან სავალდებულო წესით მონაცემთა გამოთხოვის გარდა, გათვალისწინებულია

[488] *United States v. Wong,* 334 F.3d 831, 838 (9th Cir. 2003).
[489] *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006).
[490] *Kerr S. O.,* Searches and Seizures in Digital World, Harvard Law Review, vol. 119, 531, 2005.
[491] *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
[492] *United States v. Williams,* 592 F.3d 511 (4th Cir. 2010).

ინფორმაციის ნებაყოფლობით გადაცემის შესაძლებლობაც. [493] შესაბამისად, მომსახურების მიმწოდებლები უფლებამოსილნი არიან კანონით განსაზღვრული საფუძვლის არსებობისას მომხმარებელთან დაკავშირებული როგორც შინაარსობრივი, ისე არა შინაარსობრივი ხასიათის ინფორმაცია და ჩანაწერები ნებაყოფლობით გადასცენ როგორც სახელმწიფო, ისე არასამთავრობო ორგანიზაციებს.[494]

უნდა ითქვას, რომ „შენახულ კომუნიკაციათა აქტისგან“ დამოუკიდებლად არის მოწესრიგებული კერძო პირების საკუთრებასა თუ მფლობელობაში არსებული მონაცემების მოპოვების საკითხი. მათგან, კომპიუტერული მონაცემის მოპოვება შესაძლებელია როგორც ნებაყოფლობით, მათივე თანხმობის საფუძველზე, ისე მტკიცებულების გადაცემის ბრძანების ან ჩხრეკის ორდერის საფუძველზე.

აღსანიშნავია ისიც, რომ შენახული კომპიუტერული მონაცემის მოპოვებასთან დაკავშირებული საკითხების ამომწურავი მოწესრიგების მიუხედავად, არსებობს რიგი საკითხები, რომელთა გადაფასებაც მიზანშეწონილია. კერძოდ, არსებული რეალობის გათვალისწინებით აღარ არსებობს პროვაიდერი კომპანიების ელექტრონული კომუნიკაციის პროვაიდერ (ECS) და ელექტრონული კომუნიკაციის მონაცემთა შემნახველ პროვაიდერად (RCS) გამიჯვნის საჭიროება. შესაბამისად, რეკომენდირებულია მათი ერთი ცნების ქვეშ გაერთიანება,[495] რაც თავის მხრივ ხელს შეუწყობს პროვაიდერთან არსებული შინაარსობრივი მონაცემების ერთიანი სტანდარტით, სასამართლო ბრძანებისა [496] და ჩხრეკის განჩინების საფუძველზე მოპოვებას. ამასთან, პირადი ცხოვრების უფლების სათანადოდ დაცვის მიზნით, კერძო პირთაგან მტკიცებულების გადაცემის ბრძანების საფუძველზე ელექტრონული ინფორმაციის მოპოვებისას, აუცილებელია ადრესატის მიერ ბრძანებით გაცემული ვალდებულების შეცვლის ან გაუქმების მოთხოვნის სასამართლოს წინაშე დაყენების შესაძლებლობასთან ერთად,[497] სხვა დამატებითი გარანტიების გათვალისწინება.

---

[493] SCA, 18 U.S.C. §2702.

[494] *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 135.

[495] *Kerr S. O., "*A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It", 72 The George Washington Law Review 1208, 2004, 1235.

[496] *Terry v. Ohio,* 392 U.S. 1 (1968).

[497] 18 U.S.C. Fed. R. Crim. P. Rule 17(c) (1).

2. კანადის კანონმდებლობის მიხედვით

2.1. მონაცემთა დაცვის მოთხოვნა - ბრძანება

ციფრული მტკიცებულებები ხშირად ათობით ელექტრონულ მოწყობილობასა თუ კომპიუტერულ ქსელშია მიმოფანტული და შესაძლებელია მსოფლიოს ნებისმიერ წერტილშიც კი იყოს განთავსებული. ხშირად მათი შენახვის ვადაც საკმაოდ მოკლეა. მაგალითისთვის, მონაცემთა დაცვის კანონმდებლობაზე დაყრდნობით სერვისის მომწოდებლებს მონაცემთა გარკვეული სახის დაუყოვნებლივ ან გარკვეული პერიოდის გასვლის შემდეგ წაშლის ვალდებულება აკისრიათ, ხოლო იმ ფონზე, რომ მათ ხელთ არსებულ ინფორმაციას გამოძიების მიზნებისთვის შესაძლოა განსაკუთრებული მნიშვნელობა ჰქონდეს, მონაცემთა დაუზიანებლად, სახეუცვლელად შენახვის ვალდებულების მათთვის დაკისრება ეფექტურ მექანიზმს წარმოადგენს. შესაბამისად, აღნიშნული მიზნის მისაღწევად, კანადის კანონმდებლობა როგორც მონაცემთა შენახვის მოთხოვნის, ისე მონაცემთა შენახვის ბრძანების გაცემის საქართველოსგან განსხვავებულ შესაძლებლობებს ითვალისწინებს,[498] რამაც განაპირობა ამ ქვეყნის კანონმდებლობაზე ყურადღების გამახვილება.

კერძოდ, მონაცემთა შენახვის მოთხოვნის უფლებით კანადაში მშვიდობის ოფიცერი[499] ან საჯარო მოხელე[500] სარგებლობს იმ პირის მიმართ, რომლის მფლობელობასა თუ კონტროლ ქვეშ არის ინფორმაცია. თუმცა, მონაცემთა შენახვის მოთხოვნის უფლება მხოლოდ მაშინ გააჩნია თუ არსებობს გონივრული საფუძველი ვარაუდისთვის, რომ ჩადენილია ან შესაძლოა ჩადენილ იქნას დანაშაული და პირის მფლობელობაში ან კონტროლ ქვეშ არსებული დოკუმენტი ან მონაცემი დანაშაულის გამოძიებას შეუწყობს ხელს. [501] ნიშანდობლივია, რომ აღნიშნული მოთხოვნის უფლებით სარგებლობა ერთჯერად ხასიათს ატარებს და და მასზე დაყრდნობით ინფორმაციის

[498] Criminal Code (R.S.C. 1985, c. C-46), 487.012, 487.013.

[499] მშვიდობის ოფიცრებად იწოდებიან პოლიციელი, შერიფი, შერიფის მოადგილე, საჯარო მოხელე, კანადის სასჯელაღსრულების სამსახურის წევრი, ნებისმიერი პირი, რომელიც დასაქმებულია საზოგადოებრივი მშვიდობის უზრუნველყოფის სამსახურში და ა.შ.

[500] საჯარო მოხელე გულისხმობს პირს, რომელიც დანიშნულია ფედერალური ან ოლქის კანონის აღსასრულებლად.

[501] Criminal Code (R.S.C. 1985, c. C-46), 487.012, 487.013.

შენახვის ვალდებულების მესამე პირთათვის დაკისრება მხოლოდ 21 დღემდე ვადით არის შესაძლებელი.[502]

რაც შეეხება მონაცემთა შენახვის ბრძანებას,[503] მისი გაცემის უფლებამოსილება მხოლოდ სასამართლოს, მშვიდობის ოფიცრის ან საჯარო მოხელის შუამდგომლობის საფუძველზე შეუძლია. აუცილებელია შუამდგომლობით დასტურდებოდეს რომ არსებობს გონივრული საფუძველი ვარაუდისთვის, რომ ჩადენილია ან შესაძლოა ჩადენილ იქნას დანაშაული და პირის მფლობელობაში ან კონტროლ ქვეშ არსებული დოკუმენტი ან მონაცემი დანაშაულის გამოძიებას შეუწყობს ხელს. ამასთან, უფლებამოსილი პირი აპირებს სასამართლოს მიმართოს ან უკვე მიმართა კომპიუტერული მონაცემის გადაცემის ბრძანების გაცემის შუამდგომლობით. ნიშანდობლივია, რომ მშვიდობის ოფიცრის ან საჯარო მოხელის მიერ გაცემული შენახვის მოთხოვნისგან განსხვავებით სასამართლოს ბრძანების საფუძველზე მესამე პირებისთვის მონაცემთა 90 დღემდე ვადით შენახვის დაკისრება არის შესაძლებელი .[504]

დასკვნით სახით შეიძლება ითქვას, რომ მშვიდობის ოფიცრის ან საჯარო მოხელის მიერ გაცემული მონაცემთა დაცვის მოთხოვნა და აგრეთვე სასამართლოს ბრძანება, ეფექტურ პროცესუალურ მექანიზმებს წარმოადგენენ გამოძიებისთვის ღირებული ინფორმაციის განადგურებისგან თავის დასაცავად. ფაქტი, რომ სასამართლოს თანხმობის გარეშეც, გამოძიებაზე უფლებამოსილ პირებს აქვთ შესაძლებლობა დროულად, პირდაპირი მიმართვის საფუძველზე, თუნდაც მცირე დროით, უზრუნველყონ გამოძიებისთვის შესაძლო ღირებულების მქონე კომპიუტერული მონაცემის დაცვა, ხელს შეუწყობს სამართალწარმოების ეფექტურად განხორციელებას. განსაკუთრებით ისეთ პირობებში, როდესაც მონაცემთა დაცვის მოთხოვნა სრულებით არ გულისხმობს მათი გაცნობის შესაძლებლობას. დაცულ ინფორმაციაზე წვდომა კანადის საპროცესო კანონმდებლობით გათვალისწინებული ახალი საფუძვლითა და დამოუკიდებელი საგამოძიებო მოქმედების შედეგად უნდა განხორციელდეს, რომელთაც დეტალურად ქვემოთ განვიხილავთ.

[502] იქვე, 487.012 (4).
[503] იქვე, 487.013 (2).
[504] იქვე, 487.013 (4).

2.2. დოკუმენტის გადაცემის ზოგადი ბრძანება

ნიშანდობლივია, რომ აშშ-ს კანონმდებლობის მსგავსად კანადის საპროცესო კანონმდებლობა ელექტრონული ფორმით შენახული მონაცემების მოპოვების საკითხს დეტალურად აწესრიგებს. განსაზღვრულია მონაცემთა სახეები და მათი მოპოვების წესიც კონფიდენციალურობის მიხედვით განსხვავებულია. სათანადო პროცესუალური გატანტიებით სარგებლობს უშუალოდ საგამოძიებო მოქმედების ადრესატიც. შესაბამისად, ნაშრომის მიზნებისთვის კანადის საპროცესო კანონმდებლობის კვლევა მნიშვნელოვანია.

საყურადღებოა, რომ კანადის საპროცესო კანონმდებლობით გათვალისწინებული რამდენიმე სახის „გადაცემის ბრძანებიდან“ ერთ-ერთს „დოკუმენტის გადაცემის ზოგადი ბრძანება“ წარმოადგენს.[505]

გადაცემის ზოგადი ბრძანების თანახმად, მოსამართლე უფლებამოსილია „მშვიდობის ოფიცრის“ ან საჯარო მოხელის შუამდგომლობის საფუძველზე პირს მის მფლობელობაში ან კონტროლს ქვეშ მყოფი დოკუმენტის ასლის ან ინფორმაციის მომზადების, მოძიებისა და მისი ასლის გადაცემის ვალდებულება დააკისროს.[506] თუმცა, ამგვარი ბრძანების გამოტანამდე მოსამართლე უნდა დარწმუნდეს, რომ მის წინაშე წარდგენილი ინფორმაცია იძლევა გონივრულ საფუძველს ვარაუდისთვის, რომ ჩადენილია ან შესაძლოა ჩადენილ იქნას დანაშაული და პირის მფლობელობაში ან კონტროლ ქვეშ არსებული დოკუმენტი ან მონაცემი მიუთითებს დანაშაულის შესაძლო ჩადენის ფაქტზე.[507] რაც შეეხება თავად ბრძანების რეკვიზიტებს, მასში მითითებული უნდა იყოს პირი, რომელსაც უნდა გადაეცეს მოთხოვნილი ინფორმაცია და აგრეთვე, მისი გადაცემის დრო და ფორმა.[508] საყურადღებოა, თავად გადაცემული დოკუმენტის ან ინფორმაციის მტკიცებულებითი ძალის საკითხიც, ვინაიდან ბრძანების ადრესატი როგორც წესი არა თუ დედანს გადასცემს საგამოძიებო ორგანოს, არამედ მის ასლს. თუმცა, მტკიცების პროცესში მისი გამოყენება პრობლემას არ წარმოადგენს, ვინაიდან როგორც ნორმატიულ აქტში ვკითხულობთ, დოკუმენტის

[505] იქვე, 487.014.
[506] იქვე, 487.014 (1).
[507] იქვე, 487.014 (2).
[508] იქვე, 487.0192.

ან ინფორმაციის ასლს ისეთივე მტკიცებულებითი ღირებულება გააჩნია, როგორც დედანს.[509]

ნიშანდობლივია, რომ შუამდგომლობის დაყენებისას საჯარო ხელისუფლების, ხოლო ბრძანების მიღებისას სასამართლოს უფლებამოსილება შეუზღუდავი არ არის და საკმაოდ მყარი საპროცესო გარანტიები არსებობს ბრძანების ადრესატებისათვისაც. მაგალითისთვის, მართალია ბრძანების ადრესატი არ თავისუფლდება დოკუმენტის გადაცემის ვალდებულებისგან იმ მოტივით, რომ შესაძლოა გადაცემამ, ის დანაშაულის ჩადენაში ამხილოს, თუმცა, იმ შემთხვევაში თუ სასამართლო ბრძანებით პირს დოკუმენტის შედგენისა და გადაცემის ვალდებულება დაეკისრება, ხოლო გადაცემის შემდეგ მის მიმართ დაიწყება სისხლისსამართლებრივი დევნა, აღნიშნული დოკუმენტის მის წინააღმდეგ მტკიცებულებად გამოყენება დაუშვებელია. გასათვალისწინებელია, რომ აღნიშნული დათქმა არ მოქმედებს ისეთი დანაშაულის გამოძიებისას როგორებიცაა, ცრუ ჩვენების მიცემა, ურთიერთსაწინააღმდეგო ჩვენების მიცემა და მტკიცებულების ფალსიფიკაცია. [510] გარდა ზემოაღნიშნულისა, ბრძანების ადრესატი უფლებამოსილია წერილობით მიმართოს ბრძანების მიმღებ ორგანოს და მის წინაშე მოცემული მოთხოვნის ცვლილება ან თუნდაც გაუქმება იშუამდგომლოს,[511] თუ დოკუმენტის მომზადების ან წარმოდგენის მოთხოვნა არაგონივრულია ან დოკუმენტის გადაცემის შედეგად გამოვლინდება ინფორმაცია, რომელიც კანონით არის პრივილეგირებული ან სხვაგვარად დაცული გამჟღავნებისგან. [512] ამასთან, თავად მოსამართლეც უფლებამოსილია ბრძანების გაცემისას ნებისმიერი დათქმა გაითვალისწინოს, რომელიც მისი ხედვით გონივრული და მიზანშეწონილია. მათ შორის ისეთი, რომელიც პრივილეგირებული კომუნიკაციის (ადვოკატის და კლიენტის) ან სხვა ღირებული ინტერესის დაცვას ემსახურება.[513]

ცხადია, რომ გადაცემის ზოგადი ბრძანება მძლავრ საგამოძიებო ინსტრუმენტს წარმოადგენს, რომელსაც გამოძიებაზე უფლებამოსილი ორგანოები ინდივიდებისგან, ორგანიზაციებისგან, ფინანსური ინსტიტუტებისგან, სატელეკომუნიკაციო სერვის

[509] იქვე, 487.0192 (5).
[510] იქვე, 487.0196.
[511] იქვე, 487.0191 (3).
[512] იქვე, 487.0193(4).
[513] იქვე, 487.019 (1).

პროვაიდერებისგან, [514] როგორც მომხმარებლის შესახებ ინფორმაციის (საბანკო ანგარიშის, ინტერნეტ აბონენტის და ა.შ.), ისე შინაარსობრივი მონაცემების მოსაპოვებლად იყენებენ.[515]

2.3. მაიდენტიფიცირებელი მონაცემების გადაცემის ბრძანება კომუნიკაციის იდენტიფიცირების მიზნით

სამშვიდობო ოფიცრის ან საჯარო მოხელის შუამდგომლობის საფუძველზე კომუნიკაციაში ჩართული მოწყობილობის ან პირის იდენტიფიცირების მიზნით, მოსამართლე უფლებამოსილია გამოიტანოს ბრძანება კომუნიკაციასთან დაკავშირებული ინფორმაციის გადაცემის ვალდებულების დაკისრებასთან დაკავშირებით.[516]

ნიშანდობლივია, რომ აღნიშნული საგამოძიებო მოქმედების მიზანი კონკრეტულია, რაც მისი ვიწრო მოქმედების ფარგლების გარდა, მოსაპოვებელი ინფორმაციის ერთგვაროვნებაზეც მიანიშნებს. უფრო კონკრეტულად კი კოდექსისეული განმარტების თანახმად კომუნიკაციის იდენტიფიცირებისთვის აუცილებელი მონაცემები აერთიანებს სატელეკომუნიკაციო ფუნქციების განხორციელებასთან დაკავშირებულ მონაცემებს, მონაცემებს კომუნიკაციის მარშრუტის, დანიშნულების ადგილის, მოწყობილობის იდენტიფიცირებისთვის, აქტივაციისათვის და კონფიგურაციისთვის, მათ შორის პროგრამულ უზრუნველყოფასაც. აგრეთვე, მონაცემებს, რომლებიც იქმნება კომუნიკაციის პროცესში: კომუნიკაციის ტიპი, მიმართულება, თარიღი, დრო, ხანგრძლივობა, წარმოშობის, დანიშნულების ან შეწყვეტის ადგილი და ასევე, ნებისმიერ ინფორმაციას, რომელიც არ მიუთითებს კომუნიკაციის შინაარსსა და მიზანზე.[517]

კომუნიკაციის იდენტიფიცირებისათვის საჭირო მონაცემების გადაცემის ბრძანების მიღებამდე მოსამართლე ვალდებულია დარწმუნდეს, რომ არსებობს საკმარისი საფუძველი ეჭვისთვის[518], რომ ჩადენილია ან შესაძლოა ჩადენილ იქნას დანაშაული,

---

[514] R. v. Rogers Communications Partnership, 2014 ONSC 3853.

[515] *Fehr C.,* The Constitutionality of Using Production Orders to Obtain Stored Communication Content, Canadian Criminal Law Review 171, 2018, 2. იხ. R v. Vice Media Canada Inc., 2018 SCC 53, 2018, 3 S.C.R. 374.

[516] Criminal Code (R.S.C. 1985, c. C-46), 487.015.

[517] იქვე, 487.011.

[518] საყურადღებოა, რომ აღნიშნული საგამოძიებო მოქმედების ნებართვის გასაცემად განსხვავებული მტკიცებულებითი სტანდარტი მოქმედებს. გადაცემის ზოგადი ბრძანების შემთხვევაში აუცილებელია

მოწყობილობის ან პირის იდენტიფიკაცია, რომელიც მონაწილეობს კომუნიკაციაში ხელს შეუწყობს დანაშაულის გამოძიებას ან კომუნიკაციაში მყოფი უცნობი პირების იდენტიფიცირებას.[519]

შეჯამებისთვის, მოცემული საგამოძიებო მოქმედების მიზანი მკაფიოა და მას კომუნიკაციაში მონაწილე უცნობი, დაუდგენელი მოწყობილობის ან პირის იდენტიფიცირება წარმოადგენს. აღნიშნული საგამოძიები მოქმედების განხორციელებისას უნდა გვახსოვდეს, რომ იგი მოქმედებს მხოლოდ შენახულ, წარსულში შემდგარ კომუნიკაციასთან მიმართებით და სამომავლო, ჯერ არ შემდგარ კომუნიკაციასთან დაკავშირებული ინფორმაციის შეგროვებისას არ გამოიყენება.

2.4. კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გადაცემის ბრძანება

აღნიშნული საგამოძიებო მოქმედება მსგავსად წინა საგამოძიებო მოქმედებისა კომუნიკაციის გადაცემასთან დაკავშირებული მონაცემების მოპოვებას ეხება, თუმცა განსვავებით წინამორბედისგან, მის მიზანს კომუნიკაციაში მონაწილე პირის ან მოწყობილობის იდენტიფიცირება არ წარმოადგენს. მისი მიზანი ზოგადი ხასიათისაა და საქმეზე კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შეგროვებას ემსახურება.

სწორედ ამიტომ კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გადაცემის ბრძანების მისაღებად აუცილებელია შუამდგომლობით დასტურდებოდეს, რომ არსებობს საკმარისი საფუძველი ეჭვისთვის, რომ ჩადენილია დანაშაული ან ჩაიდენენ მას, ამასთან გამოძიებისთვის საჭირო მონაცემები პირის მფლობელობაში ან კონტროლ ქვეშაა და მისი გადაცემა ხელს შეუწყობს გამოძიებას.[520]

ნიშანდობლივია, რომ ორივე საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელი მტკიცებულებითი სტანდარტი იდენტურია და ამასთან, ორივე შემთხვევაში დასაშვებია მხოლოდ დასრულებულ კომუნიკაციასთან დაკავშირებული მონაცემების შეგროვება.

დასაბუთებული/საკმარისი საფუძველი ვარაუდისთვის (Reasonable grounds to believe). ხოლო მოცემულ შემთხვევაში მოქმედებს დასაბუთებული/საკმარისი საფუძველი ეჭვისთვის(Reasonable grounds to suspect), რაც შეიძლება ითქვას, რომ წინამორბედთან შედარებით დაბალი მტკიცებულებითი სტანდარტია.

[519] Criminal Code (R.S.C. 1985, c. C-46), 487.015 (2).

[520] იქვე, 487.016.

2.5. ადგილმდებარეობის შესახებ მონაცემების გადაცემის ბრძანება

პირველ რიგში უნდა ითქვას, რომ კანადის საპროცესო კანონმდებლობაში მოცემული საგამოძიებო მოქმედების დასახელება არ მოიცავს სიტყვა „ადგილმდებარეობას“. მის ნაცვლად ტერმინი „მონაცემი მონიტორინგის, თვალთვალის შესახებ“ გამოიყენება, თუმცა კანონში მისი დეფინიციისას იკითხება, რომ მასში ინდივიდის, საგნის ან ტრანზაქციის ადგილმდებარეობა მოიაზრება.[521]

აღნიშნული საგამოძიებო მოქმედება გამოიყენება, როდესაც გამოძიებისთვის მნიშვნელოვანია იმის დადგენა თუ დროის კონკრეტულ მონაკვეთში სად იმყოფებოდა პიროვნება ან აუცილებელია მობილური ტელეფონის მდებარეობის დადგენა დროის სხვადასხვა მომენტში. [522] ამ შემთხვევაშიც, შუამდგომლობის წარდგენისას მნიშვნელოვანია დაკმაყოფილებული იყოს „დასაბუთებული ეჭვის სტანდარტი“, რომ ჩადენილია დანაშაული ან არსებობს მისი ჩადენის რისკი, გამოძიებისთვის საინტერესო მონაცემები პირის მფლობელობაში ან კონტროლ ქვეშაა და მისი მოპოვება ხელს შეუწყობს გამოძიების მიმდინარეობას.[523]

ყურადსაღებია, რომ ინფორმაცია მომხმარებლის შესახებ, შემავალი და გამავალი ზარების დეტალური ჩანაწერები, ტექსტური შეტყობინების შემავალი და გამავალი ნომრები ან ბილინგის შესახებ ინფორმაცია აღნიშნული საგამოძიებო მოქმედების ფარგლებში არ ექცევა. სასამართლოს განმარტებით თუ მხარისთვის მნიშვნელოვანია მომხმარებლის შესახებ ინფორმაციის მოპოვება, მან გადაცემის ზოგადი ბრძანებისთვის დადგენილი წესებით უნდა იხელმძღვანელოს, რაც თავის მხრივ უფრო მაღალ მტკიცებულებით სტანდარტს მოითხოვს, ვიდრე ეს ადგილმდებარეობის შესახებ მონაცემის მოპოვებისთვის არის გათვალისწინებული.[524]

2.6. ფინანსური მონაცემების გადაცემის ბრძანება

ფინანსური მონაცემების გადაცემის ბრძანების გაცემა ნებადართულია სასამართლოსთვის წარდგენილი შუამდგომლობის საფუძველზე, რომლითაც დასაბუთებული ეჭვის სტანდარტით დასტურდება, რომ ჩადენილია დანაშაული ან არსებობს დანაშაულის ჩადენის რისკი და ფინანსური მონაცემები, რომლებიც ხელს

[521] იქვე, 487.011.
[522] Re Subscriber Information [2015], Alberta Provincial Court, ABPC 178, 31.
[523] Cminal Code (R.S.C. 1985, c. C-46), 487.017 (2).
[524] Re Subscriber Information [2015], Alberta Provincial Court, ABPC 178, 33-36.

შეუწყობს გამოძიების წარმართვას პირის ან ორგანიზაციის მფლობელობაში ან კონტროლ ქვეშაა.[525]

მოცემული ნორმის საფუძველზე სასამართლოს მიერ მიღებული ბრძანებით მის ადრესატებს შესაძლოა დაეკისროთ პირის ანგარიშის ნომრის, ანგარიშის მფლობელის ვინაობის, ანგარიშის ტიპის, მისი სტატუსის, გახსნისა და დახურვის შესახებ მონაცემების(და არა ანგარიშის საშუალებით განხორციელებული აქტივობების შესახებ) გადაცემის ვალდებულება.[526] ამავე ბრძანებით შესაძლებელია დამატებით, პირის დაბადების თარიღის, მისი ამჟამინდელი ან ყოფილი საცხოვრებელი ადგილის შესახებ მონაცემების მოპოვებაც.[527]

საყურადღებოა, რომ მოცემული საგამოძიებო მოქმედების შედეგად გამორიცხულია სხვა დამატებითი სახის ფინანსური ინფორმაციის გამოთხოვა, რომელიც მითითებული არ არის ამ მუხლში. თუ დაინტერებულ პირს მუხლით განსაზღვრულ ფინანსურ ინფორმაციასთან ერთად დამატებითი ინფორმაციის მოძიებაც სურს, მან გადაცემის ზოგადი ბრძანებისთვის ან რომელიმე სხვა კონკრეტული საგამოძიებო მოქმედებისათვის დადგენილი წესებით უნდა იხელმძღვანელოს.[528]

2.7. შეჯამება

ცხადია, რომ კანადის კანონმდებლობით საკმაოდ დეტალურად არის მოწესრიგებული ელექტრონული მტკიცებულების მოპოვების საკითხი. შემოთავაზებულია რამდენიმე სახის საგამოძიებო მოქმედება, რომლებიც ზოგად მოწესრიგებასთან ერთად, სპეციფიური, კონკრეტული სახის ინფორმაციის გამოთხოვასაც ეხება.

შეიძლება ითქვას, რომ მოქმედების ფარგლების მიხედვით ყველაზე ფართო დოკუმენტის ან ინფორმაციის გადაცემის ზოგადი ბრძანებაა, ვინაიდან მის საფუძველზე ხდება როგორც შინაარსობრივი სახის ინფორმაციის, ისე მომხმარებელთან დაკავშირებული ნებისმიერი სახის ინფორმაცის მოპოვება, გარდა იმ მონაცემებისა, რომელთა გამოთხოვაც სპეციალური ნორმებით არის

[525] Criminal Code (R.S.C. 1985, c. C-46), 487.018 (3).
[526] იქვე, 487.018 (1).
[527] იქვე, 487.019 (2).
[528] *Alberta (Attorney General) v. Provincial Court of Alberta*, 2015 ABQB 728, 102.

მოწესრიგებული.[529] შესაბამისად, სწორედ პირადი ცხოვრების უფლებაში მაღალი ინტენსივობით ჩარევის შესაძლებლობის გამო მოქმედებს მის მიმართ შედარებით მაღალი მტკიცებულებითი სტანდარტი, ვიდრე ეს კანონით გათვალისწინებულ სხვა სპეციალური სახის მონაცემთა გადაცემის ბრძანებებისთვისაა დადგენილი.[530] ძირითად საიდენტიფიკაციო მონაცემებს მცირე ზეგავლენა აქვთ პირადი ცხოვრების ხელშეუხებლობის გონივრულ მოლოდინზე, მაშინ როდესაც შინაარსობრივი მონაცემების მხრივ კონფიდენციალურობის დაცვის მეტი მოლოდინია. ამიტომ უფლებაში ჩარევისთვის უფრო მაღალი სტანდარტის დაკმაყოფილებაა საჭირო.[531] მნიშვნელოვან ბერკეტს წარმოადგენს ბრძანების ადრესატებისთვის მინიჭებული უფლებამოსილება გაცემული ნებართვის გაუქმების ან შეცვლის მოთხოვნით სასამართლოსთვის მიმართვის შესაძლებლობის თაობაზე.[532] ასევე, საკმაოდ მყარ საპროცესო გარანტიას წარმოადგენს დათქმა, რომლის მიხედვითაც დაუშვებელია პირის მიერ სასამართლო ბრძანების საფუძველზე მომზადებული ან შექმნილი დოკუმენტის მის წინააღმდეგ მტკიცებულებად გამოყენება, თუ დოკუმენტის გადაცემის შემდეგ სისხლისსამართლებრივი დევნა მის მიმართ დაიწყო.[533]

აღსანიშნავია, რომ კანადის კანონმდებლობით გათვალისწინებული სხვადასხვა სახის გადაცემის ბრძანება ერთობლიობაში ეფექტურ ეროვნულ საპროცესო ინსტრუმენტს ქმნის ნებისმიერი სახის ელექტრონული ფორმით შენახული ინფორმაციის მოსაპოვებლად. ამასთან, კანონმდებლობით გათვალისწინებული მონაცემთა დაცვის მოთხოვნა და ბრძანება, გარდა იმისა, რომ ინფორმაციაზე უშუალოდ წვდომის უფლების მოპოვებამდე, უზრუნველყოფს გამოძიებისთვის მნიშვნელოვანი მონაცემების დაცვას, აგრეთვე, გარკვეულწილად ამცირებს პირადი ცხოვრების ხელშეუხებლობის უფლების არამიზნობრივ შეზღუდვის რისკს, ვინაიდან მონაცემთა დაცვის შემდეგ თუ გამოიკვეთება რომ დაცული ინფორმაცია აღარ წარმოადგენს გამოძიების ინტერესს, გამოძიებაზე უფლებამოსილი პირი აღარ მიმართავს სასამართლოს მისი გადაცემის ბრძანების გაცემის შუამდგომლობით. განსხვავებული სურათი იქნებოდა, მაშინ თუ ამგვარი პროცესუალური ინსტრუმენტი არ იარსებებდა,

---

[529] იქვე, 100.
[530] Winnipeg Police Service Officer (Re), 2015, MBPC 70, 13. იხ. *R. v. Todorov* 2008 ONCA 849.
[531] იქვე.
[532] Criminal Code (R.S.C. 1985, c. C-46), 487.0193 (1).
[533] იქვე, 487.0196.

რადგან მხარე იძულებული იქნებოდა მესამე პირის მფლობელობასა თუ კონტროლ ქვეშ არსებული ინფორმაცია პირდაპირ, გადაცემის ბრძანების საფუძველზე მოეპოვებინა.

თავი VI. კომპიუტერული მონაცემის გამოთხოვის საკითხი ქართული კანონმდებლობის მიხედვით

1. კომპიუტერული მონაცემის გამოთხოვის განვითარების ზოგადი მიმოხილვა

ქართული სისხლის საპროცესო სამართლის საფუძველს საქართველოს კონსტიტუციასთან, საერთაშორისო ხელშეკრულებებთან, შეთანხმებებთან და საქართველოს კანონებთან ერთად საქართველოს სისხლის სამართლის საპროცესო კოდექსი წარმოადგენს.[534] სწორედ, 2009 წლის 9 ოქტომბერს, საქართველოს უმაღლესი საკანონმდებლო ორგანოს მიერ მიღებული ნორმატიული აქტი გვევლინება სისხლის საპროცესო სამართლის ძირითად წყაროდ.

ერთი შეხედვით მოკლე ისტორიის მქონე, თუმცა პროგრესულ პრინციპებზე აგებული სისხლის სამართლის საპროცესო კოდექსის შემუშავების პროცესი უფრო ადრე, 2002 წლის მიწურულს დაიწყო. მიზანს, ქართული საპროცესო კანონმდებლობის ძირეული ცვლილება წარმოადგენდა, რომელიც შედეგად შეჯიბრებითობის, საჯაროობის, მხარეთა თანასწორობის, ბრალდებულის უფლებების პატივისცემისა და სხვადასხვა ღირებულებებზე აგებულ სისხლის სამართლის საპროცესო კოდექსს მოგვცემდა. ქართველი და უცხოელი ექსპერტების, საერთაშორისო ორგანიზაციებისა და სხვადასხვა უწყებების მონაწილეობით შემუშავებული პროექტი, საქართველოს პარლამენტმა პირველი მოსმენით 2006 წლის დეკემბერში მიიღო. საბოლოო რედაქციით კი მისი მიღება 2009 წლის 9 ოქტომბერს მოხდა, ხოლო ძალაში 2010 წლის პირველ ოქტომბერს შევიდა.

საყურადღებოა, რომ საპროცესო კოდექსის თავდაპირველ რედაქციაში კომპიუტერულ მონაცემთან დაკავშირებული საგამოძიებო მოქმედებები გათვალისწინებული არ ყოფილა. მათი ასახვა კანონში განხორციელებული პირველივე ცვლილებით მოხდა (24.09.2010). სისხლის სამართლის საპროცესო კოდექსის XVI თავი, რომელიც ფარულ საგამოძიებო მოქმედებებს ეძღვნებოდა, კომპიუტერულ მონაცემთან დაკავშირებულმა საგამოძიებო მოქმედებებმა

[534] *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი - ზოგადი ნაწილის მიმოხილვა, თბილისი, იურისტების სახლი, 2014, 49.

ჩაანაცვლეს. თავად ფარულ საგამოძიებო მოქმედებათა მარეგულირებელი ნორმები კი ამოღებულ იქნა საპროცესო კოდექსიდან.[535]

თავდაპირველად, კომპიუტერულ მონაცემებთან დაკავშირებულ საგამოძიებო მოქმედებებთან მიმართებაში სსსკ-ის 112-ე მუხლით დადგენილი ნორმები მოქმედებდა, რაც სასამართლოს განჩინებით ჩასატარებელ საგამოძიებო მოქმედებათა წესს განსაზღვრავდა. მოგვიანებით განხორციელებული ცვლილების თანახმად კი (2014 წლის 1 აგვისტო) საპროცესო კოდექსს კვლავ დაემატა ფარულ საგამოძიებო მოქმედებათა თავი [536] და ამავე ცვლილების მიხედვით ელექტრონული მტკიცებულების მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებების განხორციელება ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესით გადაწყდა.

განხორციელებული ცვლილების შედეგად გართულდა გამოძიების მიზნებისთვის ელექტრონული მტკიცებულების მოპოვება. მთელი რიგი ნაკლებად მძიმე კატეგორიის დანაშაულის გამოძიებისას თავდაპირველად პროკურორი, ხოლო 2017 წლის საკონსტიტუციო სასამართლოს გადაწყვეტილების [537] შემდეგ კი მხარეები [538], მოკლებულნი იყვნენ მოსამართლისთვის კომპიუტერული მონაცემის გამოთხოვის

---

[535] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებებისა და დამატებების შესახებ, N3616, 24.09.10.

[536] საქართველოს სისხლის სამართლის საპროცესო კოდექსს დაემატა ახალი XVI[1] თავი, რომელიც ფარულ საგამოძიებო მოქმედებათა სახეებს, მათი განხორციელების, ინფორმაციის მოპოვების, გამოყენების, შენახვისა და განადგურების წესს განსაზღვრავს. ცვლილების მიხედვით სსსკ-ში „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონიდან გადმოტანილ იქნა იმგვარი ღონისძიებები, რომლებიც მხოლოდ მოსამართლის განჩინებით ხორციელდება. მათ შორის: სატელეფონო საუბრის ფარული მიყურადება და ჩაწერა, ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან, საფოსტო-სატელეგრაფო გზავნილის(დიპლომატიური ფოსტის გარდა) კონტროლი და ა.შ. ამავე ცვლილებით განისაზღვრა დანაშაულთა წრე, რომელთა დროსაც შესაძლებელია ფარული საგამოძიებო მოქმედების ჩატარება. დათქმის მიხედვით კი იგი შეიძლება განხორციელდეს მხოლოდ მძიმე, განსაკუთრებით მძიმე და სსსკ-ით განსაზღვრული კონკრეტული დანაშაულის გამოძიების პროცესში. იხ. განმარტებითი ბარათი „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის თაობაზე“ საქართველოს კანონის პროექტი, N2634-რს, 31.07.14.

[537] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“.

[538] სსსკ-ის 136-ე მუხლი საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილებამდე, მხარეთა თანასწორობისა და შეჯიბრებითობის კუთხით არსებულ მნიშვნელოვან გამოწვევას წარმოადგენდა. მუხლის ნორმატიული შინაარსი, რომელიც დაცვის მხარის უფლებას, ბრალდების მხარის მსგავსად კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობით მიემართა სასამართლოსთვის ხელოვნურად ზღუდავდა, ძალადაკარგულად იქნა ცნობილი და შედეგად დოკუმენტის ან ინფორმაციის გამოთხოვის უფლებამოსილება პროკურორთან ერთად დაცვის მხარესაც მიენიჭა.

შუამდგომლობით მიმართვის შესაძლებლობას. საკითხის ამგვარმა გადაწყვეტამ განსხვავებულ სასამართლო პრაქტიკას დაუდო საფუძველი და ნაკლებად მძიმე კატეგორიის დანაშაულზე მიმდინარე გამოძიების პროცესში მხარეთათვის ელექტრონული ინფორმაციის მოპოვება „დათვალიერების“ საგამოძიებო მოქმედებით გახდა ხელმისაწვდომი.

ელექტრონული ფორმით შენახული ინფორმაციის გამოთხოვის სამართლებრივი მოწესრიგების ძირითადი მომენტი მაინც 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტთან არის დაკავშირებული.[539] სსსკ-ის 136-ე მუხლზე ფარული საგამოძიებო მოქმედებისთვის დადგენილი სტანდარტის გავრცელებიდან[540] რვა წლის შემდეგ მისი რეგულირების საკითხი კვლავ ამავე კოდექსის 112-ე მუხლის, სასამართლოს განჩინებით ჩასატარებელ საგამოძიებო მოქმედებათა წესის მიხედვით განისაზღვრა.

კომპიუტერული მონაცემის, იგივე დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო ღონისძიება, რომელიც „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით გათვალისწინებული „**კომპიუტერული მონაცემის წარმოდგენის ბრძანების**“, საქართველოს სისხლის სამართლის საპროცესო კოდექსში იმპლემენტირების შედეგია, უმეტესწილად თანხვედრაშია კონვენციის მოთხოვნებთან. თუმცა, ნორმის განვითარების სხვადასხვა ეტაპზე, პრაქტიკულმა საქმიანობამ რიგი ხარვეზები წარმოაჩინა, რაზეც აუცილებლად გავამახვილებთ ყურადღებას. საკანონმდებლო დონეზე განხორციელებული არაერთი ცვლილების მიუხედავად და აგრეთვე, იმ ფაქტის გათვალისწინებით, რომ საკითხის დღეისთვის მოქმედი სამართლებრივი გადაწყვეტა, წინამორბედებთან შედარებით ახლოს დგას კონვენციის მოთხოვნებთან, ნორმის სრულყოფის პროცესი ჯერაც არ დამთავრებულა და კონკრეტული ნაბიჯების გადადგმა კვლავ აუცილებელია.

[539] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24.05.2022.

[540] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ საქართველოს კანონი, N2634-რს, 01.08.2014.

2. საკონსტიტუციო სასამართლოს გადაწყვეტილება და მისი ზეგავლენა ნორმის განვითარებაზე

მხარეთა თანასწორობისა და შეჯიბრებითობის პრინციპი, [541] სასამართლოსადმი ხელმისაწვდომობის პრინციპი, დაცვის უფლება, ეს იმ კონსტიტუციური გარანტიების ჩამონათვალია, რომელთან მიმართებაშიც საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი და მეოთხე ნაწილების იმ ნორმატიული შინაარსის კონსტიტუციურობის საკითხი დადგა დღის წესრიგში, რომელიც დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის შესახებ განჩინების გაცემის შუამდგომლობით სასამართლოსთვის მიმართვის შესაძლებლობას გამორიცხავდა.[542]

საკონსტიტუციო სასამართლომ გადაწყვეტილების სამოტივაციო ნაწილში აღნიშნა, რომ სადავო ნორმა საგამოძიებო მოქმედებათა ზოგადი რეგულირებიდან კომპიუტერული მონაცემის სახით სპეციალურ ობიექტს გამოყოფს და სწორად ამ ობიექტს უკავშირდება მისი როგორც საგამოძიებო მოქმედების განხორციელების განსხვავებული წესები. კანონმდებელი სასამართლოსთვის შუამდგომლობით მიმართვის სუბიექტად მხოლოდ პროკურორს ასახელებდა და კონკრეტული უფლებამოსილი სუბიექტის განსაზღვრით მისი ნებაც ცალსახად გამოკვეთილი იყო. მეტიც, კომპიუტერული მონაცემის გამოთხოვაზე ფარული საგამოძიებო მოქმედებისთვის დადგენილი წესების გავრცელებით კიდევ ერთხელ დასტურდებოდა, რომ უფლებამოსილ სუბიექტს მხოლოდ პროკურორი წარმოადგენდა, ვინაიდან ფარული საგამოძიებო მოქმედების ჩატარება მხოლოდ ბრალდების მხარის პრეროგატივაა.[543] უფლებამოსილების ამგვარი შეზღუდვა დაცვის მხარეს დიდი მოცულობის ელექტრონულ ინფორმაციაზე წვდომის შესაძლებლობას ართმევდა. განსაკუთრებით ისეთ ინფორმაციაზე, რომელიც გამოძიების ინტერესებისთვის თითქმის ყოველი საქმის კვლევისას საინტერესოა. კერძოდ, ვიდეო

[541] საქართველოს საკონსტიტუციო სასამართლო, საქართველოს საკონსტიტუციო სასამართლოს მიერ 2017 წლის განმავლობაში კონსტიტუციური მართლმსაჯულების სფეროში მიღებული მნიშვნელოვანი გადაწყვეტილებები, საკონსტიტუციო სამართლის ჟურნალი, 2018(1), 21.

[542] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“.

[543] იქვე, 12.

კამერის ჩანაწერები, მობილური ოპერატორების ინფორმაცია მომსახურე ანძების შესახებ, ინფორმაცია არქივიდან, ავტომობილის ელექტრონული სისტემიდან და ა.შ. აღნიშნულის გათვალისწინებით საკონსტიტუციო სასამართლომ, მისთვის კარგად ნაცნობი და ჩამოყალიბებული მიდგომის თანახმად იმსჯელა სადავო ნორმის მზღუდავი ხასიათის კონსტიტუციურობის შესახებ. გამოარკვია რა თანაზომიერების პრინციპის შესაბამისად უფლების მზღუდავი საკანონმდებლო მოწესრიგება წარმოადგენდა თუ არა ღირებული ლეგიტიმური მიზნის მიღწევის გამოსადეგ და აუცილებელ საშუალებას და იყო თუ არა უფლების შეზღუდვის ინტენსივობა მისაღწევი საჯარო მიზნის პროპორციული. სიღრმისეული განხილვის შედეგად, სასამართლო მივიდა დასკვნამდე, რომ კანონმდებელი სრულიად ართმევდა დაცვის მხარეს კომპიუტერული წესით შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის უფლებას. აღნიშნული კი თანასწორობისა და შეჯიბრებითობის პრინციპის დარღვევასთან ერთად, მნიშვნელოვნად აბრკოლებდა საქმის გარემოებათა ყოველმხრივი გამოკვლევის შესაძლებლობას. განსაკუთრებით ისეთ პირობებში, როდესაც სასამართლოს მედიატორის როლი აქვს და მტკიცებულებათა მოპოვება და გამოკვლევა მხოლოდ მხარეთა უფლებამოსილებაა. ამასთან, დაცვის მხარე მისთვის აუცილებელი მტკიცებულების მოპოვების ნაწილში, დამოკიდებული იყო ბრალდების მხარის დისკრეციულ უფლებამოსილებაზე. ეს კი ქმნიდა საფრთხეს სასამართლოს საბოლოო გადაწყვეტილება ბრალდების მხარის გულგრილობას, შეცდომას ან/და უფლებამოსილების ბოროტად გამოყენებას დაფუძნებოდა. [544] შეზღუდვის არაგონივრულობა განსაკუთრებით ნათელი გახდა დაცვის მხარის საპროცესო უფლების ფონზე, რომლის თანახმად იგი უფლებამოსილია ჩხრეკა-ამოღების ჩატარების შუამდგომლობით მიმართოს სასამართლოს. საგამოძიებო მოქმედების, რომელიც რიგ შემთხვევებში უფრო მაღალი ინტენსივობით ქმნის მესამე პირთა პირად ცხოვრებასა თუ კერძო საკუთრებაში ჩარევის საფრთხეს.[545]

ვინაიდან საქმის მასალებითა და მოპასუხეთა არგუმენტებით არ გამოიკვეთა თუ რომელი ლეგიტიმური მიზნის მისაღწევად იზღუდებოდა დაცვის მხარის უფლება ელექტრონული მტკიცებულების მოპოვებისას, საკონსტიტუციო სასამართლომ აქაც,

[544] იქვე, 19-21.
[545] იქვე, 22.

მკაცრად ჩამოყალიბებული პრაქტიკის გათვალისწინებით განმარტა, რომ „ლეგიტიმური მიზნის არარსებობის პირობებში ადამიანის უფლებაში ნებისმიერი ჩარევა თვითნებურ ხასიათს ატარებს და მისი შეზღუდვა საფუძველშივე გაუმართლებელია“.[546]

საკანონმდებლო ხარვეზს არანაკლებ უარყოფითი ზეგავლენა ჰქონდა დაცვის უფლებაზე. [547] მიუხედავად იმისა, რომ დაცვის უფლება დამოუკიდებელი კონსტიტუციური გარანტიაა, იგი პროცესის შეჯიბრებითობის უზრუნველყოფის მნიშვნელოვან ელემენტს წარმოადგენს. განსაკუთრებით მაშინ, როდესაც სამართალწარმოებაში მხარედ სახელმწიფო გვევლინება და დაცვის მხარესთან შედარებით მის ხელთ უზარმაზარი ფინანსური თუ ადამიანური რესურსია. შესაბამისად, დაპირისპირებულ სუბიექტებს შორის არსებული სხვაობა, სწორედ დაცვის მხარის ხელთ არსებული სამართლებრივი ბერკეტებისა თუ ინსტრუმენტის შედეგად უნდა დაბალანსდეს.[548] ხოლო თუ დაცვის მხარეს არ მიეცემა შესაძლებლობა ჰქონდეს წვდომა ელექტრონულ ინფორმაციაზე და ბრალდების მხარის მტკიცებულებებს დაუპირისპიროს საკუთარი, დაცვის უფლების განხორციელება გამორიცხულია. სწორედ ამიტომ, საკონსტიტუციო სასამართლოს ხედვით, სადავო ნორმები მხარეთა შეჯიბრებითობისა და თანასწორობის პრინციპთან ერთად დაცვის უფლებასაც ხელყოფდა.

საკითხის კომპლექსურობიდან გამომდინარე პრობლემა ბრალდების შესახებ დადგენილებისა და გამამტყუნებელი განაჩენის უტყუარ მტკიცებულებებზე გამოტანის კუთხითაც იკვეთებოდა. იმგვარ ვითარებაში, სადაც მტკიცებულებათა მოპოვება და გამოკვლევა მხარეთა უფლებამოსილებაა, ხოლო სასამართლო ამ პროცესში ნეიტრალურია, მტკიცებულების სანდოობის შეფასება მხოლოდ მოწინააღმდეგე მხარის მიერ საპირისპირო ფაქტებისა და არგუმენტების წარდგენით

---

[546] საქართველოს საკონსტიტუციო სასამართლოს 2013 წლის 5 ნოემბრის გადაწყვეტილება საქმეზე N3/1/531 „ისრაელის მოქალაქეები - თამაზ ჯანაშვილი, ნანა ჯანაშვილი და ირმა ჯანაშვილი საქართველოს პარლამენტის წინააღმდეგ“ II-15.

[547] *ბერი ვ., შრამი ე.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის რეფორმირებისთვის - შედარებითი და ევროპული მოსაზრებები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, N1, 2019, 4.

[548] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“, II-25-28.

არის შესაძლებელი. შესაბამისად, შეზღუდვის პირობებში მტკიცებულების ყოველმხრივ შემოწმება შეუძლებელი იყო. ზემოაღნიშნულიდან გამომდინარე, სასამართლომ დაადგინა, რომ დაცვის უფლების შეზღუდვა თვითმიზნურ, აბსოლუტურ და ბლანკეტურ ხასიათს ატარებდა და სადავო ნორმები არაკონსტიტუციურად ცნო.[549] სწორედ, მას შემდეგ მიეცა დაცვის მხარეს უფლება კომპიუტერული სისტემიდან ან მონაცემთა შემნახველი მოწყობილობიდან ინფორმაციის მოპოვების შუამდგომლობით მიემართა სასამართლოსთვის. თუმცა, საგამოძიებო მოქმედების ჩატარებისთვის ფარული საგამოძიებო მოქმედებისთვის დადგენილი სტანდარტით ხელმძღვანელობამ და ამავდროულად, დაცვის მხარისთვის შუამდგომლობის დაყენების შესაძლებლობის მინიჭებამ, მოსამართლეთა შორის დაბნეულობა გამოიწვია. როდესაც სასამართლოს წინაშე კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობას დაცვის მხარე აყენებდა, სასამართლო ფარული საგამოძიებო მოქმედებისთვის დადგენილი სტანდარტით არ ხელმძღვანელობდა, ხოლო ბრალდების მხარის მიერ დაყენებული შუამდგომლობის განხილვა კი ფარული საგამოძიებო მოქმედებისთვის დადგენილი წესის მიხედვით ხდებოდა.[550] შესაბამისად, მკაფიო მოწესრიგების არ არსებობის ფონზე, ამ ხნის განმავლობაში სასამართლო პრაქტიკაც უჩვეულოდ ვითარდებოდა.

მართალია, საკონსტიტუციო სასამართლოს გადაწყვეტილების შემდეგ, საკანონმდებლო დონეზე განსახორციელებელ ცვლილებებზე სამუშაოდ, იურიდიულ საკითხთა კომიტეტის წევრები და გერმანიის უზენაესი ფედერალური სასამართლოს მოსამართლე დოქტორი ვოლფგანგ ბერი 2017 წელს ერთმანეთს შეხვდნენ.[551] მეტიც, სამუშაო შეხვედრის ფარგლებში განხილულ იქნა არაერთი საკითხი, მათ შორის დაცვის მხარის მიერ კომპიუტერული მონაცემის გამოთხოვის პროცედურა, ბრალდების მხარის მიერ ელექტრონული ინფორმაციის სასამართლოს

[549] იქვე, II-44.

[550] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, 5-6. <https://info.parliament.ge/file/1/BillReviewContent/297941> [10.06.23].

[551] *ბერი ვ., შრამი ე.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის რეფორმირებისთვის - შედარებითი და ევროპული მოსაზრებები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, N1, 2019, 11.

შუამდგომლობის გარეშე მოპოვების მიზანშეწონილობის საკითხი და ა.შ.,[552] თუმცა 2022 წლამდე, ამ მიმართულებით კანონში ცვლილება არ განხორციელებულა.

3. კომპიუტერული მონაცემის გამოთხოვა საპროცესო კანონმდებლობის მიხედვით

3.1. კომპიუტერული მონაცემის გამოთხოვის რეგულირების საკითხი 2022 წლის საკანონმდებლო ცვლილების განხორციელებამდე[553]

ნიშანდობლივია, რომ დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების მომწესრიგებელი ნორმების ძველი რედაქციის [554] და მოგვიანებით შესაბამისი სასამართლო პრაქტიკის შესწავლა, განზოგადება, დაგვეხმარება დავინახოთ თუ რამდენად საჭირო იყო 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტის მიღება.

იმთავითვე უნდა აღინიშნოს, რომ საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველ და მეორე ნაწილებს არსებითი ცვლილება არ განუცდიათ, არ შეცვლილა საგამოძიებო მოქმედების არსი. შესაბამისად, მათ აწმყო დროში განვიხილავთ.

სსსკ-ის 136-ე მუხლის პირველი ნაწილის მიხედვით „თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი ინახება, პროკურორი (დაცვის მხარეც)[555] უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით მიმართოს“.

---

[552] იხ. ოფიციალური განცხადება <https://parliament.ge/media/news/the-meeting-of-the-legal-issues-committee-with-the-judge-of-the-federal-supreme-court-of-germany-regarding-the-legislative-changes-to-the-article-136-of-the-criminal-code-of> [10.06.23].

[553] მოცემულ თავში განხილულია საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ 2014 წლის 1 აგვისტოდან (№2634), საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ 2022 წლის 24 მაისს განხორციელებულ ცვლილებამდე მოქმედი რედაქცია(№1575).

[554] იქვე.

[555] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“. იხ. *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 234.

შინაარსობრივად ნორმის პირველი ნაწილი მხარეებს სასამართლო ნებართვის საფუძველზე, საქართველოს ტერიტორიაზე მყოფი პირის მფლობელობასა თუ ზედამხედველობის ქვეშ არსებული საშუალებებიდან ნებისმიერი კატეგორიის კომპიუტერული მონაცემის, მათ შორის მომხმარებლის შესახებ ინფორმაციისა და შინაარსობრივი მონაცემის მოპოვების შესაძლებლობას ანიჭებს.[556]

რაც შეეხება სსსკ-ის 136-ე მუხლის მე-2 ნაწილს, მისი განმარტებაც „კიბერდანაშაულის შესახებ“ კონვენციის შესაბამისად უნდა მოხდეს. იმის გათვალისწინებით, რომ სსსკ-ის 136-ე მუხლის პირველი ნაწილი ქვეყნის ტერიტორიაზე მყოფი მომსახურების მომწოდებლისგან ინფორმაციის გამოთხოვის შესაძლებლობასაც გულისხმობს, მე-2 ნაწილი აწესრიგებს შემთხვევას, როდესაც მომხმარებლის შესახებ ინფორმაციის გამოთხოვა იმ მომსახურების მომწოდებლისგან არის საჭირო, რომელიც მართალია ფიზიკურად არ იმყოფება და რეგისტრირებული არ არის ქვეყნის ტერიტორიაზე, თუმცა მომსახურებას სთავაზობს ადგილობრივ მოსახლეობას. [557] ასეთ მოცემულობაში პროკურორის მიერ მომხმარებლის შესახებ ელექტრონული ინფორმაციის გამოთხოვისთვის მნიშვნელოვანია, მან დასაბუთებული ვარაუდის სტანდარტით ამტკიცოს, რომ პირი დანაშაულებრივ ქმედებას კომპიუტერული სისტემის გამოყენებით ახორციელებს, რაც საკმაოდ ზღუდავს ნორმის მოქმედების ფარგლებს.[558] ყურადსაღებია ის ფაქტიც, რომ სსსკ-ის 136-ე მუხლის მე-2 ნაწილით მომხმარებლის შესახებ ინფორმაციის გამოთხოვის უფლებამოსილებით მხოლოდ პროკურორი სარგებლობს, რაც მხარეთა თანასწორობისა და შეჯიბრებითობის კუთხით კითხვის ნიშნებს აჩენს, ისევე როგორც ამავე მუხლის პირველი ნაწილი წარმოშობდა კითხვებს საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილებამდე.[559]

---

[556] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 234.

[557] Production Orders for Subscriber Information (Article 18 Budapest Convention), Cybercrime Convention Committee (T-CY), Council of Europe, 2017, 6.

[558] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 235.

[559] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“.

სსსკ-ის 136-ე მუხლის ძველ რედაქციაში ყურადღებას იმსახურებდა მისი მე-4 ნაწილი, რომელიც ელექტრონული დოკუმენტის ან ინფორმაციის გამოთხოვას ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესის მიხედვით აწესრიგებდა. [560] აღნიშნული მნიშვნელოვნად ზღუდავდა მისი მოქმედების ფარგლებს, ვინაიდან ფარული საგამოძიებო მოქმედების ჩატარება მხოლოდ განზრახ მძიმე ან/და განსაკუთრებით მძიმე ან საქართველოს სისხლის სამართლის კოდექსის კონკრეტულ დანაშაულებზე დაწყებული გამოძიების ან სისხლისსამართლებრივი დევნის ფარგლებში იყო დასაშვები.[561] ამგვარი მოწესრიგების ფონზე კითხვის ნიშნებს ბადებდა ის ფაქტიც თუ დოკუმენტის ან ინფორმაციის გამოთხოვა რამდენად წარმოადგენდა ფარულ საგამოძიებო მოქმედებას.[562]

ცხადია, საგამოძიებო მოქმედება შესაძლოა ჩატარდეს როგორც ღიად, ისე ფარულად. ტრადიციულ შემთხვევებში, საგამოძიებო მოქმედების ჩატარების მიზანი წარსულში მომხდარი ფაქტის შესახებ ინფორმაციის მოპოვებაა,[563] თუმცა, ფარული საგამოძიებო მოქმედების შემთხვევაში მიზანი განჩინების გამოტანის შემდეგ განხორციელებული ქმედებების შესახებ ინფორმაციის მიმდინარე რეჟიმში მიღებაცაა.[564] მაგალითისთვის, სატელეფონო კომუნიკაციის ფარული მიყურადება ან თუნდაც საფოსტო-სატელეგრაფო გზავნილის კონტროლი მიმდინარეობს ფარულად და უწყვეტად, გარკვეული დროის განმავლობაში და მიმართულია განჩინების გამოტანის შემდგომ, მისი ადრესატის მიერ განხორციელებული ქმედების დაკვირვებისკენ.

ამასთან, კომპიუტერული მონაცემის გამოთხოვის დროს ინფორმაციაზე წვდომა ხდება ერთჯერადად, როცა ელექტრონული მონაცემის შექმნა, დამუშავება, გადაცემა და მასთან დაკავშირებული მოქმედებები უკვე დასრულებულია და დაინტერესებული მხარისთვის წინასწარ არის ცნობილი მოსაპოვებელი

---

[560] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 235.

[561] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09/10/2009, 143[3] - მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი.

[562] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 6 მაისის განჩინება №1გ/633-20, 3.

[563] *აქუბარდია ი.,* საბანკო ანგარიშების მონიტორინგის ადგილი საგამოძიებო მოქმედებათა სისტემაში, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021, 63.

[564] *კვეკვეცია ქ.,* საბანკო ანგარიშის მონიტორინგი, როგორც საგამოძიებო მოქმდება - კანონმდებლობა და პრაქტიკა, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021, 316-317.

ინფორმაციის სახე და მოცულობა. ფარული საგამოძიებო მოქმედებებისგან განსხვავებით, სსსკ-ის 136-ე მუხლის საფუძველზე ნებადართულია მხოლოდ წარსულში, სასამართლოს განჩინების ან პროკურორის დადგენილების მიღებამდე შექმნილი და შენახული ელექტრონული სახის ინფორმაციის მოპოვება.[565] ამდენად ცხადია, რომ კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედება შინაარსობრივად განსხვავდება ფარული საგამოძიებო მოქმედებისგან, რაზეც კიბერდანაშაულის შესახებ კონვენცია და საერთაშორისო გამოცდილებაც მიგვითითებს.[566]

არანაკლებ საყურადღებოა, პერსონალურ მონაცემთა დაცვის სამსახურის მხრიდან საგამოძიებო მოქმედების კონტროლისა და ზედამხედველობის საკითხი. ელექტრონული კომუნიკაციის კომპანიამ სამართალდამცავი ორგანოსთვის კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გადაცემის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურს მონაცემთა გადაცემიდან 24 საათში უნდა აცნობოს.[567] კომპანიის მიერ ვალდებულების შესრულების დადგენის მიზნით კი სამსახური უფლებამოსილია შემოწმება ჩაატაროს, რა დროსაც ამუშავებს კომპანიიდან და სასამართლოდან მიღებულ დოკუმენტაციას და მათი ანალიზისა და შედარების საფუძველზე ადგენს სამართალდარღვევის ჩადენის ფაქტს.[568] თუმცა, როგორც ითქვა აღნიშნული სახის კონტროლი მხოლოდ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებს ეხება და არა ყველა სახის ელექტრონულ ინფორმაციას.

ამდენად, შეჯამების სახით შეიძლება ითქვას, რომ სსსკ-ის 136-ე მუხლს 1-ლი ნაწილი ქვეყნის ტერიტორიაზე მყოფ პირთაგან ნებისმიერი კატეგორიის ელექტრონული მონაცემის, მათ შორის მომხმარებლის შესახებ ინფორმაციის მოპოვების საშუალებას იძლევა. ხოლო მისი მე-2 ნაწილი იმ მომსახურების მომწოდებლისგან მომხმარებლის

---

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

[566] Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, 2014, 15-28. <https://rm.coe.int/16802e7ad1> [11.06.23]. იხ. *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 234-235.

[567] საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, სსმ, 28/12/2011. მუხლი 20(4). *იხ.* საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, სსმ, 02/06/2005, მუხლი 8^2.

[568] სახელმწიფო ინსპექტორის საქმიანობის ანგარიში 2021, 303. <https://personaldata.ge/cdn/2022/03/SIS-2021-Annual-Report.pdf> [12.06.23].

შესახებ ინფორმაციის მოპოვებას აწესრიგებს, რომელიც არ იმყოფება ქვეყნის ტერიტორიაზე, თუმცა მომსახურებას სთავაზობს ადგილობრივ მოსახლეობას. [569] ამასთან, სსსკ-ის 136-ე მუხლის მე-2 ნაწილთან დაკავშირებით საგულისხმოა, რომ მომხმარებლის შესახებ ინფორმაციის გამოთხოვის შუამდგომლობის დაყენებისას, საგამოძიებო მოქმედების ჩატარების აუცილებლობასთან ერთად პროკურორმა მომხმარებლის მიერ კომპიუტერული სისტემის გამოყენებით დანაშაულის შესაძლო ჩადენის ფაქტის არსებობაც უნდა დაასაბუთოს.

3.2. ძველი რედაქცის შესაბამისობა კონვენციის მოთხოვნებთან

საინტერესოა თუ რამდენად თანხვედრაში იყო სსსკ-ის 136-ე მუხლის ძველი საკანონმდებლო რეგულაცია „კიბერდანაშაულის შესახებ“ კონვენციით დადგენილ მოთხოვნებთან. [570] განსაკუთრებით კი ნორმის მოქმედების ფარგლებისა და ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის კუთხით.
ნიშანდობლივია, რომ კონვენციის მე-14 მუხლის მე-2 ნაწილის შინაარსი საშუალებას იძლევა კომპიუტერული მონაცემის წარმოდგენის ბრძანების საგამოძიებო მოქმედება ნებისმიერი კატეგორიის დანაშაულზე მიმდინარე გამოძიების პროცესში იყოს გამოყენებული.

დანაშაულთა წრით საგამოძიებო მოქმედების ფარგლების შეზღუდვის მოთხოვნა მხოლოდ ფარულ საგამოძიებო მოქმედებებს უკავშირდება, ვინაიდან მათი გამოყენების შედეგად ხანგძლივად და იმავდროულად მაღალი ინტენსივობით იზღუდება პირადი ცხოვრების უფლება. განსხვავებულ სურათს ვხვდებით თავად კომპიუტერული მონაცემის გადაცემის ბრძანების შემთხვევაში, ვინაიდან იგი ერთადერთ საგამოძიებო მოქმედებას წარმოადგენს, რომელიც შენახული ელექტრონული ინფორმაციის მოპოვების შესაძლებლობას უფლების მომეტებული შეზღუდვის გარეშე იძლევა. [571] შესაბამისად, სსსკ-ის 136-ე მუხლის მოქმედების

[569] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 235.
[570] იქვე, 236.
[571] იქვე.

ფარგლების დანაშაულთა წრით შეზღუდვა აშკარად წინააღმდეგობაში იყო კონვენციის მოთხოვნებთან.[572]

მიუხედავად იმისა, რომ დოკუმენტის ან ინფორმაციის გამოთხოვისას ფარული საგამოძიებო მოქმედებისათვის დადგენილი რეჟიმი მოიხსნა და ამით ეროვნული კანონმდებლობა მნიშვნელოვნად დაუახლოვდა კონვენციას, დღესაც ნორმის მოქმედების ფარგლების მხრივ გამოწვევად რჩება სსსკ-ის 136-ე მუხლის მე-2 ნაწილში არსებული ჩანაწერი „პირი დანაშაულებრივ ქმედებას კომპიუტერული სისტემის გამოყენებით ახორციელებს". [573] საგულისხმოა, რომ აღმოსავლეთ პარტნიორობის მიერ საქართველოს მიმართ გაცემულ რეკომენდაციაში მითითებულია მსგავსი შეზღუდვის მოხსნის საჭიროებაზე,[574] თუმცა ამ მხრივ მუხლში შესაბამისი ცვლილება არც მანამდე და არც შემდეგ არ განხორციელებულა.[575]

ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის მოთხოვნების კუთხით ეროვნული კანონმდებლობის სასარგებლოდ უნდა აღინიშნოს, რომ როგორც ძველი, ისე მოქმედი რედაქციით დოკუმენტის ან ინფორმაციის გამოთხოვისთვის დადგენილია ფორმალური და მატერიალური წინაპირობების დაკმაყოფილების ვალდებულება.[576] საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელია სისხლის სამართლის საქმეზე ოფიციალური გამოძიების მიმდინარეობა, სასამართლოსთვის მოტივირებული შუამდგომლობის წარდგენა,[577] Ex ante და Ex post (ბრალდების მხარის

---

[572] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 58-60. იხ. Criminal Procedure Code of Austria, 30.12.1975, Article 76a, 90(7); Telecommunications Act 2003, 19.08.2003, Article 92(3); German Code of Criminal Procedure, 07/04/1987, Article 100j; Telecommunications Act (TKG), 06/22/2004, Article 113(3).

[573] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ" კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 236.

[574] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 44,<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [04.06.23].

[575] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ" კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 237.

[576] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის განჩინება №1გ/363-20, 3.

[577] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 38,<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [04.06.23].

შემთხვევაში) სასამართლო კონტროლი [578] და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ზედამხედველობის განხორციელება.[579]

დასკვნის სახით კი შეიძლება ითქვას, რომ სსსკ-ის 136-ე მუხლის ძველი რედაქცია მყარ გარანტიას წარმოადგენდა ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვის კუთხით[580] და ამით თანხვედრაში მოდიოდა კონვენციისა და საერთაშორისო სამართლის მოთხოვნებთან.[581] აშკარა შეუსაბამობას მხოლოდ მისი მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვის ნაწილში ვხვდებოდით[582], რაც წლების მანძილზე პრაქტიკაში მნიშნელოვან დაბრკოლებებს ქმნიდა.[583]

3.3. საერთო სასამართლოებში დამკვიდრებული განმარტებები კომპიუტერული მონაცემის გამოთხოვასთან დაკავშირებით

3.3.1. შუამდგომლობის დასაბუთებულობის საკითხი

სასამართლოს წინაშე დასაბუთებული შუამდგომლობის წარდგენას, გადამწყვეტი მნიშვნელობა აქვს ისეთი საგამოძიებო მოქმედების ჩატარების ნებართვის მისაღებად, რომელიც კერძო საკუთრების, მფლობელობის ან პირადი ცხოვრების ხელშეუხებლობის შეზღუდვას ითვალისწინებს. ეს წესი მოქმედებს უშუალოდ კომპიუტერული მონაცემის გამოთხოვის შემთხვევაშიც. სწორედ ამიტომ, შუამდგოლობის დაუსაბუთებლობის მოტივით ხშირია მოსამართლეთა უარი ელექტრონულად შენახული ინფორმაციის გამოთხოვის ნებართვის გაცემაზე.

---

[578] 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> [12.06.23].

[579] საქართველოს პარლამენტის გადაწყვეტილებით 2022 წლის 1 მარტიდან სახელმწიფო ინსპექტორის სამსახური გაუქმებულია. ნაცვლად ორი უწყება - სპეციალური საგამოძიებო სამსახური და პერსონალურ მონაცემთა დაცვის სამსახური იფუნქციონირებს.

[580] *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022, 237.

[581] იქვე.

[582] *სვიანიძე გ.,* დოკუმენტის ან ინფორმაციის გამოთხოვასთან დაკავშირებული სასამართლო პრაქტიკის ანალიზი, ჟურნ. მართლმსაჯულება და კანონი, N3(55), 2017, 98.

[583] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 ოქტომბრის განჩინება №1გ/1614-16, 9. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 25 დეკემბრის განჩინება №1გ/2110-19, 4-5; თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 26 დეკემბრის განჩინება №1გ/2133-19.

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 93-ე მუხლის მე-2 ნაწილის შინაარსის მიხედვით „შუამდგომლობა დასაბუთებული უნდა იყოს, მასში კონკრეტულად უნდა იყოს გადმოცემული ჯერ მოთხოვნა და შემდეგ მოთხოვნის არგუმენტაცია და იგი უნდა ეხებოდეს მხოლოდ იმ გარემოებებს, რომლებსაც უშუალო კავშირი აქვს შუამდგომლობაში დასმულ საკითხებთან“.[584] აღნიშნული კი შუამდგომლობის ავტორს სასამართლოს წინაშე ბრალდებასა და სისხლის სამართლის საქმის გარემოებებთან დაკავშირებული კონკრეტული არგუმენტაციის წარდგენის ვალდებულებას აკისრებს.[585] სხვა საგამოძიებო მოქმედებების მსგავსად, დოკუმენტის ან ინფორმაციის გამოთხოვის მიზნით ნებართვის გაცემის შემთხვევაშიც, აუცილებელია დასაბუთებული ვარაუდის არსებობა, რომელიც მოსამართლეს, შუამდგომლობაში მითითებული ფაქტებისა და მტკიცებულებების გათვალისწინებით, ინფორმაციის გამოთხოვის მართებულობაში დაარწმუნებს.[586]თუ მხარეთა მიერ წარდგენილი შუამდგომლობა ზემოხსენებულ მოთხოვნებს არ შეესაბამება, სასამართლო უარს აცხადებს შუამდგომლობის დაკმაყოფილებაზე. გასათვალისწინებელია, რომ თითოეულ სისხლის სამართლის საქმეში, განსხვავებული გარემოებები და მტკიცებულებები ქმნიან დასაბუთებული ვარაუდის სტანდარტს. შესაბამისად, საუკეთესო გზა კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობის დასაბუთებისთვის საჭირო საკითხების წარმოსაჩენად, სასამართლო პრაქტიკის კვლევაა.

სისხლის სამართლის საქმეზე, რომელშიც გამოძიება სსკ-ის 260-ე მუხლის 1-ლი ნაწილით მიმდინარეობდა, ადვოკატმა ვიდეო-კამერის ჩანაწერების გამოთხოვის შუამდგომლობით მიმართა სასამართლოს, თუმცა მოთხოვნის დაუსაბუთებლობის მოტივით უარი ეთქვა მის დაკმაყოფილებაზე. მოსამართლის განმარტებით, მითითება იმაზე, რომ ისინი გამამართლებელი მტკიცებულებებია, არასაკმარისია მოთხოვნის დასაკმაყოფილებლად. აუცილებელია მსჯელობა და მითითება იმაზე თუ რა უნდა დაადასტუროს მოცემულმა მტკიცებულებამ, რა კუთხითაა ის

[584] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 31 დეკემბრის განჩინება N1გ/2153-19, 3.

[585] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 21 სექტემბრის განჩინება N1გ/1594-21, 3.

[586] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 31 დეკემბრის განჩინება N1გ/2153-19, 3.

გამამართლებელი, რა არის სადავო და რის დადგენას შეუწყობს ხელს კონკრეტულ სისხლის სამართლის საქმეზე. მოცემულობა, რომ კონკრეტული ჩანაწერი არსებობს, არ ქმნის ამ ჩანაწერის იმთავითვე მოპოვების საჭიროებას. დასაბუთებული უნდა იყოს ჩანაწერის რელევანტურობა საქმესთან, მათი მნიშვნელობა სადავო ფაქტების გადასამოწმებლად და ა.შ.[587] სხვა სისხლის სამართლის საქმეში,[588] სადაც ადვოკატი კვლავ ვიდეო კამერის ჩანაწერის მოპოვების ნებართვას ითხოვდა, სასამართლომ ზემოაღნიშნულ ინფორმაციასთან ერთად, ვიდეო კამერის მესაკუთრის ან მფლობელის შესახებ ინფორმაციის წარდგენის აუცილებლობაზეც გაამახვილა ყურადღება.[589]

დაუსაბუთებელი აღმოჩნდა პროკურორის შუამდგომლობა პირველი ინსტანციის სასამართლოსთვის, როდესაც იგი პირთა მობილური ტელეფონებიდან საქმის ფაქტობრივ გარემოებებთან დაკავშირებული ინფორმაციის გამოთხოვის ნებართვას ითხოვდა. მოსამართლის განმარტებით შუამდგომლობა, მოთხოვნის ნაწილში ზოგადი და აბსტრაქტული იყო. პროკურორის მიერ დაკონკრეტებული არ იყო თუ რა სახის ინფორმაცია ინახებოდა კომპიუტერულ სისტემაში. ამასთან, ყურადღებას არ ამახვილებდა გამოსათხოვ სავარაუდო დოკუმენტსა და ინფორმაციაზე. აღნიშნული განჩინების გასაჩივრებისას, პროკურომა მიუთითა, რომ შუამდგომლობა დასაბუთებულია, ვინაიდან იგი ტელეფონიდან არა თუ ნებისმიერი სახის, არამედ მხოლოდ საქმის ფაქტობრივ გარემოებებთან დაკავშირებული ინფორმაციის მოპოვებას ითხოვდა. რამდენადაც გასაკვირი არ უნდა იყოს, საგამოძიებო კოლეგიის მხრიდან საჩივარი ნაწილობრივ დაკმაყოფილდა და ერთ-ერთი ადრესატის მობილური ტელეფონიდან ინფორმაციის გამოთხოვის ნებართვა გასცა.[590]

შეუძლებელია დაეთანხმო საგამოძიებო კოლეგიის ამ გადაწყვეტილებას, ვინაიდან დოკუმენტის ან ინფორმაციის გამოთხოვის შუამდგომლობის დაყენებისას წინასწარ უნდა განისაზღვროს ინფორმაციის სახე და მოცულობა, ასევე, ის თუ რა ფორმით (ელ.

[587] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 9 სექტემბრის განჩინება N1გ/1447-20 2. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 10 ივლისის განჩინება N1გ/1029-20.

[588] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 11 სექტემბრის განჩინება N1გ/1504-19.

[589] იქვე, 2-3.

[590] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 14 ივნისის განჩინება N1გ/917-2022.

მოწყობილობა, ამონაბეჭდი და ა.შ.) უნდა მიეწოდოს ელექტრონული ინფორმაცია დაინტერესებულ პირს. სსსკ-ის 136-ე მუხლის საფუძველზე დაუშვებელია დანაშაულში მამხილებელი მასალების უკონტროლო ძიება (Fishing Expedition). დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების ჩატარება მიზანშეწონილია, როდესაც არსებობს დასაბუთებული ვარაუდი, რომ მონაცემი ინახება კომპიუტერულ სისტემაში ან შემნახველ მოწყობილობაში, გარკვეულ პირთან და მისი ძებნა საჭირო არ არის. თუ გარკვეული ინფორმაციის ძებნის საჭიროება არსებობს, მაშინ ბრალდების მხარემ „კიბერდანაშაულის შესახებ“ კონვენციის მე-19 მუხლით გათვალისწინებულ „კომპიუტერული მონაცემის ჩხრეკა-ამოღების“ საგამოძიებო მოქმედებას უნდა მიმართოს, რომელიც არა თუ წინასწარ ცნობილი ინფორმაციის ამოსაღებად, არამედ დანაშაულთან დაკავშირებული მტკიცებულებების მოსაძებნად გამოიყენება.

ასევე, დაუსაბუთებლობის მოტივით არ დაკმაყოფილდა ადვოკატის შუამდგომლობა, როდესაც იგი შპს-დან მობილური ტელეფონის სააბონენტო ნომერზე განხორციელებული შემავალი/გამავალი/გამოტოვებული ზარების და მოკლე ტექსტური შეტყობინების (შესაბამისი მობილური აღჭურვილობის სადგურის საერთაშორისო იდენტიფიკატორის (IMEI) კოდების, მომსახურების ანძების დასახელებისა და ადგილმდებარეობის მითითებით მოკავშირე აბონენტთა დემოგრაფიული მონაცემების) შესახებ ინფორმაციას ითხოვდა. [591] ქართულ რეალობაში გავრცელებული პრაქტიკაა მსგავსი შუამდგომლობით სასამართლოსთვის მიმართვა. [592] თუმცა, აქ ყურადსაღები მოსაპოვებელი ინფორმაციის სახე და მოცულობაა. უშუალოდ შემავალი და გამავალი ზარების შესახებ მონაცემები არ წარმოადგენს სენსიტიურ, შინაარსობრივ ინფორმაციას, თუმცა, როდესაც მასთან ერთად ადგილმდებარეობის, მოკავშირე აბონენტთა დემოგრაფიული მონაცემების და მათი მობილური აღჭურვილობის სადგურის საერთაშორისო იდენტიფიკატორის (IMEI) გამოკვლევა ხდება, საკმაოდ დიდი მოცულობის მონაცემთა დამუშავებასთან გვაქვს საქმე. ფაქტობრივად, მოცემული

[591] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 31 დეკემბრის განჩინება N1გ/2154-19, 1.

[592] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 27 ნოემბრის განჩინება N1გ/1984-19.

შუამდგომლობის დაკმაყოფილებით, მხარეს შესაძლებლობა ეძლევა გამოთხოვილ ინფორმაციაზე დაყრდნობით, სრული სიზუსტით აღადგინოს დროის კონკრეტულ მონაკვეთში განხორციელებული კომუნიკაციის და მასში მონაწილე პირების შესახებ ინფორმაცია, რაც თავის მხრივ პირადი ცხოვრების ინტენსიურ შეზღუდვას წარმოადგენს. შესაბამისად, ამგვარი შუამდგომლობის დაკმაყოფილებას საკმაოდ მყარი დასაბუთება და არგუმენტაცია სჭირდება. მყარ დასაბუთებას მოითხოვს IP მისამართის მფლობელის მაიდენტიფიცირებელი ინფორმაციის გამოთხოვის შუამდგომლობაც.[593] მართალია, მოცემულ საქმეში დაცვის მხარეს სასამართლოს მხრიდან შუამდგომლობის დაკმაყოფილებაზე უარი სისხლის სამართლის საქმეზე ფაქტობრივი და ბრალდების გამომრიცხავი გარემოებების დადგენისთვის გამოსათხოვი ინფორმაციის მნიშვნელობის დაუსაბუთებლობის გამო ეთქვა, თუმცა IP-მისამართთან დაკავშირებით პრაქტიკული მნიშვნელობის საკითხის განხილვა აუცილებელია, რომელსაც მხარეებმა შუამდგომლობის დასაბუთებისას, ხოლო სასამართლომ კი მისი გადაწყვეტისას, ყურადღება უნდა მიაპყრონ.

ნიშანდობლივია, რომ IP მისამართი შესაძლოა სტატიკური ან დინამიური თვისების იყოს. განსხვავებით სტატიკურისა, დინამიური თვისების IP მისამართი მომხმარებლის მიერ ქსელზე ყოველი მიერთებისას ან თუნდაც კომპიუტერის პროგრამული განახლებისას იცვლება. შესაბამისად, თუ გამოძიებისთვის დინამიური IP მისამართის მფლობელის ვინაობაა საინტერესო, მის დასადგენად პროვაიდერ კომპანიას მრავალ მომხმარებელთან დაკავშირებული ტრაფიკის მონაცემების მოძიება და კვლევა უწევს, რაც კომუნიკაციის საიდუმლოებას წარმოადგენს.[594]

შემავალი, გამავალი და გამოტოვებული ზარების, მოკლე ტექსტური შეტყობინებების და ნომრის მომსახურე ანძების, მოკავშირე აბონენტთა დემოგრაფიული მონაცემების, იუსტიციის სამინისტროდან გამოძიების დაწყებისა და მოწმის გამოკითხვის რეგისტრაციის შესახებ ინფორმაციის გამოთხოვას ეხება სისხლის სამართლის საქმე, სადაც სასამართლომ მოთხოვნის დაუსაბუთებლობის მოტივით არ დააკმაყოფილა ადვოკატის შუამდგომლობა.[595] პირველ ნაწილში, შუამდგომლობის დაუსაბუთებლობა ძირითადად გამოწვეული იყო მობილური ოპერატორისა და

[593] თბილისის სააპელაციო სასამართლოს 2020 წლის 25 აგვისტოს განჩინება N1გ/1328-20.

[594] *Benedik v. Slovenia,* [2018] ECHR, 23.

[595] თბილისის სააპელაციო სასამართლოს 2019 წლის 4 ოქტომბრის განჩინება N1გ/1639-19.

ნომრის მესაკუთრის შესახებ ინფორმაციის მიუთითებლობით. ხოლო საქართველოს იუსტიციის სამინისტროდან ინფორმაციის გამოთხოვის ნაწილში წარდგენილი არ იყო ინფორმაცია ნამდვილად ინახებოდა თუ არა გამოსათხოვი მონაცემები უწყების ელექტრონულ სისტემაში. სასამართლოს სჭირდებოდა კონკრეტული მტკიცებულება, რაც წარმოდგენას შეუქმნიდა ჩანაწერების არსებობის თაობაზე. როგორც სასამართლომ განმარტა, გამოთხოვის დროს მხარემ რეალურად უნდა იცოდეს რომ კონკრეტული ელექტრონული პროგრამა მუშაობს გამართულად, მასში ინახება ინფორმაცია და ის არ წაშლილა.[596]

ასევე, ჩანაწერის რეალურად არსებობის დამადასტურებელი მტკიცებულების წარდგენის აუცილებლობაზე ამახვილებს მოსამართლე ყურადღებას, როდესაც ადვოკატი პოლიციის შენობის გარე პერიმეტრის ვიდეოკამერის ჩანაწერის გამოთხოვას ითხოვს. [597] სასამართლოს არგუმენტაციით დაცვის მხარეს არ წარმოუდგენია მტკიცებულება, რომ დამონტაჟებული სამეთვალყურეო კამერები გამართულ მდგომარეობაშია, მასში ინახება ჩანაწერი და ნამდვილად შესაძლებელია მათგან ამოღებულ იქნას მოთხოვნილი ინფორმაცია. მეტიც, მხარემ რეალურად უნდა იცოდეს, რომ გასული არ არის ჩანაწერის შენახვის ვადა.[598] კითხვის ნიშნებს ბადებს მოსამართლეთა პოზიცია, თითქოს მხარემ ზუსტად უნდა იცოდეს რომ სისტემაში ნამდვილად ინახება ჩანაწერი, რომ გამართულად ფუნქციონირებს ვიდეო კამერა ან პროგრამა და რეალურად შესაძლებელია მოწყობილობიდან ინფორმაციის ამოღება. როგორც წესი იმის დასადგენად გამართულად მუშაობს თუ არა კომპიუტერული სისტემა, საჭიროა სპეციალური ცოდნა ან მესაკუთრის ან მფლობელის ან უფლებამოსილი პირის განმარტება მოწყობილობის ფუნქციონირებასთან დაკავშირებით. თუმცა, როგორ უნდა მოიქცეს მხარე ისეთ შემთხვევაში, როდესაც მესაკუთრე ან სხვა უფლებამოსილი პირი უარს აცხადებს თანამშრომლობაზე და არ აწვდის ინფორმაციას ჩანაწერის არსებობის, მოწყობილობის გამართულად ფუნქციონირების შესახებ. ზუსტად მსგავსი პრობლემის წინაშე იდგა ადვოკატი, ვინაიდან სამართალდამცავი ორგანოსთვის ჩანაწერის არსებობის დადგენის თაობაზე

[596] იქვე, 4-5.
[597] თბილისის სააპელაციო სასამართლოს 2020 წლის 6 იანვრის განჩინება N1გ/20-20.
[598] იქვე, 4-5.

გაგზავნილ წერილზე პასუხი არ მიუღია.[599] ამასთან, მხარემ შუამდგომლობის დაყენებისას დასაბუთებული ვარაუდის სტანდარტით უნდა ამტკიცოს, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი ინახება. მტკიცების ყველაზე დაბალი სტანდარტით, რომელიც მეტია ვიდრე უბრალოდ ეჭვი, თუმცა, არა აბსოლუტური ჭეშმარიტება. როგორც თავად სიტყვა „დასაბუთებული ვარაუდი“ გვკარნახობს, საქმე ალბათობებთან გვაქვს, რაც სპეციფიკურ და გამოხატულ ფაქტებზეა დაფუძნებული და ერთობლიობაში პრაგმატულ, საღად მოაზროვნე, გონიერ და წინდახედულ ადამიანს არწმუნებს, რომ საგამოძიებო მოქმედების ჩატარება მიზანშეწონილი და გამართლებულია.[600]

თვალსაჩინოებისთვის, როდესაც დანაშაულის შემთხვევის ადგილას მდებარე ობიექტზე დამონტაჟებულია სამეთვალყურეო კამერა და მხარე შუამდგომლობს დანაშაულის ჩადენის დროის მიხედვით ჩანაწერის გამოთხოვას ბრალდებულის სხვაგან ყოფნის ფაქტის დასადასტურებლად და შუამდგომლობას თან ერთვის ბრალდებულის გამოკითხვის ოქმი, სადაც უთითებს, რომ მოცემული დროის მონაკვეთში სხვაგან იმყოფებოდა, შემთხვევის ადგილის დათვალიერების ოქმი, რომელსაც თან ერთვის ფოტოსურათები და დგინდება, რომ ხსენებულ ტერიტორიაზე მდებარეობს „შპს“, რომლის პერიმეტრზეც განთავსებულია კამერა, წარმოდგენილია სამეწარმეო რეესტრის ამონაწერი, რომლითაც ირკვევა, რომ შპს-ს იურიდიული მისამართი ემთხვევა ფაქტობრივ მისამართს და იქმნება გონივრული ვარაუდი, რომ ეს კამერები შპს-ს კუთვნილებაა, ნამდვილად აკმაყოფილებს საპროცესო კანონმდებლობით განსაზღვრულ დასაბუთებული ვარაუდის სტანდარტს.

შესაბამისად, სასამართლოს მითითება, რომ წარმოდგენილი არ არის მტკიცებულება ჩანაწერის არსებობის შესახებ, ნამდვილად ეკუთვნის თუ არა ის შპს-ს, მაშინ როდესაც მათ ობიექტზეა კამერები განთავსებული და ეს დათვალიერების ოქმით და ამონაწერით დასტურდება, ან ის თუ რა პერიოდით ინახება ჩანაწერები სისტემაში, არაგონივრულია.[601] სასამართლოს განმარტებით დაცვის მხარეს შეეძლო მესაკუთრის

[599] იქვე, 3.

[600] *Terry v. Ohio* (1968), 392 US 1, 21-2. Illinois v. Gates (1983) 462 US 213, 239.

[601] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 11 სექტემბრის განჩინება N1გ/1504-19, 3-4.

თანხმობით დაეთვალიერებინა ვიდეო ჩანაწერი და ჩანაწერის დათვალიერების ოქმი თან დაერთო შუამდგომლობისთვის, რაც სხვა მტკიცებულებებთან ერთად ნამდვილად დააკმაყოფილებდა დასაბუთებული ვარაუდის სტანდარტს. მეტიც, მოსამართლის აზრით, დათვალიერების ჩატარებაზე ან კომუნიკაციაზე უარის მიღების შემთხვევაშიც, დასაბუთებული ვარაუდის სტანდარტი დაკმაყოფილებულად ჩაითვლებოდა. კომპიუტერული მონაცემის დათვალიერებით ნამდვილად დადასტურდებოდა ჩანაწერის არსებობის საკითხი, თუმცა რაც შეეხება უარის დამადასტურებელი დოკუმენტის წარდგენით, მოცემულობა ვერ შეიცვლებოდა, ვინაიდან გარემოებები (ჩანაწერის არსებობა, შენახვის პერიოდულობა და პროგრამის გამართულად ფუნქციონირება), რომლებზეც სასამართლო აპელირებს, აღნიშნულით ვერ დადასტურდებოდა.

ნათელია, რომ სასამართლო შუამდგომლობასთან ერთად წარდგენილ მასალათა საკმარისობას ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად, საქმის გარემოებების გათვალისწინებით აფასებს, თუმცა აუცილებლად წარსადგენ ინფორმაციათა გამოყოფა მაინც შესაძლებელია. კერძოდ, აუცილებელია მითითება იმის შესახებ თუ რა გარემოებების დადგენას შეუწყობს ხელს მოთხოვნილი ინფორმაცია,[602] დასაბუთებული უნდა იყოს მოთხოვნილი ინფორმაციის სისხლის სამართლის საქმესთან რელევანტურობა, განსაზღვრული უნდა იყოს კომპიუტერული სისტემის ან მონაცემის მესაკუთრე ან მფლობელი [603] და შუამდგომლობაში მითითებული უნდა იყოს თუ რა სახის და რა მოცულობის ინფორმაციის გამოთხოვას ითხოვს მხარე. [604] რიგ შემთხვევებში სასამართლო კომპიტერული სისტემის გამართულად ფუნქციონირების, ჩანაწერის შენახვის ვადისა [605] და სისტემიდან ინფორმაციის რეალურად ამოღების შესაძლებლობის შესახებ მტკიცებულების წარდგენასაც ითხოვს, რაც პრაქტიკული თვალსაზრისით გარკვეულ დაბრკოლებებს ქმნის და როგორც ზემოთ ვახსენეთ დასაბუთებული ვარაუდის სტანდარტის დაკმაყოფილებისთვის სრულებით არ არის საჭირო ამგვარი ინფორმაციის სასამართლოს წინაშე წარდგენა.

[602] თბილისის სააპელაციო სასამართლოს 2021 წლის 14 სექტემბრის განჩინება N1გ/1553-21.
[603] თბილისის სააპელაციო სასამართლოს 2021 წლის 12 ოქტომბრის განჩინება N1გ/1709-21.
[604] თბილისის სააპელაციო სასამართლოს 2022 წლის 2 თებერვლის განჩინება N1გ/152-22.
[605] თბილისის სააპელაციო სასამართლოს 2021 წლის 7 სექტემბრის განჩინება N1გ/1518-21.

3.3.2. კომპიუტერული მონაცემის გამოთხოვის საკითხი ნაკლებად მძიმე კატეგორიის დანაშაულის გამოძიებისას

ნაკლებად მძიმე კატეგორიის დანაშაულზე მიმდინარე გამოძიების შემთხვევაში, ელექტრონული ინფორმაციის სსსკ-ის 136-ე მუხლის საფუძველზე გამოთხოვის შესაძლებლობის არქონა, წლების განმავლობაში მნიშვნელოვან დაბრკოლებას წარმოადგენდა როგორც ბრალდების, ისე დაცვის მხარისთვის. დანაშაულის კატეგორიის მიუხედავად, კომპიუტერულ მონაცემზე წვდომა მხოლოდ 2022 წლის 24 მაისს საქართველოს სისხლის სამართლის საპროცესო კოდექსში განხორციელებული ცვლილებით, სსსკ-ის 136-ე მუხლისთვის ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესების გაუქმების შედეგად გახდა შესაძლებელი.

რამდენად მნიშვნელოვან დაბრკოლებას წარმოადგენდა საკანონმდებლო ხარვეზი და რა უარყოფითი ზეგავლენა ჰქონდა ნორმის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვას მართლმსაჯულების განხორციელების პროცესზე, მის წარმოსაჩენად, საერთო სასამართლოების პრაქტიკის კვლევა-ანალიზი, საუკეთესო საშუალებაა.

სისხლის სამართლის საქმეში, [606] სადაც პირს შემაკავებელი ორდერით გათვალისწინებული ვალდებულების შეუსრულებლობა და დაკავების პროცესში პოლიციის თანამშრომლებისთვის ძალადობის გამოყენებით, მათი საქმიანობის შეცვლის მიზნით წინააღმდეგობის გაწევა ედებოდა ბრალად, დაცვის მხარე სასამართლოს წინაშე ერთ-ერთი მომსახურების ცენტრის ფილიალიდან, მათ გარე პერიმეტრზე განთავსებული სათვალთვალო კამერიდან ვიდეომასალის სახით ინფორმაციის გამოთხოვას შუამდგომლობდა. დაცვის მხარის პოზიციით, ვიდეოჩანაწერზე არსებული მასალა პოლიციელების მიმართ წინააღმდეგობის გაწევის ფაქტს გამორიცხავდა, ხელს შეუწყობდა საქმეში არსებული ჩვენებების შემოწმებას, თუმცა სსსკ-ის 136-ე მუხლის მე-4 ნაწილის (ძველი რედაქცია) დაუკმაყოფილებლობის საფუძვლით დაცვის მხარის მოთხოვნა არცერთ ინსტანციაში არ დაკმაყოფილდა. მოსამართლეთა განმარტებით, დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედებაზე სსსკ- ის 143^{2} – 143^{10} მუხლების დებულებები ვრცელდება. ხოლო სსსკ-ის 143^{3}-ე მუხლის მე-2 ნაწილი იმ კონკრეტულ

[606] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 12 ნოემბრის განჩინება N1გ/1889-19.

დანაშაულებრივ ქმედებებს განსაზღვრავს, რომელთან დაკავშირებითაც მოთხოვნილი საგამოძიებო მოქმედების ჩატარებაა შესაძლებელი. კერძოდ, განზრახ მძიმე ან/და განსაკუთრებით მძიმე დანაშაულები ან იმ კონკრეტული მუხლებით გათვალისწინებული დანაშაულები, რაც გათვალისწინებულია ნორმით.

იდენტური განმარტება გააკეთა სასამართლომ, როდესაც გამოძიება სსკ-ის 126[1] მიმდინარეობდა, ხოლო ადვოკატმა სასამართლოს წინაშე პოლიციის განყოფილებიდან

სამეთვალყურეო ჩანაწერის გამოთხოვით იშუამდგომლა. [607] მოსამართლის განმარტებით, სსსკ-ის 136-ე მუხლი ინფორმაციის გამოთხოვის სპეციალურ წესს ითვალისწინებს, რომელიც კონკრეტულად ადგენს იმ დანაშაულთა წრეს, რომლის ფარგლებშიც შესაძლებელია კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან ინფორმაციის გამოთხოვა. ოჯახში ძალადობა, რომელიც ნაკლებად მძიმე კატეგორიის დანაშაულს განეკუთვნება, არ არის გათვალისწინებული სსსკ-ის 143[3]-ე მუხლის მე-2 ნაწილით გათვალისწინებულ საგამონაკლისო შემთხვევებში. შესაბამისად, არ არსებობს ინფორმაციის გამოთხოვის კანონისმიერი საფუძველიც.

რასაკვირველია, საკანონმდებლო შეზღუდვის მიუხედავად, მხარეებს სისხლის სამართლის საქმისთვის მნიშვნელოვან ელექტრონულ ინფორმაციაზე წვდომა ესაჭიროებოდათ. სწორედ ამიტომ, გაჩნდა ე.წ. „შემოვლითი“ პრაქტიკა, რაც არა თუ ელექტრონული ფორმით მტკიცებულების მოპოვებას, არამედ მის დათვალიერებას გულისხმობდა. [608] ასე მაგალითად, ერთ-ერთ სისხლის სამართლის საქმეზე მხარე მობილური ტელეფონიდან მოწმესა და დაზარალებულს შორის შემდგარი საუბრების აუდიო-ჩანაწერის გამოთხოვის ნებართვას ითხოვდა, სასამართლომ სსსკ-ის 143[3]-ე მუხლის მე-2 ნაწილის მოთხოვნების დაუკმაყოფილებლობის საფუძვლით შუამდგომლობა არ დააკმაყოფილა. თუმცა, იქვე განმარტა, რომ „მიუხედავად იმისა, რომ გამოძიება ნაკლებად მძიმე კატეგორიის დანაშაულზე მიმდინარეობს, შესაძლოა მობილურ ტელეფონში არსებული ინფორმაცია დანაშაულის შესაძლო ჩადენის ფაქტს

[607] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 17 თებერვლის განჩინება N1გ/235-22.

[608] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 24 თებერვლის განჩნება N1გ/272-16. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 4 ოქტომბრის განჩინება N1გ/1537-16, 4.

ეხებოდეს. ამიტომ, კანონი მხარეებს საშუალებას აძლევს საქმისათვის მნიშვნელოვანი ინფორმაცია დათვალიერების გზით მოიპოვონ“.[609] თუმცა, საგამოძიებო კოლეგიის მიერ დადგენილი პრაქტიკით კომპიუტერული სისტემის ან მონაცემთა შემნახველი საშუალების დათვალიერებისას, განსხვავებით ტრადიციული დათვალიერებისგან, აღმოჩენილი ინფორმაციის ან დოკუმენტის ამოღება არ ხდება. ამგვარი განმარტების მიზეზი დოკუმენტის ან ინფორმაციის გამოთხოვაზე ფარული საგამოძიებო მოქმედებისათვის დადგენილი წესების გავრცელება იყო. ხოლო თუ დაგეგმილ დათვალიერებას შესაძლოა თან კომპიუტერული მონაცემის მოპოვების აუცილებლობაც სდევდეს, მხარემ სასამართლოს წინაშე როგორც დათვალიერების, ისე ინფორმაციის გამოთხოვის თაობაზეც უნდა იშუამდგომლოს, რადგან მათი ჩატარების წესი განსხვავებულია.[610] შესაბამისად, დღევანდელი მოცემულობით, როდესაც სსსკ-136-ე მუხლზე აღარ ვრცლდება ფარული საგამოძიებო მოქმედებისთვის დადგენილი წესები და მოქმედებს საგამოძიებო მოქმედების ჩატარების საერთო წესი, თუ მხარე პირის თანხმობის საფუძველზე კომპიუტერული მონაცემის დათვალიერებას ჩაატარებს და მის ფარგლებში ამოიღებს მონაცემს, მოპოვებული ინფორმაცია დასაშვებ მტკიცებულად იქნება მიჩნეული.

ერთი შეხედვით, სასამართლომ და მხარეებმაც ეფექტურ გამოსავალს მიაგნეს, თუმცა ფაქტია, რომ დათვალიერების საგამოძიებო მოქმედება ვერ ჩაანაცვლებს კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედებას და ვერც ელექტრონული ინფორმაციის დათვალიერების ოქმს ვერ ექნება ისეთივე მტკიცებულებითი ღირებულება, როგორც უშუალოდ ინფორმაციის დედანს ან ზუსტ ასლს, რომელზეც საჭიროების შემთხვევაში შესაძლებელია ექსპერტიზის ჩატარება.

ამასთან, ნაკლებად მძიმე კატეგორიის დანაშაულებზე კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობის დაუკმაყოფილებლობის დასაბუთებისთვის მოსამართლეთა მხრიდან ხშირად გამოყენებული ლეგიტიმური მიზანი, პერსონალურ მონაცემთა დაცვა, დათვალიერების დროს, მიუღწეველი რჩება. კომპიუტერული სისტემის, მონაცემთა შემნახველი საშუალების და მათში დაცული

[609] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 18 ნოემბრის განჩინება N1გ/1924-21.

[610] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 სექტემბრის განჩინება N1გ/1497, 6.

ინფორმაციის დათვალიერებისას ისეთივე დოზით ხდება პერსონალური მონაცემების დამუშავება, როგორც ეს სსსკ-ის 136-ე მუხლის საფუძველზე ინფორმაციის გამოთხოვისას.

საინტერესო განმარტება გაკეთდა ერთ-ერთ სისხლის სამართლის საქმეზე, რომელზეც გამოძიება ძალადობის განხორციელების ფაქტზე მიმდინარეობდა.[611] რა თქმა უნდა, დანაშაულის კატეგორიის გამო მხარეს უარი ეთქვა შუამდგომლობის დაკმაყოფილებაზე, თუმცა მნიშვნელოვანი აქ სასამართლოს დასაბუთებაა. თბილისის სააპელაციო სასამართლოს განმარტებით „სსსკ-ის 136-ე მუხლის მე-4 ნაწილის ჩანაწერი ღრმა შინაარსს ატარებს და ის ამ ნორმაში შემთხვევით არ გაჩენილა. აშკარაა, რომ ადამიანის პირადი ცხოვრება, მისი ხელშეუხებლობა ძალზედ მაღალი ღირებულებებია, რეალურად იმაზე მაღალი ვიდრე ნაკლებად მძიმე დანაშაულის გახსნის ინტერესის ღირებულებითი მნიშვნელობა“.[612] მართალია, პირადი ცხოვრების ხელშეუხებლობის და კონფიდენციალურობის დაცვა, ინფორმაციაზე წვდომის შეზღუდვა, ეპოქაში, როდესაც ამდენი ციფრული ინფორმაცია გროვდება, მუშავდება და ინახება მობილური ქსელის პროვაიდერების, სოციალური მედიის კომპანიების, მდებარეობაზე დაფუძნებული აპლიკაციების მიერ, სამართლიანია. თუმცა, კეთილშობილური განზრახვის მქონე კანონმა გამოძიების სრულყოფილად წარმართვას, მართლმსაჯულების დაუბრკოლებლად განხორციელებას და არაერთი საერთაშორისო დოკუმენტით განმტკიცებულ დაცვის უფლებით სარგებლობას, ხელი არ უნდა შეუშალოს.

ზემოაღნიშნულ მნიშველოვან გარემოებებზეც რომ აღარ გავამახვილოთ ყურადღება, დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების დანაშაულთა წრით შეზღუდვა, წინააღმდეგობაში იყო „კიბერდანაშაულის შესახებ“ კონვენციის მე-14 მუხლის მოთხოვნებთან. მოთხოვნებთან, რომელთა მიხედვითაც საგამოძიები მოქმედების გამოყენება **ა) თავად კონვენციით გათვალისწინებული დანაშაულის გამოსაძიებლად; ბ) იმგვარი დანაშაულის გამოსაძიებლად, რომელიც კომპიუტერული სისტემის გამოყენებით არის ჩადენილი და გ) ნებისმიერი დანაშაულის გამოძიებისას,**

[611] თბილისის სააპელაციო სასამართლოს 2019 წლის 25 დეკემბრის განჩინება N1გ/2109-19.

[612] იქვე, 5-6. იხ. თბილისის სააპელაციო სასამართლოს 2020 წლის 21 იანვრის განჩინება N1გ/125-20.

სადაც შესაძლებელია მტკიცებულება ელექტრონული ფორმით არსებობდეს, დასაშვებია.[613]

კონვენციის ავტორთა მხრიდან მოქმედების ფარგლების ასე ფართოდ განსაზღვრა წარმოადგენს დასტურს, რომ კომპიუტერული მონაცემი, ანუ ელექტრონული ინფორმაცია შესაძლოა გამოყენებულ იქნას მტკიცებულებად, მიუხედავად დანაშაულის ხასიათისა და სიმძიმისა.[614]

სამწუხაროდ, რამდენიმე წელიწადი აღმოჩნდა საჭირო იმის გასაცნობიერებლად, რომ კომპიუტერული მონაცემის გამოთხოვა ფარულ საგამოძიებო მოქმედებას არ წარმოადგენს და ნორმის მოქმედების ფარგლების მუხლობრივი შეზღუდვის წესი, ბლანკეტურად ართმევდა მხარეებს მტკიცებულების მოპოვების შესაძლებლობას.[615] ხოლო, დანაშაულთა მთელი რიგი, რომელთა გამოძიების შემთხვევაშიც მხარეები მოკლებულნი იყვნენ შესაძლებლობას, სსსკ 136-ე მუხლის მეშვეობით ელექტრონული ინფორმაცია მოეპოვებინათ, საქართველოს პარლამენტის მიერ განმარტებით ბარათში ფარული საგამოძიებო მოქმედებისთვის დადგენილი წესების გაუქმების აუცილებლობის დასაბუთებისას არის გამოყენებული.[616]

3.3.3. დათვალიერებისა და დოკუმენტის ან ინფორმაციის გამოთხოვის ერთმანეთისგან გამიჯვნის საკითხი

იმის გათვალისწინებით, რომ წლების განმავლობაში ნაკლებად მძიმე კატეგორიის დანაშაულზე მიმდინარე გამოძიებისას კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში დაცული ინფორმაციის მოპოვების გზა, მისი დათვალიერება იყო, მხარეები ცდილობდნენ დათვალიერების ოქმით რაც შეიძლება ზუსტად აღეწერათ ჩანაწერი და როგორღაც გაეზარდათ საქმეზე მისი მტკიცებულებითი ღირებულება. სწორედ მტკიცებულებითი ღირებულების

---

[613] 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> [15.06.23].

[614] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 22. *იხ. Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018, 100.

[615] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, 4-5. <https://info.parliament.ge/file/1/BillReviewContent/297941> [15.06.23].

[616] იქვე.

გაზრდის მიზნით, დაცვის მხარემ კომპიუტერული მონაცემის დათვალიერების ოქმს საგამოძიებო მოქმედების მიმდინარეობის ამსახველი ფოტომასალა დაურთო თან.[617] თუმცა, წინასასამართლო სხდომაზე მტკიცებულებათა დასაშვებობის თაობაზე მხარეთა შუამდგომლობების განხილვისას, მოსამართლემ ბრალდების მხარის შუამდგომლობა დაცვის მხარის მიერ შედგენილი დათვალიერების ოქმზე თანდართული ფოტოილუსტრაციის დაუშვებელ მტკიცებულებად ცნობის თაობაზე დააკმაყოფილა. [618] მოსამართლის განმარტებით აღნიშნული გადაწყვეტილების საფუძველი ოქმზე ფოტოების დართვა გახდა, რაც ახალ, სხვა საგამოძიებო მოქმედებას წარმოადგენს და არღვევს სსსკ-ის 136-ე მუხლის მოთხოვნებს.[619]

თუ სსსკ-ის 126-ე მუხლის მე-3 ნაწილს დავაკვირდებით „დათვალიერება შეიძლება ტექნიკური საშუალებებით ჩატარდეს, თუ ეს არ გამოიწვევს საგნის, დოკუმენტის, ნივთიერებისა თუ ინფორმაციის შემცველი სხვა ობიექტის ან მასზე არსებული კვალის განადგურებას ან დაზიანებას“. ამასთან, სსსკ-ის 134-ე მუხლის მე-4 ნაწილის მიხედვით თუ საგამოძიებო მოქმედების ჩატარებისას გამოყენებული იყო ხმის ან/და გამოსახულების ნებისმიერი ტექნიკური საშუალებით ჩაწერა, შედგა ნახაზი ან სქემა, საგამოძიებო მოქმედების ოქმში უნდა აღინიშნოს გამოყენებული ტექნიკური საშუალებების ტექნიკური მახასიათებლები, მათი გამოყენების პირობები და მიღებული შედეგები. ხოლო, ამავე კოდექსის 135-ე მუხლის მე-4 ნაწილის მიხედვით, დათვალიერების ოქმში, სხვა გარემოებებთან ერთად უნდა აღინიშნოს რა ტექნიკური საშუალება იქნა გამოყენებული და რა შედეგი იქნა მიღებული. ერთობლიობაში კი ყოველივე მიანიშნებს, რომ დაცვის მხარე უფლებამოსილი იყო დათვალიერებისას ტექნიკური საშუალება გამოეყენებინა, მათ შორის ფოტოკამერით დაეფიქსირებინა საგამოძიებო ღონისძიების მიმდინარეობა.

სააპელაციო სასამართლოს საგამოძიებო კოლეგიამ პირველი ინსტანციის სასამართლოს განჩინებაზე საჩივრის განხილვისას, მოცემულ მუხლებზე დაყრდნობით განმარტა, რომ დათვალიერებისას განხორციელებული ფოტოგადაღება ფაქტებისა და მოვლენების ფიქსაციის საშუალებას იძლევა, რომელიც ჩატარებული

[617] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2018 წლის 2 თებერვლის განჩინება N1გ/133-18. იხ. სამაგისტრო ნაშრომი: *ხიდეშელი თ.,* კომპიუტერული მონაცემის გამოთხოვის პრობლემა სისხლის სამართლის პროცესში.

[618] იქვე, 1-2.

[619] იქვე.

საგამოძიებო მოქმედების ცალკეული ეპიზოდების ან თუნდაც, მთლიანი საგამოძიებო მოქმედების, სურათის აღდგენას, დემონსტრირებას ან თვალსაჩინოდ წარმოდგენას უწყობს ხელს. მოცემულ შემთხვევაში ფოტოგადაღება დათვალიერების პროცესის შემადგენელი ნაწილია და მასში თვალსაჩინოების სახით არის ასახული ის, რაც დათვალიერების ოქმში სიტყვიერი ფორმით არის აღწერილი.[620]

პირველი ინსტანციის სასამართლოს შეფასების გამო, თითქოს, დათვალიერების ოქმზე ფოტოების დართვა ახალ საგამოძიებო მოქმედებას წარმოადგენს, სააპელაციო სასამართლოს დათვალიერების დროს ჩატარებულ ფოტოგადაღებასა და დოკუმენტის ან ინფორმაციის გამოთხოვას შორის არსებულ სხვაობაზეც მოუწია მსჯელობა.

მოსამართლის განმარტებით, სხვაობა არსებობს, როგორც არსით, ისე პროცესუალური თვალსაზრისით. კომპიუტერული მონაცემის გამოთხოვისგან განსხვავებით, დათვალიერების დროს ინფორმაციის ელექტრონული ფორმით მოპოვება (ასლის შექმნა) და საქმეზე დართვა არ ხდება. ამასთან, დათვალიერების დროს გადაღებული ფოტოების შედეგად მიღებულ ინფორმაციას ვერ ექნება უტყუარობის პრეტენზია, ვინაიდან ის არ არის მოპოვებული პირველწყაროდან და მასზე ექსპერტიზის დანიშვნა შეუძლებელია. შესაბამისად, იგი დოკუმენტის ან ინფორმაციის გამოთხოვას ვერც მტკიცებულებითი ძალის და ვერც პროცესუალური კუთხით ვერ შეცვლის.[621]

მართებულია მოსამართლის მსჯელობა არსობრივ და პროცესუალურ სხვაობასთან დაკავშირებით. არსობრივად, დოკუმენტის ან ინფორმაციის გამოთხოვის დროს ორიგინალი მონაცემის ზუსტი ასლის შექმნა და ამოღება ხდება, რომელზეც საჭიროებიშემთხვევაში ექსპერტიზის დანიშვნაც შესაძლებელია. ხოლო დათვალიერების დროს, ორიგინალი დოკუმენტის დათვალიერება და აღწერა ხდება, რაც უფრო მეტად ნაწარმოების შინაარსის გადმოცემას ჰგავს, ვიდრე უშუალოდ ნაწარმოების დედანში გაცნობას (ჩვენს შემთხვევაში კომპიუტერული მონაცემის გამოთხოვა). შესაბამისად, ამ ორ დამოუკიდებელ მოცემულობაში მოპოვებული ინფორმაციის სანდოობაც და მტკიცებულებითი ღირებულებაც განსხვავებულია.

[620] იქვე, 5.
[621] იქვე, 6.

ყოველივეს ურთიერთშეჯერებით ნათელი ხდება, რომ დათვალიერების დროს ფოტო გადაღება, ხოლო სსსკ-ის 136-ე მუხლის საფუძველზე ელექტრონული ინფორმაციის გამოთხოვა სრულიად განსხვავებული და დამოუკიდებელი საგამოძიებო მოქმედებებია, რომელთა ერთმანეთთან გაიგივება შეუსაბამოა.

3.3.4. დოკუმენტის ან ინფორმაციის გამოთხოვისა და ამოღების გამიჯვნის საკითხი

საერთო სასამართლოების პრაქტიკა იცნობს შემთხვევებს, როდესაც მხარეები ელექტრონული ინფორმაციის მოპოვების მიზნით არა თუ სსსკ-ის 136-ე მუხლის, არამედ ამავე კოდექსის 119-120 მუხლების მიხედვით მოქმედებდნენ. მიზეზი, შესაძლოა ნორმის შინაარსობრივი მხარის არასწორი გაგება ან თუნდაც მისი მოქმედების ფარგლების დანაშაულთა კატეგორიით შეზღუდვა ყოფილიყო, რაც მხარეებს აიძულებდათ სხვადასხვა სამართლებრივი გზა გამოენახათ კომპიუტერულ მონაცემზე წვდომისთვის და მის სისხლის სამართლის საქმეზე დამაგრებისთვის.

სისხლის სამართლის საქმეზე, რომელზეც გამოძიება 218-ე მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით მიმდინარეობდა, სასამართლოს წინაშე პროკურორმა შ.პ.ს.-დან საფინანსო-სამეურნეო საქმიანობასთან დაკავშირებული წერილობითი და ელექტრონული ინფორმაციის ამოღება იშუამდგომლა. შუამდგომლობა ნაწილობრივ, წერილობითი დოკუმენტის მოპოვების ნაწილში დაკმაყოფილდა, ხოლო ელექტრონულ ინფორმაციასთან მიმართებით უარი ეთქვა, ვინაიდან მოსამართლის მითითებით მოთხოვნა არა თუ ამოღებას, არამედ ინფორმაციის გამოთხოვის საგამოძიებო მოქმედებას წარმოადგენდა.[622]

სასამართლოს გადაწყვეტილების გასაჩივრებისას, პროკურორმა აღნიშნა, რომ სსსკ-ის 136-ე მუხლით დაცულ სფეროში, კომპიუტერულ სისტემაში ან მონაცემთა შესანახ საშუალებაში არსებული ინფორმაცია ან დოკუმენტი ექცევა, რომელიც მომსახურების მომწოდებელთან, მესამე პირთან ინახება. მისი განმარტებით, კანონმდებელმა განსაკუთრებული დაცვის სფეროდ არა ინფორმაციის ელექტრონული ფორმა, არამედ სუბიექტი გამოყო. სწორედ ამიტომ, მომსახურების მომწოდებელთან არსებული

[622] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2014 წლის 9 დეკემბრის განჩინება N1გ/1245, 2.

ინფორმაციის მოპოვება სსსკ-ის 136-ე მუხლზე დაყრდნობით უნდა მოხდეს, ხოლო მესაკუთრისგან, ამავე კოდექსის 119-ე მუხლის მიხედვით.[623]

რთულია გაიზიარო ბრალდების მხარის მიერ ნორმის ამგვარად განმარტება, ვინაიდან დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება გულისხმობს, როგორც მომსახურების მომწოდებლისგან მომხმარებლის შესახებ ინფორმაციის გამოთხოვას, ისე კომპიუტერული სისტემიდან ან მონაცემთა შემნახველი საშუალებიდან სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის ან დოკუმენტის მოპოვებასაც. შესაბამისად, მისი რეგულირების ფარგლებში ექცევა ელექტრონული ინფორმაციის მოპოვება პროცესორიდან, დისკიდან, ფლეშ-ბარათიდან თუ სხვა ელექტრონული ინფორმაციის მატარებლიდან.[624]

კიდევ ერთ სისხლის სამართლის საქმეში, ბრალდებულის ადვოკატმა პოლიციის დეპარტამენტის მთავარი შესასვლელის მაკონტროლებელი ვიდეოკამერიდან ჩანაწერის ამოღების ნებართვის გაცემა ითხოვა, რომელიც პირველი ინსტანციის სასამართლოს მიერ ასევე არ დაკმაყოფილდა.[625]

სააპელაციო საჩივრის განხილვისას, სასამართლომ ამოღებისა და დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედებებს შორის არსებულ სხვაობაზე იმსჯელა და განმარტა, რომ ძირითადი განსხვავება საგამოძიებო მოქმედების ობიექტის თავისებურებას უკავშირდება. გამოთხოვის დროს ელექტრონული ფორმით არსებული ინფორმაციის მოპოვება ხდება, ხოლო ამოღების მიზანი საქმისათვის მნიშვნელობის მქონე საგნის, დოკუმენტის, ნივთირების ან ინფორმაციის შემცველი სხვა ობიექტის (ისეთი ობიექტის, რომელიც არ არის ელექტრონული სახის) ამოღებაა.[626]

საინტერესოა სისხლის სამართლის საქმე, რომელშიც ბრალდების მხარე გადაუდებელი აუცილებლობის პირობებში ჩატარებული საგამოძიებო მოქმედების, რადიო მაუწყებლის ოფისიდან ორ ელექტრონულ დისკზე გადატანილი ვიდეო ჩანაწერის ამოღების კანონიერად ცნობას ითხოვდა. სასამართლოს მიერ აღნიშნული

[623] იქვე.
[624] იქვე, 4.
[625] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 6 სექტემბრის განჩინება N1გ/1430.
[626] იქვე, 3.

მოთხოვნა არ დაკმაყოფილდა, ხოლო ჩანაწერი დაუშვებელ მტკიცებულებად იქნა ცნობილი.[627]

განჩინების გასაჩივრებისას, ბრალდების მხარემ აღნიშნა, რომ საქმეში არსებობს მოწმის გამოკითხვის ოქმი, სადაც იგი აღნიშნავს, რომ მას ხელთ ჰქონდა კონფლიქტის ამსახველი ვიდეო ჩანაწერი და თანახმა იყო გადაეცა გამოძიებისთვის. ამასთან, მისი ხედვით, გარდა იმისა, რომ ვიდეო ჩანაწერის ამოღება არ განეკუთვნება ფარულ საგამოძიებო მოქმედებას, მოპოვებული ინფორმაცია არც კომპიუტერულ სისტემაში და არც მონაცემთა შესანახ საშუალებაში ყოფილა განთავსებული. ამ არგუმენტზე დაყრდნობით, ჩანაწერის მოპოვება სსსკ-ის 136-ე მუხლის შესაბამისად არ უნდა განხორციელებულიყო.

რასაკვირველია, სააპელაციო სასამართლოს გადაწყვეტილებით ბრალდების მხარის საჩივარი არ დაკმაყოფილდა. მოსამართლემ მართებულად შეაფასა 136-ე მუხლის შინაარსი და განმარტა, რომ თავდაპირველად ჩანაწერი გაკეთდა კომპიუტერული სისტემის მეშვეობით, ხოლო შემდეგ მისი განთავსება მოხდა ინფორმაციის შემნახველ მოწყობილობაში. მათ შორის კომპაქტურ დისკში.[628]

შეჯამებისთვის, მართალია დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება ამოღების სპეციალურ შემთხვევას წარმოადგენს, თუმცა განსხვავებულია მოსაპოვებელი ობიექტი.[629] კერძოდ, დოკუმენტის ან ინფორმაციის გამოთხოვის დროს ხდება ელექტრონული სახით არსებული ინფორმაციის მოპოვება, ხოლო ამოღების დროს ისეთი ობიექტის, რომელიც მართალია არ არის ელექტრონული სახის, თუმცა იგი შესაძლებელია ელექტრონული ინფორმაციის მატარებელი იყოს. მაგალითისთვის, თუ გამოძიების მიზნებისთვის მნიშვნელოვანია შემთხვევის ადგილას ნაპოვნი მობილური ტელეფონი, ვიდეო კამერა ან თუნდაც პერსონალური კომპიუტერი, მიუხედავად იმისა, რომ ეს მოწყობილობები განუსაზღვრელი რაოდენობის ელექტრონული ინფორმაციის მატარებლები არიან, მათი მოპოვება საგამოძიებო მოქმედება - ამოღებისათვის დადგენილი წესის მიხედვით მოხდება.

---

[627] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 4 ოქტომბრის განჩინება N1გ/1537-16.

[628] იქვე, 6.

[629] *ავტორთა კოლექტივი,* საქართველოს სისხლის საპროცესო სამართალი, კერძო ნაწილი, თბილისი, მერიდიანი, 2017, 428.

და მაინც, შედარებული საგამოძიებო მოქმედებების მიზანი და სამართლებრივი საფუძველი იდენტურია. ძირითადი განსხვავება ამოსაღებ ობიექტშია. ერთის მხრივ ობიექტი მატერიალურია, ხოლო მეორეს მხრივ არამატერიალური ნიშან-თვისებების მატარებელი.

3.3.5. კომპიუტერული მონაცემის ნებაყოფლობით გადაცემის შემთხვევები

დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების დანაშაულთა კატეგორიით შეზღუდვის პერიოდში, საერთო სასამართლოების პრაქტიკაში დაფიქსირდა შემთხვევები, როდესაც ბრალდების მხარე სისხლის სამართლის საქმისთვის მნიშვნელოვანი ელექტრონული ინფორმაციის მოპოვებას, მფლობელებისადმი პირდაპირი მიმართვის წარდგენის გზით ცდილობდა.

ერთ-ერთ სისხლის სამართლის საქმეზე პროკურორმა სასამართლოს წინაშე, მოწმის მიერ დაკითხვის დროს ნებაყოფლობით წარმოდგენილი DVD დისკისა და მასზე არსებული ვიდეოჩანაწერის დათვალიერების ნებართვის გაცემა იშუამდგომლა, თუმცა სასამართლოს მხრიდან მოთხოვნა არ დაკმაყოფილდა.[630]

აღნიშნულ განჩინებაზე საჩივრის განხილვისას საგამოძიებო კოლეგიამ განმარტა, რომ ინფორმაცია რომლის დათვალიერების ნებართვასაც პროკურორი ითხოვდა, საპროცესო ნორმების მოთხოვნათა უგულვებელყოფით იქნა მოპოვებული. კერძოდ, გამოძიებამ იგი მოწმის მიერ ნებაყოფლობით წარმოდგენის გზით მოიპოვა, რაც შემდეგ საქმეზე დათვალიერების ოქმით დაამაგრა. „ნებაყოფლობით წარმოდგენის“ საგამოძიებო მოქმედებას კი საქართველოს სისხლის სამართლის საპროცესო კოდექსი არ იცნობს. სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის მოპოვება საპროცესო კოდექსის ნორმების საფუძველზე ხორციელდება. აღნიშნულის გათვალისწინებით კი დისკისა და ვიდეოჩანაწერის დათვალიერების ოქმი დაუშვებელ მტკიცებულებად იქნა მიჩნეული.[631]

ანალოგიურად, სხვა სისხლის სამართლის საქმეზე, მოსამართლემ, წინასასამართლო სხდომაზე, გამომძიებლის მიმართვის საფუძველზე შ.პ.ს-ს მიერ ნებაყოფლობით გადაცემული ვიდეოჩანაწერი და მისი დათვალიერების ოქმი დაუშვებელ

---

[630] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 25 იანვრის განჩინება N1გ/109, 1.

[631] იქვე, 4-5.

მტკიცებულებად ცნო.[632] სასამართლოს მითითებით კომპიუტერულ სისტემაში გამოძიებისთვის საჭირო შენახული ინფორმაციის მოსაპოვებლად სასამართლო ნებართვა და შესაბამისი განჩინების მიღებაა საჭირო. შესაბამისად, დარღვეულია მტკიცებულებათა მოპოვების საპროცესო წესი.

რა თქმა უნდა, ზემოაღნიშნული განჩინება პროკურორის მხრიდან სააპელაციო სასამართლოს საგამოძიებო კოლეგიაში გასაჩივრდა. ბრალდების მხარემ საჩივრის დასაბუთებისას აღნიშნა, რომ წინასასამართლო სხდომის მოსამართლის გადაწყვეტილება უნდა გაუქმდეს, ვინაიდან სსსკ-ის 136-ე მუხლის თანახმად, პროკურორი უფლებამოსილია და არა ვალდებული მიმართოს სასამართლოს განჩინების გაცემის შუამდგომლობით. ამასთან, ორგანიზაციის დირექტორმა არა თუ იძულებით, არამედ ნებაყოფლობით გადასცა ბრალდების მხარეს დანაშაულის შემცველი მასალა.[633] საგამოძიებო კოლეგიამ არ დააკმაყოფილა ბრალდების მხარის მოთხოვნა და განმარტა, რომ მტკიცებულების მოპოვების დროს საპროცესო კანონმდებლობის დაუცველობის გარდა, საქმეში არ მოიპოვება უფლებამოსილი პირის მოქმედების ამსახველი საპროცესო დოკუმენტი. ამრიგად, ყველა მონაცემი მიუთითებს, რომ კომპიუტერული მონაცემის გამოთხოვა გამომძიებლის წერილის საფუძველზე მოხდა, რაც დაუშვებელია.[634]

აგრეთვე, კვლავ დაუშვებელ მტკიცებულებად ცნო მოსამართლემ გამომძიებლის მიმართვის საფუძველზე მოპოვებული სამეთვალყურეო კამერის ჩანაწერი სხვა სისხლის სამართლის საქმეში.[635] ამ შემთხვევაშიც, მოსამართლის განმარტებით, სსსკ-ის 136-ე მუხლის საფუძველზე განჩინების მოპოვების ნაცვლად, ბრალდების მხარემ პირდაპირ მიმართა მფლობელს და ისე მოიპოვა ჩანაწერი, რაც წინააღმდეგობაშია კანონმდებლობის მოთხოვნებთან.

ნებაყოფლობით გადაცემული კომპიუტერული მონაცემის დასაშვებობის საკითხზე მსჯელობისას მოსამართლეთა პოზიცია ერთიანი იყო და შეიძლება ითქვას, შუამდგომლობის განხილვისას გაკეთებული განმარტებები იმ დროისთვის

---

[632] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 30 მარტის განჩინება N1გ/548-16.

[633] იქვე, 4.

[634] იქვე, 7.

[635] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 9 მარტის განჩინება N1გ/337-17.

არსებითად სწორი იყო, თუმცა თუ მხედველობაში მივიღებთ იმ ფაქტს, რომ განხორციელებული საკანონმდებლო ცვლილებით დოკუმენტის ან ინფორმაციის გამოთხოვა საგამოძიებო მოქმედების ჩატარების საერთო წესს დაექვემდებარა, როგორც ბრალდების, ისე დაცვის მხარე, სსსკ-ის 112-ე მუხლის პირველი ნაწილის თანახმად თანამესაკუთრის, თანამფლობელის ან კომუნიკაციის ერთი მხარის თანხმობის საფუძველზე უფლებამოსილნი არიან მათთვის მნიშვნელოვანი კომპიუტერული მონაცემი მოიპოვონ. მართალია, სასამართლო განჩინების გარეშე საგამოძიებო მოქმედების ჩატარებამ შესაძლოა თანხმობის ფარგლების ან ლეგიტიმურობის კუთხით გარკვეული კითხვები წამოჭრას. განსაკუთრებით იმ პირობებში, როდესაც ელექტრონული ინფორმაციის მატარებელი რამდენიმე ადამიანის საერთო სარგებლობაშია ან გამოძიებისთვის საინტერესო ინფორმაცია სერვის პროვაიდერის ზედამხედველობის ქვეშაა. თუმცა, პირადი ცხოვრების ხელშეუხებლობის უფლების სათანადო დაცვის უზრუნველყოფისა და არამიზნობრივი ან საჭიროზე მეტი მოცულობის ინფორმაციის დამუშავების რისკის თავიდან აცილების მიზნით, შესაძლებელია მომსახურების მომწოდებელთათვის განისაზღვროს იმ მონაცემთა სახე (მაგ. მომხმარებლის ძირითადი მონაცემები), რომლის თანხმობის საფუძველზე გადაცემაც დასაშვები იქნება, ხოლო კერძო პირების შემთხვევაში, შემუშავდეს მათგან მიღებული თანხმობის კანონიერების დადგენისთვის საჭირო კრიტერიუმები. ნიშანდობლივია, რომ საკითხის ამგვარად გადაწყვეტით, მხარეებს საშუალება ეძლევათ დროულად და ამასთან, ადამიანის ძირითადი უფლებების დაცვით, იქონიონ წვდომა მათთვის მნიშვნელოვან კომპიუტერულ მონაცემზე, ხოლო ისეთ შემთხვევაში თუ მიმართვის ადრესატი უარს განაცხადებს თანამშრომლობაზე ან აშკარაა, რომ პირს არ გააჩნია თანხმობის გაცემის უფლებამოსილება, დაინტერესებულ მხარეს რჩება საშუალება მისთვის ხელსაყრელი ინფორმაცია სასამართლო ნებართვის საფუძველზე მოიპოვოს.

3.4. 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტი

2022 წლის 24 მაისს საქართველოს პარლამენტის მიერ მიღებულ იქნა საკანონმდებლო ცვლილებათა პაკეტი, რომლითაც შეიძლება ითქვას არსებითად შეიცვალა ელექტრონული ფორმით შენახული კომპიუტერული მონაცემის გამოთხოვის

მარეგულირებელი კანონმდებლობა. [636] ძირითადი ხარვეზი, რომელიც არაერთ პრობლემას ქმნიდა მართლმსაჯულების განხორციელების კუთხით და ხელს უშლიდა გამოძიების ეფექტურობას, აღმოიფხვრა და კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული კომპიუტერული მონაცემის გამოთხოვაზე საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143^2 – 143^{10} მუხლების, კერძოდ კი ფარული საგამოძიებო მოქმედებების განხორციელებისთვის დადგენილი სტანდარტების მიხედვით მოქმედების ვალდებულება მოიხსნა.[637]

გარდამტეხი მნიშვნელობის ცვლილების განხორციელების გარდა, დაიხვეწა და გამოსწორდა რიგი სხვა ნაკლოვანებანი. მიუხედავად იმისა, რომ საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილებით სსსკ-ის 136-ე მუხლის 1-ლი ნაწილის ნორმატიული შინაარსი, რომელიც დაცვის მხარეს უზღუდავდა უფლებას, დამოუკიდებლად მოეპოვებინა კომპიუტერულ სისტემაში შენახული ინფორმაცია, არაკონსტიტუციურად იქნა ცნობილი და მას შემდეგ ელექტრონული ფორმით შენახული ინფორმაციის გამოთხოვაზე ნებართვის გაცემის შუამდგომლობით ბრალდების მხარის მსგავსად მათაც მიეცათ უფლება მიმართონ სასამართლოს, კანონში ტექსტობრივი ცვლილება 2022 წლის 24 მაისამდე არ შესულა. ამას გარდა, ნორმის პირველ ნაწილს დაემატა მითითება, რომ გადაუდებელი აუცილებლობის პირობებში, საგამოძიებო მოქმედების პროკურორის დადგენილების საფუძველზე ჩატარება დასაშვებია.[638]

სიახლეს წარმოადგენს ნორმის 4^1 და 4^2 ნაწილებიც. სსსკ-ის 136-ე მუხლის 4^1 ნაწილი ადგენს, რომ საგამოძიებო მოქმედებაზე ამავე კოდექსის 111-ე (საგამოძიებო მოქმედების ჩატარების ზოგადი წესი), 112-ე (სასამართლოს განჩინებით ჩატარებული საგამოძიებო მოქმედება) და 134-ე მუხლების (ზოგადი დებულებანი საგამოძიებო მოქმედების ოქმის შესახებ) დებულებები ვრცელდება. აღნიშნული, ერთობლიობაში კიდევ ერთხელ უსვამს ხაზს, რომ დოკუმენტის ან ინფორმაციის გამოთხოვა ჩვეულებრივი საგამოძიებო მოქმედებისათვის დადგენილი წესების მიხედვით

[636] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24.05.22.

[637] იქვე.

[638] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09.10.2009, მუხლი 136.

ხორციელდება, თუმცა ნიშანდობლივია ამავე საკანონმდებლო ცვლილებათა პაკეტით 112-ე მუხლში განხორციელებული დამატება, კერძოდ კი შემდეგი შინაარსის 3^1 ნაწილი: *„კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინებაში აგრეთვე აღნიშნული უნდა იყოს ის ფიზიკური ან იურიდიული პირი, რომლისგანაც უნდა იქნეს გამოთხოვილი კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში არსებული ინფორმაცია (თუ მისი ვინაობა ცნობილია); გვარეობითი ნიშნის მიხედვით - ის კომპიუტერული სისტემა ან კომპიუტერულ მონაცემთა შესანახი საშუალება, საიდანაც უნდა იქნეს გამოთხოვილი კომპიუტერული მონაცემი; კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან გამოსათხოვი სავარაუდო დოკუმენტი ან ინფორმაცია; წინააღმდეგობის გაწევისას იძულების პროპორციული ზომის გამოყენების უფლება. კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინება (გარდა სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის გარგლებში გაცემული განჩინებისა) ძალადაკარგულია, თუ ეს საგამოძიებო მოქმედება არ დაწყებულა 30 დღის ვადაში“.*[639] დადებითად უნდა შეფასდეს 136-ე მუხლის საფუძველზე გაცემული განჩინებისთვის დამატებითი მოთხოვნების დაკმაყოფილების ვალდებულება. მათი, სასამართლო ნებართვაში გათვალისწინება ხელს შეუწყობს როგორც განჩინების დეტალიზაციის მოთხოვნას, ისე შეამცირებს პირის პირად ცხოვრებაში უკანონოდ ჩარევის რისკს, თუმცა, სსსკ-136-ე მუხლზე დაყრდნობით ელექტრონული ფორმით შენახული ინფორმაციის გამოთხოვისას, კითხვის ნიშანს ბადებს შესაძლებლობა, რომელიც უფლებამოსილ პირს **„წინააღმდეგობის გაწევისას იძულების პროპორციული ზომის გამოყენების უფლებას“** ანიჭებს, ვინაიდან თავისი არსით „კიბერდანაშაულის შესახებ“ კონვენციის მე-18 მუხლით განსაზღვრული „კომპიუტერული მონაცემის წარმოდგენის ბრძანება“, ხოლო ეროვნული კანონმდებლობით „დოკუმენტის ან ინფორმაციის გამოთხოვა“ განსხვავდება ჩხრეკა-ამოღების იძულებითი საგამოძიებო ღონისძიებისაგან.[640] ამასთან, როგორც წესი, მის ჩატარებაზე უფლებამოსილი პირი

[639] იქვე, მუხლი $12(3^1)$.
[640] Explanatory Report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 29.

სასამართლო ნებართვას წარუდგენს მის ადრესატს, ხოლო ელექტრონული ინფორმაციის მფლობელი, დამოუკიდებლად, სამართალდამცავი უწყების წარმომადგენლის მხრიდან ყოველგვარი ჩარევის ან ზემოქმედების გარეშე, გადასცემს მონაცემებს. ეს არის ერთგვარი წინასწარი საგამოძიებო ღონისძიება, ვიდრე პირის მიმართ გამოყენებული იქნება სხვა, თუნდაც ისეთი იძულებითი ღონისძიება, როგორიცაა კომპიუტერული სისტემის ან მონაცემის ჩხრეკა-ამოღება.[641]

რაც შეეხება, 4^2 ნაწილს, აღნიშნულის 136-ე მუხლში დამატება „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით განსაზღვრული ვალდებულების საფუძველზე განხორციელდა.[642] კერძოდ, ელექტრონული კომუნიკაციის კომპანიები ვალდებულნი არიან დანაშაულის შესაძლო ჩადენის შედეგად დაუფლებული მობილური საკომუნიკაციო აღჭურვილობის აქტივაციის ფაქტი დააფიქსირონ. შესაბამისად, გამომძიებლის წერილობითი ან მობილური საკომუნიკაციო აღჭურვილობის მოძიების ერთიანი სისტემის საშუალებით წარდგენილი მოთხოვნის საფუძველზე პროვაიდერი კომპანია აქტივაციის ფაქტის დაფიქსირების ან საჭიროების შემთხვევაში მისი ფუნქციონირების შეზღუდვის (ბლოკირების) შესახებ დაუყოვნებლივ აცნობებს საგამოძიებო უწყებას. აღნიშნული ინფორმაციის მიღება კი პროკურორს საშუალებას აძლევს ამავე მუხლის 1-ლი ნაწილით დადგენილი წესების დაცვით პროვაიდერი კომპანიისგან სატელეფონო ნომრისა და მისი მფლობელის, მობილური საკომუნიკაციო აღჭურვილობის აქტივაციის დაფიქსირების დროისა და ადგილმდებარეობის შესახებ ინფორმაცია გამოითხოვოს.[643]

ფაქტია, რომ საკანონმდებლო ცვლილების რამდენიმე წლიანი საჭიროების შემდეგ, სსსკ-ის 136-ე მუხლმა ძირეული ცვლილება განიცადა, რის შედეგადაც ელექტრონული ფორმით შენახული ინფორმაციის გამოთხოვაზე ფარული საგამოძიებო მოქმედების განხორციელებისათვის გათვალისწინებული მუხლობრივი შეზღუდვის წესი მოიხსნა და პროცესის მხარეებს ნაკლებად მძიმე კატეგორიის დანაშაულთა გამოძიებისას მათთვის ღირებულ ელექტრონულ მტკიცებულებაზე წვდომის შესაძლებლობა მიეცათ. აშკარაა, რომ აღნიშნულმა ცალსახად დაახლოვა

[641] იქვე, 30.

[642] საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, სსმ, 02/06/2005, 19-ე მუხლის 2^1 ნაწილის „დ“ და „ე“ ქვეპუნქტები.

[643] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09/10/2009. მუხლი 136 (4^2)

ეროვნული კანონმდებლობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, თუმცა საკითხს დეტალურად ქვემოთ განვიხილავთ.

3.4.1. პრივილეგირებული ინფორმაციის დაცვის საკითხი კომპიუტერული მონაცემის გამოთხოვისას

კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედება დასაბუთებული ვარაუდის სტანდარტის არსებობის პირობებში მხარეებს, კომპიუტერული სისტემიდან ან ინფორმაციის შემნახველი საშუალებიდან სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის მოპოვების შესაძლებლობას ანიჭებს. თავის მხრივ ელექტრონული სახით არსებული ინფორმაცია შესაძლოა ნებისმიერ საკითხს უკავშირდებოდეს, მათ შორის ისეთ ურთიერთობას, რომლის საიდუმლოების დაცვის ინტერესი უფრო აღმატებულია, ვიდრე დანაშაულის გახსნისა და დამნაშავის დასჯის საჯარო ინტერესი. მაგალითისთვის, ასეთ ურთიერთობას განეკუთვნება ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაცია, რომლის საიუდუმლოების დაცვა სამართლიანი სასამართლო უფლების ერთ-ერთ ფუნდამენტურ გარანტიას წარმოადგენს.[644] კონფიდენციალურობის დაცვის მოთხოვნა ვრცელდება ნებისმიერი გზით თუ საშუალებით შემდგარ კომუნიკაციაზე, მათ შორის ელექტრონული საშუალებითაც,[645] თუმცა, გამონაკლისია ადვოკატის დანაშაულებრივ საქმიანობასთან დაკავშირებული ინფორმაცია.[646]

გარდა ადვოკატისა და კლიენტის ურთიერთობისა, სისხლის სამართლის საპროცესო კანონმდებლობით გათვალისწინებულია იმ პირთა ჩამონათვალი, რომელთაც მოწმედ დაკითხვისა და საქმისათვის მნიშვნელობის მქონე ინფორმაციის შემცველი საგნის, დოკუმენტის გადაცემის ვალდებულება არ ეკისრებათ.[647] აგრეთვე, სსსკ-ის 143[7]-ე მუხლის თანახმად დაუშვებელია სასულიერო პირის, ადვოკატის, ექიმის,

---

[644] *Khodorkovsky and Lebedev v. Russia,* [2013], ECHR.

[645] *Niemietz v. Germany,* [1992] ECHR, 32-33. *Petri Sallinen and Others v. Finland*, [2005] ECHR, 71. *Wieser and Bicos Beteiligungen GmbH v. Austria*, [2008] ECHR, 66-68.

[646] Versini-Campinchi and Crasnianski v. France, ECHR, 2016.

[647] *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი - ზოგადი ნაწილის მიმოხილვა, თბილისი, იურისტების სახლი, 2014, 250-251. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09/10/2009, მუხლი 50. იხ. *ბერი ვ., შრამი ე.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის რეფორმირებისთვის - შედარებითი და ევროპული მოსაზრებები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, N1, 2019.

ჟურნალისტისა და იმუნიტეტის მქონე პირის მიმართ ფარული საგამოძიებო მოქმედების ჩატარება, თუ ის დაკავშირებულია სასულიერო მოღვაწეობის ან პროფესიული საქმიანობის დროს კანონით დაცული ინფორმაციის მოპოვებასთან. ამასთან, აუცილებლად უნდა გაიმიჯნოს ერთმანეთისგან ადვოკატის პირადი და მასსა და კლიენტს შორის შემდგარი კომუნიკაცია, რის შემდეგაც მის პროფესიულ საქმიანობასთან დაკავშირებული კომუნიკაციის შინაარსი დაუყოვნებლივ უნდა განადგურდეს.

ფაქტია, საპროცესო კანონმდებლობით ადვოკატისა და კლიენტის, სასულიერო პირისა და მრევლის და სხვა პირთა კომუნიკაცია თუ ურთიერთობა დაცულია იძულებითი გამჟღავნებისგან, თუმცა ამგვარი აკრძალვა გათვალისწინებული არ არის დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების განხორციელებისას. აღნიშნულის გათვალისწინება კი თანამედროვე საკომუნიკაციო ტექნოლოგიების განვითარების ფონზე შეიძლება ითქვას აუცილებელია. ყოველდღიურად ადამიანთა შორის კომუნიკაცია ძირითადად ელექტრონული საშუალების გამოყენებით ხორციელდება, ტრადიციული მომსახურება, დისტანციურმა მომსახურებამ ჩაანაცვლა და სხვადასხვა სერვისს, მათ შორის იურიდიულ მომსახურებას, ადამიანები სახლიდან გაუსვლელად იღებენ. ხშირად დისტანციურად დგება კომუნიკაცია ექიმსა და პაციენტს შორის, ხოლო სამედიცინო შემოწმების შედეგები კი პაციენტს ელექტრონული ფოსტით ეგზავნება. ამრიგად, როდესაც მხარე სასამართლოს წინაშე შუამდგომლობს მობილური ტელეფონიდან ან კომპიუტერიდან დროის კონკრეტულ მონაკვეთში მიღებული და გაგზავნილი შეტყობინებების შესახებ ინფორმაციის გამოთხოვას, შესაძლოა დანაშაულთან კავშირში მყოფი დოკუმენტების გარდა, მასში ბრალდებულსა და ადვოკატს, ბრალდებულსა და სასულიერო პირს ან ოჯახის წევრებს შორის განხორციელებული კომუნიკაციაც მოექცეს, რომელთაც კავშირი არ აქვს მიმდინარე სისხლის სამართლის საქმესთან.

შესაბამისად, მიზანშეწონილია საპროცესო კანონმდებლობაში გათვალისწინებული იყოს სპეციალური დებულებები, რომელიც გამორიცხავს ან მინიმუმამდე შეამცირებს „პრივილეგირებულ პირებს“ შორის არსებული კომუნიკაციის შესახებ ინფორმაციის მოპოვებას.

3.4.2. მესამე მხარის თანხმობა კომპიუტერული მონაცემის გამოთხოვისას

დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება მასთან დაკავშირებული უახლესი საკანონმდებლო ცვლილებით, საგამოძიებო მოქმედების ჩატარების საერთო წესს დაექვემდებარა და შეიძლება ითქვას სსსკ-ის 112-ე მუხლის პირველი ნაწილის შინაარსი, რომელიც საგამოძიებო მოქმედების სასამართლო განჩინების გარეშე, თანამესაკუთრის, თანამფლობელის ან კომუნიკაციის ერთი მხარის თანხმობის საფუძველზე ჩატარების შესაძლებლობას გულისხმობს, აქტუალურობას იძენს სსსკ-ის 136-ე მუხლის გამოყენების პროცესში.

ახლა, ამ ეპოქაში, სადაც მობილური ტელეფონები, პერსონალური კომპიუტერები და ზოგადად ურთიერთდაკავშირებული მოწყობილობები ფართოდ არის გავრცელებული და ისინი, ადამიანთა უმრავლესობისთვის პირადი ცხოვრების განუყოფელ ნაწილს წარმოადგენს, მასში არსებულ ინფორმაციაზე საზოგადოების წვდომაც შეზღუდულია.[648] შესაბამისად, მესამე მხარის თახმობის საფუძველზე, სასამართლო განჩინების გარეშე, საგამოძიებო მოქმედების ჩატარებამ შესაძლოა გარკვეული სამართლებრივი საკითხები წამოჭრას თანხმობის ფარგლებსა თუ ლეგიტიმურობის კუთხით. განსაკუთრებით მაშინ, როდესაც კომპიუტერული მოწყობილობა შესაძლოა ერთდროულად ოჯახის სხვადასხვა წევრის საერთო სარგებლობაში იყოს და თითოეულ მათგანთან დაკავშირებულ პირადი სახის ინფორმაციას შეიცავდეს.[649] საყურადღებოა აგრეთვე, მოცემულობა, როდესაც ინდივიდის პირად ცხოვრებასთან დაკავშირებულ მონაცემებს სერვის პროვაიდერი კომპანია ინახავს და საგამოძიებო ორგანოები მათი გადაცემის შუამდგომლობით მიმართავენ.

ნიშანდობლივია, რომ თანხმობის ლეგიტიმურობის დადგენის მხრივ საპროცესო კანონმდებლობა ყურადღებას არა თუ მესამე პირების ქონებასთან პრაქტიკულ კავშირზე, არამედ საკუთრების ელემენტზე ამახვილებს.[650] შესაბამისად, თანხმობის გაცემა პირის მიერ, რომელსაც მართალია საკუთრებაში აქვს მოწყობილობა, თუმცა ყოველდღიურ რეჟიმში, პირადი ინტერესებისთვის მას სხვა ადამიანი მოიხმარს და

---

[648] *ფაფიაშვილი ლ.,* ციფრული მტკიცებულებების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებულში „ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში“ რედ. კორკელია კ., თბილისი, 2014, 163.

[649] იქვე.

[650] იქვე.

მესაკუთრეს არ გააჩნია ზიარი ინტერესი მასში დაცულ ინფორმაციაზე, შეიცავს მოსარგებლე პირის პირადი ცხოვრების უფლების ხელყოფის რისკს, ვინაიდან, კომპიუტერული სისტემიდან მონაცემთა გამოთხოვის დროს დაცვის ობიექტი არა თუ ინდივიდის ქონებებრივი ინტერესი, არამედ პირადი ცხოვრების ხელშეუხებლობის უფლებაა. [651] ამასთან, კითხვის ნიშანს ბადებს აგრეთვე თანხმობის ფარგლების განსაზღვრის საკითხი. კერძოდ, კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედებისთვის მნიშვნელოვანია, რომ დაინტერესებულმა პირმა ზუსტად იცოდეს ინახება თუ არა კომპიუტერულ სისტემაში მისთვის საინტერესო ელექტრონული ინფორმაცია. შესაბამისად, პირს, რომელსაც კავშირი არ აქვს მასში არსებულ მონაცემებთან, შეუძლებელია ზუსტი ინფორმაცია მიაწოდეს მხარეს მათი არსებობის შესახებ, რომ აღარაფერი ვთქვათ მონაცემზე წვდომის უფლების ფარგლების განსაზღვრასა და მათი გადაცემის მოცულობაზე.

აგრეთვე საინტერესოა მოცემულობა, როდესაც რამდენიმე პირს ერთდროულად აქვს წვდომა ან კონტროლი კომპიუტერულ ტექნიკაზე, იზიარებენ პაროლებს, ელექტრონულ ფოსტას და სხვა. ცხადია, ასეთ ვითარებაში მათ საერთო უფლებამოსილება გააჩნიათ მოწყობილობაზე. შესაბამისად, ივარაუდება, რომ თანამფლობელიდან ერთ-ერთის თანხმობა საკმარისია საგამოძიებო მოქმედების ჩასატარებლად.[652] განსხვავებული ვითარება იარსებებს, როდესაც მართალია პირები იზიარებენ კომპიუტერულ მოწყობილობას, თუმცა საკუთარი პერსონალური ინფორმაცია ან ანგარიში გამოყოფილი აქვთ პაროლით ან დაშიფვრის სხვა მეთოდით. ასეთი დოკუმენტების მიმართ ივარაუდება, რომ პირადი ცხოვრების დაცვის გონივრული მოლოდინი მაღალია. შესაბამისად, მესამე მხარის თანხმობა ვერ ჩაითვლება ვალიდურად.[653]

ასევე, არანაკლებ მნიშვნელოვანი ფაქტორია, როდესაც ელექტრონული სახის ინფორმაცია სერვის პროვაიდერების ხელშია და საგამოძიებო ორგანო მათ გადაცემის მოთხოვნით მიმართავს. მათ მონაცემთა კონფიდენციალურობის დაცვის ვალდებულება ცალსახად აკისრიათ და ეს ვალდებულება შინაარსობრივი მონაცემების შემთხვევაში კიდევ უფრო მაღალია. შესაბამისად, ჩნდება კითხვა.

---

[651] იქვე.

[652] *United States v. Matlock,* 415 U.S. 164 (1974). იხ. *Georgia v. Randolph*, 547 U.S. 103 (2006).

[653] *United States v. Kimoana,* 383, F.3d 1215 (10th Circuit 2004).

მიზანშეწონილია თუ არა პროვაიდერი კომპანიის თანხმობის საფუძველზე მომხმარებელთან დაკავშირებული მონაცემების გამოთხოვა და თუ კი რა მოცულობით. შესაძლოა, პროვაიდერი კომპანიების თანხმობის საფუძველზე მომხმარებლის ძირითადი მონაცემების, კერძოდ, სახელი, გვარის, საფოსტო ან საცხოვრებელი მისამართის, საკონტაქტო მონაცემების შესახებ ინფორმაციის გადაცემა მართებულად ჩაითვალოს, თუმცა, იგივეს ვერ ვიტყვით მომხმარებელთან დაკავშირებული ტრაფიკისა თუ შინაარსობრივი ხასიათის მონაცემების გამჟღავნებაზე, ვინაიდან აღნიშნული, დასაბუთებული შუამდგომლობის არსებობის და ჯეროვანი სასამართლო კონტროლის განხორციელების გარეშე ინდივიდის პირად ცხოვრებაში თვითნებურად, მაღალი ინტენსივობით ჩარევის რისკს ზრდის. [654] ამრიგად, პირადი ცხოვრების დაცვის გონივრული მოლოდინიდან გამომდინარე და უფლებაში თვითნებური ჩარევისგან დაცვის მიზნით, სასამართლო ნებართვის მოპოვება აუცილებელია.[655]

ფაქტია, დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედებაზე სსსკ-ის 112-ე მუხლის დებულებების გავრცელებით, ელექტრონული სახით შენახული ინფორმაციის გამოთხოვა მხარეთათვის, სასამართლო განჩინების გარეშე, თანხმობის საფუძველზე ხელმისაწვდომი გახდა. თუმცა, პირადი ცხოვრების ხელშეუხებლობის უფლების სათანადოდ დაცვის მიზნით აუცილებელია, მომსახურების მომწოდებელთათვის, საკანონმდებლო დონეზე განისაზღვროს ინფორმაციის სახე, რომლის თანხმობის საფუძველზე გამჟღავნების უფლებამოსილებაც ექნებათ. ამასთან, უფლებაში თანაზომიერი ჩარევის უზრუნველყოფის მიზნით, მნიშვნელოვანია, სსსკ-ით გათვალისწინებულ იქნას მესამე პირების მიერ გაცემული თანხმობის კანონიერების დადგენის კრიტერიუმები.

3.5. მოქმედი კანონმდებლობის შესაბამისობა კონვენციის მოთხოვნებთან

ნორმის მოქმედი რედაქციის კონვენციის მოთხოვნებთან შესაბამისობის საკითხი აუცილებლად კანონში განხორციელებულ ცვლილებამდე არსებულ მოწესრიგებასა და მასთან არსებულ ხარვეზებთან თანხვედრაში უნდა შეფასდეს. სსსკ-ის 136-ე

[654] *Goldfoot J.,* Compelling Online Providers to Produce Evidence under ECPA, Obtaining and Admitting Electronic Evidence, The United States Attorneys' Bulletin, Vol. 59, №6, 2011, 37.
[655] *Carpenter v. United States*, 585 U.S. (2018).

მუხლში განხორციელებული ცვლილების მიუხედავად, დოკუმენტის ან ინფორმაციის გამოთხოვის, როგორც ელექტრონული ფორმით შენახული ინფორმაციის მოპოვების საგამოძიებო ღონისძიების არსი უცვლელი დარჩა, თუმცა შეიცვალა მისი შესრულების ფორმა. შესაბამისად, საკითხზე მსჯელობისას მნიშვნელოვანია იმის შეფასება თუ განხორციელებული ცვლილებით რამდენად აღმოიფხვრა მანამდე არსებული ნაკლოვანებანი, რომლებიც „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან ეროვნული კანონმდებლობის შეუსაბამობით იყო გამოწვეული.

ძირითადი ხარვეზი საგამოძიებო ღონისძიების მოქმედების ფარგლებს უკავშირდებოდა. მაშინ როდესაც კონვენციის მე-14 მუხლის მე-2 ნაწილი იმგვარად არის ფორმულირებული, რომ შენახული კომპიუტერული მონაცემის გამოთხოვა ნებისმიერი დანაშაულის გამოძიების დროს იყოს ხელმისაწვდომი და მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვის იმპერატიულ მოთხოვნას მხოლოდ ფარულ საგამოძიებო მოქმედებასთან, კერძოდ კი ელექტრონული კომუნიკაციის შინაარსობრივი მონაცემების მიმდინარე რეჟიმში მოპოვების ნაწილში ვხვდებით, ეროვნული კანონმდებლობით მსგავსი შეზღუდვა 136-ე მუხლზეც ვრცელდებოდა.

მოქმედი რედაქციით კი მოცემული პრობლემა აღმოიფხვრა და მხარეებს, ნებისმიერი კატეგორიის დანაშაულზე მიმდინარე გამოძიების პროცესში, დასაბუთებული ვარაუდის სტანდარტის დაკმაყოფილების შემთხვევაში, ელექტრონული ფორმით შენახული ინფორმაციის მოპოვება შეუძლიათ. შესაბამისად, სსსკ-ის 136-ე მუხლის 1-ლი ნაწილი სრულ თანხვედრაში მოვიდა კონვენციის მოთხოვნებთან.[656]

მოქმედების ფარგლების კუთხით, შეუსაბამობას წარმოადგენდა ასევე სსსკ-ის 136-ე მუხლის მეორე ნაწილში არსებული ჩანაწერი „პირი დანაშაულებრივ ქმედებას კომპიუტერული სისტემის გამოყენებით ახორციელებს“. მიუხედავად იმისა, რომ აღმოსავლეთ პარტნიორობის ფარგლებში მომზადებულ სადისკუსიო ნაშრომში საქართველოს მიმართ გაცემულ იქნა რეკომენდაცია ნორმის მოქმედების არეალის

[656] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 58-60. იხ. Criminal Procedure Code of Austria, 30.12.1975, Article 76a, 90(7); Telecommunications Act 2003, 19.08.2003, Article 92(3).

გასაფართოებლად,[657] გასული დროის მიუხედავად, ნორმის ამ ნაწილს ცვლილება არ განუცდია.

არაერთხელ აღინიშნა, რომ საგამოძიებო ღონისძიების განხორციელებისას მნიშვნელოვანია მინიმუმამდე იქნას შემცირებული უფლებაში თვითნებურად ჩარევის რისკი. ასეთ დროს გადამწყვეტ როლს პროცედურული გარანტიები თამაშობს. დოკუმენტის ან ინფორმაციის გამოთხოვისთვის ფორმალური და მატერიალური წინაპირობების დაკმაყოფილების აუცილებლობა, [658] სისხლის სამართლის საქმეზე ოფიციალური გამოძიების წარმოება, სასამართლოს წინაშე მოტივირებული შუამდგომლობის დაყენება და დასაბუთებული ვარაუდის სტანდარტით ხელმძღვანელობა, [659] Ex ante და Ex post (ბრალდების მხარის შემთხვევაში) სასამართლო კონტროლი [660] და საგამოძიებო ღონისძიებაზე პერსონალურ მონაცემთა დაცვის სამსახურის მიერ ზედამხედველობის განხორციელება, სრულებით უზრუნველყოფენ საერთაშორისო სამართლის მოთხოვნების დაკმაყოფილებას. მეტიც, საკანონმდებლო ცვლილებათა პაკეტით, სსსკ-ის 112-ე მუხლში განხორციელებული მე-3[1] ნაწილის დამატებით, რომელიც კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინებისთვის დამატებით მოთხოვნებს ითვალისწინებს, ელექტრონული ინფორმაციის მოპოვების პროცესში კიდევ უფრო განმტკიცდა პირადი ცხოვრების დაცვის საკითხი. თუმცა, როგორც წინა თავებში ვახსენეთ, ასევე, მიზანშეწონილია პრივილეგირებულ კომუნიკაციასთან დაკავშირებული დებულებების გათვალისწინება, რომლებიც გამორიცხავს ან მინიმუმამდე შეამცირებს მასთან დაკავშირებული ინფორმაციის მოპოვებას. ხოლო

---

[657] *Dragicevic D., Juric M.,* Article 15 – Safeguards in the Eastern Partnership Region" Prepared under the Cybercrime EAP, Council of Europe, 2013, 44. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [14.06.23].

[658] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის განჩინება №1გ/363-20, 3.

[659] *Dragicevic D., Juric M.,* "Article 15 – Safeguards in the Eastern Partnership Region" Prepared under the Cybercrime EAP, Council of Europe, 2013, 38, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [14.06.23].

[660] 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> [14.06.23].

საგამოძიებო მოქმედების სასამართლო განჩინების, მხარეთა თანხმობის საფუძველზე ჩატარების შემთხვევაში, თანაზომიერების პრინციპის დაცვას, რაც შესაძლოა უზრუნველყოფილ იყოს, როგორც თანხმობის კანონიერების დადგენის კრიტერიუმების, ისე პროვაიდერი კომპანიებისთვის თანხმობის საფუძველზე გასაცემი მონაცემთა სახეების განსაზღვრით.

ინფორმაციათა შეჯერებით, ცხადია, რომ სსსკ-ის 136-ე მუხლის მოქმედი რედაქცია, ამავე მუხლის მე-2 ნაწილის გარდა, აკმაყოფილებს კონვენციით გათვალისწინებულ მოთხოვნებს. საკითხის ამგვარად მოწესრიგებით, საგამოძიებო ორგანოებს და არამარტო მათ, ბლანკეტურად აღარ ერთმევათ მტკიცებულების მოპოვების შესაძლებლობა. აღნიშნული კი ამავდროულად ხელს შეუწყობს საგამოძიებო მოქმედებასთან დაკავშირებული არაერთგვაროვანი სასამართლო პრაქტიკის აღმოფხვრას და მხარეთათვის ერთიანი სტანდარტის მოქმედებას. სასამართლოს წინაშე წარდგენილი შუამდგომლობის გადაწყვეტა, რაციონალურად, სსსკ-ის 112-ე მუხლის მოთხოვნების დაცვით მოხდება.[661]

3.6. სასამართლოს ტენტენცია დაცვის მხარის შუამდგომლობის საფუძველზე მოპოვებული სასამართლო განჩინების შესრულების საკითხთან დაკავშირებით

საქართველოს პარლამენტის მიერ 2022 წლის 24 მაისს მიღებული საკანონმდებლო ცვლილებათა პაკეტით არსებითად შეიცვალა კომპიუტერული მონაცემის გამოთხოვის წესი [662] და შეიძლება ითქვას, ახალი სასამართლო პრაქტიკის ჩამოყალიბებას ჩაეყარა საფუძველი.

ყურადსაღებია, რომ დაცვის მხარის მიერ სსსკ-ის 136-ე მუხლის პირველი ნაწილის მოთხოვნებით დაყენებული დასაბუთებული შუამდგომლობის დაკმაყოფილების შემთხვევაში, სასამართლოს განჩინების შესრულებისა და საგამოძიებო მოქმედების ჩატარების ვალდებულება შუამდგომლობის ავტორის ნაცვლად, გამომძიებელს ეკისრება. ასე მაგალითად, საქმეში, სადაც დაცვის მხარე, ბრალდებულის პირადი ჩხრეკისას ამოღებული ტელეფონიდან, კერძოდ კი მასში არსებული „messenger" –ის

---

[661] განმარტებითი ბარათი საქართველოს კანონის პროექტზე საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ, 5-6 <https://info.parliament.ge/file/1/BillReviewContent/297941> [15.06.23].

[662] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24.05.22.

აპლიკაციიდან, კონკრეტულ პიროვნებასთან დროის გარკვეულ მონაკვეთში განხორციელებული მიმოწერის შესახებ ინფორმაციის გამოთხოვას ითხოვდა, სასამართლომ მოთხოვნის დაკმაყოფილების შემდეგ განჩინებაში მიუთითა, რომ საგამოძიებო მოქმედება საქართველოს შსს სენაკის რაიონული სამმართველოს ხელმძღვანელი პირის მიერ შერჩეულ გამომძიებელს უნდა ჩაეტარებინა.[663]

ანალოგიურად, თბილისის საქალაქო სასამართლოს საგამოძიებო და წინასასამართლო სხდომის კოლეგიის მიერ მიღებული განჩინების შესრულება, რომლითაც დაცვის მხარის მოთხოვნა მობილური ტელეფონიდან ფოტოსურათისა და ერთ-ერთი აპლიკაციით განხორციელებული მიმოწერის შესახებ ინფორმაციის გამოთხოვაზე დაკმაყოფილდა, საქართველოს შსს ქ. თბილისის პოლიციის დეპარტამენტის ერთ-ერთი სამმართველოს გამომძიებელს დაევალა.[664] მიუხედავად იმისა, რომ დაცვის მხარის შუამდგომლობა დაკმაყოფილდა, ბრალდებულის ინტერესების დამცველმა, ადვოკატმა გაასაჩივრა განჩინება და მოთხოვნილი საგამოძიებო მოქმედების ჩატარების შუამდგომლობის ავტორისთვის დაკისრება ითხოვა.[665] მოთხოვნის მიუხედავად სასამართლომ არ დააკმაყოფილა საჩივარი და განმარტა, რომ კომპიუტერული მონაცემის გამოთხოვა მიეკუთვნება ისეთ საგამოძიებო მოქმედებათა რიგს, რომელსაც ბრალდებული ან მისი ადვოკატი დამოუკიდებლად ვერ ჩაატარებს. შესაბამისად, ისინი უფლებამოსილნი არიან განჩინების გამოტანის შუამდგომლობით მიმართონ მოსამართლეს.[666] ხოლო სსსკ-ის 111-ე მუხლის პირველი ნაწილის თანახმად *დაცვის მხარის დასაბუთებული შუამდგომლობით, სასამართლოს განჩინების საფუძველზე საგამოძიებო მოქმედებას ჩაატარებს გამომძიებელი, რომელიც მოცემულ საქმეზე გამოძიებას არ აწარმოებს. გამომძიებელს შეარჩევს საგამოძიებო ორგანოს ხელმძღვანელი და მის ვინაობას და საკონტაქტო მონაცემებს დაცვის მხარეს საგამოძიებო მოქმედების ჩატარებამდე შეატყობინებენ. ამასთან, დაცვის მხარეს მიეცემა უფლება მონაწილეობა მიიღოს თავისი მოთხოვნით ჩატარებულ საგამოძიებო მოქმედებაში.* საკუთარი პოზიციის

[663] ქუთაისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლი 16 სექტემბრის განჩინება N1/გ-858-22, 19.

[664] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 26 ოქტომბრის განჩინება N1გ/1636-22, 1.

[665] იქვე, 2.

[666] იქვე, 6.

დასაბუთებისთვის სასამართლომ ყურადღება გაამახვილა ასევე სსსკ-ის 112-ე მუხლის 3^1 ნაწილზე, რაც კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის პროცესში „წინააღმდეგობის გაწევისას იძულების პროპორციული ზომის გამოყენების უფლებას“, ითვალისწინებს.

კვლავ იდენტური პოზიცია ეკავა სასამართლოს დაცვის მხარის ერთ-ერთი საჩივრის განხილვისას, რომელიც კომპიუტერული სისტემიდან ან მონაცემთა შესანახი საშუალებიდან ინფორმაციის გამოთხოვის გამომძიებლისთვის დავალების არამართებულობას უკავშირდებოდა.[667] თუმცა, განსხვავებული აღმოჩნდა თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის ერთ-ერთი მოსამართლის ხედვა, როდესაც ბრალდებულის ინტერესების დამცველის მოთხოვნა დააკმაყოფილა და შემავალი და გამავალი ზარების, გაგზავნილი და მიღებული მოკლე ტექსტური შეტყობინებების, ასევე, მომსახურე ანძების შესახებ დეტალური ინფორმაციის გამოთხოვა თავად ბრალდებულის ინტერესების დამცველ ადვოკატს დაავალა.[668] სასამართლომ გაიზიარა დაცვის მხარის პოზიცია, რომ ეს არ არის ჩხრეკა ან ამოღება, რომელსაც ადვოკატი დამოუკიდებლად ვერ ჩაატარებს. შესაბამისად, სსსკ-ის 111-ე მუხლის საფუძველზე მიზანშეუწონლად მიიჩნია განჩინების შესრულების საგამოძიებო ორგანოსთვის დავალება.[669]

საინტერესოა თუ რატომ მიიჩნია სასამართლომ დაცვის მხარე ისეთ სუბიექტად, რომელსაც სსსკ-ის 136-ე მუხლით გათვალისწინებული საგამოძიებო მოქმედების დამოუკიდებლად ჩატარება არ შეუძლია. კითხვას ბადებს ასევე დოკუმენტის ან ინფორმაციის გამოთხოვის დროს წინააღმდეგობის გაწევისას პროპორციული ძალის გამოყენების საკითხიც.

მართალია, შესაძლებელია არსებობდეს შემთხვევები, როდესაც დაცვის მხარემ დამოუკიდებლად ვერ შეძლოს საგამოძიებო მოქმედების ჩატარება. ამის მაგალითი შეიძლება იყოს მოცემულობა, როდესაც კომპიუტერული სისტემიდან ან მონაცემთა შესანახი საშუალებიდან ინფორმაციის გამოთხოვას გარკვეული უნარ-ჩვევები ან

---

[667] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 6 სექტემბრის განჩინება N1გ/1385-22.

[668] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 25 მაისის განჩინება N1გ/800-22.

[669] იქვე, 2-5.

სპეციალური ცოდნა სჭირდება. თუმცა უნდა ითქვას, რომ ასეთი საჭიროების არსებობის შემთხვევაში პრობლემას გამომძიებელთანაც წავაწყდებით. საყურადღებოა, რომ ასეთი შემთხვევების პარალელურად არსებობს მოცემულობა, როდესაც დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება არ მოითხოვს ბრალდების ან დაცვის მხარის განსაკუთრებულ უნარ-ჩვევებს. კერძოდ, როდესაც დაინტერესებული პირისთვის მნიშვნელოვანია მობილურ ნომერზე შემავალი და გამავალი ზარების, შეტყობინებების შესახებ ინფორმაცია და მისი მოპოვება მომსახურების მომწოდებლის მეშვეობით ხდება. შესაბამისად, თითოეული შემთხვევა დამოუკიდებელ შეფასებს საჭიროებს და სასამართლოს მიდგომა თითქოს დაცვის მხარეს ცალსახად არ ძალუძს დამოაუკიდებლად დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების ჩატარება, არაგონივრულია.

წინააღმდეგობის გაწევისას პროპორციული ძალის გამოყენების უფლებას რომ შევეხოთ, ყურადსაღებია როგორც მისი პრაქტიკაში რეალიზების, ისე საჭიროების საკითხი. წარმოვიდგინოთ ვითარება, როდესაც გამოძიებისთვის მნიშვნელოვანია მომსახურების მომწოდებელთან შენახული მომხმარებლის კომუნიკაციის მაიდენტიფიცირებელი მონაცემები, გამომძიებელი წარუდგენს პროვაიდერ კომპანიას სასამართლოს განჩინებას, თუმცა იგი უარს აცხადებს მონაცემთა გამჟღავნებაზე. საინტერესოა ასეთ დროს როგორ უნდა იმოქმედოს გამომძიებელმა ან რა მეთოდებს უნდა მიმართოს ინფორმაციის მოსაპოვებლად. ამ კითხვებზე პასუხი კიდევ უფრო აქტუალური ხდება, როდესაც პროვაიდერის ხელთ არსებული ინფორმაციიდან გამოძიებისთვის საინტერესო და განჩინებით გათვალისწინებული კონკრეტული ინფორმაციის მოძიებას, დამუშავებას, გამოცალკევებას და გადასაცემად ვარგისი ფორმით მომზადებას რამდენიმე საათია ან თუნდაც დღე სჭირდება.

პროპორციული ძალის გამოყენების უფლება შესაძლოა ქმედითი იყოს როდესაც კომპიუტერული მონაცემი კერძო პირის მფლობელობაშია და სასამართლო განჩინების არსებობის მიუხედავად უარს აცხადებს ინფორმაციის გადაცემაზე. თუმცა, ამ შემთხვევაშიც რამდენიმე საკითხი რჩება პასუხგაუცემელი. მაგალითისთვის, წინააღმდეგობის გაწევისას, როდესაც კომპიუტერულ სისტემაში სხვადასხვა პირთან დაკავშირებული დიდი მოცულობის ინფორმაციაა

განთავსებული, როგორ და ვის მიერ უნდა მოხდეს განჩინებაში დაფიქსირებული მონაცემების მოძიება და გამოცალკევება ისე რომ არ დაირღვეს სხვა პირთა ძირითადი უფლებები და თავისუფლებები. შესაბამისად, პერსონალურ მონაცემთა და პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის მიზნით ქმედით და ეფექტურ მექანიზმად სასამართლო გადაწყვეტილების შეუსრულებლობის ან მისი შესრულების ხელის შეშლისთვის პასუხისმგებლობის დაკისრება მიმაჩნია. აღნიშნული ბერკეტი უზრუნველყოფს როგორც კერძო პირებისგან, ისე მომსახურების მომწოდებლებისგან ბრალდების თუ დაცვის მხარისთვის მნიშვნელოვანი ელექტრონული ინფორმაციის დროულ და შეუფერხებელ გადაცემას.

შეჯამების სახით შეიძლება ითქვას, რომ სასამართლოს მიერ განვითარებული პრაქტიკა დაცვის მხარის შუამდგომლობის საფუძველზე მოპოვებული განჩინების გამომძიებლის მიერ შესრულების ნაწილში, არამართებულია. განსაკუთრებით ისეთ პირობებში, როდესაც შუამდგომლობის ავტორს ამგვარი მოთხოვნა არ დაუყენებია და არც სასამართლოს უმსჯელია მისი საჭიროების შესახებ. ამასთან, სასამართლო განჩინების შესრულების ვადა 30 დღეს წარმოადგენს, რაც დაცვის მხარეს დამოკიდებულს ხდის ბრალდების მხარეზე. ეს კი შესაძლოა უარყოფითად აისახოს დაცვის უფლების განხორციელებაზე. გადაფასებას საჭიროებს აგრეთვე წინააღმდეგობის გაწევისას პროპორციული ძალის გამოყენების საკითხი, გარდა იმისა, რომ რიგ შემთხვევებში მისი გამოყენება შესაძლოა არ იყოს ქმედითი, საფრთხეს უქმნის სხვა პირთა პირადი ცხოვრების ხელშეუხებლობის უფლებას.

3.7. შეჯამება

საქართველოს სისხლის სამართლის საპროცესო კოდექსში 2014 წლის 1 აგვისტოს განხორციელებული ცვლილებით კომპიუტერული მონაცემის გამოთხოვა ფარულ საგამოძიებო მოქმედებათა განხორციელებისათვის დადგენილ წესებს დაექვემდებარა და მისი ჩატარების წინაპირობად განსაზღვრული დანაშაულის შემადგენლობათა ჩამონათვალი, წლების განმავლობაში, კერძოდ კი 2022 წლის 24 მაისის საკანონმდებლო ცვლილებების განხორციელებამდე, როგორც ბრალდების, ისე დაცვის მხარეს, მთელ რიგ ნაკლებად მძიმე კატეგორიის დანაშაულთა საქმეებზე კომპიუტერული მონაცემის გამოთხოვის შესაძლებლობას ართმევდა.

გარდა იმისა, რომ საკითხის ამგვარი მოწესრიგება წინააღმდეგობაში მოდიოდა „კიბერდანაშაულის შესახებ“ კონვენციის მე-14 მუხლის მოთხოვნებთან, [670] მან, განსხვავებულ და არაერთგვაროვან სასამართლო პრაქტიკასაც დაუდო საფუძველი. საერთო სასამართლოების პრაქტიკის კვლევის შედეგად გამოიკვეთა თუ რამდენად მნიშვნელოვან დაბრკოლებას წარმოადგენდა საკანონმდებლო ხარვეზი და რა უარყოფითი ზეგავლენა ჰქონდა ნორმის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვას მართლმსაჯულების განხორციელების პროცესზე.

საერთო სასამართლოების პრაქტიკა იცნობს შემთხვევებს, როდესაც მხარეები, ნორმის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვის გამო იძულებულნი იყვნენ ელექტრონული ინფორმაციის მოპოვების მიზნით სხვადასხვა სამართლებრივი გზა მოენახათ და დათვალიერების საგამოძიებო მოქმედებასთან ერთად, სსსკ-ის 119-120-ე მუხლებს მიმართავდნენ, რაც საბოლოო ჯამში მტკიცებულების დაუშვებლად ცნობას იწვევდა.

ზემოაღნიშნულის გარდა, მხარეებს, ელექტრონული ინფორმაციის მოპოვება და სისხლის სამართლის საქმეზე დამაგრება სსსკ-ის 136-ე მუხლის ნაცვლად, საგამოძიებო მოქმედების „დათვალიერების“ ჩატარების გზით უწევდათ.

რა თქმა უნდა, დათვალიერების საგამოძიებო მოქმედება ვერ გაუტოლდებოდა კომპიუტერული მონაცემის გამოთხოვის საგამოძიებო მოქმედებას და ვერც ელექტრონული ინფორმაციის დათვალიერების ოქმს ექნებოდა ისეთივე მტკიცებულებითი ღირებულება, როგორც უშუალოდ ინფორმაციის დედანს ან ზუსტ ასლს, რომელზეც საჭიროების შემთხვევაში ექსპერტიზის ჩატარებაც იქნებოდა შესაძლებელი. ამასთან, პერსონალურ მონაცემთა დაცვის ლეგიტიმური მიზანი, რომელსაც საერთო სასამართლოები ნაკლებად მძიმე კატეგორიის დანაშაულებზე კომპიუტერული მონაცემის გამოთხოვის შუამდგომლობის დაკმაყოფილებაზე უარის თქმის დასაბუთებისთვის ხშირად იყენებდნენ, კომპიუტერული მონაცემის დათვალიერების გზით მოპოვების დროს, მიუღწეველი რჩებოდა, ვინაიდან დათვალიერების დროს პერსონალური მონაცემების გაცნობა და დამუშავება იდენტური მოცულობით ხდებოდა.

[670] Convention on Cybercrime, Budapest, European Treaty Series, 23.11.2001, Article 14.

ცხადია, რომ სსსკ-ის 136-ე მუხლის მოქმედების ფარგლების შეზღუდვა მრავალ ბარიერს ქმნიდა გამოძიებისა და მართლმსაჯულების განხორციელების პროცესში.

ამასთან, გამოიკვეთა, რომ დოკუმენტის ან ინფორმაციის გამოთხოვა თავისი ბუნებით არ განეკუთვნება ფარულ საგამოძიებო მოქმედებას. ფარული საგამოძიებო მოქმედებისათვის დამახასიათებელია გარკვეული დროის განმავლობაში, უწყვეტად და ფარულად ადრესატის ქმედების დაკვირვება,[671] მაშინ როდესაც კომპიუტერული მონაცემის გამოთხოვის დროს ინფორმაციაზე წვდომა ხდება ერთჯერადად, როდესაც, ელექტრონული მონაცემის შექმნა, დამუშავება, გადაცემა და მასთან დაკავშირებული მოქმედებები უკვე დასრულებულია და დაინტერესებული მხარისთვის წინასწარ არის ცნობილი მოსაპოვებელი ინფორმაციის სახე და მოცულობა.

საბედნიეროდ, სსსკ-ის 136-ე მუხლთან დაკავშირებული ძირითადი ხარვეზი და მასთან დაკავშირებული პრობლემები, 2022 წლის 24 მაისს მიღებულმა საკანონმდებლო ცვლილებებმა მოხსნა, თუმცა საფუძველი დაუდო ახალ საკითხს, რაც დაცვის მხარის შუამდგომლობის საფუძველზე მიღებული სასამართლო განჩინების შესრულების ვალდებულების გამომძიებლისთვის დაკისრებას გულისხმობს. გადაჭრით შეიძლება ითქვას, რომ აღნიშნული მიდგომა ძირითად შემთხვევაში მიზანშეუწონელია და სასამართლოს მიერ განმარტების გაკეთებას და ერთიანი სტანდარტის ჩამოყალიბებას საჭიროებს.

დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედებასთან დაკავშირებული საკანონმდებლო ცვლილებებისა და საერთო სასამართლოების რამდენიმე წლიანი პრაქტიკის კვლევამ გვაჩვენა თუ რაოდენ მნიშვნელოვანია როგორც გამოძიებისთვის, ისე ობიექტური მართლმსაჯულების განხორციელებისთვის გამართული საკანონმდებლო ბაზის არსებობა. მნიშვნელოვანია, მომავალში გამოირიცხოს კომპიუტერული მონაცემის გამოთხოვის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვის საკითხი. მართალია ელექტრონული სახით არსებულ მონაცემებზე წვდომისას ყოველთვის არსებობს სხვისი პერსონალური მონაცემების არამიზნოვრივად ან თვითნებურად დამუშავების

[671] *კვეკვეცია ქ.,* საბანკო ანგარიშის მონიტორინგი, როგორც საგამოძიებო მოქმედება - კანონმდებლობა და პრაქტიკა, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021, 316-317.

რისკი, თუმცა აღნიშნული არა თუ ამგვარი შეზღუდვით, არამედ კანონმდებლობაში სათანადო მატერიალური და პროცესუალური წინაპირობების გათვალისწინებით უნდა დაბალანსდეს. მიზანშეწონილია, პროფესიული საიდუმლოების ან სხვაგვარად დაცული ინფორმაციის გამჟღავნებისგან დაცვის მიზნით ეროვნულ კანონმდებლობაში ზოგადი დებულებების პარალელურად ქმედითი მექანიზმები გაჩნდეს, რომლებიც სსსკ-ის 136-ე მუხლის საფუძველზე მოპოვებული პრივილეგირებული მონაცემების გამოძიებისა და სისხლის სამართლის საქმისთვის რელევანტური ინფორმაციისგან გამოცალკევებას და განადგურებას უზრუნველყოფს.

თავი VII. რეკომენდაციები კომპიუტერული მონაცემების გამოთხოვის საკანონმდებლო ბაზის სრულყოფისათვის

1. რეკომენდაციების მნიშვნელობა

დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება ეფექტური საშუალებაა ელექტრონული ფორმით შენახული ინფორმაციის გამოძიების მიზნებისთვის მოსაპოვებლად. „კიბერდანაშაულის შესახებ“ კონვენციის შესაბამისად, ეროვნული კანონმდებლობით, იგი დამოუკიდებელი საგამოძიებო მოქმედების სახით არის გათვალისწინებული და მისი მოქმედი რედაქცია აკმაყოფილებს კონვენციით განსაზღვრულ პირობებსა და გარანტიებს. გათვალისწინებულია ადამიანის ძირითად უფლებებსა და თავისუფლებებში თვითნებურად ჩარევისგან დამცავი მთელი რიგი მექანიზმები, თუმცა კომპიუტერული მონაცემის გამოთხოვისას პრივილეგირებული და პროფესიულ საიდუმლოებას მიკუთვნებული ინფორმაციის სათანადოდ დაცვის საკითხი კვლავ გამოწვევად რჩება.

ადამინის ძირითადი უფლებებისა და თავისუფლებების სათანადო დაცვის და მათ შორის დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების უფრო ეფექტურად სარგებლობის მიზნით, აგრეთვე მიზანშეწონილია კონვენციის მე-16 მუხლით გათვალისწინებული „ შენახული კომპიუტერული მონაცემის დაჩქარებული დაცვის“ საგამოძიებო მოქმედების ეროვნულ კანონმდებლობაში დანერგვა.

2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტისა და წარსული გამოცდილების გათვალისწინებით ასევე მოწესრიგებას და სრულყოფას საჭიროებს ნებაყოფლობით, თანხმობის საფუძველზე კომპიუტერული მონაცემის მოპოვება და მისი საპროცესო დამაგრება.

შესაბამისად, მოცემული საჭიროებებისა და დისერტაციის კვლევის შედეგების გათვალისწინებით შემოთავაზებული იქნება სსსკ-ის 136-ე მუხლის სრულყოფისთვის საჭირო კონკრეტული რეკომენდაციები.

2. მონაცემთა დაჩქარებული დაცვა

თანამედროვე სამყაროსთვის დამახასიათებელია, როდესაც ელექტრონული ინფორმაცია სხვადასხვა მოწყობილობასა თუ კომპიუტერულ ქსელშია განთავსებული. ხშირია შემთხვევებიც, როდესაც მონაცემთა დაცვის შესახებ

კანონმდებლობა, სერვის პროვაიდერებს გარკვეული სახის ინფორმაციის დაუყოვნებლივ ან გარკვეული პერიოდის გასვლის შემდეგ მათ განადგურებას ავალდებულებს, ან თუნდაც, აღარ არსებობს მონაცემთა დამუშავებისა და შენახვის კანონით გათვალისწინებული საფუძველი [672] და მონაცემთა მფლობელი მის განადგურებას გეგმავს. ასეთ ვითარებაში შესაძლოა ინფორმაციას განსაკუთრებული მნიშვნელობა ჰქონდეს გამოძიების მიზნებისთვის, თუმცა იმის მხედველობაში მიღებით რომ „კიბერდანაშაულის შესახებ“ კონვენციით გათვალისწინებული „მონაცემთა დაჩქარებული დაცვის“ საგამოძიებო მოქმედება საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობით გათვალისწინებული არ არის, მსგავს შემთხვევებში მხარეებს ამავე კოდექსის 136-ე მუხლით ხელმძღვანელობა უწევთ.

თუ საქმის გარემოებებით გამოიკვეთება, რომ დაყოვნებით გამოძიებისთვის შესაძლო მნიშვნელობის მონაცემები შეიძლება შეიცვალოს, დაიკარგოს ან განადგურდეს, ბრალდების მხარე საგამოძიებო მოქმედებას გადაუდებელი აუცილებლობის საფუძველზე პროკურორის დადგენილებით ჩაატარებს. ხოლო, დაცვის მხარეს, რომელსაც საგამოიებო მოქმედების გადაუდებელი აუცილებლობის შემთხვევაში ჩატარების უფლებამოსილება არ გააჩნია, მსგავს ვითარებაში იძულებული იქნება სსსკ-ის 112-ე მუხლით დადგენილი წესით სასამართლოს შუამდგომლობით მიმართოს.

გარდა იმისა, რომ ასეთ ვითარებაში დაცვის მხარე არახელსაყრელ მდგომარეობაშია ბრალდების მხარესთან შედარებით, კომპიუტერული მონაცემის დაჩქარებული დაცვის დამოუკიდებელ საგამოძიებო მოქმედებად გათვალისწინება პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის მიზნითაც გამართლებულია.

ზემოთხსენებულის მაგალითზე რომ განვიხილოთ, შესაძლოა გადაუდებელი აუცილებლობით მოპოვებული ინფორმაციის შესწავლისას გამოიკვეთოს, რომ მას გამოძიებისთვის მტკიცებულებითი ღირებულება არ გააჩნია, თუმცა ვინაიდან შესაძლებელი იყო კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში არსებული ინფორმაცია შეცვლილიყო ან განადგურებულიყო, მხარე იძულებული იყო დაჩქარებული წესით, სასამართლო ნებართვის გარეშე ჩაეტარებინა საგამოძიებო მოქმედება.

[672] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 25.

აღნიშნული, ცალსახად მიუთითებს კონვენციის მე-16 მუხლით გათვალისწინებული საგამოძიებო მოქმედების ეფექტურობაზე. იგი მხარეებს საშუალებას აძლევს გარკვეული დროით მოსთხოვონ პირს კონკრეტული ინფორმაციის უსაფრთხოდ შენახვა, რა დროსაც მათ მეტი დრო რჩებათ როგორც გამოძიებისთვის მისი შესაძლო ღირებულების დასადგენად, ისე დასაბუთებული ვარაუდის სტანდარტით სასამართლო განჩინების მისაღებად. აღნიშნული კი მინიმუმამდე ამცირებს პირად ცხოვრებაში გაუმართლებლად ჩარევის რისკს, ვინაიდან მონაცემთა დაცვის მოთხოვნა სრულებით არ გულისხმობს მონაცემზე წვდომისა და გაცნობის შესაძლებლობას.[673]

შესაბამისად, ჩვენს მიერ დისერტაციის ფარგლებში მონაცემთა დაჩქარებული დაცვის საგამოძიებო მოქმედებასთან დაკავშირებული „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებისა და კანადის კანონმდებლობის გათვალისწინებით, შესაძლებელია მისი ეროვნულ კანონმდებლობაში დანერგვა.[674]

3. პრივილეგირებული ინფორმაციის დაცვის საკითხი

თანამედროვე ტექნოლოგიების განვითარების შედეგად ტრადიციული ურთიერთობები, მათ შორის კომუნიკაცია, მომსახურება თუ სხვა, ელექტრონულმა მოწყობილობებმა და დისტანციურმა სერვისებმა ჩაანაცვლეს.

ადამიანები ერთმანეთთან სახლიდან გაუსვლელად ამყარებენ კომუნიკაციას. დისტანციურად დგება კომუნიკაცია ადვოკატსა და კლიენტს შორის, ექიმსა და პაციენტს შორის, ხოლო იურიდიული დოკუმენტი ან სამედიცინო შემოწმების შედეგები კი ელექტრონული ფოსტით იგზავნება. შესაბამისად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის 1-ლი ნაწილი, რომელიც დასაბუთებული ვარაუდის სტანდარტის არსებობის პირობებში მხარეებს, კომპიუტერული სისტემიდან ან ინფორმაციის შემნახველი საშუალებიდან სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის მოპოვების შესაძლებლობას ანიჭებს, სათანადო გარანტიების არარსებობის პირობებში ზრდის იმ მონაცემებისა თუ ინფორმაციის მოპოვების რისკს, რომლის საიდუმლოების დაცვის ინტერესი

[673] დეტალური ინფორმაციისთვის გაეცანით ამავე დისერტაციის მე-2 თავს.
[674] იხ. დისერტაციის დანართი 2.

უფრო მაღალია, ვიდრე დანაშაულის გახსნისა და დამნაშავის დასჯის საჯარო ინტერესი.[675] ამას გარდა, გამოთხოვისას შესაძლოა ისეთი ინფორმაციაც იქნას მოპოვებული, რომელსაც კავშირი არ აქვს მიმდინარე სისხლის სამართლის საქმესთან და ამავდროულად დაკავშირებული იყოს პირის რასობრივ ან ეთნიკურ წარმომავლობასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, გენეტიკურ და ბიომეტრიულ მონაცემებთან. ამრიგად, მიზანშეწონილია საპროცესო კანონმდებლობა ითვალისწინებდეს დებულებებს, რომლებიც გამორიცხავს ან მინიმუმამდე შეამცირებს როგორც პრივილეგირებულ პირებს შორის კომუნიკაციის, ისე ზოგადად გამჟღავნებისგან დაცული ინფორმაციის მოპოვებას.

თუ ადამიანის უფლებათა ევროპული სასამართლოს გამოცდილებასაც დავეყრდნობით, ვნახავთ, რომ საქმეში კოპი შვეიცარიის წინააღმდეგ[676], სასამართლომ ადვოკატსა და კლიენტს შორის შემდგარი კომუნიკაციის საიდუმლოების დაცვისთვის აუცილებელი სათანადო გარანტიების ეროვნულ კანონმდებლობაში არ არსებობის გამო, კონვენციის მე-8 მუხლის დარღვევა დაადგინა. მართალია, კანონმდებლობა ამგვარი ურთიერთობის კონფიდენციალურობის დაცვის ვალდებულებას ითვალისწინებდა, თუმცა მოცემული არ იყო თუ ვის მიერ, როგორ და რა პროცედურების დაცვით უნდა მომხდარიყო პრივილეგირებული კომუნიკაციის გამოცალკევება არაპრივილეგირებულისგან.[677]

რა თქმა უნდა, დასმული საკითხის გადაწყვეტა სირთულეს წარმოადგენს. განსაკუთრებით ისეთ პირობებში, როდესაც საგამოძიებო მოქმედების ჩატარების უფლებამოსილება როგორც ბრალდების, ისე დაცვის მხარეს, გააჩნია. ბრალდების მხარის შემთხვევაში შესაძლოა ინფორმაციის განცალკევების ვალდებულება მისი მოპოვების შემდეგ პროკურორს დაეკისროს,[678] ხოლო დაცვის მხარის შემთხვევაში, ადვოკატს. მნიშვნელოვანია აგრეთვე, მოპოვებული მონაცემების განადგურების ვალდებულების შემოტანა, რომელიც შესაძლოა საპროცესო კანონმდებლობაში ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის/მასალის

[675] *Khodorkovsky and Lebedev v. Russia,* [2013] ECHR.
[676] *Kopp. V. Switzerland*, [1998] ECHR.
[677] იქვე, 73-75.
[678] *Manon Harriet AALMOES and 112 Others v. The Netherlands*, 16269/02, Annex II, 2004.

განადგურებისათვის დადგენილი წესების მიხედვით (სსსკ-ის 143[8]) ან ახალი ნორმების გათვალისწინებით გადაწყდეს.[679]

პრივილეგირებული კომუნიკაციის გამჟღავნებისგან დაცვის თვალსაზრისით შესაძლოა კანადის გამოცდილების გაზიარებაც.[680] როგორც ჩვენთვის უკვე ცნობილია, ბრძანების ადრესატი უფლებამოსილია წერილობით ბრძანების მიმღებ ორგანოს მიმართოს და მის წინაშე გაცემული მოთხოვნის ცვლილება ან თუნდაც გაუქმება იშუამდგომლოს, [681] თუ დოკუმენტის გადაცემის შედეგად გამოვლინდება ინფორმაცია, რომელიც კანონით არის პრივილეგირებული ან სხვაგვარად დაცული გამჟღავნებისგან.[682] რა თქმა უნდა, აღნიშნულის განხორციელება შეიძლება ითქვას მარტივია, როდესაც დოკუმენტის ან ინფორმაციის გადაცემის მოთხოვნა სასამართლო ნებართვის საფუძველზე[683] უშუალოდ ფიზიკური პირისგან ხდება.[684] სირთულეს შეიძლება გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის დადგენილების საფუძველზე ინფორმაციის მოპოვებისას წავაწყდეთ, თუმცა ასეთ დროს შესაძლებელია სასამართლოს მიენიჭოს უფლებამოსილება, გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედების კანონიერების შემოწმებისას, საკუთარი ინიციატივით ან იმ პირის შუამდგომლობის საფუძველზე, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება,[685] პროკურორს დაავალოს გამჟღავნებისგან დაცული ინფორმაციის განცალკევება და მათ შორის მისი განადგურება, რაც აუცილებლად სასამართლოს კონტროლს დაექვემდებარება. განსაკუთრებით მნიშვნელოვანია სასამართლოს როლის გაზრდა ისეთ ვითარებაში, როდესაც ინფორმაციის მოპოვება მომსახურების მომწოდებლისგან ხდება, ვინაიდან, როგორც წესი ასეთ დროს სუბიექტი, რომლის შესახებაც ხდება მონაცემთა შეგროვება, არ არის ინფორმირებული მის მიმართ ჩატარებული საგამოძიებო მოქმედების

---

[679] იხ. დისერტაციის დანართი 3.

[680] Criminal Code (R.S.C. 1985, c. C-46), 487.0191 (3).

[681] იქვე, 487.0193(4).

[682] *R. v. Vice Media Canada Inc.*, 2018 SCC 53, 3 S.C.R. 374, 68.

[683] შესაბამისი ცვლილების განხორციელების შემთხვევაში მნიშვნელოვანია სსსკ-ის 112-ე მუხლის 3^1 -ით განსაზღვრულ კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინებისთვის დადგენილ მოთხოვნებს დაემატოს სიტყვები „განჩინების გაუქმების ან შეცვლის მოთხოვნით სასამართლოსთვის მიმართვის უფლება“.

[684] იხ. დისერტაციის დანართი 3.

[685] აღსანიშნავია, რომ სსსკ-ის 112-ე მუხლის მე-5 ნაწილის მესამე წინადადების საფუძველზე სასამართლო უფლებამოსილია შუამდგომლობა იმ პირის მონაწილეობით განხილოს, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება.

შესახებ. შესაბამისად, მნიშვნელოვანია სასამართლო განჩინება გამჟღავნებისგან დაცული ინფორმაციის მოპოვების მინიმუმამდე შემცირების ან აკრძალვის, ხოლო თუ ამის შეცნობა მასალის გამოკვლევის გარეშე შეუძლებელია, მოპოვების შემდეგ მისი გამოცალკევებისა და განადგურების ვალდებულებას ითვალისწინებდეს.

შეჯამებისას, შეიძლება ითქვას, რომ პროფესიული საიდუმლოების ან სხვაგვარად დაცული ინფორმაციის გამჟღავნებისგან დაცვის მიზნით ეროვნულ კანონმდებლობაში ზოგადი დებულებების არსებობა არ წარმოადგენს ქმედით მექანიზმს და აუცილებელია შესაბამისი პროცედურული წესების გათვალისწინება თუ როგორ, ვის მიერ და რა წესების დაცვით უნდა მოხდეს სსსკ-ის 136-ე მუხლის საფუძველზე მოპოვებული პრივილეგირებული მონაცემების გამოძიებისა და სისხლის სამართლის საქმისთვის რელევანტური ინფორმაციისგან გამოცალკევება და განადგურება. ამ პროცესში კი, შეიძლება ითქვას ეროვნული სასამართლოების მონაწილეობას გარდამტეხი მნიშვნელობა უნდა ენიჭებოდეს.

4. კომპიუტერული მონაცემის ნებაყოფლობით გადაცემა

საერთო სასამართლოების პრაქტიკა იცნობს შემთხვევებს როდესაც ბრალდების მხარე სისხლის სამართლის საქმისათვის მნიშვნელოვანი ელექტრონული ინფორმაციის მოპოვებას მფლობელისადმი პირდაპირი მიმართვის წარდგენის გზით ცდილობდა. აღნიშნული, სსსკ-ის 136-ე მუხლით გათვალისწინებული დოკუმენტის ან ინფორმაციის გამოთხოვის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვით იყო განპირობებული.

ელექტრონული ინფორმაციის ამგვარი ხერხით მოპოვების შემთხვევა მუდამ უშედეგოდ მთავრდებოდა, ვინაიდან მტკიცებულების მოპოვებისა და საპროცესო დამაგრების წესების უგულვებელყოფის მოტივით სასამართლო მოპოვებულ ინფორმაციას ყოველ ჯერზე დაუშვებელ მტკიცებულებად ცნობდა.[686]

შეიძლება ითქვას, მოსამართლეთა მიერ გაკეთებული განმარტებები იმ დროისთვის არსებითად სწორი იყო, თუმცა 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტით, როგორც ბრალდების, ისე დაცვის მხარე, სსსკ-ის 112-ე მუხლის პირველი

[686] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 25 იანვრის განჩინება N1გ/109. იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 30 მარტის განჩინება N1გ/548-16.

ნაწილის თანახმად თანამესაკუთრის, თანამფლობელის ან კომუნიკაციის ერთი მხარის თანხმობის საფუძველზე, უფლებამოსილნი გახდნენ მათთვის მნიშვნელოვანი კომპიუტერული მონაცემი სასამართლო განჩინების გარეშე მოიპოვონ.

როდესაც შენახული კომპიუტერული მონაცემის ნებაყოფლობით მოპოვებაზე ვსაუბრობთ, სამი დამოუკიდებელი შემთხვევის გამიჯვნაა შესაძლებელი. პირველი, როდესაც კომპიუტერული მონაცემის გადაცემა მფლობელის ან მესაკუთრის ინიციატივით, ბრალდების ან დაცვის მხარის წინასწარი მიმართვის გარეშე ხდება. მეორე, როდესაც კომპიუტერული მონაცემის გადაცემა ბრალდების ან დაცვის მხარის მიმართვისა და პირის თანხმობის საფუძველზე ხდება და მესამე, როდესაც შენახული კომპიუტერული მონაცემის გადაცემას მხარე მომსახურების მომწოდებელს სთხოვს.

საინტერესოა როგორ უნდა მოხდეს ელექტრონული ინფორმაციის საპროცესო დამაგრება როდესაც მისი მფლობელი ან მესაკუთრე საკუთარი ინიციატივით წარუდგენს მას გამოძიებას. როგორც ჩვენთვის ცნობილია მოქმედი სისხლის სამართლის საპროცესო კოდექსი არ იცნობს „ნებაყოფლობით წარმოდგენის“ საგამოძიებო მოქმედებას [687] და ამასთან, ნებაყოფლობით წარმოდგენილი ელექტრონული ინფორმაციის ამოღების საგამოძიებო მოქმედებით მოპოვება, მუდამ მისი დაუშვებლად ცნობის საფუძველი ხდებოდა. თუმცა, დღეს, როდესაც სსსკ-ის 136-ე მუხლი ამავე კოდექსის 112-ე მუხლით განსაზღვრულ წესებს ექვემდებარება, ვფიქრობთ, ნებაყოფლობით წარმოდგენილი ინფორმაციის, დოკუმენტის ან ინფორმაციის გამოთხოვის ოქმით საპროცესო დამაგრება, რომელშიც უშუალოდ მესაკუთრის ან მფლობელის წერილობითი თანხმობაც ასახული იქნება, დასაშვები უნდა იყოს.

რაც შეეხება კომპიუტერული მონაცემის უშუალოდ პირის თანხმობის საფუძველზე მოპოვებას, ყურადსაღებია, რომ თუ ელექტრონული ინფორმაციის მატარებელი რამდენიმე ადამიანის საერთო სარგებლობაშია და ერთ-ერთ მათგანს გააჩნია ზიარი

[687] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 25 იანვრის განჩინება N1გ/109, 4-5.

ინტერესი ან უფლებამოსილება მასზე,[688] მისი თანხმობა საკმარისად ჩაითვლება საგამოძიებო მოქმედების სასამართლოს განჩინების გარეშე ჩასატარებლად.[689]

როგორც წესი, ერთობლივი უფლებამოსილება ქონების ერთობლივი გამოყენებით, უმეტესი მიზნებისთვის მასზე წვდომითა და კონტროლით განისაზღვრება, რა დროსაც გონივრულია იმის განსაზღვრა, რომ თანამფლობელიდან ერთ-ერთს გააჩნია ნებართვის გაცემის უფლებამოსილება და მეორე მხარე აცნობიერებს რისკს, რომ საერთო საკუთრებაში არსებული ქონების მიმართ თანამფლობელის თანხმობის საფუძველზე შესაძლოა საგამოძიებო მოქმედება ჩატარდეს. [690] განსხვავებული სურათი იქნება თუ საერთო სარგებლობის მიუხედავად პირი საკუთარ მონაცემებზე წვდომისთვის პაროლს იყენებს და მას სხვას არ უზიარებს.[691]

პრაქტიკაში შესაძლოა თავი იჩინოს შემთხვევებმა, როდესაც პირი ცრუობს უფლებამოსილების არსებობაზე. შესაბამისად, დაინტერესებული მხარის მხრიდან აუცილებელია თანხმობის კანონიერების და მისი ფარგლების დადგენის მიზნით წინასწარი ზომების გატარება. აღნიშნული, შესაძლოა უფლებამოსილების დადგენისთვის საჭირო საკითხების გამოკვლევით, კითხვების დასმითა და არსებული გარემოებების ფრთხილი შეფასებით იქნას მიღწეული.

მომსახურების მომწოდებლის მიერ კომპიუტერული მონაცემის ნებაყოფლობით გადაცემის საკითხს რომ შევეხოთ, თავიდანვე უნდა აღინიშნოს, რომ სსსკ-ის 136-ე მუხლის 4^1 ნაწილი იმგვარად არ უნდა იქნას გაგებული, თითქოს პროვაიდერი კომპანიები უფლებამოსილნი არიან სასამართლო განჩინების ან პროკურორის დადგენილების გარეშე, მომხმარებლის მაიდენტიფიცირებელი ან მასთან დაკავშირებული შინაარსობრივი მონაცემები გასცენ. მართალია მომხმარებლები პროვაიდერ კომპანიას ნებაყოფლობით, მომსახურების ხელშეკრულების საფუძველზე აძლევენ მათ მიერ განხორციელებული კომუნიკაციის ან აქტივობის მაიდენტიფიცირებელი ან შინაარსობრივი მონაცემების დამუშავებისა და შენახვის უფლებას, თუმცა აღნიშნული ფაქტი, „მესამე მხარის“ დოქტრინის საფუძველზეც კი

---

[688] *ფაფიაშვილი ლ.,* თანხმობის საფუძველზე ჩხრეკის წარმოების პრობლემური საკითხები, ჟურ. საკონსტიტუციო სამართლის მიმოხივა, VII გამოცემა, 2014, 52.

[689] *Jarret M. H., Bailie W. M., Hagen E., Judish N.,* Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009, 19.

[690] *United States v. Matlock,* 415 U.S. 164 (1974).

[691] *Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir. 2001).

არ გამორიცხავს პირადი ცხოვრების ხელშეუხებლობისა და ინფორმაციის კონფიდენციალურობის დაცვის გონივრულ მოლოდინს.[692]

პირველ რიგში ყურადსაღებია, მესამე მხარის მიერ შეგროვებული ინფორმაციის ბუნება. ინტერნეტ ეპოქაში მათთვის გამჟღავნებული მონაცემები პრაქტიკულად ყველა სახის ინფორმაციას, მათ შორის კომუნიკაციის შინაარსს, პირის ადგილმდებარეობას, ბიომეტრულ მონაცემებს მოიცავს, რაც ერთობლიობაში სამედიცინო, სოციალური, სექსუალური ცხოვრებისა თუ სხვა ინტიმური საკითხების დეტალურად შესწავლისა და დაკვირვების საშუალებას იძლევა.[693]

გასათვალისწინებელია მოთხოვნილი ინფორმაციის მოცულობაც, ვინაიდან რაც უფრო მეტი ინფორმაციის გადაცემას ითხოვს მხარე, მით უფრო იზრდება პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის ვალდებულება. [694] ამასთან, მოთხოვნილმა ინფორმაციამ შესაძლოა არა მარტო სავარაუდო დამნაშავის, არამედ მასთან დაკავშირებული ინდივიდების პირად ცხოვრებაზეც იქონიოს ზეგავლენა.[695]

საგულისხმოა ის ფაქტიც, რომ ელექტრონული მოწყობილობები და მომსახურების მომწოდებლების მიერ შემოთავაზებული სერვისები ჩვენი ყოველდიურობის ნაწილია. სხვა სიტყვებით რომ ვთქვათ, ელექტრონული მოწყობილობების როლის გათვალისწინებით, ადამიანს თითქმის არ რჩება არჩევანის თავისუფლება უარი თქვას მათ გამოყენებაზე და შესაბამისად პროვაიდერთა მხრიდან ინფორმაციის შენახვა-დამუშავებაზე. ამასთან, ელექტრონული მოწყობილობით განხორციელებული აქტივობის შესახებ მონაცემების პროვაიდერი კომპანიისთვის გადაცემა ავტომატურ რეჟიმში, მომხმარებლის კონტროლისგან თავისუფლად წარმოებს. [696] ზემოთხსენებული ფაქტორების გათვალისწინებით კი მომხმარებელთა მიერ მესამე პირებისთვის გამჟღავნებული ინფორმაციის კონსტიტუციურ-სამართლებრივი დაცვის ვალდებულება არა თუ მცირდება, არამედ მატულობს.

შესაბამისად, პირადი ცხოვრების ხელშეუხებლობის უფლების სათანადო დაცვის, უფლების შეზღუდვისას თანაზომიერების მოთხოვნის უზრუნველყოფის მიზნით,

---

[692] *Tokson M.*, Automation and the Fourth Amendment, Iowa Law Review, Vol. 96, 2011, 585. იხ. *Carpenter v. United States,* N16-402, 2018.

[693] *Tokson M.,* The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021, Harvard Law Review, 2022. 1801.

[694] იქვე, 1802.

[695] იქვე,1803-1804.

[696] იქვე, 1803.

მომსახურების მომწოდებლებს მომხმარებლის მაიდენტიფიცირებელი თუ შინაარსობრივი მონაცემების სასამართლო განჩინების ან გადაუდებელი აუცილებლობის საფუძველზე პროკურორის დადგენილების გარეშე გამჟღავნების უფლებამოსილება არ უნდა მიენიჭოთ. ზოგადი დათქმიდან შესაძლებელია გამონაკლისების გათვალისწინებაც და ამ მხრივ შესაძლოა ამერიკის შეერთებული შტატების კანონმდებლობის გაზიარებაც. მაგალითისთვის, როგორც ჩვენთვის ცნობილია აშშ-ს კანონმდებლობით (იხ. თავი V) მონაცემთა ნებაყოფლობით გადაცემა დასაშვებია, როდესაც მომსახურების მომწოდებელს კეთილსინდისიერად სჯერა, რომ სახეზეა გადაუდებელი აუცილებლობა, საფრთხე ემუქრება პირის სიცოცხლეს ან ჯანმრთელობას და საგანგებო მდგომარეობასთან დაკავშირებული კომუნიკაციის შინაარსის გამჟღავნება აუცილებელია.[697] ასეთ დროს პროვაიდერთა მოთხოვნაა, სახელმწიფო უწყებებმა მიაწოდონ დეტალური ინფორმაცია თუ როგორ დაეხმარებათ მათ მოთხოვნილი ინფორმაცია საკითხის მოგვარებაში.[698] ამას გარდა, მონაცემთა ნებაყოფლობით გადაცემა დასაშვებია, როდესაც მომხმარებლის ან კომუნიკაციის მხარის თანხმობა სახეზეა[699] ან ინფორმაციის გამჟღავნება პროვაიდერის უფლებებისა თუ საკუთრების დაცვისთვის არის აუცილებელი.[700] დამატებით, პროვაიდერმა კომპანიამ შესაძლოა საგამოძიებო უწყებას ინფორმაცია მიაწოდოს თუ მან უნებლიედ მოიპოვა ის და აშკარად დაკავშირებულია დანაშაულის ჩადენასთან.[701] ყურადსაღებია კომუნიკაციის მხარის ან მომხმარებლის თანხმობის არსებობის პირობებში პროვაიდერი კომპანიისგან ინფორმაციის გამოთხოვა. რა თქმა უნდა, თანხმობა უნდა იყოს ნებაყოფლობით და გასაგებად გაცხადებული, ამასთან კონკრეტული. ნიშანდობლივია, რომ მომხმარებლის ან კომუნიკაციის ერთი მხარის თანხმობის, პროვაიდერი კომპანიისგან ინფორმაციის გამოთხოვის სამართლებრივ საფუძვლად საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლში გათვალისწინება მნიშვნელოვნად დაეხმარება როგორც ბრალდების, ისე დაცვის მხარეს კომპიუტერული მონაცემის მოპოვებაში. ამასთან, აღნიშნული სრულ

[697] SCA, 18 U.S.C. §2702 (b)(8), (c)(4).
[698] *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016, 61.
[699] SCA, 18 U.S.C. §2702 (b)(3), (c)(2).
[700] იქვე, §2702 (b)(5), (c)(3).
[701] იქვე, §2702 (b)(7).

თანხვედრაში იქნება პირადი ცხოვრების ხელშეუხებლობის უფლების, პერსონალურ მონაცემთა დაცვის ეროვნულ თუ საერთაშორისო მოთხოვნებთან.

შეჯამების სახით უნდა ითქვას, რომ მნიშვნელოვანია საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობამ კომპიუტერული მონაცემის თანხმობის საფუძელზე მოპოვების საკითხი რაც შეიძლება დროულად და კიდევ უფრო დეტალურად მოაწესრიგოს. დისერტაციაში გამოთქმული მოსაზრებების გათვალისწინებებით სრულყოფას საჭიროებს როგორც ნებაყოფლობით წარმოდგენილი ელექტრონული ინფორმაციის საპროცესო დამაგრების წესი, თანხმობის კანონიერებისა და ლეგიტიმურობის დადგენის წინაპირობები, ასევე დასაზუსტებელია მომსახურების მომწოდებლის მიერ გამონაკლის შემთხვევებში კომპიუტერული მონაცემის ნებაყოფლობით გამჟღავნების სამართლებრივი საფუძვლები.

დასკვნა

სადისერტაციო ნაშრომზე მუშაობის ფარგლებში გამოიკვეთა, რომ კომპიუტერული მონაცემი გარდამტეხ როლს თამაშობს გამოძიებისა და სასამართლო განხილვის პროცესში. მისთვის დამახასიათებელი სპეციფიკური თუ ტექნიკური ნიშან-თვისებების სათანადოდ შესწავლამ კი აჩვენა, რომ აუცილებელია საპროცესო კანონმდებლობა მასზე მორგებულ საგამოძიებო მოქმედებებს ითვალისწინებდეს და გამოძიებისა თუ სისხლის სამართლის საქმისათვის მნიშვნელოვანი მონაცემების შეგროვება მათი მეშვეობით ხდებოდეს.

შესაფერის საგამოძიებო მოქმედებას წარმოადგენს თავად საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებული „დოკუმენტის ან ინფორმაციის გამოთხოვა“. ნიშანდობლივია, რომ მისი პირველწყაროს, „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნების შესაბამისად, ეროვნული კანონმდებლობით, საგამოძიებო მოქმედება დამოუკიდებელი სახით არის გათვალისწინებული, აკმაყოფილებს სიზუსტისა და განჭვრეტადობის მოთხოვნებს და შეიცავს თვითნებური ჩარევისგან დასაცავ მთელ რიგ ქმედით პროცესუალურ გარანტიებს.

დოკუმენტის ან ინფორმაციის გამოთხოვისას მხარეებისთვის დადგენილია ფორმალური და მატერიალური წინაპირობების დაკმაყოფილების ვალდებულება,[702] საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელია სისხლის სამართლის საქმეზე ოფიციალური გამოძიების მიმდინარეობა, სასამართლოს წინაშე მოტივირებული შუამდგომლობის დაყენება და დასაბუთებული ვარაუდის სტანდარტით ხელმძღვანელობა, [703] Ex ante და Ex post (ბრალდების მხარის

[702] თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის განჩინება №1გ/363-20, 3.

[703] *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013, 38,<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [02.07.23].

შემთხვევაში) სასამართლო კონტროლი [704] და პერსონალურ მონაცემთა დაცვის სამსახურის მიერ საგამოძიებო ღონისძიებაზე ზედამხედველობის განხორციელება.[705] იმავდროულად სადისერტაციო კვლევის ფარგლებში გამოიკვეთა, რომ უფლებაში თვითნებური ჩარევისგან დასაცავი ბერკეტების არსებობის მიუხედავად კვლავ პრობლემურ საკითხად რჩება პროფესიული საიდუმლოების ან სხვაგვარად დაცული ინფორმაციის გამჟღავნებისგან დაცვა. ფაქტია, ეროვნული კანონმდებლობით გათვალისწინებული ზოგადი დებულებები ვერ შეფასდება საკმარისად. სათანადო გარანტიების არარსებობის პირობებში იზრდება იმ მონაცემებისა თუ ინფორმაციის მოპოვების რისკი, რომლის საიდუმლოების დაცვის ინტერესი უფრო მაღალია, ვიდრე დანაშაულის გახსნისა და დამნაშავის დასჯის საჯარო ინტერესი.[706] აუცილებელია შესაბამისი პროცედურული წესების გათვალისწინება თუ როგორ, ვის მიერ და რა წესების დაცვით უნდა მოხდეს სსსკ-ის 136-ე მუხლის საფუძველზე სისხლის სამართლის საქმისთვის მოსაპოვებელი რელევანტური ინფორმაციისგან პრივილეგირებული მონაცემების გამოცალკევება ან/და განადგურება.

საპროცესო დებულებების სრულყოფის გზაზე და პრივილეგირებული კომუნიკაციის გამჟღავნებისგან დაცვის თვალსაზრისით შესაძლოა კანადის კანონმდებლობით გათვალისწინებული საინტერესო გამოცდილების გაზიარება. [707] კერძოდ, თუ ინფორმაციის გადაცემა პრივილეგირებული კომუნიკაციის ან კანონით გამჟღავნებისგან დაცული ურთიერთობის შესახებ მონაცემების გამჟღავნებას გამოიწვევს, [708] კანადის კანონმდებლობით ბრძანების ადრესატი უფლებამოსილია წერილობით მიმართოს ბრძანების მიმღებ ორგანოს და მოთხოვნის ცვლილება ან თუნდაც გაუქმება იშუამდგომლოს. [709] საგულისხმოა, რომ აღნიშნულის განხორციელება კიდევ უფრო მარტივია, როდესაც ინფორმაციის გამოთხოვა უშუალოდ ფიზიკური პირისგან ხდება. საკითხის მსგავსი გადაწყვეტის შემთხვევაში

[704] 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> [02.07.23].

[705] საქართველოს პარლამენტის გადაწყვეტილებით 2022 წლის 1 მარტიდან სახელმწიფო ინსპექტორის სამსახური გაუქმებულია. ნაცვლად ორი უწყება - სპეციალური საგამოძიებო სამსახური და პერსონალურ მონაცემთა დაცვის სამსახური იფუნქციონირებს.

[706] *Khodorkovsky and Lebedev v. Russia,* [2013] ECHR.

[707] Criminal Code (R.S.C. 1985, c. C-46), 487.0191 (3).

[708] *R. v. Vice Media Canada Inc.*, 2018 SCC 53, 3 S.C.R. 374, 68.

[709] Criminal Code (R.S.C. 1985, c. C-46), 487.0193(4).

საქართველოს კანონმდებლობით სირთულეს, შესალოა გადაუდებელი აუცილებლობისას პროკურორის დადგენილების საფუძველზე ინფორმაციის მოპოვებისას წავაწყდეთ. თუმცა, შესაძლებელია სასამართლოს მიენიჭოს უფლებამოსილება, გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედების კანონიერების შემოწმებისას, საკუთარი ინიციატივით ან იმ პირის შუამდგომლობის საფუძველზე, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება,[710] პროკურორს გამჟღავნებისგან დაცული ინფორმაციის განცალკევება და მეტიც, სასამართლოს კონტროლს ქვეშ მისი განადგურება დაავალოს.

აღნიშნული პროცედურების არსებობა განსაკუთრებით მნიშვნელოვანია ისეთ ვითარებაში, როდესაც ინფორმაციის მოპოვება მომსახურების მომწოდებლისგან ხდება, ვინაიდან, როგორც წესი, ასეთ დროს სუბიექტი, რომლის შესახებაც ხდება მონაცემთა შეგროვება, ინფორმირებული არ არის მის მიმართ განხორციელებული საგამოძიებო მოქმედების თაობაზე. შესაბამისად, მნიშვნელოვანია სასამართლო ნებართვა გამჟღავნებისგან დაცული ინფორმაციის მოპოვების მინიმუმამდე შემცირების ან აკრძალვის მოთხოვნას, ხოლო თუ ამის შეცნობა მასალის გამოკვლევის გარეშე შეუძლებელია, მონაცემთა მოპოვების შემდეგ მისი გამოცალკევებისა და განადგურების ვალდებულებას ითვალისწინებდეს.

პირადი ცხოვრების ხელშეუხებლობისა და უფლების შეზღუდვისას თანაზომიერების პრინციპის უზრუნველყოფის მიზნით ასევე აუცილებელია კომპიუტერული მონაცემის თანხმობის საფუძელზე მოპოვების საკითხი საპროცესო კანონმდებლობით რაც შეიძლება დროულად და კიდევ უფრო დეტალურად მოწესრიგდეს. აღნიშნულის საჭიროებაზე არა მარტო 2022 წლის 24 მაისის საკანონმდებლო ცვლილებათა პაკეტი მიუთითებს, [711] არამედ გასული წლების სასამართლო პრაქტიკაც, როდესაც ელექტრონული ინფორმაციის მოპოვება გამომძიებლის მიმართვის ან უშუალოდ მესაკუთრის ან მფლობელის ნებართვის საფუძველზე ხორციელდებოდა. მნიშვნელოვანია ზუსტად განისაზღვროს ნებაყოფლობით წარმოდგენილი ელექტრონული ინფორმაციის საპროცესო დამაგრების წესი, თანხმობის

[710] აღსანიშნავია, რომ სსსკ-ის 112-ე მუხლის მე-5 ნაწილის მესამე წინადადების საფუძველზე სასამართლო უფლებამოსილია შუამდგომლობა იმ პირის მონაწილეობით განხილოს, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება.

[711] საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24/05/2022.

კანონიერებისა და ლეგიტიმურობის დადგენის წინაპირობები, დაზუსტდეს მომსახურების მომწოდებლის მიერ გამონაკლის შემთხვევებში კომპიუტერული მონაცემის ნებაყოფლობით გამჟღავნების სამართლებრივი საფუძვლები. უნდა აღინიშნოს, რომ ამ მხრივ შესაძლოა ამერიკის შეერთებული შტატების კანონმდებლობის მოშველიება, სადაც დეტალურად არის განსაზღვრული თუ რა საფუძლით შეუძლია მომსახურების მომწოდებელს გადასცეს ინფორმაცია სამართალდამცავ ორგანოებს.[712]

საერთო სასამართლოების პრაქტიკის კვლევამ ასევე გვიჩვენა, რომ ხშირი იყო შუამდგომლობის დასაბუთებულობასთან დაკავშირებული პრობლემებიც. გარდა დასაბუთებული ვარაუდის სტანდარტით შედგენილი შუამდგომლობისა, რიგ შემთხვევებში სასამართლო, დამატებით, მხარეებისგან კომპიტერული სისტემის გამართულად ფუნქციონირების, ჩანაწერის შენახვის ვადისა და სისტემიდან ინფორმაციის რეალურად ამოღების შესაძლებლობის შესახებ მტკიცებულების წარდგენას ითხოვდა, რაც პრაქტიკული თვალსაზრისით მხარისთვის ხელოვნურ ბარიერს ქმნიდა.

მეტიც, გამოიკვეთა შემთხვევები, როდესაც სასამართლო დაცვის მხარის შუამდგომლობის საფუძველზე მიღებული განჩინების აღსრულებას ბრალდების მხარეს აკისრებდა. მოტივს ძირითადად დაცვის მხარის მიერ საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელი უნარ-ჩვევებების არ ქონა წარმოადგენდა. მართალია რიგ შემთხვევებში დაცვის მხარეს შესაძლოა არ გააჩნდეს კომპიუტერული სისტემიდან ან მონაცემთა შესანახი საშუალებიდან ინფორმაციის გამოთხოვის გარკვეული უნარ-ჩვევები ან სპეციალური ცოდნა, თუმცა ასეთ დროს საგამოძიებო მოქმედება არა თუ ბრალდების მხარის ხელმძღვანელობით, არამედ ექსპერტის მონაწილეობით უნდა ჩატარდეს. ამასთან, დაცვის მხარის მსგავსად იდენტური პრობლემა გამორიცხული არაა ბრალდების მხარესაც შეექმნას. გარდა ამისა, უთუოდ გასათვალისწინებელია ის შემთხვევები, როდესაც დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედება არ მოითხოვს ბრალდების ან დაცვის მხარის განსაკუთრებულ უნარ-ჩვევებს. ამის ნათელი მაგალითია, მომსახურების

[712] იხ. ამავე დისერტაციის თავი V.

მომწოდებლის დახმარებით მობილურ ნომერზე შემავალი და გამავალი ზარების, შეტყობინებების შესახებ ინფორმაციის მოპოვება.

ამრიგად, თითოეული შემთხვევა დამოუკიდებელ შეფასებს საჭიროებს და სასამართლოს მიდგომა თითქოს დაცვის მხარეს ცალსახად არ ძალუძს დამოუკიდებლად დოკუმენტის ან ინფორმაციის გამოთხოვის საგამოძიებო მოქმედების ჩატარება, გაუმართლებელია. საყურადღებოა ისიც რომ, სასამართლო განჩინების შესრულების ვადა 30 დღეს წარმოადგენს და სასამართლოს ამგვარი მიდგომა დაცვის მხარეს არსებითად დამოკიდებულს ხდის ბრალდების მხარეზე, რაც საფრთხეს უქმნის დაცვის უფლებით სათანადოდ სარგებლობას.

სრულყოფას საჭიროებს „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნების პრაქტიკული გამოყენება. ფაქტია, ელექტრონულ მტკიცებულებასა და თანამედროვე მსოფლიოში არსებულ გამოწვევებზე მორგებული პროცედურული მექანიზმებიდან, კომპიუტერული მონაცემის გადაცემის ბრძანებასთან ერთად, ჩვენთვის თავისი არსითა და ეფექტურობით არც „შენახული კომპიუტერული მონაცემების დაჩქარებული დაცვაა“ ნაკლებად მნიშვნელოვანი. აღნიშნული იმ საგამოძიებო მოქმედებათა რიგს მიეკუთვნება, რომლებიც საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში დამოუკიდებელი სახით ჯერ იმპლემენტირებული არ არის და „დოკუმენტის ან ინფორმაციის გამოთხოვის“ საგამოძიებო მოქმედების ეფექტური გამოყენებისთვის მნიშვნელოვანია. პრაქტიკაში უკვე გვხვდება შემთხვევები, როდესაც მონაცემთა დაცვის შესახებ კანონმდებლობა, სერვის პროვაიდერებს გარკვეული სახის ინფორმაციის დაუყოვნებლივ ან გარკვეული დროის გასვლის შემდეგ განადგურებას ავალდებულებს, ან აღარ არსებობს მონაცემთა დამუშავებისა და შენახვის კანონით გათვალისწინებული საფუძველი[713] და მონაცემთა მფლობელი მის განადგურებას გეგმავს, დაჩქარებული დაცვის ბრძანების საფუძველზე, მონაცემთა კანონიერი მფლობელი ან/და ზედამხედველი ვალდებულია გარკვეული დროით ინფორმაცია დაუზიანებლად და სახეუცვლელად შეინახოს.[714] ნიშანდობლივია, რომ დისერტაციაში მონაცემთა დაჩქარებული წესით დაცვის საკითხი „კიბერდანაშაულის შესახებ“ კონვენციისა და კანადის

[713] Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001, 25.
[714] იქვე, 27.

კანონმდებლობის [715] მაგალითზე საკმაოდ დეტალურად არის განხილული, რაც ეროვნულ კანონმდებლობაში შესაბამისი ცვლილებების შესატანად ნოყიერ ნიადაგს ქმნის.

საბოლოოდ, სადისერტაციო კვლევის ფარგლებში ნათლად წარმოჩნდა, რომ სსსკ-ის 136-ე მუხლის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვა არა მარტო გაუმართლებელ დაბრკოლელებს ქმნიდა გამოძიებისა და მართლმსაჯულების განხორციელების პროცესში, არამედ ეწინააღმდეგებოდა კონვენციის დებულებებს. ამასთან, გამოიკვეთა, რომ დოკუმენტის ან ინფორმაციის გამოთხოვა თავისი ბუნებით არ წარმოადგენს ფარულ საგამოძიებო მოქმედებას და არ ატარებს მისთვის დამახასიათებელ ნიშან-თვისებებს. [716] შესაბამისად, მნიშვნელოვანია, სამომავლოდ კომპიუტერული მონაცემის გამოთხოვის მოქმედების ფარგლები აღარ შეიზღუდოს დანაშაულთა წრით. ცხადია, ელექტრონული სახით არსებულ მონაცემებზე წვდომისას ყოველთვის არსებობს სხვა პირთა პერსონალური მონაცემების არამიზნოვრივად ან თვითნებურად დამუშავების რისკი. მაგრამ, აღნიშნული არა ნორმის მოქმედების ფარგლების დანაშაულთა წრით შეზღუდვით, არამედ კანონმდებლობაში სათანადო მატერიალური და პროცესუალური წინაპირობების გათვალისწინებით უნდა გამოირიცხოს.

[715] იხ. ამავე ნაშრომის თავი V.

[716] *კვეკვეცია ქ.,* საბანკო ანგარიშის მონიტორინგი, როგორც საგამოძიებო მოქმდება - კანონმდებლობა და პრაქტიკა, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021, 316-317.

ბიბლიოგრაფია

ქართულენოვანი ნორმატიული მასალა

- საქართველოს კონსტიტუცია, სპუ, 24.08.1995.
- საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, სსმ, 26.06.2005.
- საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 09.10.2009.
- საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებებისა და დამატებების შესახებ, N3616, 24.09.10.
- საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, სსმ, 28.12.2011.
- საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ საქართველოს კანონი, N2634-რს, 01.08.2014.
- საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ, სსმ, №1575, 24.05.2022.

ქართულენოვანი სამეცნიერო ლიტერატურა

- *ავტორთა კოლექტივი,* საქართველოს სისხლის საპროცესო სამართალი, კერძო ნაწილი, თბილისი, მერიდიანი, 2017.
- *ავტორთა კოლექტივი,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბილისი, ამერიკის იურისტთა ასოციაცია, 2015.
- *აქუბარდია ი.,* საბანკო ანგარიშების მონიტორინგის ადგილი საგამოძიებო მოქმედებათა სისტემაში, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021.
- *გერი ვ., შრამი ე.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის რეფორმირებისთვის - შედარებითი და ევროპული მოსაზრებები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, N1, 2019.
- *ბოძაშვილი ლ., კოხრეიძე ნ.,* კიბერსივრცის სამართალი 2012. <https://www.lit.ge/book/643-kibersivrcis-samartali-levan-bodzashvili,-nikoloz-koxreidze> [20.05.2023].
- *ზაქაშვილი უ.,* სადისერტაციო ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, 2013. <http://press.tsu.ge/data/image_db_innova/disertaciebi_samartali/ucha_zaqarashvilii.pdf> [20.05.2023].

- *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი - ზოგადი ნაწილის მიმოხილვა, თბილისი, იურისტების სახლი, 2014.
- *კავთუაშვილი ე.,* კიბერდანაშაული და კიბერუსაფრთხოების პრობლემატიკა, ჟურნალი „მართლმსაჯულება და კანონი“ N1, 2013.
- *კუბლაშვილი კ.,* ადამიანის ძირითადი უფლებები და თავისუფლებები, მე-5 გამოცემა, თბილისი, იურისტების სამყარო, 2019.
- *კვეკვეცია ქ.,* საბანკო ანგარიშის მონიტორინგი, როგორც საგამოძიებო მოქმედება - კანონმდებლობა და პრაქტიკა, საიუბილეო კრებული ნონა თოდუა 60, თბილისი, 2021.
- მოსამართლეთა ტრენინგი ქსელურ დანაშაულში, ევროპის საბჭო, 2010. <https://rm.coe.int/16802fa3c1> [20.05.23].
- *ოთხოზორია ვ., ცირამუა ზ.,* ინფორმაციული ტექნოლოგიები, თბილისი, 2015. <https://drive.google.com/file/d/1LyzJT-xOLJAlGNUyONrUvhhC_tOnppPu/view> [20.05.2023].
- *საქართველოს საკონსტიტუციო სასამართლო,* საქართველოს საკონსტიტუციო სასამართლოს მიერ 2017 წლის განმავლობაში კონსტიტუციური მართლმსაჯულების სფეროში მიღებული მნიშვნელოვანი გადაწყვეტილებები, საკონსტიტუციო სამართლის ჟურნალი, 2018.
- სახელმწიფო ინსპექტორის საქმიანობის ანგარიში 2021. <https://personaldata.ge/cdn/2022/03/SIS-2021-Annual-Report.pdf> [12.06.23].
- *საქართველოს იურიდიული ფირმების ასოციაცია,* დაცვის მხარის მიერ მტკიცებულებათა მოპოვება სასამართლოს მეშვეობით, კვლევა და რეკომენდაციები, 2016.
- *სვიანიძე გ.,* დოკუმენტის ან ინფორმაციის გამოთხოვასთან დაკავშირებული სასამართლო პრაქტიკის ანალიზი, ჟურ. მართლმსაჯულება და კანონი, N3(55), 2017.
- *ფაფიაშვილი ლ.,* „თანხმობის საფუძველზე ჩხრეკის წარმოების პრობლემური საკითხები“ ჟურ. საკონსტიტუციო სამართლის მიმოხივა, VII გამოცემა, 2014.
- *ფაფიაშვილი ლ.,* ციფრული მტკიცებულებების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებულში

„ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში“ *რედ. კორკელია კ.,* თბილისი, 2014.

- *ხატიაშვილი გ.,* როგორ განვითარდა კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვის კანონმდებლობა და პრაქტიკა, ჟურნ. საკონსტიტუციო სამართლის მიმოხილვა, 2019.
- *ხიდეშელი თ.,* კომპიუტერული მონაცემის ცნების, მახასიათებლებისა და მისი ავთენტურობის საკითხისათვის, სამართლის ჟურნალი N1, 2021.
- *ხიდეშელი თ.,* კომპიუტერული მონაცემების გამოთხოვის მოწესრიგება ქართულ კანონმდებლობაში და მისი შესაბამისობა „კიბერდანაშაულის შესახებ“ კონვენციის მოთხოვნებთან, სამართლის ჟურნალი, N1, 2022.

საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილებები

- საქართველოს საკონსტიტუციო სასამართლოს 2018 წლის 26 ივლისის გადაწყვეტილება საქმეზე N2/4/665, 683, „საქართველოს მოქალაქე ნანა ფარჩუკაშვილი საქართველოს სასჯელაღსრულებისა და პრობაციის მინისტრის წინააღმდეგ“.
- საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის გადაწყვეტილება საქმეზე N1/1/650,699 „საქართველოს მოქალაქეები - ნადია ხურციძე და დიმიტრი ლომიძე საქართველოს პარლამენტის წინააღმდეგ“.
- საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება საქმეზე N1/1/625,640 „საქართველოს სახალხო დამცველი და მოქალაქეები პარლამენტის წინააღმდეგ“.
- საქართველოს საკონსტიტუციო სასამართლოს 2015 წლის 31 ივლისის გადაწყვეტილება საქმეზე N2/2/579, „საქართველოს მოქალაქე მაია რობაქიძე საქართველოს პარლამენტის წინააღმდეგ“.
- საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 26 ივნისის გადაწყვეტილება საქმეზე N3/1/512 „დანიის მოქალაქე ჰეიკე ქრონქვისტი საქართველოს პარლამენტის წინააღმდეგ“.

- საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 29 თებერვლის გადაწყვეტილება საქმეზე N2/1/484 „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე თამარ ჩუგოშვილი საქართველოს პარლამენტის წინააღმდეგ“.
- საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის გადაწყვეტილება საქმეზე N1/3/407 „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე - ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ“.

საქართველოს უზენაესი სასამართლოს გადაწყვეტილებები

საქართველოს უზენაესი სასამართლოს 2018 წლის 18 სექტემბრის განაჩენი საქმეზე N138ას-18.

სააპელაციო სასამართლოს საგამოძიებო კოლეგიის განჩინებები

- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 26 ოქტომბრის განჩინება N1გ/1636-22.
- ქუთაისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლი 16 სექტემბრის განჩინება N1/გ-858-22.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 6 სექტემბრის განჩინება N1გ/1385-22.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 14 ივნისის განჩინება საქმეზე N1გ/917-2022.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 25 მაისის განჩინება N1გ/800-22.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 17 თებერვლის განჩინება N1გ/235-22.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2022 წლის 2 თებერვლის განჩინება N1გ/152-22.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 18 ნოემბრის განჩინება N1გ/1924-21.
- თბილისის სააპელაციო სასამართლოს 2021 წლის 12 ოქტომბრის განჩინება N1გ/1709-21.

- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 21 სექტემბრის განჩინება საქმეზე N1გ/1594-21.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2021 წლის 14 სექტემბრის განჩინება N1გ/1553-21.
- თბილისის სააპელაციო სასამართლოს 2021 წლის 7 სექტემბრის განჩინება N1გ/1518-21.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 9 სექტემბრის განჩინება საქმეზე N1გ/1447-20.
- თბილისის სააპელაციო სასამართლოს 2020 წლის 25 აგვისტოს განჩინება საქმეზე N1გ/1328-20.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 10 ივლისის განჩინება საქმეზე N1გ/1029-20.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 6 მაისის განჩინება საქმეზე №1გ/633-20.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2020 წლის 28 თებერვლის განჩინება საქმეზე №1გ/363-20.
- თბილისის სააპელაციო სასამართლოს 2020 წლის 21 იანვრის განჩინება N1გ/125-20.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 31 დეკემბრის განჩინება საქმეზე N1გ/2154-19.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 31 დეკემბრის განჩინება საქმეზე N1გ/2153-19.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 26 დეკემბრის განჩინება საქმეზე №1გ/2133-19.
- თბილისის სააპელაციო სასამართლოს 2019 წლის 25 დეკემბრის განჩინება N1გ/2109-19.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 25 დეკემბრის განჩინება საქმეზე №1გ/2110-19.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 27 ნოემბრის განჩინება საქმეზე N1გ/1984-19.

- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 12 ნოემბრის განჩინება N1გ/1889-19.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2019 წლის 11 სექტემბრის განჩინება საქმეზე N1გ/1504-19.
- საქართველოს უზენაესი სასამართლოს 2018 წლის 18 სექტემბრის განაჩენი საქმეზე N138ას-18.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2018 წლის 2 თებერვლის განჩინება N1გ/133-18.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 9 მარტის განჩინება N1გ/337-17.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 25 იანვრის განჩინება N1გ/109.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2017 წლის 25 იანვრის განჩინება N1გ/109.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 ოქტომბრის განჩინება საქმეზე №1გ/1614-16.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 4 ოქტომბრის განჩინება N1გ/1537-16.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 20 სექტემბრის განჩინება N1გ/1497.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 6 სექტემბრის განჩინება N1გ/1430.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 30 მარტის განჩინება N1გ/548-16.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2016 წლის 24 თებერვლის განჩნება N1გ/272-16.
- თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის 2014 წლის 9 დეკემბრის განჩინება N1გ/1245.

უცხოენოვანი ნორმატიული მასალა

- Charter of Fundamental Rights of The European Union, 2012/C 326/02.
- Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), Strasbourg, 28/01/2003 < https://rm.coe.int/168008160f> [27.05.2023].
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [05.06.23].
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Directive for Police and Criminal Justice Authorities) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [05.06.23].
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058> [05.06.23].
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC >https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32006L0024> [05.06.23].
- Communication from The Commission to The European Parliament and The Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 2013. <https://eur-lex.europa.eu/resource.html?uri=cellar:551c0723-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF> [05.06.23].
- Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the

Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02000D0520-20000825> [05.06.23].

- Telecommunications Act 2003, 19.08.2003.
- German Code of Criminal Procedure, 07.04.1987.
- Telecommunications Act (TKG), 06.22.2004.
- Criminal Procedure Code of Austria, 30.12.1975.
- Federal Rules of Evidence, USA, 20.11.1972.
- Canada Evidence Act (RSC, 1985, c. C-5).
- Convention on Cybercrime, Budapest, European Treaty Series, 23.11.2001.
- International Covenant on Civil and Political Rights (ICCPR), 1966.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018.
- Explanatory report to the Convention on Cybercrime, European Treaty Series – No.185, 23/11/2001.
- Criminal Procedure Code of the Republic of Armenia, 01/09/1998.
- Code of Criminal Procedure of the Azerbaijan Republic, 14/07/2000.
- Criminal Procedure Code of Republic of Belarus, 16/07/1999.
- Law on the Internal Affairs Bodies of the Republic of Belarus, 17/07/2007.
- Decree of The President of The Republic of Belarus on measures to improve the use of the national segment of the internet, №60, 01/02/2010.
- Law on the prevention and fight agains crime in the field of computer information, №20, 03/02/2009.
- Criminal Procedure Code of The Republic of Moldova, №122, 14/03/2003.
- Criminal Procedural Code of Ukraine, BVR, 20/11/2012, Art. 159.
- Stored Communications Act, (SCA), 18 U.S.C, 21/10/1986.
- Electronic Communications Privacy Act (ECPA), 18 U.S.C, 21/10/1986.
- Wiretap Act, 18 U.S.C., 21/10/1986.
- 18 U.S.C. Federal Rules of Criminal Procedure, 26/12/1944.
- Criminal Code (R.S.C. 1985, c. C-46).

- Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, EDPS, 2017, 4 <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> [05.06.23].
- *Burchill J.,* Alibi Evidence: Responsibility for disclosure and investigation, Manitoba Law Journal, 2018, Vol. 41, Issue 3.
- *Capra D.,* Authenticating Digital Evidence, Baylor Law Review, vol.69(1), 2017.
- *Casey E,* "Digital Evidence and Computer Crime", 3rd Edition, USA, Academic Press, 2011.
- *Casey E.,* Digital Evidence and Computer Crime, 2nd edition, USA, Academic Press, 2004.
- *Casey E.*, Foundations of Digital Forensics, Digital Evidence and Computer Crime, 3rd ed., USA, Academic Press, 2011.
- *Colombo E.*, The Garlasco case and the digital alibi evidence: A difficult relationship between law and informatics, Digital Evidence and Electronic Signature Law Review, vol. 14, 2017.
- Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership, Council of Europe, 2018 <https://rm.coe.int/conditions-and-safeguards-under-article-15-of-the-convention-on-cyberc/16808f1e39> [03.06.23].
- Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime: Towards Common Guidelines, Council of Europe, 2020, 5. < https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7> [01.06. 2023].
- *Corstens G., Pradel J.*, European Criminal Law, The Hague, The Netherlands, Kluwer Law International, 2002.
- *Diana J. A., Esteban A. A., Guglielmo P. J., Hiser S. T., Kuckelman D., Mandel P. E., Opstnick M. T., Ragan R. C., Sharp C. D., Tully T. M.,,* The Sedona Principles, Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3th edition., The Sedona Conference Journal, Vol. 19, №1, 2018.

- *Degani M., Marion L.,* Making the Most of Your Statutory Electronic Evidence Toolbox, The United States Attorneys' Bulletin, Vol. 64, №3, 2016.
- *Dragicevic D., Juric M.,* Article-15 – Safeguards in the Eastern Partnership region, Council of Europe, 2013 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e5> [04.06.23].
- *Dysart E. J., Strange D.*, Beliefs about alibis and alibi investigations: A Survey of Law Enforecement, Psychology, Crime & Law, Vol. 18, Issue 1, 2012.
- *Fehr C.,* The Constitutionality of Using Production Orders to Obtain Stored Communication Content, Canadian Criminal Law Review 171, 2018.
- 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, 6. < https://rm.coe.int/general-report-on-mapping-the-current-strengths-weaknesses-opportuniti/16808f1e1b> [27.05.2023].
- *Goldfoot J.,* Compelling Online Providers to Produce Evidence under ECPA, Obtaining and Admitting Electronic Evidence, The United States Attorneys' Bulletin, Vol. 59, №6, 2011.
- *Gonzales R. A., Schofield B. R., Hagy W. D.*, Investigations Involving the Internet and Computer Networks, National Institute of Justice, USA, 2007.
- *Gonzales R.A., Schofield B.R., Hagy W.D.,* Digital Evidence in the Courtroom – A Guide for Law Enforcement and Prosecutors, NIJ, USA, 2007.
- *Goodison E. S., Davis C. R., Jackson A.B.*, Digital Evidence and U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, NIJ, USA, 2015.
- *Gregory D.J,,* Authentication rules and electronic evidence, The Canadian Bar Review, vol. 81(3), 2002.
- Handbook on European Data Protection Law, 2018, 44. <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> [05.06.23].

- *Mukasey B. M., Sedgwick L. J., Hagy W. D* Electronic Crime Scene Investigation: A Guide fo First Responders" 2nd edition, NIJ, 2008.
- *Hoffmeister A. T.,* Social Media in the Courtroom: A New Era for Criminal Justice?, USA, Praeger, 2014.
- *Harris D.J., O'Boyle M., Warbrick C., Buckley C., Kamber K.,* Law of the European Convention on Human Rights, London, Oxford University Press, 2018.
- *Johnson A.M.,* Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability, Marquette Law Review, vol. 75, 1992.
- *Jarret M. H., Bailie W. M., Hagen E., Judish N.*, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, USA, Office of Legal Education Executive Office for United States Attorneys, 2009.
- *Kerr S. O.,* A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 The George Washington Law Review 1208, 2004.
- *Kerr S. O.,* Searches and Seizures in a Digital World, Harvard Law Review, Vol. 119, 2006.
- *Kronke C.,* Data Regulation in the Internet of Things, Paradigms of Internet Regulation in the European Union and China, *Kronke, Muller, Yu, Tian,* (eds.), 2018.
- *Lloyd J. I.,* Privacy, technology and the law, Information Technology Law, 4th edition, Oxford University Press, 2004.
- *Mason S., Weir R.S. G.,* The sources of electronic evidence, Electronic Evidence, Mason. S., Seng D., (eds.), 4th edition, London, 2017.
- *Murdoch J.S., Seng D., Schafer B., Mason S.,* The sources and characteristics of electronic evidence and artificial intelligence, Electronic Evidence and Electronic Signature, *Mason. S., Seng D.*, (eds.) 5th edition, London, 2021.
- *Mason S.*, *Stanfield A.,* Authenticating electronic evidence, Mason S., Seng D., (eds.), 4th edition, London, 2017.
- *Moore D. A.,* Privacy Rights – Moral and Legal Foundations, USA, The Pennsylvania State University Press, 2021.
- *Murphy T., Cuinn O. G.,* Works In Progress: New Technologies and the European Court of Human Rights, Human Rights Law Review 10(4), 2010.

- Practical Guide on the Use of Personal Data in the Police Sector, Strasbourg, 2018, 5. <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> [05.06.23].
- Production Orders for Subscriber Information (Article 18 Budapest Convention), Cybercrime Convention Committee (T-CY), Council of Europe, 2017, 8. <https://rm.coe.int/16806f943e#:~:text=Article%2018%20%E2%80%93%20Production%20order&text=Under%20paragraph%201(a)%2C,that%20person's%20possession%20or%20control.> [01.06.23].
- *Riley J.,* Understanding Metadata, National Information Standards Organization, Baltimore, MD, 2017. <https://groups.niso.org/higherlogic/ws/public/download/17446/Understanding%20Metadata.pdf> [23/05.2023].
- Rules on Obtaining Subscriber Information, Adopted by T-CY at its 12th Plenary, 2014, 15-28. < https://rm.coe.int/16802e7ad1> [03.06.2023].
- *Schermer W. B.,* Surveillance and Privacy in the Ubiquitous Network Society*,* Amsterdam Law Forum, vol. 1, No. 4, 2009.
- *Sunde M. I.,* Cybercrime Law, Digital Forensics, *Arnes A. (eds.)*, Norway, John Wiley & Sons Ltd, 2018.
- *Schafer B., Mason S.*, The Characteristics of Electronic Evidence, Electronic Evidence, 4th edition., *Mason S., Seng D.* (eds.), London, 2017.
- *Stanfield R. A.,* The Authentication of Electronic Evidence, Queensland University of Technology, Australia, 2016 <https://eprints.qut.edu.au/93021/1/Allison_Stanfield_Thesis.pdf> [23.05.2023].
- Scientific Working Group on Digital Evidence (SWDGE), SWDGE Digital and Multimedia Evidence Glossary, 2016 <https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Digital-Multimedia-Evidence-Glossary-062316.pdf> [21.05.2023].
- *Tokson M.*, Automation and the Fourth Amendment, Iowa Law Review, Vol. 96, 2011.

- *Tokson M.,* The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021, Harvard Law Review, 2022.
- Understanding Cybercrime: Phenomena, challenges and legal response, 2012, 177. <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> [28.05.2023].
- *Walden I.*, Privacy and Data Protection, Computer Law –The Law and Regulation of Information Technology, 6th edition, *Reed C., Angel J.* (eds.), Oxford University Press, 2007.
- *Westin F. A.,* Information technology in a democracy, USA, Harvard University Press, 1971.
- *Warren S., Brandeis D. L.,* The Right to Privacy, Harvard Law Review 4, 1890.

უცხოური სასამართლო გადაწყვეტილებები

ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები

- *Mamaladze v. Georgia,* [2023] ECHR.
- *Adomaitis v. Lithuania,* [2022] ECHR.
- *Big Brother Watch and Others v. The United Kingdom,* [2021] ECHR.
- *Vavricka and Others v. The Czech Republic,* [2021] ECHR.
- *Beizaras and Levickas v. Lithuania*, [2020] ECHR.
- *Klaus Muller v. Germany,* [2020] ECHR.
- *Saber v. Norway,* [2020] ECHR.
- *Lopez Ribalda and Others v. Spain,* [2019] ECHR.
- *Liber v. France,* [2018], ECHR.
- *Benedik v. Slovenia*, [2018] ECHR.
- *Yonchev v. Bulgaria,* [2018] ECHR.
- *Denisov v. Ukraine,* [2018] ECHR.
- *Antovic and Mirkovic v. Montenego*, [2017] ECHR.
- *Barbulescu v. Romania*, [2017], ECHR.
- *Lebois v. Bulgaria*, [2017] ECHR.

- *Paradiso and Campanelli v. Italy,* [2017] ECHR.
- *Satakunnan Markkinaporssi OY and Satamedia OY v. Finland,* [2017] ECHR.
- *Orlandi and Others v. Italy*, [2017] ECHR.
- *Karabeyoglu v. Turkey,* [2016], ECHR.
- *Zakharov v. Russia,* [2015], ECHR.
- *Maximillian Schrems v. Data Protection Commissioner,* [2015] CJEU.
- *Fernandez Martinez v. Spain,* [2014] ECHR.
- *Khodorkovsky and Lebedev v. Russia,* [2013], ECHR.
- *Dordevic v. Croatia*, [2012] ECHR.
- *K. U. v. Finland,* [2009] ECHR.
- *Bykov v. Russia,* [2009] ECHR.
- *S. and Marper v. The United Kingdom,* [2008] ECHR.
- *Wieser and Bicos Beteiligungen GmbH v. Austria*, [2008] ECHR.
- *Iliya Stefanov v. Bulgaria*, [2008] ECHR.
- *Copland v. The United Kingdom*, [2007] ECHR.
- *Petri Sallinen and Others v. Finland*, [2005] ECHR.
- *Manon Harriet AALMOES and 112 Others v. The Netherlands,* [2004] ECHR.
- Peck v. The United Kingdom, [2003] ECHR.
- *Pretty v. The United Kingdom,* [2002] ECHR.
- *P.G and J.H v. The United kingdom*, [2001] ECHR.
- *Rotaru v. Romania*, [2000] ECHR.
- *Osman v. The United Kindgom*, [1998], ECHR.
- *Kopp. V. Switzerland,* [1998] ECHR.
- *Botta v. Italy,* [1998] ECHR.
- *Z v. Finland,* [1997] ECHR.
- *Halford v. The United Kingdom,* [1997] ECHR.
- *Kroon and Others v. the Netherlands*, [1994] ECHR.
- *Murray v. United Kingdom*, [1994] ECHR.
- *Costello-Roberts v. The United Kingdom,* [1993] ECHR.
- *Niemietz v. Germany,* [1992] ECHR.

- *Margareta and Roger Andersson v. Sweden,* [1992] ECHR.
- *B v. France,* [1992] ECHR.
- *Observer and Guardian v. United Kingdom*, [1991], ECHR.
- *Chappell v. United Kindgom,* [1989] ECHR.
- *Olsson v. Sweden,* [1988] ECHR.
- *Leander v. Sweden,* [1987] ECHR.
- *X and Y v. The Netherlands,* [1985] ECHR.
- *Malone v. The United Kingdom,* [1984] ECHR.
- *Silver v. United Kingdom*, [1983] ECHR.
- *Marckx v. Belgium,* [1979] ECHR.
- *Sunday Times v. United Kingdom,* [1979] ECHR.
- *Klass and Others v. Germany,* [1978] ECHR.
- *Handyside v. United Kingdom*, [1976] ECHR.
- *Golder v. United Kindgom,* [1975] ECHR.

ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებები

- *La Quadrature Du Net and Others v. Premier Ministre and Others,* C-511/18, C-512/18 and C-520/18, [GC], [2020], CJEU.
- *Tele2 Sverige AB* (C-203/15) *v Post- och telestyrelsen and Secretary of State for the Home Department (*C-698/15) *v Tom Watson and Others.* GC, [2016] CJEU.
- *Digital Rights Ireland Ltd* (C-293/12) *v. Minister of Communications, Marine and Natural Resources and Others and Kartner Landesregierung and Others* (C-594/12), GC, 2014.https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=511178 [05.06.23].
- *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* Opinion of Advocate General Cruz Villalon, [2011] CJEU.
- *Volker unda Markus Schecke GbR and Hartmunt Eifert v. Land Hessen,* [2010] CJEU.

ამერიკის შეერთებული შტატების სასამართლოების გადაწყვეტილებები

- *Facebook, Inc. V. Pepe,* A.3d. WL 1870591, (2020).
- *United States v. Spencer*, WL 1400401, N.D. Cal., (2018).
- *Carpenter v. United States*, 585 U.S. (2018).
- *United States of America v. Kim Dotcom,* US, №1:12CR3, (2012).
- *United States v. Williams,* 592 F.3d 511 (4th Cir. 2010).
- *United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009).*
- *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008).
- *United States v. Park,* 2007 WL 1521573 (N.D. Cal. 2007).
- *United States v. Grubbs, 547* U.S. 90 (2006).
- *Georgia v. Randolph*, 547 U.S. 103 (2006).
- *United States v. Morgan, 435 F.3d 660* (6th Cir. 2006).
- *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006).
- *United States v. Young,* WL 1302667, 13, (2006).
- *United States v. Riccardi, 405, F.3d 852, 862* (10th Cir. 2005).
- *Freedman v. America Online Inc.,* 325 F. Supp. 2d 638, 634 n.4 (E.D. Va. 2004).
- *United States v. Kimoana,* 383, F.3d 1215 (10th Circuit 2004).
- *United States v. Wong,* 334 F.3d 831, 838 (9th Cir. 2003).
- *R. v. Morgan,* N.J., 15, NLPC, (2002).
- *Trulock v. Freeh, 275 F.3d 391, 403* (4th Cir. 2001).
- *United States v. Allen*, 53 M.J. 402, 2000.
- *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
- *United States v. Barth*, 26 F. Supp. 2d (1998).
- *United States v. Pena,* 143 F.3d 1363, (10th Cir. 1998).
- *United States v. Smith, 27 F. Supp. 2d 1111* (C.D. I11. 1998).
- *United States v. Ortiz,* 84 F.3d 977, 984 (7th. Cir. 1996).
- *C.f. Brown v. Waddell*, 50 F.3d 285, 292 (4th. Cir. 1995).
- *United States v. Doe,* 61 F.3d 107-111 (1st Cir. 1995).
- *Steve Jackson Games, Inc. v. US Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993)

- *United States v. David,* 756 F. Supp. 1385 (1991).
- *United States v. Whitfield,* 939 F.2D 1071, 1075 (D.C. Cir. 1991).
- *Florida v. Jimeno,* 500 U.S. 248, 251, (1991).
- *Ilinois v. Rodriguez, 497* U.S. 177 (1990).
- *Horton v. California*, 496 U.S. 128, 136, (1990).
- *Illinois v. Gates*, 462, U.S. 213, 238, 1983.
- *Andresen v. Maryland, 427* U.S. 463, 482, n.11, 1976.
- *United States v. Matlock,* 415 U.S. 164 (1974).
- *Schneckloth v. Bustamonte,* 412 U.S. 218, 219 (1973).
- *Terry v. Ohio,* 392 U.S. 1 (1968).
- *Marron v. United States, 275,* U.S. 192, (1927).

კანადის სასამართლოების გადაწყვეტილებები

- *R. v. Vice Media Canada Inc.*, SCC 53, 3 S.C.R. 374, (2018).
- *Alberta (Attorney General) v. Provincial Court of Alberta*, ABQB 728, (2015).
- Re Subscriber Information, Alberta Provincial Court, ABPC 178, (2015).
- Winnipeg Police Service Officer (Re), MBPC 70, (2015).
- R. v. Rogers Communications Partnership, ONSC 3853, (2014).
- R. v. Nichols, No 6186, CarswellOnt 8225, (Ont. C.J.), (2004).

ირლანდიის სასამართლოების გადაწყვეტილებები

- *DPP v. Joseph O'Reilly, The Court of Criminal Appeal,* IECCA 18, (2009).

ადამიანის უფლებათა კომიტეტის გადაწყვეტილება

- *Toonen v. Australia,* Communication No. 488/1992, Human Rights Committee, (1992).

ვებ-რესურსები:

- აშშ-ს იუსტიციის ეროვნული ინსტიტუტის ოფიციალური ვებ-გვერდი, https://nij.ojp.gov/ [28.06.23].

- ევროპის საბჭოს ოფიციალური ვებ-გვერდი, https://www.coe.int/en/web/portal/home [28.06.23].
- ადამიანის უფლებათა ევროპული სასამართლოს ვებ-გვერდი, https://www.echr.coe.int/grand-chamber# [28.06.23].
- მართლმსაჯულების ევროპული სასამართლოს ოფიციალური ვებ-გვერდი, https://curia.europa.eu/jcms/jcms/j_6/en/ [28.06.23].
- ევროკავშირის ფუნდამენტურ უფლებათა სააგენტოს ოფიციალური ვებ-გვერდი, http://fra.europa.eu/en [28.06.23].
- ევროკავშირის ოფიციალური ვებ-გვერდი, https://eur-lex.europa.eu/homepage.html [28.06.23].
- საქართველოს პროკურატურის ოფიციალური ვებ-გვერდი, https://pog.gov.ge/ [28.06.23].
- ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ოფიციალური ვებ-გვერდი, https://tsu.ge/ [28.06.23].
- საქართველოს პარლამენტის ოფიციალური ვებ-გვერდი, https://parliament.ge/ [28.06.23].
- საქართველოს საკონსტიტუციო სასამართლოს ოფიციალური ვებ-გვერდი, https://www.constcourt.ge/ka [28.06.23].
- თბილისის სააპელაციო სასამართლოს ოფიციალური ვებ-გვერდი, http://www.tbappeal.court.ge/?category=g [28.06.23].
- პერსონალურ მონაცემთა დაცვის სამსახურის ოფიციალური ვებ-გვერდი, https://personaldata.ge/ka [28.06.23].
- ელექტრონული წიგნების პორტალი, https://www.lit.ge/eleqtronuli-wignebi/ [28.06.23].

სხვა წყაროები

- საქართველოს პარლამენტის ოფიციალური განცხადება ოფიციალური განცხადება <https://parliament.ge/media/news/the-meeting-of-the-legal-issues-committee-with-the-judge-of-the-federal-supreme-court-of-germany-regarding-the-legislative-changes-to-the-article-136-of-the-criminal-code-of> [28.06.23].

- საქართველოს პროკურატურის ოფიციალური განცხადება <https://pog.gov.ge/news/saqarTvelos-prokuraturis-gancxadeba-Tamar-bachaliashvilis-saqmeze> [28.06.2023].
- საქართველოს პროკურატურის ოფიციალური განცხადება <https://pog.gov.ge/news/saqa-1> [28.06.2023].

მუხლი 112. სასამართლოს განჩინებით ჩატარებული საგამოძიებო მოქმედება

3[1]. კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინებაში აგრეთვე აღნიშნული უნდა იყოს: ის ფიზიკური ან იურიდიული პირი, რომლისგანაც უნდა იქნეს გამოთხოვილი კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში არსებული ინფორმაცია (თუ მისი ვინაობა ცნობილია); გვარეობითი ნიშნის მიხედვით – ის კომპიუტერული სისტემა ან კომპიუტერულ მონაცემთა შესანახი საშუალება, საიდანაც უნდა იქნეს გამოთხოვილი კომპიუტერული მონაცემი; კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან გამოსათხოვი სავარაუდო დოკუმენტი ან ინფორმაცია; განჩინების გაუქმების ან შეცვლის მოთხოვნით სასამართლოსთვის მიმართვის უფლება; წინააღმდეგობის გაწევისას იძულების პროპორციული ზომის გამოყენების უფლება. კომპიუტერული სისტემიდან ან კომპიუტერულ მონაცემთა შესანახი საშუალებიდან დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინება (გარდა სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის ფარგლებში გაცემული განჩინებისა) ძალადაკარგულია, თუ ეს საგამოძიებო მოქმედება არ დაწყებულა 30 დღის ვადაში

136[1]. მონაცემთა დაცვის მოთხოვნა

1. თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი და არსებობს მისი განადგურების, დაკარგვის, დაზიანების ან შეცვლის საფრთხე, პროკურორი, დაცვის მხარე უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის 30 დღემდე ვადით უსაფრთხოდ შენახვის განჩინების გაცემის შუამდგომლობით. გადაუდებელი აუცილებლობის შემთხვევაში ამ მუხლით გათვალისწინებული საგამოძიებო მოქმედება შესაძლებელია ჩატარდეს პროკურორის დადგენილების საფუძველზე, ამ კოდექსის 112-ე მუხლის მე-5 ნაწილით განსაზღვრული წესით

2. ამ მუხლის 1-ლი ნაწილით განსაზღვრული შენახვის ვადა შესაძლოა 90 დღემდე გახანგრძლივდეს სასამართლო განჩინების საფუძველზე.

3. ამ მუხლის მე-2 ნაწილით გათვალისწინებულ საგამოძიებო მოქმედებაზე ვრცელდება ამ კოდექსის 111-ე, 112-ე და 134-ე მუხლების დებულებები.

მუხლი 136. დოკუმენტის ან ინფორმაციის გამოთხოვა

1. თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, პროკურორი, დაცვის მხარე უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით. გადაუდებელი აუცილებლობის შემთხვევაში ამ მუხლით გათვალისწინებული საგამოძიებო მოქმედება შესაძლებელია ჩატარდეს პროკურორის დადგენილების საფუძველზე, ამ კოდექსის 112-ე მუხლის მე-5 ნაწილით განსაზღვრული წესით.

1[1]. ნებისმიერი პირი, რომელსაც ამ მუხლის 1-ლი ნაწილის საფუძველზე ინფორმაციის ან დოკუმენტის გადაცემის ვალდებულება ეკისრება, უფლებამოსილია განჩინების ან/და დადგენილების გაცნობიდან 24 საათში სასამართლოს პრივილეგირებული ან/და გამჟღავნებისგან სხვაგვარად დაცული ინფორმაციის განადგურების მოთხოვნით მიმართოს.

1[2]. ამ მუხლის 1[2] ნაწილით გათვალისწინებულ შუამდგომლობას სასამართლო ამ კოდექსის 112-ე მუხლით დადგენილი წესით განიხილავს.

2. თუ არსებობს დასაბუთებული ვარაუდი, რომ პირი დანაშაულებრივ ქმედებას ახორციელებს კომპიუტერული სისტემის გამოყენებით, პროკურორი უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს მომსახურების მომწოდებლისაგან მომხმარებლის შესახებ არსებული ინფორმაციის გამოთხოვის განჩინების გაცემის შუამდგომლობით.

2[1]. მომსახურების მომწოდებლისგან მომხმარებლის შესახებ ინფორმაციის გამოთხოვა შესაძლებელია მომხმარებლის წერილობითი თანხმობით, მხარის შუამდგომლობის საფუძველზე სასამართლო განჩინებით ან/და გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის დადგენილების საფუძველზე, ამ კოდექსის 112-ე მუხლის მე-5 ნაწილით განსაზღვრული წესით.

3. ამ მუხლის მიზნებისათვის, მომხმარებლის შესახებ არსებული ინფორმაცია არის ნებისმიერი ინფორმაცია, რომელსაც მომსახურების მომწოდებელი ინახავს

კომპიუტერული მონაცემების ან ნებისმიერი სხვა ფორმით, რომელიც დაკავშირებულია მისი მომსახურების მომხმარებლებთან, განსხვავდება ინტერნეტტრაფიკისა და შინაარსობრივი მონაცემებისაგან 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, ანგარიშისა და გადასახადების შესახებ ინფორმაცია, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე;

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

[3[1]. დანაშაულის გამოძიების, სისხლისსამართლებრივი დევნისა და მართლმსაჯულების განხორციელების, აგრეთვე ამ კოდექსის 138[1] მუხლით გათვალისწინებული მიზნებისთვის ელექტრონული კომუნიკაციის კომპანიისგან დასაშვებია მხოლოდ იმ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემის გამოთხოვა, რომლის შენახვისთვის „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის 8[5] მუხლით დადგენილი ვადა გასული არ არის. *(ამოქმედდეს 2024 წლის 1 მარტიდან)*]

4. (ამოღებულია - 24.05.2022, №1575).

4[1]. ამ მუხლით გათვალისწინებულ საგამოძიებო მოქმედებაზე ვრცელდება ამ კოდექსის 111-ე, 112-ე, 134-ე, 143[7]-143[8] მუხლების დებულებები. სასამართლო ვალდებულია ამ კოდექსის 112-ე მუხლის მე-5 ნაწილით განსაზღვრული წესით ჩატარებული საგამოძიებო მოქმედების კანონიერების შემოწმებისას იმსჯელოს პრივილეგირებული ან კანონით დაცული ინფორმაციის/მასალის განადგურების თაობაზე.

4[2]. გამომძიებელი უფლებამოსილია „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით გათვალისწინებულ ელექტრონული კომუნიკაციის კომპანიას, რომელიც ახორციელებს მობილური საკომუნიკაციო ქსელებითა და

საშუალებებით უზრუნველყოფას ან/და მომსახურებას, წერილობით ან მობილური საკომუნიკაციო აღჭურვილობის მოძიების ერთიანი სისტემის საშუალებით წარუდგინოს მოთხოვნა დანაშაულის შესაძლო ჩადენის შედეგად დაუფლებული მობილური საკომუნიკაციო აღჭურვილობის აქტივაციის ფაქტის დაფიქსირების დაუყოვნებლივ შეტყობინების შესახებ და საჭიროების შემთხვევაში მისი ფუნქციონირების შეზღუდვის (ბლოკირების) დაუყოვნებლივ შეტყობინების თაობაზე. აღნიშნული ინფორმაციის მიღების შემთხვევაში პროკურორი ამ მუხლის პირველი ნაწილით დადგენილი წესით „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონით გათვალისწინებული ელექტრონული კომუნიკაციის კომპანიისგან გამოითხოვს ინფორმაციას სატელეფონო ნომრისა და მისი მფლობელის, მობილური საკომუნიკაციო აღჭურვილობის აქტივაციის ფაქტის დაფიქსირების დროისა და ადგილმდებარეობის შესახებ. გამომძიებლისა და პროკურორის მიერ ამ ნაწილით გათვალისწინებული მოთხოვნის ელექტრონული დოკუმენტის ფორმით წარდგენის შემთხვევაში ელექტრონული დოკუმენტის მთლიანობისა და წარმომავლობის უტყუარობის დასადასტურებლად საკმარისია მასზე კვალიფიციური ელექტრონული შტამპის დასმა.

5. ამ მუხლით გათვალისწინებული საგამოძიებო მოქმედების კონტროლსა და ზედამხედველობას პერსონალურ მონაცემთა დაცვის სამსახური ახორციელებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად.