ელექტრონული თვალთვალის კონტროლის ,როგორც საპოლიციო რეგულაციების სამართლებრივი პრობლემა

მინდაძე ომარი *– ასოცირებული პროფესორი, სამართლის დეპარტამენტი, აკაკი წერეთლის სახელმწიფო უნივერსიტეტი, ქუთაისი, საქართველო*
ოსიპოვა კაროლინა *– დოქტორანტი, სამართლის დეპარტამენტი, აკაკი წერეთლის სახელმწიფო უნივერსიტეტი, ქუთაისი, საქართველო*

Electronic Tracking Control as a Police Regulation of the Legal System

Mindadze Omari *– Associate Professor, Department of Law, Akaki Tsereteli State University, Kutaisi, Georgia*
Osipova Karolina *– Ph.D Student, Department of Law, Akaki Tsereteli State University, Kutaisi, Georgia*

Abstract

Introduction and aim: Introduction: Future lawyers training and education issues are related to the exact performance of current legislation requirements, because the current technical means of communication, it is clear that the issue of personal privacy faces new and difficult challenges. The reality is particularly acute in the field of criminal law. The aim of the research: Developing recommendations that should be considered to be able to maintain a balance between protecting human rights and privacy intact and preventing crime in a democratic society.
Research methodology: The novelty of the research: Teaching future lawyers and giving them a proper education in terms of supervision of electronic tracking. The methods of the research: Historical, statistical, logical and systematic studies.
Results and implications: In the process of electronic tracking several institutions involvement will ensure the effectiveness of the package of legislative changes, which introduce the concept of covert investigative activities.
Conclusion: In the study there are briefly discussed electronic tracking measures provided by the Criminal Code of the Republic of Georgia. During the survey revealed a major part of the problems, around which the research will be made on the following stage. The first issue that can cause a difference among opinions is whether the State Security Service has the exclusive right to use electronic tracking measures.

Keywords: electronic tracking, police regulation

შესავალი

კომუნიკაციის სფეროში დღეს არსებული ტექნიკური საშუალებებისა და მათი გამოყენების მასშტაბების გათვალისწინებით, ცხადი ხდება, რომ პირადი ცხოვრების ხელშეუხებლობის საკითხი დღითიდღე ახალი და რთული გამოწვევების წინაშე დგება.არსებული რეალობა განსაკუთრებით მწვავედ სისხლის სამართლის სფეროში იჩენს თავს. სამართალდამცავ სფეროში პერსონალურ მონაცემთა დაცვის უფრო მაღალი სტანდარტის დანერგვის მიზნით, 2014 წელს მიღებულ იქნა საკანონმდებლო ცვლილებათა პაკეტი,[1] რომელსაც უნდა განეხორციელებინა ე.წ. ,,ფარული მოსმენებისა“ და კომუნიკაციის მაიდენტიფიცირებელ მონაცემებთან წვდომის საკითხების მოწესრიგება.მართალია, ელექტრონული თვალთვალის სფეროში აღნიშნულმა რეფორმამ რიგი პროგრესული დებულებები გაითვალისწინა, თუმცა, სამართალდამცველთა მხრიდან, მობილური ოპერატორების სერვერებზე პირდაპირმა წვდომამ, მნისვნელოვნად განაპირობა განხორციელებული საკანონმდებლო ცვლილებების უარყოფითი გავლენა პრაქტიკაზე. კერძოდ, ცვლილებებმა ელექტრონული თვალთვალი,ოპერატიულ-სამძებრო საქმიანობის ნაცვლად,სისხლის სამართლის პროცესისათვის დამახასიათებელ უფრო მაღალ გარანტიებს დაუქვემდებარა; პერსონალურ მონაცემთა დაცვის ინსპექტორს მიენიჭა თვალთვალზე

[1] http:parliament.ge/#law-drafting [04.06.2016]

წინასწარი და შემდგომი კონტროლის განხორციელების მანდატი. მიუხედავად აღნიშნულისა, 2016 წლის საკონსტიტუციო სასამართლოს გადაწყვეტილებამ[2]კიდევ ერთხელ დაადასტურა,რომ მოდელი, რომელიც 2014 წლის საკანონმდებლო ცვლილებათა პაკეტმა გაიზიარა, არ ითვალისწინებდა, ადამიანის უფლებათა კუთხით, დაცვის ეფექტურ მექანიზმს.მიღებული ნორმების არაკონსტიტუციურობა ერთდროულად რამოდენიმე ფაქტორმა განაპირობა.კერძოდ,საგამოძიებო ფუნქციების მქონე და, შესაბამისად, უშუალოდ დაინტერესებული ორგანოს ხელში შეუზღუდავი ტექნიკური შესაძლებლობების თავმოყრამ, თვითნებობის დიდი საფრთხე წარმოშვა, აღნიშნულ პირობებში კი პერსონალურ მონაცემთა დაცვის ინსპექტორის ჩართულობა ფარული მიყურადება - ჩაწერის პროცესში ფორმალური ხასიათის მატარებელი გახდა. ნორმათა არაკონსტიტუციურობისა და კრიტიკის დამატებით საფუძვლათ ინტერნეტით გადაცემულ მონაცემთა მოპოვებაზე კონტროლის არარსებობა დასახელდა.

ზემოაღნიშნულიდან გამომდინარე, საკითხის კვლევა და იმის დადგენა, თუ რა ნაკლოვანებები არსებობს ელეკრტონული თვალთვალის განხორციელების, მასზე ზედამხედველობისა და კონტროლის პროცესში აქტუალურია იმდენად, რამდენადაც იგი ყველაზე მეტად უქმნის საფრთხეს კონსტიტუციით, ევროპული კონვენციითა და სხვა საერთაშორისო აქტებით აღიარებულ პირადი ცხოვრების ხელშეუხებლობის უფლებას. გასათვალისწინებელია, ასევე, საქართველო-ევროკავშირის ასოცირების ხელშეკრულებით[3] საქართველოს მიერ აღებული ვალდებულებაც, მოახდინოს პერსონალური მონაცემების დაცვა ევროპული სტანდარტების შესაბამისად.ევროკავშირში საქართველოს სამომმავლო წევრობის საკითხი,სხვა ძირითად თემებთან ერთად, სწორედ პერსონალური მონაცემების მაღლი სტანდარტებით დაცვასთან არის დაკავშირებული.

მოცემული ნაშრომის კვლევის ობიექტს საპოლიციო საქმიანობის სპეციფიკური სფერო-ელექტრონული თვალთვალი წარმოადგენს, ხოლო, კვლევის უშუალო საგნად მის განხორციელებაზე საქართველოში არსებული ზედამხედველობისა და კონტროლის საკანონმდებლო მექანიზმები განიხილება.

ნაშრომის ამოცანაა,ერთი მხრივ, კანონმდებლობაში არსებული ხარვეზებისა და ნაკლოვანებების გამოვლენა,ხოლო ,მეორე მხრივ- ევროპის განვითარებული ქვეყნების მასშტაბით,ამ კუთხით არსებული პრაქტიკის ანალიზი.თანამედროვე მზარდი და განვითარებადი ტექნოლოგიების პირობებში, ბუნებრივია, კანონის გვერდის ავლით ფარული ღონისძიებების განხორციელების საფრთხე ყოველთვის იარსებებს და სისტემის შექმნა, რომელმაც შეიძლება უზრუნველყოს ამ საფრთხისაგან აფსოლუტური დაცვა,შეუძლებელია.თუმცა, მოდელი, რომელიც ითვალისწინებს შესაბამისი უწყებებისათვის ელექტრონული თვალთვალის განხორციელების ექსკლუზიუზი უფლებამოსილების მინიჭებას, ამავე დროულად უნდა ახთენდეს, როგორც ადამიანის უფლებების, ისე ეროვნული უსაფრთხოების თვალსაზრისით არსებული რისკების მინიმალიზებას. სამაგისტრო ნაშრომის საბოლოო მიზანს, სწორედ, იმ რეკომენდაციების შემუშავება წარმოადგენს, რომელთა გათვალისცინებაც შეძლებს შეინარჩუნოს ბალანსი, ერთი მხრივ, ადამიანის პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვასა და მეორე მხრივ- დემოკრატიულ საზოგადოებაში დანაშაულის პრევენციის ლეგიტიმურ მიზანს შორის.

ზემოაღნიშნული მიზნის მისაღწევად, ნაშრომის სიახლეს წარმოადგენს ზედამხედველობის საკითხის კომპლექსური განხილვა.იგი გულისხმობს კონტროლის განხორციელებას არა ერთი,

[2] საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება საქმეზე №1/1/625/640

[3] ასოცირების შესახებ შეთანხმება ერთის მხრივ , ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებსა და მეორე მხრივ, საქართველოს შორის.

არამედ რამოდენიმე ინსტიტუტის მეშვეობით, კომბინირებულად. ნაშრომის ძირითადი ჰიპოტეზაც სწორედ იმაში მდგომარეობს, რომ ელექტრონულ თვალთვალზე კონტროლის პროცესში ერთდროულად რამოდენიმე დაწესებულების ჩართულობაა, მის ეფექტურობას უზრუნველყოფს.

კვლევის სირთულეს წარმოადგენს გარემოება იმის შესახებ, რომ საკანონმდებლო ცვლილებების პაკეტი ,რომლითაც შემოღებულ იქნა ფარული საგამოძიებო მოქმედების შესახებ კონცეფცია,სულ ახლახანს ,2014 წელს იქნა მიღებული და შესაბამისად, ელექტრონული თვალთვალის, როგორც საგამოძიებო მოქმედების შესახებ კვლევას, თანამედროვე სამეცნიერო ლიტერატურა არ იცნობს.

ელექტრონული თვალთვალი და მისი განხორციელების მეთოდები

კომუნიკაციის სფეროში დღეს არსებული ტექნოლოგიური მიღწევებისა და ზოგადად, ტექნოლოგიური პროგრესის გასაოცარი ტემპების გათვალისწინებით, ელექტრონული საშუალებებით თვალთვალი დანაშაულთან ბრძოლის ერთ-ერთ ყველაზე ქმედით და ეფექტურ მექანიზმად გვევლინება.დანაშაულთან ბრძოლის აღნიშნული მექანიზმის სამართლებრივ რეგულირებას სსსკ-ი ახდენს 2014 წლამდე იგი ოპერატიული საქმიანობის ნაწილად მოიაზრებოდა.2014 წლის 30 ნოემბრის საკანონმდებლო ცვლილების შემდეგ კი ელექტრონული თვალთვალი სსსკ-ის ჩარჩოებში მოექცა.სამართლებრივი რეგულაციების არსებითი ცვლილება პერსონალურ მონაცემებზე წვდომის ეფექტიანი ზედამხედველობის სისტემის ჩამოყალიბების მიზნით [4] იქნა განპირობებული.

1.1 ძირითადი ცნებები

საზღვარგარეთის ქვეყნებში დამკვიდრებული პრაქტიკის შესაბამისად ელექტრონული საშუალებით, ძირითადად, დაინტერესების ობიექტის ფარულ აუდიო თუ ვიდეო ჩაწერას, მისი ადგილ-სამყოფლის ამოცნობასა და, კომპიუტერული სისტემების მონიტორინგს გულისხმობს.[5] თუმცა,დასახელებული არ მოიცავს ღონისძიებათ სრულ ჩამონათვალს, რადგან ელექტრონული თვალთვალის საშუალებები ტექნოლოგიური განვითარების პარალელურად ვითარდება.ვინაიდან, სამაგისტრო ნაშრომის ფარგლებში ელექტრონული თვალთვალის მხოლოდ გარკვეული ნაწილი გახდა კვლევის უშუალო საგანი, მოცემული ქვეთავიც სსსკ-ით გათვალისწინებულ რელევანტურ ღონისძიებებს მიმოიხილავს.

1.1.1 სატელეფონო საუბრის ფარული მიყურადება და ჩაწერა

სსსკ-ის 143[1]-ე მუხლი ამომწურავად განსაზღვრავს ფარული საგამოძიებო მოქმედებების სახეებს. პირველ მათგანს სატელეფონო საუბრების ფარული მიყურადება -ჩაწერა წარმოადგენს.ნორმით გათვალისწინებული სატელეფონო საუბრის ქვეშ, პირის მიერ ნებისმიერი სახის ტელეფონით განხორციელებული კომუნიკაცია იგულისხმება.[6] მიუხედავად იმისა, რომ სატელეფონო თუ სხვა საშუალებებით ნებისმიერ ადამიანთნ ურთიერთობა /კომუნიკაცია, პირადი ცხოვრების ცნებიდან არის ნაწარმოები, საქართველოს კონსტიტუციის მე-20 მუხლის პირველ პუნქტში იგი ცალკეა გამოყოფილი.აღნიშნული კიდევ ერთხელ ადასტურებს ინდივიდის იზოლირებული სფეროს

[4] განმარტებითი ბარათი ,, საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილებების შეტანის შესახებ“ საქართველოს კანონის პროექტზე გვ.1

[5] საქართველოს პარლამენტი.კვლევითი დეპარტამენტი . კანონშემოქმედებითი საქმიანობის საინფორმაციო უზრუნველყოფის განყოფილება. ფაქტობრივი ცნობა. მიყურადებისა და კავშირგაბმულობის არხებიდან ინფორმაციის მოხსნის საკანონმდებლო რეგულირების მექანიზმები საზღვარგარეთის ქვეყნებში 25.11.2014

[6] ფაფიაშვილი ლ., თუმანიშვილი გ., კვაჭანტირაძე გ., ლიპარტელიანი ლ., დადეშქელიანი გ., გუნცაძე შ., მეზვრიშვილი ნ., თოლორაია ლ., საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი 2015 წლის 1 ოქტომბრის მდგომარეობით. გამომცემლობა ,, მერიდიანი“ . თბილისი 2015 გვ. 427

(პირადი ცხოვრების) ამ ინსტიტუტის განსაკუთრებულ მნიშვნელობას.სსსკ-ის 143[1]-ე მუხლის პირველი ნაწილის ,,ა“ ქვეპუნქტიტ გათვალისწინებული ზემოაღნიშნული ღონისძიება მხოლოდ ვერბალური ფორმით განხორციელებული კომუნიკაციის მიყურადებასა და ჩაწერას გულისხმობს.იგი არავერბალური ფორმით განხორცილებული კომუნიკაციის მონიტორინგს არ მოიცავს.

1.1.2 ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან ან/და კომპიუტერული სისტემიდან

სსსკ-ის 143[1]-ე მუხლის პირველი ნაწილის ,,ბ“ ქვეპუნქტში მოცემული ფარული საგამოძიებო ღონისძიება ითვალისწინება ინფორმაციის მოხსნასა და ფიქსაციას კავშირგაბმულობის არხიდან ან/და კომპიუტერული სისტემიდან. კავშირგაბმულობის არხის ქვეშ ნორმა მოიაზრებს კომპიუტერულ ქსელებს, კავშირგაბმულობის საშუალებებს, სახაზო კომუნიკაციებსა და სასადგურო აპარატურას .[7]თუმცა უფრო გასაგებად, ღონისძიება ეხება თანამედროვე საკომუნიკაციო საშუალების, მათ შორის ინტერნეტის მეშვეობით გადაცემული ინფორმაციის მოპოვებასა და ფიქსაციას.სსსკ-ის მე-3 მუხლის 27-ე პუნქტში მოცემული განმარტების მიხედვით კომპიუტერულ სისტემას წარმოადგენს პერსონალური კომპიუტერი, მობილური ტელეფონიდა სხვა ნებისმიერი მოწყობილობა მიკროპროცესორით, რომელიც ახდენს ინფორმაციის ავტომატურ დამუშავებას.განსახილველი საგამოძიებო მოქმედება ითვალისწინებს კომპიუტერულ სისტემაში ან/და კავშირგაბმულობის სხვა საშუალებებში არსებული ინფორმაციის მონიტორინგსა და ფიქსაციას.აღნიშნული შეიძლება მიღწეულ იქნეს, როგორც უშუალოდ, ისე დისტანციურად. ეს უკანასკნელი გულისხმობს კომპიუტერულ სისტემებში ვირუსული პროგრამების ინსტალაციას.[8]

1.1.3 ელექტრონული კომუნიკაციების მაიდენტიფიცირებელი მონაცემების კოპირება

ელექტრონული კომუნიკაციების მაინდენტიფიცირებელი მონაცემების კოპირებას, როგორც ცალკე აღებულ საგამოძიებო ღონისძიებას, სსსკ-ი არ იცნობს. ქმედების შინაარსის განმარტება მიზანშეწონილია, რამდენადაც მონაცემების კოპირება შესაბამისი უწყების მხრიდან, სსსკ-ით გათვალისწინებული ფარული საგამოძიებო მოქმედებების უზრუნველყოფის საშუალებას წარმოადგენს.

ელექტრონული კომუნიკაციების მაინდენტიფიცირებელი მონაცემების ქვეშ კომუნიკაციის შინაარსის გარდა მასთან დაკავშირებული სხვა ნებისმიერი სახის ინფორმაცია მოიაზრება.[9] ეს შეიძლება იყოს მონაცემები ამასთან დაკავშირებით თუ ვინ, ვის, როდის, რა ტექნიკური საშუალებით, რომელი ლოკაციიდან და როგორი ხანგრძლივობით დაუკავშირდა.[10] ოტო-ს ,რომელსაც პირდაპირი წვდომა გააცჰნია საკომუნიკაციო მომსახურეობის მიმწოდებელი კომპანიების ქსელზე პირთა წრისა და ლოკაციის თვალსაზრისით შეუზღუდავად მოახდინოს ინფორმაციის კოპირება და შენახვა.თუმცა, ნორმა, რომელიც შესაბამის ამის უფლებამოსილებას ანიჭებს ,იმავდროულად განსაზღვრავს კოპირებულ მონაცემებზე წვდომის წესებს.[11]

---

[7] საქართველოს სისხლის სამართლი საპროცესო კოდექსი.143[1]-ე მუხლის პირველი ნაწილის ,, ბ“ ქვეპუნქტი

[8] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება, II-73

[9] საქართველოს კანონი ,, ელექტრონული კომუნიკაციების შესახებ“ . 1-ლი მუხლის 1-ლი პუნქტის ჰ[62]-ე ქვეპუნქტი

[10] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1.1.6256640 გადაწყვეტილება , II-91

[11] საქართველოს კანონი ,, ელექტრონული კომუნიკაციების შესახებ“. მე-8[3]-ე მუხლის 1-ლი პუნქტი

იმის გათვალისწინებით ,რომ მეტადატას[12] ანალიზი ინდივიდის შესახებ მნიშვნელოვან ინფორმაციას[13] გვაწვდის, მაიდენტიფიცირებელი მონაცემების კოპირება გამოძიებისათვის რელევანტური მტკიცებულებების მოპოვების ძლიერი მექანიზმია .

1.2 ელექტრონული თვალთვალის განხორციელებაზე უფლებამოსილი ორგანოები

სსსკ-ის მე-3 მუხლის 32-ე პუნქტის მიხედვით,ელექტრონული თვალთვალის განხორციელებაზე უფლებამოსილ ორგანოს სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური დეპარტამენტი წარმოადგენს.დეპარტამენტი, ფარული საგამოძიებო მოქმედებების კონცეფციის ჩამოყალიბების პერიოდში შსს-ს შემადგენლობაში შედიოდა, თუმცა მისი გადასვლა სახელმწიფო უსაფრთხოების სამსახურში, 2015 წელს, ამ უკანასკნელის ცალკე, დამოუკიდებელი უწყების სახით ჩმოყალიბებამ განაპირობა, ორგანიზაციული გამიჯვნის საფუძველს ,საპოლიციო და სახელმწიფო უსაფრთხოების ფუნქციების შესრულების ეფექტიანობის უზრუნველყოფა წარმოადგენდა.[14] მიუხედავად აღნიშნულისა, დღეს არსებული მდგომარეობით შსს-ს შენარჩუნებული აქვს ელექტრონული თვალთვალის უფლებამოსილება, თუმცა ამ შემთხვევაში იყენებს ოტო-ს ტექნიკურ მომსახურებას. ოტო ტექნიკურ მომსახურებას უწევს არა მხოლოდ შსს-ს ,არამედ ყველა სხვა სამინისტროს საგამოძიებო სამსახურს, რომელიც მის ქვემდებარეობას მიკუთვნებული დანასაულის გამოძიებისას იყენებს სსსკ-ით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას, ასევე ოპერატიულ -სამძებრო საქმიანობის განმახორციელებელ ორგანოებს - ,,ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-3 პუნქტით გათვალისწინებულ შემთხვევებში.

სუს-ს ,რომლის ძირითად ფუნქციასაც დღეს, სახელმწიფო უსაფრთხოების დაცვა წარმოადგენს, მინიჭებული აქვს ,როგორც ანალიტიკური, ისე საგამოძიებო საქმიანობის წარმოების უფლება-მოსილება .[15] ამასთან, მის მიერ ანალიტიკური მიზნებისათვის ელექტრონული თვალთვალის განხორციელება არ საჭიროებს იმ სტანდარტების დაცვას,რასაც სსსკ-ი ადგენს. მაგალითად, ელექტრონული თვალთვალის განხორციელების საფუძველი შეიძლებ აიყოს მონაცემები ფაქტებისა და მოვლენების შესახებ, რომელიც საფრთხეს უქმნის ქვეყნის უსაფრთხოებას.[16] ამ შემთხვევაში უწყების ხელმძღვანელი სასამართლოსათვის შუამდგომლობით მიმართვისას ,[17] არ არის ვალდებული ზემოაღნიშნული მონაცემების არსებობის დასადასტურებლად, წარადგინოს დასაბუთებული ვარაუდის სტანდარტით გათვალისწინებული მტკიცებულებები. ამასთან, ზოგ შემთხვევაში, იგი უფლებამოსილია სასამართლოს გადაწყვეტილების გარეშეც მოახდინოს სატელეფონო საუბრების ფარული მიყურადება და ჩაწერა,[18] აღნიშნული თავისთავად ქმნის საფრთხეს იმისა, რომ სუს-მა ანალიტიკური მიზნებისათვის დაიწყოს ინფორმაციის მიღება, თუმცა მისი გამოყენება რადიკალურად განსხვავებული, საგამოძიებო მიზნების მისაღწევად მოახდინოს. გასათვალისწინებელია ისიც, რომ უსაფრთხოების სამსახურის საქმიანობის სამსახურის სპეციფიკიდან გამომდინარე, მასზე არ ვრცელდება გამჭვირვალობის ის სტანდარტი ,რაც

---

[12] ინფორმაცია მობილური სატელეფონო საშუალებების ადგილმდებარეობის , განხორციელებული თუ შემოსული ზარების , ღიად თუ ანონიმურად განხორციელებული ძიებისა თუ სხვა ონლაინ ქმედებებთან დაკავშირებით.

[13] ინდივიდის ქცევა , სოციალური ურთიერთობები , პირადი მახასიათებლები

[14] განმარტებითი ბარათი ,, სახელმწიფო უსაფრთხოების სამსახურის სამსახურის შესახებ „ საქართველოს კანონის პროექტზე

[15] საქართველოს კანონი ,, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის შესახებ“. მე-11 მუხლი

[16] საქართველოს კანონი კონტრდაზვერვითი საქმიანობის შესახებ. მე-10 მუხლი ,, ა“ პუნქტი

[17] იხ. იქვე მე-12 მუხლი

[18] იხ. იქვე მე-15 მუხლი

მაგალითად შსს-ს შემთხვევაში გვაქვს. აღნიშნულზე უფრო დაწვრილებით მომდევნო თავებში ვისაუბრებთ.

1.3 ელექტრონული თვალთვალის განხორციელების მეთოდები და მიზნები

სსსკ-ის 143[1]-ე მუხლის პირველი ნაწილის ,,ა“ და ,,ბ“ ქვეპუნქტებით გათვალისწინებული საგამოძიებო მოქმედებების განხორციელების მეთოდები განსაზღვრულია ,,ელექტრონული კომუნიკაციის შესახებ“ საქართველოს კანონის მე-8[3]-ე მუხლით. კომუნიკაციის ხაზებზე წვდომის წვდომის მოქმედი მოდელის შესაბამისად, ინფორმაციის რეალურ დროში მოპოვების ტექნიკურ აღჭურვილობას ფლობს საგამოძიებო ფუნქციების მქონე სახელმწიფო უწყება.[19] იგი უფლებამოსილია, საკომუნიკაციო ხაზებთან ჰქონდეს, აღნიშნული ტექნიკური აღჭურვილობით პირდაპირი მიერთების შესაძლებლობა, სატელეფონო საუბრების ფარული მიყურადება-ჩაწერისათვის ტექნიკური აღჭურვილობის გააქტიურება საჭიროებს ,დამატებით, პერსონალურ მონაცემთა დაცვის ინსპექტორის ელექტრონულ თანხმობას. ე.ი.პმდი-ს ელექტრონული თანხმობის გარეშე შესაბამისი ორგანოსათვის შეუძლებელი უნდა აღმოჩნდეს სატელეფონო საუბრების ფარული მიყურადება და ჩაწერა, თუმცა, ქსელებთან განთავსებულია აპარატურაც ,რომელზე კონტროლი ინსპექტორის კომპეტენციაში არ შედის, აღნიშნული, ქმნის საფრთხეს, რომ ელექტრონულ კომუნიკაციებთან დაკავშირებული მონაცემები სახელმწიფომ ინსპექტორის გვერდის ავლით, პარალელური ინფრასტრუქტურის გამოყენებით შეიძლება მოიპოვოს .

სსსკ-ის 143[1]-ე მუხლის ,,ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიების უზრუნველსაყოფად, ოტო ინფორმაციას, ზემოხსენებული ტექნიკური აღჭურვილობის გამოყენებით, კოპირებულ მონაცემთა ბანკებიდან იღებს. მონაცემთა ბანკებში განხორციელებული აქტივობის კონტროლს კი პმდი-ი ახდენს. თუმცა აქვე უნდა აღნიშნოს, რომ სერვისპროვაიდერებთან განთავსებული პარალელური ინფრასტრუქტურა ქმნის ალტერნატიული მონაცემთა ბანკების ფორმირების საფრთხეს, ამ უკანასკნელზე პმდი-ის კონტროლს კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ“ არ ითვალისწინებს, იმის გათვალისწინებებით ,რომ მოხსნასა და ფიქსაციას შეიძლება დაექვემდებაროს, არა მხოლოდ კომუნიკაციის მაინდენტიფიცირებელი, არამედ ინტერნეტით გადაცემული მონაცემების შინაარსიც, საგამოძიებო მოქმედების განხორციელებისათვის სახელმწიფო უწყებას მუდმივი მიერთების სისტემა ინტერნეტპროვაიდერებთანაც გააჩნია, [20] თუმცა, სისტემის გამოუსადეგარობის გამო, რეალურად ე.წ. ,,დავირუსების“ ტექნიკა გამოიყენება. [21] ამ შემთხვევაში გაუგებარი რჩება ინტერნეტპროვაიდერებთან ტექნიკური აღჭურვილობის განთავსების მიზანი .

ელექტრონული თვალთვალის მიზნებისაგან [22] დამოუკიდებლად, მისი განხორციელების მეთოდები იდენტურია. კერძოდ, სახელმწიფო უწყებას, ყველა ზემოდ განხილულ შემთხვევაში ,პირდაპირი წვდომა აქვს ელექტრონული კომუნიკაციის შინაარსსა, თუ მასთან დაკავშირებულ სხვა მონაცემებზე. [23] ამასთან, ელექტრონული კომუნიკაციების კომპანიებისათვის უცნობი რჩება ფაქტი იმის შესახებ, თუ როდის და რა სახის ინფორმაცია მიაქვს საგამოძიებო უწყებას, კანონი ან უკანასკნელს აკისრებს ვალდებულებას იქონიოს განხორციელებული კომუნიკაციის შინაარსისა და მისი მაიდენტიფიცერებელი მონაცემების უფლებამოსილი ორგანოსათვის რეალურ დროში

[19] საქართველოს სისხლის სამართლის საპროცესო კოდექსი . მე-3 მუხლის 32-ე პუნკტი

[20] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1.1.625ნ640 გადაწყვეტილება , II-73

[21] იხ. იქვე , II-73

[22] მიზნები განისაზღვრება იმის მიხედვით , თუ რომელი უწყება აწარმოებს ელექტრონულ თვალთვალს

[23] მეტადატა- ელექტრონული კომინიკაციების მაიდენტიფიცირებელი მონაცემები

მიწოდების ტექნიკური შესაძლებლობა. [24] სისტემის ფუნქციონირება, რომლიც მეშვეობითაც ოტო ელექტრონნული კომუნიკაციების კომპანიებიდან ინფორმაციის ამოღებას ახდენს, ამ უკანასკნელის მონაცილეობას არ საჭიროებს.

ფარული საგამოძიებო მოქმედების, მათ შორის ელექტრონული თვალთვალის განხორცილებეის მიზნები ამომწურავადაა ჩამოთვლილი სსსკ-ის 143[3] -ე მუხლის პირველი ნაწილის ,,გ“ ქვეპუნქტში, ესენია : ეროვნული უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფა ; უწესრიგობის ან დანაშაულის ჩადენის თავიდან აცილება; ქვეყნის ეკონომიური ქეთილდღეობის ინტერესების ან სხვა პირთა უფლებებისა და თვისუფლებების დაცვა, გარდა აღნიშნულისა, ელექტრონული თვალთვალი, როცა იგი კონტრდაზვერვითი საქმიანობის ფარგლებში წარმოებს, სულაც არ ატარებს სამართალდაცვით მიზნებს და ემსახურება სახელმწიფო უსაფრთხოების უზრუნველსაყოფად სადაზვერვო ან/და ტერორისტული საქმიანობის შესახებ ინფორმაციის მოპოვება, დამუშავებასა და განზოგადებას. იმის მიხედვით, თუ რა მიზანი აქვს ელექტრონული თვალთვალის განხორციელებას, მისი ჩატარების წესი და საფუძვლები სხვადასხვაა, რაზეც ზემოთ უკვე ვგქონდა საუბარი,

დასკვა

წინამდებარე თავის ფარგლებში მოკლედ იქნა განხილული ელექტრონნული თვალთვალის, სსსკ-ით გათვალისწინებული ღონისძიებები, განხილვის პროცესში გამოიკვეთა პრობლემათა ის ძირითადი ნაწილი, რომლის გარშემო კვლავაც სამაგისტრო ნაშრომის მომდევნო თავებში იქნება განვითარებული, პირველი საკითხი, რომელმაც შეიძლება გამოიწვიოს აზრთა სხვადასხვაობა, იმაში მდგომარეობს, უნდა ქონდეს თუ არა სუს-ს ელექტრონულ თვალთვალს მიკუთვნებული ღონისძიებების განხორციელების ექსკლუხიური უფლებამოსილე, საკითხის პრობლემურობას განაპირობებს ყველა ის ზემოთჩამოთვლილი გარემოება, რაზეც მეორე ქვეთავის ფარგლებში იყო საუბარი (სუს-ის საქმიანობის გამჭირვალობის არასაკმარისი სტანდარტები ; უწყების პროფესიული დაინტერესება, ფლობდეს ადამიანების შესახებ პირადად ინფორმაციას ; ელექტრონულ კომუნიკაციებზე წვდომის მეთოდები). ცალსახად მტკიცება იმისა, რომ კანონის გვერდის ავლით ელექტრონული თვალთვალის განხორციელების რისკების მინიმალიზება, სახელმწიფო უსაფრთხოების სამსახურისათვის, ზემოაღნიშნული ექსკლუზიური უფლებამოსილების ჩამორთმევიტ იქნება შესაძლებელი, დაუშვებელია, მით უფრო, როცა ქვეყანა ოკუპაციის პირობებში იმყოფება სახელმწიფო საზღვრებს გარედან მომდინარე საფრთხეების რაოდენობა დიდია. სახელმწიფოებრივი ინტერესი მოითხოვს, რომ კონტრსადაზვერვო საქმიანობის გამახორციელებელი უწყებები სხელმწიფო უსაფრთხოების დაცვისათვის ეფექტური მექანიზმებით იყვნენ აღჭურვილნი, სახელმწიფო უსაფრთხოება თითოეული მოქალაქის ინტერესს წარმოადგენს, თუმცა რამდენადაც უსაფრთხოება კანონის გარეშე არ არსებობს, ხოლო კანონი ადამიანისა და მისი ფუნდამეტური უფლებების დაცვის გარეშე, საკითხი დეტალურ კვლევას მოიტხოვს .[25]

სსსკ-ის 143[1]- ე მუხლის ,,ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიებების უზრუნველსაყოფად, როგორც აღინიშნა, შესაბამისი ორგანო ინფორმაციას იღებს მის მიერვე შექმნილი ე.წ. მონაცემთა ბანკებიდან, მასთან მიმართებით პრობლემას შემდეგ გარემოებათა ერთობლიობა განაპირობებს : მონაცემთა ბანკები იქმნება სასმართლოს გადაწყვეტილების გარეშე ; მათ შექმნაში არ მონაწილეობს პმდი-ი ; პმდი-ი სპეციალური ელექტრონული სისტემის მეშვეობით, მართალია, აკონტროლებს ბანკებში განხორციელებულ აქტივობას, თუმცა

[24] საქართველოს კანონი ,, ელექტრონნული კომუნიკაციების შესახებ“ . მე-8[1] მუხლი
[25] საკითხის დეტალური შესწავლა დარჩენილი თავების ფარგლებში მოხდება

რამდენადაც იგი უშუალოდ არ მონაწილეობს ბანკების ფორმირებაში, აღნიშნული ქმნის ე.წ. ალტერნატიული ბანკების ფორმირების რისკს;

პირველი თავის ფარგლებში დასმულ მომდევნო პრობლემურ საკითხს ინტერნეტპროვაიდერებთან სუს-ის მიერ განთავსებული ტექნიკური ინფრასტრუქტურა წარმოადგენს. იმ ვითარებაში, როცა ოტო ინფორმაციის მოპოვებისათვის ,,დავირუსების“ ტექნიკას იყენებს, ინფრასტრუქტურის განთავსების მიზანი უცნობია, გასათვალისწინებელია ისიც, რომ ტექნიკური აღჭურვილობა, რასაც სახელმწიფო უსაფრთხოების სამსახური ფლობს, გასაიდუმლოებულია, შესაბამისად, დადგენა იმისა, ნამდვილად გამოუსადეგარია თუ არა იგი ინფორმაციის მოპოვებისათვის, შეუძლებელია .

გამოყენებული ლიტერატურა

ნორმატიული აქტები

1. საქართველოს კონსტიტუცია
2. საკართველოს კანონი ოპერატიულ- სამძებრო საქმიანობის შესახებ (08.07.2015 მდგომარეობით)
3. საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ (27.04.2016 მდგომარეობით)
4. საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ (27.04.2016 მდგომარეობით)
5. საქართველოს კანონი კონტრდაზვერვითი საქმიანობის შესახებ (08.07.2015 მდგომარეობით)
6. საქართველოს კანონი საქართველოს სახელმწიფო უსაფრთხოების სამსახურის შესახებ (16.12.2015 მდგომარეობით)
7. საქართველოს კანონი. საქართველოს სისხლის სამართლის საპროცესო კოდექსი (27.04.2016 მდგომარეობით)
8. საქართველოს მთავრობა. განკარგულება № 382, ერთი მხრივ, ევროკავშირს და, მეორე მხრივ, საქართველოს შორის ასოცირების შესახებ შეთანხმებისა და საქართველოს და ევროკავშირს ასოცირების დღს წესრიგის განხორციელების 2016 წლის ეროვნული სამოქმედო გეგმის დამტკიცების შესახებ, 2016 წლის 7 მარტი, თბილისი
9. საქართველოს კანონი სახელმწიფო საიდუმლოების შესახებ (08.07.2015 მდგომარეობით)

საზღვარგარეთის ქვეყნების ნორმატიული აქტები

1. ,,Gesets zur Beschrankung des Brief-, Post- unda Fernmeldegeheimnisses”. Ausvertigungsdatum : 26.06.2001

2. Strafprozessordnung (S t PO) Ausfertigungsdatum : 12.09.1950 http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf

3. Telekommunikationsgesetz (TGK) Ausfertigungsdatum : 12.09.2004

http://www.gesetze-im-internet.de/tgk_2004/index.html

4. Code des Postes et des communications electroniques

5. ΑΠΟΡΡΗΤΟ ΕΠΙΚΟΙΝΩΝΙΑΣ 2225/1994

http://old.law.uaoa.gr/crime-research/apporito.pdf [01.06.2016]