ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება – ქართული სამართალი და საერთაშორისო სტანდარტები

დოქტორანტი ***თამარ გეგეშიძე***, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

I. შესავალი

ბოლო ათწლეულების ტექნიკური პროგრესის ფონზე კერძო პირებს შორის ურთიერთობამ ვირტუალურ სივრცეში გადაინაცვლა. ელექტრონული კომუნიკაციის საშუალებები, როგორიცაა ინტერნეტი, მობილური სმარტფონები, Wi-Fi ტექნოლოგია, ყოველდღიური ცხოვრების ნაწილი გახდა[1]. კომპიუტერული ტექნოლოგიებისა და ელექტრონული საკომუნიკაციო საშუალებების დახვეწის შედეგად თანამედროვე ელექტროკავშირგაბმულობის ქსელები და მოწყობილობები იძლევიან დროის უმოკლეს მონაკვეთში დედამიწის ნებისმიერი წერტილიდან დიდ მანძილზე ნებისმიერი სახის ინფორმაციის გადაცემის, გავრცელების ან მიღების შესაძლებლობას, რაც, თავის მხრივ, აფართოებს სამართალდამცავი ორგანოების შესაძლებლობებს ელექტრონული მეთვალყურეობის სფეროში. პირადი ცხოვრების დაცვა ელექტრონული დაკვირვების განხორციელების პროცესში არ არის მხოლოდ ერთი კონკრეტული სახელმწიფოს პრობლემა, არამედ დიდი ხანია გლობალური ხასიათი შეიძინა. ინტერნეტ სივრცეში საზღვრების არარსებობა და თანამედროვე ტექნოლოგიების სწრაფი განვითარების ტემპი თანდათანობით მეტი გამოწვევის წინაშე აყენებს საერთაშორისო საზოგადოებას და საკითხი საერთაშორისო დონეზე მუდმივ აქტუალურობას ინარჩუნებს.

აღსანიშნავია, რომ საქართველოში აქტიურად მიმდინარეობს ევროინტეგრაციისაკენ სწრაფვის პროცესი, რომლის ფარგლებშიც საქართველოსა და ევროკავშირს შორის დადებულია ასოცირების შეთანხმება. შეთანხმებით საქართველოს ერთ-ერთ ვალდებულებას წარმოადგენს პერსონალურ მონაცემთა მაღალ დონეზე დაცვა წინამდებარე შეთანხმების I დანართში მითითებული ევროკავშირის, ევროპის საბჭოსა და საერთაშორისო სამართლებრივი დოკუმენტების შესაბამისად. აქედან გამომდინარე, საქართველოსთვის ძალიან მნიშვნელოვანია კომუნიკაციის ფარული ელექტრონული მეთვალყურეობის სფეროში არსებული კანონმდებლობის საერთაშორისო სტანდარტებთან შესაბამისობაში მოყვანა.

აღნიშნულის გათვალისწინებით, წინამდებარე სტატიაში განხილული იქნება მოცემულ სფეროში დამკვიდრებული საერთაშორისო სტანდარტები, აღნიშნული საკითხის გარშემო საქართველოში წამოჭრილი პრობლემური სამართლებრივი საკითხები და ამ მიმართულებით კანონმდებლობაში განხორციელებული ნოვაციები.

II. ელექტრონული მეთვალყურეობის მიმართულებით ქართულ კანომდებლობაში განხორციელებული ნოვაციები

აღსანიშნავია, რომ პირადი ცხოვრების უფლება საქართველოს კონსტიტუციით უზრუნველყოფილი ერთ-ერთი ფუნდამენტური გარანტიაა. საქართველოს კონსტიტუცია უზრუნველყოფს პირადი ჩანაწერის, სატელეფონო საუბრის, მიმოწერის და ტექნიკური საშუალებებით გადაცემული შეტყობინებების ხელშეუხებლობას და მის შეზღუდვას ითვალისწინებს მხოლოდ სასამართლოს გადაწყვეტილებით ან კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას.

მოცემულმა საკითხმა განსაკუთრებული აქტუალურობა შეიძინა საქართველოში. „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს

[1] „The right to privacy in the digital age“, Report of the Office of the United Nations High Commissioner for Human Rights; 2014, 3 (ხელმისაწვდომია ვებ-გვერდზე: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf) (უკანასკნელად ნანახია: 20.04.2017).

კანონი, რომელიც 2014 წლის აგვისტომდე არეგულირებდა მოცემული ღონისძიების ჩატარების წესსა და პროცედურას, ითვალისწინებდა ადამიანის უფლებების დაცვის დაბალ სტანდარტებს, რის გამოც დიდ პრობლემებს ქმნიდა საერთაშორისო სამართლებრივ მოთხოვნებთან შეუსაბამობის გამო. აღნიშნულიდან გამომდინარე, 2014 წლის 1 აგვისტოს საქართველოს პარლამენტმა მიიღო ახალი საკანონმდებლო პაკეტი ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით, რომელმაც ძირეულად გარდაქმნა მოცემული სფეროს მარეგულირებელი კანონმდებლობა და გაითვალისწინა გაცილებით მეტი გარანტიები ადამიანის უფლებების დასაცავად. განხორციელებული ცვლილებების შედეგად საქართველოს სისხლის სამართლის საპროცესო კოდექსში[2] არაერთი ნოვაცია განხორციელდა; კოდექსს დაემატა ახალი თავი – ფარული საგამოძიებო მოქმედებები. აღნიშნულ თავში ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მიმართულებით შემდეგი მოქმედებები არის გათვალისწინებული:

- სატელეფონო საუბრის ფარული მიყურადება და ჩაწერა;
- ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებებთან, კომპიუტერულ ქსელებთან, სახაზო კომუნიკაციებთან და სასადგურო აპარატურასთან მიერთებით), კომპიუტერული სისტემიდან (როგორც უშუალოდ, ისე დისტანციურად) და ამ მიზნით კომპიუტერულ სისტემაში შესაბამისი პროგრამული უზრუნველყოფის საშუალებების ინსტალაცია.

ცვლილებების შედეგად სატელეფონო საუბრის ფარული მიყურადების და ინტერნეტურთიერთობის მონიტორინგის ღონისძიებების გამოყენება შესაძლებელია მხოლოდ საგამოძიებო მოქმედების სახით, ანუ მხოლოდ მას შემდეგ, რაც დაიწყება გამოძიება და არსებობს დასაბუთებული ვარაუდი, რომ კანონმდებლობით გათვალისწინებული დანაშაული იქნა ჩადენილი. აგრეთვე განისაზღვრა რომელ დანაშაულთა შემთხვევაში არის დასაშვები აღნიშნული ღონისძიებების გამოყენება და შეიზღუდა დანაშაულთა კატეგორიები, რომელთა შემთხვევაშიც შესაძლებელია მათი განხორციელება. ასევე კანონმდებლობამ შეზღუდა და დააკონკრეტა პირთა წრე, რომელთა მიმართაც გამოიყენება მოცემული ღონისძიება. გათვალისწინებული იქნა პროპორციულობისა და აუცილებლობის პრინციპის დაცვის საჭიროება ფარული საგამოძიებო მოქმედების წარმართვის დროს, რაც ნიშნავს, რომ ფარული საგამოძიებო მოქმედება შეიძლება ჩატარდეს მხოლოდ იმ შემთხვევაში, თუ ის აუცილებელია დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნების მისაღწევად. ამასთან, თუკი არის ლეგიტიმური მიზნის მიღწევის პროპორციული და აუცილებელი საშუალება და მხოლოდ მაშინ, როდესაც სხვა საშუალებით გამოძიებისათვის არსებითი მნიშვნელობის მქონე მტკიცებულებების მოპოვება შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს. გარდა აღნიშნულისა, ფარული საგამოძიებო მოქმედება უნდა პასუხობდეს მინიმიზაციის მოთხოვნას, რაც გულისხმობს, რომ მაქსიმალურად უნდა შეიზღუდოს იმ პირის კომუნიკაციის მონიტორინგი, რომელსაც გამოძიებასთან კავშირი არ აქვს. განისაზღვრა ასევე ღონისძიების ჩატარების საკმაოდ მკაცრი ვადები, თავდაპირველი ხანგრძლივობა შეადგენს ერთ თვეს, რომლის გაგრძელება შესაძლებელია მაქსიმუმ ორჯერ. დადგინდა ღონისძიების ჩატარების დეტალური პროცედურა, აგრეთვე ღონისძიების შედეგად მოპოვებული მასალის განადგურების და შენახვის წესი. ერთ-ერთ ნოვაციას წარმოადგენს ასევე ფარული საგამოძიებო მოქმედების ჩატარების შემდეგ მისი ადრესატისათვის შეტყობინების ვალდებულების სამართლებრივი რეგლამენტაცია საპროცესო კოდექსში.

III. საქართველოს კანონმდებლობაში წამოჭრილი პრობლემური საკითხები

1. შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობა

აღსანიშნავია, რომ ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული საკითხები კიდევ ერთხელ მძაფრად წამოჭრა საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებამ, რომელმაც არაკონსტიტუციურად ცნო მოცემული სფეროს მარეგულირებელი რამდენიმე ფუნდამენტური დებულება, კერძოდ, საკონსტიტუ-

[2] ტექსტში სისხლის სამართლის საპროცესო კოდექსი შემოკლებულია როგორც სსსკ.

ციო სასამართლომ კონსტიტუციასთან შეუსაბამოდ მიიჩნია „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის ის ნორმა, რომელიც ფარული საგამოძიებო მოქმედებების განსახორციელებლად შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს ანიჭებდა უფლებამოსილებას, ჰქონოდა კავშირგაბმულობის საშუალებებიდან ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობა და ამ მიზნით კომუნიკაციის საშუალებებთან განეთავსებინა მართლზომიერი გადაჭერის მენეჯმენტის სისტემა, სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები.[3]

ქართული რეგულაციების არაკონსტიტუციურად ცნობა განაპირობა იმ გარემოებამ, რომ კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობით აღჭურვილი იყო „პროფესიულად დაინტერესებული ორგანო“[4] – სახელმწიფო უსაფრთხოების სამსახური, რომელიც პასუხისმგებელი იყო წარმატებულ გამოძიებაზე, რაც საკონსტიტუციო სასამართლოს შეხედულებით, „განუზომლად ზრდიდა ცდუნებას და რისკებს გამოძიების ინტერესებიდან გამომდინარე, უფლებაში დაუსაბუთებელი ჩარევისათვის“.

აღსანიშნავია, რომ სამართალდამცავი ორგანოების მიერ კავშირგაბმულობის არხებთან პირდაპირი წვდომის შესაძლებლობა უკვე გახდა ევროპული სასამართლოს მსჯელობის საგანი საქმეში Zakharov v. Russia. სასამართლომ მიიჩნია, რომ „სისტემა, რომელიც უსაფრთხოების სამსახურებსა და პოლიციას შესაძლებლობას აძლევს, კომუნიკაციის პროვაიდერებისათვის ან სხვა უფლებამოსილი პირებისათვის შესაბამისი ნებართვის წარდგენის გარეშე, უშუალოდ ჰქონდეთ წვდომა ნებისმიერი მოქალაქის კომუნიკაციის საშუალებებზე, განსაკუთრებით მიდრეკილია უფლების ბოროტად გამოყენებისკენ. შესაბამისად, საჭიროებს უფლების დაცვის განსაკუთრებით ძლიერი გარანტიების არსებობას, რომლის კონტექსტშიც ზედამხედველობის სისტემის ეფექტიანობა უნდა იქნეს შეფასებული, რომელმაც უნდა უზრუნველყოს კომუნიკაციის მონიტორინგის კანონიერად განხორციელება სასამართლოს ნებართვის საფუძველზე“.[5]

არსებული სისტემის პირობებში საქართველოს საკონსტიტუციო სასამართლომ ხაზი გაუსვა „პროცესის დამაჯერებელი გამჭვირვალობისა და კონტროლის მექანიზმების“ აუცილებლობას საკანონმდებლო დონეზე[6]. აღსანიშნავია, რომ ფარული ელექტრონული დაკვირვების ღონისძიებებზე ზედამხედველობა ერთ-ერთ ყველაზე პრობლემურ და ამავე დროს მნიშვნელოვან საკითხს წარმოადგენს საერთაშორისო დონეზე. უფლების ბოროტად გამოყენების საწინააღმდეგო გარანტიები დამოუკიდებელი ორგანოს კონტროლის გარეშე არაეფექტიანად არის აღიარებული საერთაშორისო სტანდარტის მიხედვით. მიუხედავად იმისა, რომ ასეთი გარანტიები შესაძლოა მრავალფეროვან წესებში გამოიხატოს, ხელისუფლების ყველა შტოს, მათ შორის, დამოუკიდებელი ორგანოს ჩართულობა ზედამხედველობის პროცესში უფლების დაცვის ფუნდამენტურ გარანტიად ითვლება[7].

---

[3] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N1/1/625, 640, 16.04.2016, 73, 74 (ხელმისაწვდომია ვებ-გვერდზე: http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page) (უკანასკნელად ნანახია: 15.04.2017).

[4] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N1/1/625, 640, 16.04.2016, 63 (ხელმისაწვდომია ვებ-გვერდზე: http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page) (უკანასკნელად ნანახია: 15.04.2017).

[5] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Roman Zakharov v. Russia, N47143/06, 04.12.2015; პარაგ. 270-271 (ხელმისაწვდომია ვებ-გვერდზე: http://hudoc.echr.coe.int/eng?i=001-159324) (უკანასკნელად ნანახია: 14.04.2017).

[6] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N1/1/625, 640, 16.04.2016, 44-45 (ხელმისაწვდომია ვებ-გვერდზე: http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page) (უკანასკნელად ნანახია: 15.04.2017).

[7] „The right to privacy in the digital age“, Report of the Office of the United Nations High Commissioner for Human Rights; 2014, 12-13 (ხელმისაწვდომია ვებ-გვერდზე: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf) (უკანასკნელად ნანახია: 20.04.2017).

აღსანიშნავია, რომ საქართველოს საკონსტიტუციო სასამართლომ როგორც სატელეფონო მოსმენებთან, ასევე ინტერნეტურთიერთობის მონიტორინგის ღონისძიებასთან დაკავშირებული კონტროლის ბერკეტები არაეფექტიანად მიიჩნია. სატელეფონო მიყურადებასთან დაკავშირებით სასამართლოს უკმაყოფილება გამოიწვია იმ გარემოებამ, რომ არსებული კანონმდებლობის პირობებში არ იყო გამორიცხული სატელეფონო მოსმენის წარმართვა ინსპექტორის გვერდის ავლით, ვინაიდან კანონმდებლობა უსაფრთხოების სამსახურს ანიჭებდა უფლებამოსილებას, გამოეყენებინა ისეთი ტექნიკური შესაძლებლობები, რომელთან დაკავშირებითაც ინსპექტორი კონტროლს ვერ განახორციელებდა[8]. რაც შეეხება ინტერნეტურთიერთობის მონიტორინგის ღონისძიებას, საკონსტიტუციო სასამართლომ ჩათვალა, რომ ინტერნეტსივრცეში ინფორმაციის რეალურ დროში მოპოვების პროცესზე კანონმდებლობა ფაქტობრივად არ განსაზღვრავდა კონტროლის არანაირ მექანიზმს, გარდა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ ინსპექტირების შესაძლებლობისა, რომელიც არაეფექტიანად იქნა მიჩნეული.

2. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვა

საკონსტიტუციო სასამართლოს ზემოთაღნიშნული გადაწყვეტილებით წარმოჩენილი კიდევ ერთი მნიშვნელოვანი საკითხი უკავშირდება კომუნიკაციის მაიდენტიფიცირებელი მონაცემების, ე.წ. მეტადატის შენახვას. აღნიშნული მონაცემები შეიცავს ინფორმაციას კომუნიკაციის წყაროს, თარიღის, ტიპის და ხანგრძლივობის, მომხმარებლის საკომუნიკაციო საშუალების, მისი ადგილმდებარეობის, რეგისტრირებული მომხმარებლის ვინაობის, ტელეფონის ნომრის, ინტერნეტ პროტოკოლის (IP) მისამართის შესახებ. ამ მონაცემთა ანალიზის შედეგად შეიძლება გაირკვეს კონკრეტული პირის ვინაობა, ვისთანაც მომხმარებელმა დაამყარა კომუნიკაცია, ამგვარი კომუნიკაციის დრო და ადგილმდებარეობა, კომუნიკაციის სიხშირე დროის განსაზღვრულ პერიოდში[9]. შესაბამისად, აღნიშნული ინფორმაციის ერთობლივი შეფასების საფუძველზე შესაძლებელია ადამიანის პირადი ცხოვრების შესახებ დეტალური პროფილის შექმნა.[10]

აღსანიშნავია, რომ საქართველოს პარლამენტმა მოახდინა „მონაცემთა შენახვის შესახებ“ ევროკავშირის დირექტივის იმპლემენტაცია, რომელიც ევროკავშირის მართლმსაჯულების სასამართლოს 2014 წლის 8 აპრილის გადაწყვეტილებით გაუქმებულ იქნა. დირექტივის იმპლემენტაციის შედეგად, ეროვნული კანონმდებლობით განისაზღვრა ნორმები ამგვარ მონაცემთა 2 წლის ვადით შენახვასთან დაკავშირებით, მონაცემთა კოპირების უფლებამოსილებით კი აღიჭურვა სახელმწიფო უსაფრთხოების სამსახური.

ზემოთ ხსენებული გადაწყვეტილებით საქართველოს საკონსტიტუციო სასამართლომ არაკონსტიტუციურად ცნო სამართლებრივი დებულებები, რომლებიც ითვალისწინებდა სახელმწიფო უსაფრთხოების სამსახურის აღჭურვას როგორც ტექნიკური შესაძლებლობით, ისე უშუალო უფლებამოსილებით, მოახდინა მაიდენტიფიცირებელი მონაცემების კოპირება და 2 წლამდე ვადით შენახვა. არაკონსტიტუციურობის მიზეზი გახდა ის გარემოება, რომ კანონმდებლობამ „გამოძიებაზე პასუხისმგებელი“ და „პროფესიულად დაინტერესებული ორგანო“ – სახელმწიფო უსაფრთხოების სამსახური აღჭურვა ასეთი მნიშვნელობის მქონე ინფორმაციასთან შეუზღუდავი წვდომის უფლე-

[8] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N1/1/625, 640, 16.04.2016, 49-50 (ხელმისაწვდომია ვებ-გვერდზე: http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page) (უკანასკნელად ნანახია: 15.04.2017).

[9] ევროკავშირის მართლმსაჯულების სასამართლოს ერთობლივი გადაწყვეტილება საქმეზე „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“, NC-293/12, C-594/12, 2014, პარაგ. 26 (ხელმისაწვდომია ვებ-გვერდზე: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN) (უკანასკნელად ნანახია: 19.04.2017).

[10] ევროკავშირის მართლმსაჯულების სასამართლოს ერთობლივი გადაწყვეტილება, NC-203/15, C-698/15, 2016, პარაგ. 99 (ხელმისაწვდომია ვებ-გვერდზე: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422) (უკანასკნელად ნანახია: 19.04.2017).

ბამოსილებით. ამასთან, ინფორმაციის შენახვა ორი წლის ვადით, აბსოლუტურად თითოეული პიროვნების შესახებ, ყოველგვარი ფილტრაციის გარეშე ადამიანის პირად ცხოვრებაში ძალიან მაღალი ინტენსივობით ჩარევად ჩათვალა. სასამართლომ ყურადღება გაამახვილა ასევე მონაცემთა შენახვის პროცესზე ეფექტიანი კონტროლის მექანიზმების არარსებობაზე. მისი შეფასებით, მართალია, კანონი შენახულ მაიდენტიფიცირებელ მონაცემებზე გამოძიების ორგანოს ხელმისაწვდომობისთვის წინაპირობად ითვალისწინებდა მოსამართლის ბრძანებას ან, გადაუდებელი აუცილებლობის შემთხვევაში – პროკურორის დადგენილებას, მაგრამ ამ შემთხვევაში არ არსებობდა კონტროლის მექანიზმი თავად ინფორმაციის კოპირების და შედეგად, მისი მოპოვების პროცესზე. ამ თვალსაზრისით, გამოიკვეთა, რომ ტექნიკურად შესაძლებელი იყო, მაიდენტიფიცირებელი მონაცემის კოპირების და შენახვის პროცესში შექმნილიყო ე.წ. „ალტერნატიული ბანკი, რომლის არსებობის შესახებ შესაძლოა არავინ იცოდეს და მასზე დაშვება არც პერსონალურ მონაცემთა დაცვის ინსპექტორს ჰქონდეს“.[11]

აღსანიშნავია, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვა საერთაშორისო დონეზეც ერთ-ერთ აქტუალურ საკითხს განეკუთვნება. ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკის მიხედვით, კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის მარეგულირებელი ეროვნული კანონმდებლობა უნდა შეიცავდეს მკაფიო და ნათელ წესებს, მონაცემთა შენახვის მასშტაბთან და გამოყენების ფარგლებთან მიმართებაში. სასამართლოს აუცილებელ მოთხოვნას წარმოადგენს ეროვნულ კანონმდებლობაში ობიექტური კრიტერიუმის არსებობა, რომლის მიხედვითაც დადგინდება კავშირი შესანახ მონაცემებსა და მისაღწევ ლეგიტიმურ მიზანს შორის და გამოიკვეთება პირები, რომელთა შესახებ მონაცემებს შესაძლოა კავშირი (თუნდაც არაპირდაპირი) ჰქონდეთ სერიოზულ დანაშაულთან და რაიმე ფორმით წვლილი შეიტანონ ასეთ დანაშაულთან ბრძოლის ან საზოგადოების მიმართ სერიოზული საფრთხის აცილების საქმეში. სასამართლო კიდევ უფრო მკაცრია, როდესაც საქმე აღნიშნულ მონაცემებზე წვდომას ეხება – სამართალდამცავი ორგანოების დაშვება, როგორც წესი, დასაშვებია იმ პირთა მონაცემებზე, რომლებთან დაკავშირებითაც არსებობს ეჭვი სერიოზული დანაშაულის დაგეგმვის, ჩადენის ან ასეთ დანაშაულში რაიმე გზით მონაწილეობის შესახებ.[12]

IV. ახალი საკანონმდებლო ცვლილებები ფარული მეთვალყურეობის ღონისძიებებთან დაკავშირებით

საკონსტიტუციო სასამართლოს ზემოაღნიშნული გადაწყვეტილების აღსრულების მიზნით, საქართველოს პარლამენტმა 2017 წლის 22 მარტს მიიღო ახალი საკანონმდებლო ცვლილებათა პაკეტი, რომელიც ახლებურად არეგულირებს არაერთ საკითხს ამ სფეროში. საკონსტიტუციო სასამართლოს ძირითად მოთხოვნასთან დაკავშირებით, რომელიც მდგომარეობს ფარული საგამოძიებო მოქმედებების ტექნიკურად აღსრულებაში დამოუკიდებელი ორგანოს მიერ, შეიქმნა ახალი უწყება – ოპერატიულ ტექნიკური სააგენტო, რომელიც ტექნიკურად უზრუნველყოფს ფარული მეთვალყურეობის ღონისძიებების განხორციელებას და არ არის აღჭურვილი საგამოძიებო ფუნქციებით. აღნიშნული ორგანო შეიქმნა საჯარო სამართლის იურიდიული პირის სახით სახელმწიფო უსაფრთხოების სამსახურის მმართველობის ქვეშ. როგორ წარიმართება მომავალში ფარული საგამოძიებო მოქმედებების ტექნიკური აღსრულების პროცესი და რამდენად შეძლებს ახლადშექმნილი უწყება საკონსტიტუციო სასამართლოს მოთხოვნების გათვალისწინებას, პრაქტიკაში გამოვლინდება.

[11] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება, N1/1/625, 640, 16.04.2016, 64-65 (ხელმისაწვდომია ვებ-გვერდზე: http://constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page) (უკანასკნელად ნანახია: 15.04.2017).

[12] ევროკავშირის მართლმსაჯულების სასამართლოს ერთობლივი გადაწყვეტილება, NC-203/15, C-698/15, 2016, პარაგ. 109-111, 119 (ხელმისაწვდომია ვებ-გვერდზე: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422) (უკანასკნელად ნანახია: 19.04.2017).

ცვლილებების მიხედვით, ფარული მიყურადების ღონისძიებასთან დაკავშირებით მისასალმებელ სიახლეს წარმოადგენს ის გარემოება, რომ ზუსტდება, თუ რომელ ტექნიკურ შესაძლებლობებს გამოიყენებს სააგენტო აღნიშნული ღონისძიების განსახორციელებლად, კერძოდ, სატელეფონო მოსმენის განსახორციელებლად ელექტრონული კომუნიკაციის კომპანიის მიერ გადაცემული კომუნიკაციის რეალურ დროში მოპოვების სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში სააგენტო უფლებამოსილია გამოიყენოს მხოლოდ მართლზომიერი გადაჭერის მენეჯმენტის სისტემა ან/და მასთან დაკავშირებული/მისი ფუნქციონირებისთვის აუცილებელი აპარატურა და პროგრამული უზრუნველყოფის საშუალებები. გარდა აღნიშნულისა, ნოვაციას წარმოადგენს ის გარემოება, რომ ინსპექტორს ღონისძიების დაწყებაზე თანხმობის გაცემის ნაცვლად, ექნება ღონისძიების მიმდინარეობის შეჩერების უფლებამოსილება კანონმდებლობით გათვალისწინებულ შემთხვევებში, მაგალითად, თუკი არ მიეწოდა სასამართლოს ნებართვის ან გადაუდებელი აუცილებლობის საფუძველზე ღონისძიების ჩატარებისას პროკურორის დადგენილების ეგზემპლარი ელექტრონული და მატერიალური სახით.

საერთო ჯამში, ფარული მეთვალყურეობის ღონისძიებებზე ზედამხედველობის მექანიზმთან დაკავშირებით, უნდა ითქვას, რომ საქართველოს კანონმდებლობით ფარული საგამოძიებო მოქმედებების განხორციელებასთან დაკავშირებული კონტროლის მექანიზმები, ძირითადად, ეხება საწყის ეტაპს, ანუ როდესაც ხდება ამ ღონისძიების დაწყება, ინსპექტორის ზედამხედველობაც ძირითადად ამ ღონისძიების ჩატარების საფუძვლების კანონიერების შემოწმებაში გამოიხატება, საუკეთესო გამოსავალი ამ ღონისძიების მთელ პროცესზე ეფექტიანი ზედამხედველობის განსახორციელებლად სასამართლოს ჩართულობა შეიძლება იყოს. დღესდღეობით სასამართლოს საზედამხედველო როლი ძირითადად ღონისძიების ჩატარების საწყის ეტაპზე მონაწილეობაში და შემდგომში მისი გაგრძელების საკითხის გადაწყვეტაში მდგომარეობს, მართალია, კანონმდებლობით არის გათვალისწინებული გარკვეული გარანტიები, მაგალითად, მისი მონაწილეობა მოპოვებული მასალის განადგურების პროცედურაში, თუმცა საერთო ჯამში, სსსკ-ით უზრუნველყოფილი შეჯიბრობითობის პრინციპიდან გამომდინარე, სასამართლო ნაკლებად ერევა ღონისძიების აღსრულების მთლიან პროცესში, მაგალითად, მისი მიმდინარეობის დროს ან დასრულების შემდგომ, რაც განაპირობებს სირთულეებს ფარული მეთვალყურეობის ღონისძიებებზე ზედამხედველობის საკითხთან დაკავშირებით.

რაც შეეხება ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვას, ცვლილებების მიხედვით, შენახვის ვადა მცირდება 12 თვემდე. მისი გაგრძელება შესაძლებელია არაუმეტეს სამი თვით მკაცრად განსაზღვრული გამონაკლისების არსებობისას. მეტადატის შენახვის ვადასთან დაკავშირებით, აღსანიშნავია, რომ მართალია ევროკავშირის მართლმსაჯულების სასამართლომ ე.წ. მონაცემთა შენახვის შესახებ დირექტივით გათვალისწინებული ვადა – მინიმუმ 6 თვე და მაქსიმუმ 2 წელი, არაპროპორციულად მიიჩნია, მაგრამ არც 2014 და არც 2016 წლების გადაწყვეტილებებში შენახვის კონკრეტული ვადა არ დაუდგენია, ამიტომ ერთმნიშვნელოვნად ვერ ვიტყვით, მონაცემთა შენახვის რა კონკრეტული ვადა ჩაითვლება პროპორციულად საერთაშორისო სტანდარტის მიხედვით. ევროკავშირის მართლმსაჯულების სასამართლოს მოთხოვნა ამ შემთხვევაში მდგომარეობს იმაში, რომ ეროვნული კანონმდებლობით განსაზღვრული ვადა უნდა პასუხობდეს აუცილებლობის მოთხოვნას.[13]

ზედამხედველობის საკითხთან დაკავშირებით აღსანიშნავია, რომ ელექტრონული კომუნიკაციის მონაცემთა ცენტრალური ბანკის კონტროლის სისტემის მეშვეობით მოხდება მომხმარებლის და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების ლოგირების მონაცემების და შესაბამისი სამართლებრივი საფუძვლების ინსპექტორისთვის რეალურ დროში მიწოდება. რაც შეეხება ე.წ. „ალტერნატიული ბანკის“ წარმოების თეორიულ შესაძლებლობასთან დაკავშირებულ საფრთხეებს, აღნიშნული საფრთხის გამორიცხვა მთლიანად არის დამოკიდებული იმ ორგანოს დამოუკიდებლობის ხარისხზე, რომელიც მონაცემთა

[13] ევროკავშირის მართლმსაჯულების სასამართლოს ერთობლივი გადაწყვეტილება, NC-203/15, C-698/15, 2016, პარაგ. 108 (ხელმისაწვდომია ვებ-გვერდზე: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=544422) (უკანასკნელად ნანახია: 19.04.2017).

ბაზების კოპირებას მოახდენს, ვინაიდან ასეთი ორგანოს მიუკერძოებლობა, ასეთი ბანკის შექმნის თეორიულ რისკს ამცირებს.

V. დასკვნა

საბოლოოდ უნდა ითქვას, რომ საქართველოს რეალობაში წამოჭრილი ძირითადი პრობლემა უკავშირდება სახელმწიფოს ტექნიკურ შესაძლებლობებს, რაც კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობაში გამოიხატება, რომელიც უნდა დააბალანსოს იმ ორგანოს დამოუკიდებლობამ, რომელიც ფარული მეთვალყურეობის ღონისძიებების ტექნიკურ აღსრულებას მოახდენს. უდავოა, რომ საქართველოს კანონმდებლობაში ბოლო დროს გადაიდგა არაერთი მნიშვნელოვანი ნაბიჯი ამ სფეროში ადამიანის უფლებების დაცვის სტანდარტის გაზრდის მიზნით, თუმცა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება და პროცესუალური მიზნით გამოყენება იყო და კვლავაც დარჩება ერთერთ ყველაზე აქტუალურ და რთულ საკითხად სისხლის სამართლის პროცესში. აღსანიშნავია ისიც, რომ საერთაშორისო დონეზე მოცემულ სფეროში უფლების დაცვის ინსტრუმენტების გაძლიერების ღონისძიებები აქტიურად მიმდინარეობს, საქართველომაც თავის მხრივ, ფეხი უნდა აუწყოს ევროპაში მიმდინარე პროცესებს. ამ თვალსაზრისით აუცილებელია გაგრძელდეს მუშაობა ქართული კანონმდებლობის ევროპულ სტანდარტთან დაახლოების მიზნით.