

ნინო ცაგარიშვილი¹

**„პირადი კომუნიკაციის შესახებ ინფორმაციის მოპოვების მართლზომიერება
საერთაშორისო და საქართველოს სამართლებრივ სისტემებში: თანამედროვე
ტექნოლოგიები vs პირადი ცხოვრება“**

**“Legitimacy of Obtaining Information on Private Communication in International and
Georgian Legal Systems: Modern Technologies vs Privacy “**

აბსტრაქტი

თანამედროვე ეპოქის ერთ-ერთი მთავარი გამოწვევა საკომუნიკაციო ტექნოლოგიების განვითარების კვალდაკვალ ადამიანის უფლებების ეფექტიანი დაცვაა. ხშირ შემთხვევაში, სამართალდამცავი ორგანოების წარმომადგენლები ადამიანის პირადი მიმოწერის კონტროლს ეროვნული უსაფრთხოების უზრუნველყოფის საფუძვლით ახორციელებენ, რაც ზრდის ადამიანის უფლებაში გაუმართლებელი ჩარევის რისკებს. სტატიის მიზანია სწორედ პირადი კომუნიკაციის შესახებ ინფორმაციის მოპოვების მართლზომიერების შესწავლა, რომლის ფარგლებშიც განხილულია: პირადი კომუნიკაციის კონტროლი და მასთან დაკავშირებული ასპექტები; მიმოწერის პატივისცემის უფლებასა და ეროვნულ უსაფრთხოებას შორის ბალანსის დაცვის საკითხი; საგარეო დაზვერვის შესაბამისობა საერთაშორისო სამართლის ძირითად პრინციპებთან; სამართალდამცავი ორგანოების საქმიანობაზე ზედამხედველობა; საერთაშორისო და ეროვნული სამართლებრივი მექანიზმები პირადი კომუნიკაციის პატივისცემის უფლების ჭრილში; ადამიანის პირადი ცხოვრების დაცულობის უფლებაში მართლზომიერი ჩარევის ტესტი; ადამიანის უფლებათა ევროპული სასამართლოსა და ევროპის კავშირის მართლმსაჯულების სასამართლოს პრაქტიკა.

საკვანძო სიტყვები: *პირადი ცხოვრება, კომუნიკაციები, საგარეო დაზვერვა, ევროპული სასამართლო.*

Abstract

One of the main challenges in the modern era is the effective protection of human rights amid the development of communication technologies. Often law enforcement agencies

¹ თსუ იურიდიული ფაკულტეტის მაგისტრატურის მე-2 კურსის სტუდენტი. ელ. ფოსტა: ntsagareishvili7@yahoo.com.

exercise control over the private correspondence of individuals based on the argument of protecting national security, which increases the risks of illegal interference in human rights. The purpose of this article is to examine the legitimacy of obtaining information on private communication by addressing the following issues: monitoring of private communications and related aspects; balancing the interest in protecting national security against the right to respect correspondence; compliance of foreign intelligence surveillance with the main principles of international law; overseeing activities of law enforcement agencies; international and national legal mechanisms for protecting the right to respect for personal correspondence; the test for the legitimacy of the aim pursued by the interference in the right to respect for private life; case-law of the European Court of Human Rights and the Court of Justice of the European Union.

Keywords: *Personal life, communications, foreign intelligence, ECtHR.*

შესავალი

თანამედროვე ტექნოლოგიების განვითარებასთან ერთად ადამიანის უფლებათა დაცვის საკითხი სულ უფრო აქტუალური ხდება. კომუნიკაციის სფეროში არსებული ტექნიკური საშუალებებისა და მათი გამოყენების მასშტაბების გათვალისწინებით, სამართალდამცავი ორგანოების წარმომადგენელთა მხრიდან იზრდება პირად მიმოწერაზე მეთვალყურეობის შესაძლებლობა, რაც, თავის მხრივ, წარმოშობს თვითნებობის რისკებს. ტექნოლოგიური პროგრესის გამოყენებით, კომუნიკაციის კონტროლი ხორციელდება როგორც ქვეყნის შიგნით, ისე მის ფარგლებს გარეთ.

საერთაშორისო საზოგადოება სამართალდამცავი ორგანოების საქმიანობით განსაკუთრებით დაინტერესდა აშშ-ის ეროვნული უსაფრთხოების სააგენტოს ყოფილი კონტრაქტორის² მიერ მასობრივი თვალთვალის შესახებ საიდუმლო ინფორმაციის გამჟღავნების შემდეგ, რამაც დიდი ვნებათაღელვა გამოიწვია. გამოიკვეთა კომუნიკაციებზე არამართლზომიერი მეთვალყურეობის ფაქტები ეროვნულ და საგარეო დონეზე, შედეგად ადამიანებს გაუჩნდათ განცდა, რომ მათი პირადი ცხოვრება მუდმივი კონტროლის ქვეშ იყო.

წინამდებარე სტატიაში ადამიანის პირადი კომუნიკაციის შესახებ ინფორმაციის მოპოვების მართლზომიერების თვალსაზრისით, განხილული იქნება: პირადი კომუნიკაციის მონიტორინგის არსი; პირადი ცხოვრების უფლებისა და პერსონალურ მონაცემთა დაცვის მიმართულებით არსებული საერთაშორისო სამართლებრივი

² 2013 წელს ედუარდ სნოუდენმა ამხილა სახელმწიფოები მასობრივი თვალთვალის განხორციელებაში, რაც იწვევდა პირად კომუნიკაციაში არამართლზომიერ ჩარევას.

მექანიზმები; კომუნიკაციის პატივისცემის უფლებისა და ეროვნულ უსაფრთხოებას შორის ბალანსის დაცვის საკითხები; საგარეო დაზვერვის შესაბამისობა საერთაშორისო სამართლის ძირითად პრინციპებთან; სამართალდამცავ ორგანოთა საქმიანობაზე ეფექტიანი კონტროლის განხორციელება; ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლო პრაქტიკა; საქართველოში არსებული საკანონმდებლო ჩარჩო; საკონსტიტუციო სასამართლოს პრაქტიკა; სახალხო დამცველისა და პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშები.

დასკვნით ნაწილში, შეჯამდება კომუნიკაციის შესახებ ინფორმაციის მოპოვების მიმართულებით არსებული გამოწვევები, როგორც საერთაშორისო, ისე ეროვნულ დონეზე და წარმოდგენილი იქნება რეკომენდაციები.

1. პირადი კომუნიკაციის მონიტორინგი და საგარეო დაზვერვის თავისებურებები

1.1. პირადი კომუნიკაციის მონიტორინგის³არსი

ცივილიზებული სამყაროს პირობებში შესაძლებელია მრავალფეროვანი ტექნოლოგიური საშუალებებით სარგებლობა, რაც ეროვნული უსაფრთხოების სამსახურებს შესაძლებლობას აძლევს ტექნოლოგიური პროგრესი ტერორიზმსა და სხვა დანაშაულებთან ბრძოლის უზრუნველსაყოფად გამოიყენონ. ამ მიზნით, კომუნიკაციებზე წვდომა სხვადასხვაგვარად ხორციელდება.

პირად კომუნიკაციაში ჩარევა მოიცავს: მონიტორინგს, პერსონალურ მონაცემთა შეგროვებას, შენახვას, რომელიც ხორციელდება საკომუნიკაციო ქსელების მიმღებ პირთა საშუალებით მესამე მხარის მიერ. მესამე მხარე შეიძლება იყოს: სამართალდამცავი ორგანო, სადაზვერვო ორგანო, კერძო კომპანია ან განხორციელდეს ბოროტად სხვა პირის ან ორგანოს მიერ, რაც ზრდის პირად სივრცეში გაუმართლებელი ჩარევის რისკებს.⁴

³ სტატიაში გამოყენებულ ტერმინებს: „კომუნიკაციის მონიტორინგი“, „კომუნიკაციებზე მეთვალყურეობა“, „კომუნიკაციის კონტროლი“, „კომუნიკაციაზე ზედამხედველობა“ „კომუნიკაციებზე თვალთვალი“ - ერთი და იგივე მნიშვნელობა აქვს.

⁴ Privacy International, *Communications Surveillance*. ხელმისაწვდომია: <http://bit.do/eSMW7> (ბოლოს ნანახია: 19.05.2019).

კომუნიკაციაში ჩარევა კანონიერია მაშინ, როდესაც ხორციელდება სამართლებრივი საფუძვლით, კერძოდ გაცემულია შესაბამისი ნებართვა უფლებამოსილი ორგანოს მიერ და მიზანი სხვადასხვა დანაშაულთან ბრძოლაა.⁵

პირად კომუნიკაციაზე მეთვალყურეობა შესაძლებელია განხორციელდეს როგორც ეროვნულ, ისე საერთაშორისო დონეზე გამიზნულ ან/და განუსაზღვრელ პირთა წრის მიმართ. გამიზნულში მოიაზრება დანაშაულში ექვმიტანილი იდენტიფიცირებული პირის ან პირთა ჯგუფის მიმოწერების კონტროლი, ხოლო უკონტროლო/განურჩეველი ზედამხედველობის ფარგლებში: პირი არ არის წინასწარ განსაზღვრული; მიზანი დამნაშავის გამოვლენაა; კომუნიკაციაზე წვდომა დანაშაულის პრევენციისთვის ხორციელდება.⁶

1.2. „საგარეო დაზვერვა“ და მისი საერთაშორისო სამართლებრივი რეგულირება

„საგარეო დაზვერვა“⁷ გულისხმობს ერთი სახელმწიფოს მიერ სხვა სახელმწიფოს თანამდებობის პირებისა თუ მოქალაქეების კომუნიკაციის მონიტორინგს ტერიტორიის ფარგლებს გარეთ (სრულად ან ნაწილობრივ). აღნიშნულ პროცესში გამოიყენება: ელექტრონული საშუალებები, კიბერ-მონიტორინგი, სატელეკომუნიკაციო მონიტორინგი, სატელიტები ან დრონები.

საგარეო დაზვერვა შესაძლოა იყოს „ტრანსნაციონალური“ და „ექსტრატერიტორიული“ ხასიათის. ტრანსნაციონალური მიემართება იმ კომუნიკაციებზე მეთვალყურეობას, რომელიც კვეთს სახელმწიფოს საზღვრებს და ითვალისწინებს სახელმწიფოს ტერიტორიაზე დაწყების და საზღვარგარეთ დამთავრების შემთხვევასაც.⁸ ექსტრატერიტორიული თვალთვალის დროს, კომუნიკაციებზე ზედამხედველობა მთლიანად ქვეყნის ფარგლებს გარეთ ხორციელდება. ამის საპირისპიროდ, სახელმწიფოს ტერიტორიის ფარგლებში განხორციელებული მონიტორინგის დროს სახეზე გვაქვს - „შიდა ზედამხედველობა.“⁹

ედუარდ სნოუდენის მიერ საიდუმლო ინფორმაციის გაცემის შემდეგ¹⁰ კიდევ უფრო ნათლად გამოიკვეთა სხვა სახელმწიფოს თანამდებობის პირებისა და

⁵ Investigatory Powers Act, Factsheet. ხელმისაწვდომია: <http://bit.do/eSMVj> (ბოლოს ნანახია: 19.05.2019).

⁶ Ibid.

⁷ Foreign Surveillance.

⁸ Deeks S. A., *An International Framework for Surveillance*, Virginia Journal of International Law, 2015, 299.

⁹ Ibid. p. 300.

¹⁰ აშშ-ის უსაფრთხოების სამსახურის ყოფილი კონტრაქტორი, რომელმაც 2013 წელს ამხილა უსაფრთხოების სამსახურები მასობრივ თვალთვალში.

მოქალაქეების მიმართ განხორციელებული თვალთვალის ფაქტები.¹¹ საერთაშორისო საზოგადოებამ გააცნობიერა მასობრივი თვალთვალის უარყოფითი შედეგები. შეერთებული შტატები გახდა საკმაოდ ძლიერი პოლიტიკური წნეხის სამიზნე გერმანიის, ბრაზილიის და საფრანგეთის თანამდებობის პირთა მხრიდან, ხოლო ეკონომიკურ სფეროში, შეერთებული შტატების კორპორაციებმა (Google, Facebook და Microsoft) დაინახეს საზღვარგარეთ ბიზნესის დაკარგვის საშიშროება, ეროვნული უსაფრთხოების სააგენტოსთვის¹² დაზვერვის განხორციელებაში ხელშეწყობისთვის. მათ მოუწოდეს მთავრობას შეეზღუდა საგარეო დაზვერვის განხორციელება.¹³ ასევე, გაეროს გენერალური ასამბლეის რეზოლუციაში: „პირადი ცხოვრება ციფრულ ეპოქაში“¹⁴ დაიგმო კომუნიკაციებზე მასობრივი მეთვალყურეობა და ხაზი გაესვა მის უარყოფით გავლენას ადამიანის უფლებებზე (განსაკუთრებით ფართომასშტაბიანი ხასიათის).¹⁵

სამართლებრივი საფუძვლის გარეშე საგარეო დაზვერვის განხორციელების საერთაშორისო სამართლებრივი რეგულირების საკითხზე მსჯელობისას მეცნიერთა აზრები იყოფა: ერთი ნაწილი მიიჩნევს, რომ საერთაშორისო სამართლით არ რეგულირდება; მეორე ნაწილი ფიქრობს, რომ საერთაშორისო სამართლით თვალთვალი ნებადართულია, ხოლო ზოგიერთი ამტკიცებს, რომ საერთაშორისო სამართლით აკრძალულია ამგვარი ქმედება.¹⁶

ლოტუსის მიდგომა - მართლმსაჯულების მუდმივმოქმედმა სასამართლომ¹⁷ ლოტუსის საქმეში¹⁸ მხარი დაუჭირა წინადადებას, რომ სავალდებულო წესის არარსებობის შემთხვევაში, სახელმწიფოებს შეუძლიათ თავისუფლად იმოქმედონ.¹⁹ სასამართლოს გადაწყვეტილების შესაბამისად, საერთაშორისო სამართალი სახელმწიფოს ანიჭებს ფართო დისკრეციას, რომელიც შეიძლება შეიზღუდოს მხოლოდ განსაზღვრულ შემთხვევებში. ამდენად, ლოტუსის პრინციპი ხდება

¹¹ ედუარდ სნოუდენი საგარეო დაზვერვაში განსაკუთრებით ამხელდა: შეერთებულ შტატებს; გაერთიანებულ სამეფოს; გერმანიას; ავსტრალიას და შვედეთს.

¹² NSA - National Security Agency.

¹³ Deeks S. A., *Regulating Foreign Surveillance through International Law*, 2017, 3.

¹⁴ U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014).

¹⁵ Privacy International (PI is a UK-based registered charity that defends and promotes the right to privacy across the world), *Guide to International Law and Surveillance*, August 2017, p. 29.

¹⁶ სამართლებრივი საფუძვლის გარეშე სხვა სახელმწიფოს საიდუმლო ინფორმაციის მოპოვება „ჯაშუშობასთანაა“ გაიგივებული.

¹⁷ PCIJ –Permanent Court of International Justice.

¹⁸ PCIJ, S.S. Lotus (France v. Turkey), 1927, No. 10, at 19 (Sept.7).

¹⁹ PCIJ, S.S. Lotus (France v. Turkey), 1927, No. 10, at 19 (Sept.7).

რელევანტური, როდესაც საკითხი სამართლებრივად არ რეგულირდება²⁰. ამ მიდგომის შესაბამისად, სხვა სახელმწიფოს მოქალაქეების კომუნიკაციის კონტროლი და საიდუმლო ინფორმაციის მოპოვება (თვალთვალი, ჯაშუშობა)²¹ არ არის აკრძალული.

საერთაშორისო სამართალი, როგორც თვალთვალის/ჯაშუშობის განხორციელებაზე ნებადართველი - ლოტუსის საქმისგან განსხვავდება მიდგომა, რომლითაც საერთაშორისო სამართალი სამართლებრივი საფუძვლის გარეშე ფარულ მიყურადებას და საიდუმლო ინფორმაციის მოპოვებას დასაშვებად ცნობს. სხვადასხვა მკვლევარები მიუთითებენ, რომ თვალთვალი/ჯაშუშობა სახელმწიფოს მიერ თავდაცვის უფლებით სარგებლობის წინაპირობაა. შესაბამისად, საერთაშორისო სამართალში ჯაშუშობის უკანონოდ მიჩნევით სახელმწიფო თავდაცვის უფლებას ვეღარ გამოიყენებს.²² გარდა ამისა, მიუთითებენ სახელმწიფო ჯაშუშობის დამკვიდრებულ პრაქტიკაზე, რომლის დასაშვებობის შესახებ თანამდებობის პირებს არაერთხელ განუცხადებიათ. მაგალითად, აშშ-ის პრეზიდენტი ბარაკ ობამა ღიად აცხადებდა,²³ რომ მტრულ სახელმწიფოზე ჯაშუშობის განხორციელებაში საწინააღმდეგოს ვერაფერს ხედავდა. ასევე, ბრიტანეთის პრემიერ-მინისტრმა ევროკავშირის სამიტზე აღნიშნა, რომ თვალთვალი ტერორისტული აქტების თავიდან არიდების შესაძლებლობაა.²⁴

საერთაშორისო სამართალი, როგორც საგარეო დაზვერვის ამკრძალავი - ზემოაღნიშნული მიდგომებისგან განსხვავებით, ყურადღებას ამახვილებენ საერთაშორისო სამართლის წყაროებზე. საერთაშორისო ჩვეულებითი სამართლის 2 პრინციპის შესაბამისად, სახელმწიფოებს ეკისრებათ სხვა სახელმწიფოს *სუვერენიტეტისა და ტერიტორიული მთლიანობის* პატივისცემის ვალდებულება.²⁵ *სუვერენიტეტის* პატივისცემა სახელმწიფოსგან მოითხოვს, რომ არ ჩაერიოს სხვა სახელმწიფოს საშინაო საქმეებში ამ უკანასკნელის თანხმობის გარეშე. მიმოწერების მონიტორინგის განხორციელებისას კი შესაძლებელია ინფორმაციის მოპოვება, რომელიც უკავშირდება სახელმწიფოს საშინაო საქმეებს.

ტერიტორიული მთლიანობის პატივისცემა გულისხმობს, რომ ერთი სახელმწიფო არ უნდა შევიდეს სხვა სახელმწიფოს ტერიტორიაზე, საჰაერო სივრცეში

²⁰ Ibid.

²¹ Spying, Espionage.

²² UN Charter, Article 51.

²³ Obama NSA Speech, *supra* note 1.

²⁴ Embassy Espionage: The NSA's Secret Spy Hub in Berlin, Oct. 27, 2013.

²⁵ *ob. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. (202-205 discussing non-intervention), (212-214 discussing sovereignty and territorial integrity).

ან ტერიტორიულ წყლებში სახელმწიფოს თანხმობის გარეშე.²⁶ ბუნდოვანია საკითხი, როდესაც კომუნიკაციების ფარული მონიტორინგი ხორციელდება სახელმწიფოს ტერიტორიასა და საჰაერო სივრცეში შეღწევის გარეშე ვირტუალურად, ტექნოლოგიური მიღწევების საშუალებით.

აღნიშნულ გარემოებებზე დაყრდნობით, რთულია ცალსახა დასკვნის გამოტანა თუ რამდენად ექცევა „ჯაშუშობა“ საერთაშორისო სამართლის რეგულირების ფარგლებში, თუმცა, აუცილებელია ითქვას, რომ სწრაფი ტექნოლოგიური პროგრესისა და გლობალიზაციის გათვალისწინებით, არსებული მიდგომები საჭიროებს მოდერნიზებას.

2. პირადი ცხოვრების და პერსონალურ მონაცემთა დაცვის საერთაშორისო სამართლებრივი მექანიზმები

არსებული საერთაშორისო სამართლებრივი დოკუმენტებით, პირადი ცხოვრების ხელშეუხებლობის უფლება აღიარებულია, როგორც ადამიანის ერთ-ერთი ძირითადი უფლება, რომლის პატივისცემა თითოეული სახელმწიფოს ვალდებულებაა. პირადი ცხოვრების უფლების ფარგლებში ექცევა მიმოწერის პატივისცემის უფლებაც, რომელიც გულისხმობს კომუნიკაციის პარტნიორებს შორის აზრთა გაცვლას, მესამე პირთა მხრიდან მათი შინაარსის გაცნობის გარეშე.²⁷ პირადი ცხოვრების ხელშეუხებლობის ჯეროვანი დაცვის უზრუნველყოფის მიზნით, მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის სათანადო მექანიზმების არსებობა.

ადამიანის უფლებათა საყოველთაო დეკლარაციის (UDHR)²⁸ მე-12 მუხლით საერთაშორისო დონეზე პირველად დადგინდა ადამიანის პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, რომლის შესაბამისადაც დაუშვებელია ადამიანის პირად სივრცეში არამართლზომიერი ჩარევა. შეიძლება ითქვას, რომ მოცემულმა დეკლარაციამ საფუძველი ჩაუყარა ადამიანის უფლებათა საერთაშორისო სამართლის განვითარებას.²⁹

ადამიანის სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის (შემდგომში - პაქტი/ICCPR) მე-17 მუხლის თანახმად, დაუშვებელია პირად

²⁶ Ibid.

²⁷ არსებობს გამონაკლისი შემთხვევები, რომელიც შესაბამისობაში უნდა მოდიოდეს მართლზომიერების კრიტერიუმებთან.

²⁸ United Nations (UN), Universal Declaration of Human Rights, 10 December 1948.

²⁹ European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018 edition, p. 21.

სივრცეში, საცხოვრებელში ან მიმოწერის განხორციელებაში თვითნებური და უკანონო ჩარევა.³⁰

ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლის³¹ შესაბამისად, დადგენილია პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის დაცვის უფლება და განსაზღვრულია ამ უფლებათა შეზღუდვის წინაპირობები.

ევროსაბჭოს ფარგლებში პირველი იურიდიულად სავალდებულო საერთაშორისო დოკუმენტია „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 108-ე კონვენცია და მისი დამატებითი ოქმი,³² რომელიც იცავს ფიზიკურ პირებს მათი პერსონალური მონაცემების დამუშავების პროცესში.

ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) (შემდგომში - რეგულაცია), ძალაში 2018 წლის 25 მაისს შევიდა. აღნიშნული რეგულაცია ევროკავშირის მთელ ტერიტორიაზე მონაცემთა დაცვის ერთიან სავალდებულო წესებს ადგენს, კერძოდ ამკვიდრებს ახალ სტანდარტებს პერსონალურ მონაცემთა დაცვის სფეროში, რომლის მიზანია ტექნოლოგიური პროგრესისა და თანამედროვე გამოწვევების პირობებში ინდივიდთა უფლებების სათანადო დაცვა.

2.1. ადამიანის პირადი ცხოვრების დაცულობის უფლებაში მართლზომიერი ჩარევის ტესტი ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლის შესაბამისად

ევროპული კონვენციის მე-8 მუხლის 1-ლი პუნქტი ადგენს უფლებებს, ხოლო მე-2 პუნქტი საჯარო ხელისუფლების მხრიდან უფლების შეზღუდვის მართლზომიერებას ითვალისწინებს, რომელიც 3 პირობას უნდა აკმაყოფილებდეს:

- კანონთან შესაბამისობა;
- კანონიერი მიზანი;
- დემოკრატიულ საზოგადოებაში აუცილებლობა.

კანონთან შესაბამისობა - უფლების შეზღუდვა უნდა იყოს „კანონის შესაბამისი“ ან „კანონით გათვალისწინებული“. მას უნდა გააჩნდეს სამართლებრივი საფუძველი.

³⁰ United Nations (UN), International Covenant on Civil and Political Rights, 16 December 1966.

³¹ CoE, European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

³² №108 Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, 1981.

მაგალითად, საქმეში - *Malone v. the United Kingdom*³³ სასამართლომ განიხილა საკითხი, თუ რამდენად გააჩნია სატელეფონო საუბრების შემოწმებას კანონიერი საფუძველი. ამ შემთხვევაში, სატელეფონო საუბრების ფარულ მოსმენებს არეგულირებდა ადმინისტრაციული პრაქტიკა, რომელიც არ მოიცავდა კანონით გათვალისწინებულ უფლებამოსილებას. აქედან გამომდინარე, სასამართლომ აღნიშნა, რომ არ არსებობდა საკმარისი სიზუსტე გამოყენების სფეროსთან ან მოქმედების ხასიათთან დაკავშირებით. შესაბამისად, დადგინდა მე-8 მუხლის დარღვევა.³⁴

გარდა ამისა, კანონმა აუცილებელია დააკმაყოფილოს 2 მოთხოვნა: „ხელმისაწვდომობა“ და „განჭვრეტადობა“. ხელმისაწვდომობის მოთხოვნების დასაკმაყოფილებლად, კანონი მარტივად ხელმისაწვდომი უნდა იყოს,³⁵ იმისათვის, რომ მოქალაქეს ჰქონდეს შესაძლებლობა გაერკვეს, თუ რომელი სამართლებრივი ნორმები გამოიყენება. განჭვრეტადობასთან მიმართებით,³⁶ მოქალაქეს უნდა შეეძლოს წინასწარ განსაზღვროს, თუ რა შედეგი შეიძლება მოჰყვეს მის ქმედებას.³⁷

საქმეზე *Klass v. Germany*³⁸ ევროპულმა კომისიამ და სასამართლომ მიუთითეს, რომ ადამიანის უფლების შეზღუდვისთვის საკმარისი არ არის ზოგადი სამართლებრივი საფუძვლის არსებობა. განიმარტა, რომ აუცილებელია კანონმდებლობამ კონკრეტულად გაითვალისწინოს უფლების შეზღუდვის პირობები და პროცედურები.³⁹

პრობლემურია საკითხი „განჭვრეტადობასთან“ მიმართებით, როდესაც ხორციელდება საიდუმლო მეთვალყურეობა. ასევე *Malone*⁴⁰ - ის საქმეში, სასამართლომ დაადასტურა, რომ კონვენციის მოთხოვნები განჭვრეტადობის თაობაზე შეუძლებელია განიხილებოდეს კომუნიკაციების შემოწმების კონტექსტში, ვინაიდან, ამ შემთხვევაში, ინდივიდს არ აქვს შესაძლებლობა განჭვრიტოს ხელისუფლების მხრიდან მის პირად კომუნიკაციაზე თვალთვალი. ამავე გადაწყვეტილებაში დაზუსტდა ტერმინი „კანონის“ მნიშვნელობა და განიმარტა, რომ შიდასახელმწიფოებრივ კანონმდებლობაში უნდა არსებობდეს საჯარო ხელისუფლების მიერ კონვენციის მე-8 მუხლის 1-ლი პუნქტით გათვალისწინებულ უფლებათა დაცვის მექანიზმი არამართლზომიერი შეზღუდვისაგან, განსაკუთრებით

³³ *Malone v. the United Kingdom*, ECtHR, App. No. 8691/79, 2 August 1984.

³⁴ Ibid.

³⁵ *Silver and Others v. The United Kingdom*, ECtHR, Judgment of 25 March 1983.

³⁶ *Anderson v. Sweden*, ECtHR, Judgment of 25 February 1992.

³⁷ ირინე ქურდაძე, კონსტანტინე კორკელია, ადამიანის უფლებათა საერთაშორისო სამართალი ადამიანის უფლებათა ევროპული კონვენციის მიხედვით, გვ. 175, 2004 წლის თებერვალი.

³⁸ *Klass and Others v. Germany*, ECtHR, Appl. No. 5029/71, 6 September 1978.

³⁹ Ibid.

⁴⁰ *Malone v. the United Kingdom*, ECtHR, App. No. 8691/79, 2 August 1984.

მაშინ, როდესაც ღონისძიებები ტარდება საიდუმლოდ და დიდია არამართლზომიერი მოქმედების რისკი.⁴¹

სატელეფონო საუბრების მოსმენა ისევე, როგორც სატელეფონო საუბრების სხვაგვარი მიყურადება, პირადი ცხოვრების და მიმოწერის უფლების შეზღუდვას წარმოადგენს, რომელიც უნდა ემსახურობდეს „ზუსტ“ კანონს. ამ საკითხზე საკმაოდ მნიშვნელოვანია ზუსტი და დეტალური წესების არსებობა, განსაკუთრებით იმის გათვალისწინებით, რომ ტექნოლოგია, რომელიც შეიძლება გამოყენებულ იქნეს, ყოველდღიურად ვითარდება.⁴²

კანონიერი მიზანი - ადამიანის უფლების მართლზომიერი შეზღუდვის შემდეგი პირობაა, რომ ჩარევა ემსახურობდეს კანონიერ მიზანს მე-8 მუხლის მე-2 პუნქტის შესაბამისად. მე-2 პუნქტში გაწერილია მიზანთა ნუსხა, რომელსაც შეიძლება დაეყრდნოს სახელმწიფო: ეროვნული უშიშროება; საზოგადოებრივი უსაფრთხოება ან ქვეყნის ეკონომიკური კეთილდღეობის ინტერესების დაცვა; უწესრიგობის ან დანაშაულის თავიდან აცილება; ჯანმრთელობის ან მორალისა თუ სხვათა უფლებათა და თავისუფლებათა დაცვა.

მოცემულ შემთხვევაში, მოპასუხე სახელმწიფოს ეკისრება ვალდებულება განსაზღვროს შეზღუდვის მიზანი/მიზნები. დაუშვებელია უფლების შეზღუდვა იმ მიზნით, რომელიც არ არის გათვალისწინებული კონვენციით. ხშირ შემთხვევაში, სწორედ ამ კუთხით შეინიშნება პრაქტიკაში პრობლემა, რადგან განმცხადებლები დავობენ, რომ სახელმწიფოს მიერ წარმოდგენილი მიზეზი არ არის რეალური.

დემოკრატიულ საზოგადოებაში აუცილებლობა - მე-8 მუხლის ტესტის ბოლო საფეხურზე უნდა განისაზღვროს არის თუ არა შეზღუდვა „აუცილებელი დემოკრატიულ საზოგადოებაში“. „აუცილებლობის“ ცნება გულისხმობს, რომ შეზღუდვა წარმოადგენდეს გადაუდებელ სოციალურ აუცილებლობას და იყოს კანონიერი მიზნის პროპორციული.⁴³

მოცემულ შემთხვევაში, სასამართლო ცდილობს დაიცვას ბალანსი სახელმწიფოსა და მოსარჩელის ინტერესებს შორის. ამისათვის, აუცილებელია არსებობდეს „მწვავე საზოგადოებრივი საჭიროება“ უფლებაში ჩარევისთვის, რომელიც თავდაპირველად უნდა შეფასდეს სახელმწიფოს მიერ. მოპასუხე სახელმწიფომ უნდა ამტკიცოს, რომ სახეზე იყო სწორედ მწვავე საზოგადოებრივი საჭიროება.⁴⁴ ამის

⁴¹ Malone v. the United Kingdom, ECtHR, App. No. 8691/79, 2 August 1984.

⁴² იხ. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები საქმეებზე: Kruslin v. France, ECtHR, App. No. 11801/85, 24 April 1990; Huvig v. France, ECtHR, App. No. 11105/84, 24 April 1990.

⁴³ Olsson v. Sweden (No. 1), ECtHR, Appl. No. 10465/83, 24 March 1988.

⁴⁴ Piechowicz v. Poland, ECtHR, App. No. 20071/07, 17 April 2012.

შემდეგ, სასამართლო განიხილავს თუ რამდენად გადააჭარბა/არ გადააჭარბა სახელმწიფომ დისკრეციული უფლებამოსილების ზღვარს, შეაფასებს წარმოდგენილ მტკიცებულებებს და იმსჯელებს, თუ რამდენად პროპორციული იყო გამოყენებული საშუალება ლეგიტიმური მიზნის მისაღწევად.⁴⁵

მნიშვნელოვანია ყურადღება გამახვილდეს, თუ რა მოიაზრება „დემოკრატიულ საზოგადოებაში.“ სასამართლომ საქმეში *Dudgeon v. the United Kingdom*⁴⁶ იმსჯელა შემწყნარებლობისა და ფართო აზროვნების შესახებ, როგორც დემოკრატიული საზოგადოების მახასიათებლებზე. სასამართლომ მე-8 მუხლის კონტექსტში ხაზი გაუსვა კანონის უზენაესობის მნიშვნელობას და კონვენციით განმტკიცებული უფლებების თვითნებური შეზღუდვის აღკვეთის საჭიროებას. დამატებით აღინიშნა, რომ კონვენციის მიზანია შეინარჩუნოს და განამტკიცოს დემოკრატიული საზოგადოების ღირებულებები. თუმცა, საბოლოოდ, აუცილებლობა დემოკრატიულ საზოგადოებაში განისაზღვრება ინდივიდუალურ უფლებებსა და საზოგადოებრივ ინტერესებს შორის ბალანსის დადგენით პროპორციულობის პრინციპის შესაბამისად.⁴⁷

პროპორციულობის პრინციპი გულისხმობს, რომ შეზღუდვა უნდა იყოს კონვენციით გათვალისწინებული ერთ-ერთი მიზნის მიღწევის პროპორციული. სასამართლომ თავის პრეცედენტულ სამართალში არაერთხელ განაცხადა, რომ ბალანსი პირის უფლებასა და საზოგადოების ინტერესებს შორის მხოლოდ იმ შემთხვევაში შეიძლება დადგინდეს, თუ პირის უფლების შეზღუდვა პროპორციულია იმ კანონიერი მიზნისა, რომლის მიღწევაც სურს სახელმწიფოს. ასევე, სახელმწიფომ უნდა ამტკიცოს, რომ გატარებული ღონისძიება ადეკვატური და აუცილებელია კანონიერი მიზნის მისაღწევად.⁴⁸

ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა რამდენიმე კრიტერიუმი, რომლის შესაბამისადაც განისაზღვრება იმ ღონისძიებათა პროპორციულობა, რომლითაც იზღუდება კონვენციით გათვალისწინებული უფლება. მაგალითად, თუ სახელმწიფოს კანონიერი მიზნის მიღწევა შეუძლია ნაკლებად მკაცრი, მაგრამ თანაბრად ეფექტიანი ღონისძიების გატარებით, მაშინ უფრო მკაცრი

⁴⁵ ECtHR, *Guide on Article 8 of the European Convention on Human Rights*, updated on 31 August 2018, p. 11.

⁴⁶ *Dudgeon v. The United Kingdom*, ECtHR, Appl. No. 7525/76, 22 October 1981.

⁴⁷ *Ibid.*

⁴⁸ ირინე ქურდაძე, კონსტანტინე კორკელია, *ადამიანის უფლებათა საერთაშორისო სამართალი ადამიანის უფლებათა ევროპული კონვენციის მიხედვით*, გვ. 75, 2004.

ღონისძიების გატარება გაუმართლებელი იქნება და არ ჩაითვლება დასახული მიზნის პროპორციულად.⁴⁹

სწორედ ამ სამი პირობის საფუძველზე აფასებს ადამიანის უფლებათა ევროპული სასამართლო ადამიანის უფლების შეზღუდვის მართლზომიერებას, რომლითაც უნდა იხელმძღვანელონ ეროვნულმა სასამართლოებმაც. საკითხზე მსჯელობისას, ეროვნულმა სასამართლოებმა პასუხი უნდა გასცენ კითხვებს: ეხება თუ არა ადამიანის უფლების შეზღუდვა კონვენციით გათვალისწინებულ უფლებებს? ითვალისწინებს თუ არა ქვეყნის კანონმდებლობა ამ შეზღუდვას? ემსახურება თუ არა კანონიერ მიზანს? არის თუ არა სახეზე მწვავე საზოგადოებრივი საჭიროება? ყველა კითხვაზე დადებითი პასუხის გაცემის შემდეგ, ადამიანის უფლებათა შეზღუდვა მართლზომიერად ჩაითვლება.⁵⁰

რაც შეეხება უშუალოდ მიმოწერის პატივისცემის უფლებას, მასში მოიაზრება როგორც სატელეფონო, ისე ნებისმიერი საშუალებით კომუნიკაციის დამყარება და პირთა შორის უწყვეტი და ცენზურის გარეშე კომუნიკაცია.

ადამიანის უფლებათა ევროპულმა სასამართლომ კომუნიკაციის პატივისცემის უფლების დაცვის სფეროში, სახელმწიფოთა მიმართ დაადგინა პოზიტიური ვალდებულებები,⁵¹ დაიცვან კონვენციით გათვალისწინებული უფლებები: სამუშაო ადგილზე არაპროფესიული ხასიათის კომუნიკაცია;⁵² პირადი საუბრების საჯარო სივრცეში გავრცელებისაგან თავის შეკავება;⁵³ პატიმართათვის ადამიანის უფლებათა ევროპულ სასამართლოსთან კომუნიკაციის ხელშეწყობა;⁵⁴ ჩანაწერების განადგურებაზე საკონსტიტუციო სასამართლოს გადაწყვეტილების აღსრულება, რომელიც ეხება სატელეფონო საუბრებს ადვოკატსა და მის კლიენტს შორის;⁵⁵ დაიცვან ბალანსი კომუნიკაციის პატივისცემის უფლებასა და გამოხატვის თავისუფლებას შორის.⁵⁶

⁴⁹ Campbell v. the United Kingdom, ECtHR, App. No. 13590/88, 25 March 1992.

⁵⁰ ირინე ქურდაძე, კონსტანტინე კორკელია, *ადამიანის უფლებათა საერთაშორისო სამართალი ადამიანის უფლებათა ევროპული კონვენციის მიხედვით*, გვ. 100, 2004.

⁵¹ ECtHR, *Guide on Article 8 of the European Convention on Human Rights*, updated on 31 August 2018, at 78.

⁵² Barbulescu v. Romania, ECtHR, Appl. No. 61496/08, Grand Chamber, Judgment of 5 September 2017.

⁵³ Craxi v. Italy (No. 2), ECtHR, Appl. No. 25337/94, Judgment of 17 October 2003.

⁵⁴ ECtHR, *Guide on Article 8 of the European Convention on Human Rights*, updated on 31 August 2018, p. 78.

⁵⁵ Ibid.

⁵⁶ Benediktssdottir v. Iceland, ECtHR, Appl. No. 38079/06, 16 June 2009.

3. პირადი კომუნიკაციის მონიტორინგის შემთხვევები სასამართლო პრაქტიკაში და სასამართლოთა მიდგომების შეფასება

3.1. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებათა ანალიზი და მისი მიდგომები კომუნიკაციაზე ზედამხედველობასთან მიმართებით

მოცემული თავის მიზანია კომუნიკაციის მონიტორინგთან მიმართებით ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებების განხილვა და მასთან დაკავშირებულ რელევანტურ საკითხებზე მსჯელობა.

ადამიანის უფლებათა ევროპული სასამართლოს 2018 წლის 13 სექტემბრის გადაწყვეტილება საქმეზე - *Big Brother Watch and Others v. the United Kingdom*⁵⁷ ერთ-ერთი ყველაზე რეზონანსულია და დღემდე განხილვის საგანს წარმოადგენს. ეს იყო პირველი შემთხვევა, როდესაც ადამიანის უფლებათა ევროპულმა სასამართლომ იმსჯელა გაერთიანებულ სამეფოში კომუნიკაციებზე მასობრივი თვალთვალის კუთხით არსებულ რეჟიმზე 2013 წელს ედუარდ სნოუდენის მიერ საიდუმლო ინფორმაციის გაცემის შემდეგ.

საქმე შეეხებოდა⁵⁸ მასობრივ თვალთვალს და კომუნიკაციების შესახებ ინფორმაციის უკონტროლო მოპოვებას. მოსარჩელები მიიჩნევდნენ, რომ ეროვნული რეჟიმი არღვევდა ადამიანის უფლებათა ევროპული კონვენციის მე-8, მე-10, მე-6 და მე-14 მუხლებს. სტატიის მიზნებისთვის, ყურადღება გამახვილდება მხოლოდ მე-8 მუხლით გათვალისწინებულ საკითხებზე.⁵⁹ სარჩელის საფუძველს წარმოადგენდა ედუარდ სნოუდენის მიერ გამჟღავნებული საიდუმლო ინფორმაცია, რომლის გამოაშკარავებთაც იკვეთებოდა კომუნიკაციაში უკონტროლო ჩარევის შემთხვევები.

მოსარჩელები დავობდნენ, რომ გაერთიანებული სამეფოს კანონმდებლობა, რომელიც არეგულირებდა კომუნიკაციების მოპოვების, გამოყენების, გაზიარების და განადგურების საკითხებს, არღვევდა კონვენციით გათვალისწინებულ სხვადასხვა უფლებებს. მოპასუხე სახელმწიფოს მთავარი არგუმენტი იყო ეროვნული უსაფრთხოების უზრუნველყოფა (მაგ. ტერორიზმთან ბრძოლა) და რეჟიმის არსებობას სწორედ ამ საფუძველით ამართლებდა.⁶⁰

⁵⁷Big Brother Watch and Others v. The United Kingdom, ECtHR, Appl. Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

⁵⁸ საქმეში გაერთიანდა 3 სხვადასხვა სარჩელი: Big Brother Watch and Others v. the United Kingdom (no. 58170/13); Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14); and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15).

⁵⁹ მე-8 მუხლთან ერთად, სასამართლომ დაადგინა მე-10 მუხლის დარღვევა.

⁶⁰ Big Brother Watch and Others v. The United Kingdom, ECtHR, Appl. Nos. 58170/13, 62322/14 and 24960/15, 13 September 2018, p. 120.

სასამართლომ პირველ რიგში განმარტა, რომ ინფორმაციის უკონტროლო მოპოვება *per se* არ არღვევს კონვენციას და ხელისუფლებას აქვს ფართო დისკრეცია გადაწყვიტოს, თუ რა სახის საზედამხედველო მექანიზმების გამოყენებაა აუცილებელი ეროვნული უსაფრთხოების დასაცავად.⁶¹ თუმცა, ამგვარი ქმედება უნდა აკმაყოფილებდეს შესაბამის მოთხოვნებს.⁶²

სასამართლომ დაადგინა, რომ შეინიშნებოდა სუსტი საზედამხედველო ორგანო, რომელიც ეფექტიანად გააკონტროლებდა კომუნიკაციის შესახებ ინფორმაციის მოპოვების პროცესს და მიუთითა პერსონალურ მონაცემთა დაცვის შესაბამისი გარანტიების არარსებობაზე.⁶³ შესაბამისად, მოცემულ ნაწილში განიმარტა, რომ რადგან პირად ცხოვრებაში ჩარევა არ იყო „აუცილებელი დემოკრატიულ საზოგადოებაში“, დაირღვა კონვენციის მე-8 მუხლი.⁶⁴

ასევე, სასამართლომ აღნიშნა, რომ კომუნიკაციებში ჩარევა მხოლოდ სერიოზულ დანაშაულებთან ბრძოლის მიზნებისთვის უნდა განხორციელდეს და ექვემდებარებოდეს დამოუკიდებელ სასამართლო კონტროლს. საქმეში არსებული ფაქტობრივი გარემოებების შესაბამისად, ამგვარი კონტროლი არ არსებობდა და ადგილი ჰქონდა მე-8 მუხლის დარღვევას.⁶⁵

უსაფრთხოების სამსახურთა შორის მონაცემთა გაზიარების/გაცვლის პროცედურებთან დაკავშირებით, სასამართლომ განმარტა, რომ კანონმდებლობით მკაფიოდ და ზუსტადაა განსაზღვრული მონაცემთა გადაცემის წესები სახელმწიფოთა შორის. შესაბამისად, ამ ნაწილში დარღვევას არ ჰქონდა ადგილი.⁶⁶

გარდა ზემოაღნიშნული გადაწყვეტილებისა, ევროპულმა სასამართლომ კომუნიკაციებზე თვალთვალის კუთხით იმსჯელა ქვემოთ მოცემულ საქმეებშიც, რომელთა ნაწილსაც *Big brother watch-ის* საქმეზე მსჯელობის დროს შეეხო.

საქმეში *Klass and Others v. Germany*⁶⁷ სასამართლომ იმსჯელა სახელმწიფოს მიერ საიდუმლო თვალთვალის განხორციელებაზე, რომლის შესაბამისადაც პირები, რომელთა კომუნიკაციაც კონტროლდება, არ არიან ინფორმირებულნი ამ ფაქტის

⁶¹ Ibid. p. 3.

⁶² იხ. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე, რომელშიც გაწერილია ხელისუფლების ორგანოების საქმიანობის განხორციელებისას ძირითადი მოთხოვნები: *Weber and Cesar Richard Saravia v. Germany*, ECtHR, Appl. No. 54934/00, decision on the admissibility, 29 June 2006.

⁶³ Ibid.

⁶⁴ Ibid.

⁶⁵ Ibid.

⁶⁶ ECtHR, *Some aspects of UK surveillance regimes violate Convention*, Press Release, issued by the Registrar of the Court, 13.09.2018, p. 4.

⁶⁷ *Klass and Others v. Germany*, ECtHR, Appl. No. 5029/71, 6 September 1978.

შესახებ. შედეგად, მე-8 მუხლით დაცულ სფეროში ჩარევა ხდება ისე, რომ ადამიანი ვერ იცავს საკუთარ თავს.⁶⁸ სასამართლომ ასევე მიუთითა საზოგადოებრივი ინტერესის მნიშვნელობაზე - გამოკვეთა ტერორიზმთან დაკავშირებული საფრთხეები და სახელმწიფოს მოვალეობა უზრუნველყოს ქვეყნის უსაფრთხოება. აქედან გამომდინარე, კანონმდებლობით სახელმწიფოს ენიჭება უფლებამოსილება ჩაერიოს პირად კომუნიკაციაში მხოლოდ გამონაკლის შემთხვევებში ეროვნული უსაფრთხოებისა და დანაშაულის პრევენციის ინტერესებიდან გამომდინარე. აღინიშნა, რომ ეროვნული კანონმდებლობა უნდა ითვალისწინებდეს შესაბამის გარანტიებს ხელისუფლების ორგანოების მხრიდან უფლებამოსილების ბოროტად ან თვითნებურად გამოყენებაზე.⁶⁹

სასამართლომ *Weber and Saravia v. Germany*⁷⁰ საქმეში განსაზღვრა კომუნიკაციებზე მეთვალყურეობისას გასათვალისწინებელი მინიმალური გარანტიები, რომელსაც უნდა ითვალისწინებდეს ხელშემკვრელ სახელმწიფოთა კანონმდებლობა: კანონით უნდა განისაზღვროს დანაშაულთა სახეების ჩამონათვალი, რა შემთხვევაშიც შეიძლება გაიცეს კომუნიკაციის კონტროლის ბრძანება; დადგინდეს კომუნიკაციის კონტროლის ან ფარული თვალთვალის ვადები და ხანგრძლივობა; შემუშავდეს ფარული თვალთვალის შედეგად მოპოვებული ინფორმაციის გამოკვლევის, გამოყენებისა და შენახვის წესები და მესამე მხარისათვის გადაცემის პროცედურები.⁷¹

საქმეში - *Liberty and Others v. the United Kingdom*⁷² სასამართლომ დაადგინა, რომ მოქმედი კანონმდებლობა პირებს ჯეროვანი სამართლებრივი დაცვის გარანტიებით ვერ უზრუნველყოფდა და იზრდებოდა ხელისუფლების ორგანოების მხრიდან თვითნებობის რისკი. შესაბამისად, სასამართლომ დიდი ბრიტანეთის მასობრივი თვალთვალისათვის განსაზღვრული სამართლებრივი ჩარჩო კონვენციასთან შეუთავსებლად ცნო.

⁶⁸ ECtHR, *Guide on Article 8 of the European Convention on Human Rights*, Updated on 30 April 2019, p. 40.

⁶⁹ ECtHR, Factsheet – *Mass Surveillance*, February 2019, p.1. ხელმისაწვდომია: <http://bit.do/eUngP> (ბოლოს ნანახია: 06.06.2019).

⁷⁰ *Weber and Cesar Richard Saravia v. Germany*, ECtHR, Appl. No. 54934/00, decision on the admissibility, 29 June 2006.

⁷¹ ბესარიონ ბოხაშვილი, კონსტანტინე კორკელია, *პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკისა და საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკის მიმოხილვა*, 2017 წლის ოქტომბერი, გვ. 194.

⁷² *Liberty and Others v. the United Kingdom*, ECtHR, Appl. No. 58243/00, 1 July 2008.

*Kennedy v. the United Kingdom*⁷³ - ის საქმის განხილვისას სასამართლომ განაცხადა, რომ კანონში ასახული უნდა იყოს პირადი კომუნიკაციის მონიტორინგის განხორციელებისთვის შესაბამისი დანაშაულის კატეგორიები, თუმცა მიუთითა, რომ კანონის განჭრეტადობის პირობა არ მოითხოვს კონკრეტული დანაშაულების ამომწურავი ჩამონათვალის განსაზღვრას. შესაბამისად, სახელმწიფოებს არ ეკისრებათ ვალდებულება ამომწურავად განსაზღვრონ ის დანაშაულები, რომელთა ჩადენის ან საფრთხის არსებობის შემთხვევაში ნებადართული იქნება კომუნიკაციის კონტროლის განხორციელება.⁷⁴ დამატებით განიმარტა, რომ საფრთხე, რომელიც ხელყოფს ეროვნული უსაფრთხოების ინტერესებს, შეიძლება განსხვავდებოდეს თავისი ბუნებით და, შესაბამისად, საკმაოდ რთულია მისი განსაზღვრა.

ევროპული სასამართლო დიდ მნიშვნელობას ანიჭებს სამართალდამცავი ორგანოების საქმიანობაზე ზედამხედველობას. *Roman Zakharov v. Russia*⁷⁵ საქმის განხილვისას, სასამართლომ ყურადღება გაამახვილა საკანონმდებლო პროცედურებსა და მაკონტროლებელი ორგანოების საქმიანობაზე. დაადგინა, რომ რუსეთის კანონმდებლობა ვერ უზრუნველყოფდა მოსარჩელეთა დაცვას კომუნიკაციის თვითნებური კონტროლისაგან. უფრო კონკრეტულად, სასამართლომ აღმოაჩინა ხარვეზები ეროვნულ კანონმდებლობაში, რომელიც უკავშირდებოდა: გარემოებებს, რომლის დროსაც სამართალდამცავ ორგანოებს წარმოეშობოდათ კომუნიკაციის კონტროლის უფლება; კომუნიკაციაზე ზედამხედველობის შეწყვეტის საფუძვლებს; ფარული მიყურადების განხორციელების ავტორიზაციისთვის შესაბამის პროცედურებს; მონაცემთა შენახვისა და განადგურების საკითხებს.⁷⁶

*Szabo and Vissy v. Hungary*⁷⁷ - ის საქმე უკავშირდებოდა უნგრეთის კანონმდებლობას საიდუმლო ანტიტერორისტულ ზედამხედველობაზე. სასამართლომ დაადგინა, რომ ადგილი ჰქონდა კონვენციის მე-8 მუხლის დარღვევას. ერთი მხრივ, აღინიშნა, რომ ტერორიზმთან ბრძოლისა ან დანაშაულის თავიდან აცილების მიზნით, ხელისუფლების ორგანოს აქვს უფლებამოსილება განახორციელოს მონიტორინგი კომუნიკაციებზე, თუმცა, მეორე მხრივ, არსებული კანონმდებლობა ვერ უზრუნველყოფდა ეფექტიან გარანტიებს თვითნებობის შემცირებისთვის. გამოიკვეთა, რომ მიმოწერის კონტროლის დროს, შესაბამისად არ ფასდებოდა ზომის გამოყენების აუცილებლობა.

⁷³ *Kennedy v. the United Kingdom*, ECtHR, Appl. No. 26839/05, 18 May 2010.

⁷⁴ *Ibid.* P. 45.

⁷⁵ *Roman Zakharov v. Russia*, ECtHR, Appl. No. 47143/06, Grand Chamber, 4 December 2015.

⁷⁶ ECtHR, Factsheet – *Mass Surveillance*, February 2019, p.3. ხელმისაწვდომია: <http://bit.do/eUngP> (ბოლოს ნანახია: 09.06.2019).

⁷⁷ *Szabo and Vissy v. Hungary*, ECtHR, Appl. No. 37138/14, 12 January 2016.

3.2. მართლმსაჯულების ევროპული კავშირის სასამართლოს მიდგომები კომუნიკაციებზე მეთვალყურეობისას

მართლმსაჯულების ევროპული კავშირის სასამართლოს⁷⁸ პრაქტიკაში კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვა ერთ-ერთი აქტუალური საკითხია.

*Digital Rights Ireland and Seitlinger and Others*⁷⁹ საქმით სასამართლომ ძალადაკარგულად გამოაცხადა დირექტივა მონაცემთა დაცვის შესახებ,⁸⁰ რომლითაც ვალდებულება ეკისრებოდათ საკომუნიკაციო ქსელების პროვაიდერებს მოეგროვებინათ ინფორმაცია მხარეებს შორის კომუნიკაციის დროისა და ხანგრძლივობის შესახებ - „ტრაფიკის მონაცემები“ და ასევე მონაცემები, რომელიც ეხება საკომუნიკაციო მოწყობილობის ადგილმდებარეობას, ე. წ. „ადგილმდებარეობის შესახებ მონაცემები“. აღნიშნული მონაცემები 6 თვიდან 2 წლამდე ინახებოდა, კატეგორიებს შორის ყოველგვარი დიფერენციაციის გარეშე, დანაშაულთან ბრძოლის მიზნებისთვის.

გადაწყვეტილების შესაბამისად, მიუხედავად იმისა, რომ დირექტივა კომუნიკაციის შინაარსის მოპოვებას არ ითვალისწინებდა, არსებული ინფორმაცია შეიძლებოდა ყოფილიყო კავშირში პირად ცხოვრებასთან. შესაბამისად, დადგენილი ვალდებულება მოიაზრებდა პირადი ცხოვრების და მიმოწერის პატივისცემის უფლებაში ჩარევას, რაც გარანტირებულია ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7 და პერსონალურ მონაცემთა დაცვის მე-8 მუხლის შესაბამისად.⁸¹

სასამართლომ განმარტა, რომ უფლებაში ჩარევა მხოლოდ ეროვნული უსაფრთხოების მიზნით შეიძლება განხორციელდეს. მოცემულ შემთხვევაში კი, პროპორციულობის მოთხოვნა ვერ კმაყოფილდებოდა.

დირექტივის შესაბამისად, მონაცემთა შეგროვება ხდებოდა ყოველგვარი დიფერენციაციის, შეზღუდვის ან გამონაკლისის გარეშე, რომელიც ითვალისწინებს მძიმე დანაშაულების წინააღმდეგ ბრძოლას. დირექტივის ნაკლოვანებას წარმოადგენდა ისიც, რომ არ იყო დადგენილი ობიექტური კრიტერიუმი, რომელიც განსაზღვრავდა, თუ რომელი სამართალდარღვევა შეიძლება ჩათვლილიყო საკმარისად მძიმედ ქარტიის მე-7 და მე-8 მუხლის მოთხოვნების

⁷⁸ CJEU - Court of Justice of the European Union.

⁷⁹ Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others and Seitlinger and Others (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238), CJEU.

⁸⁰ EU, Data Retention Directive 2006/24/EC.

დასაკმაყოფილებლად. კომპეტენტური ორგანოების მიერ მონაცემებზე წვდომა და მათი გამოყენება არ ექვემდებარებოდა წინასწარ განხილვას სასამართლო ან დამოუკიდებელი ადმინისტრაციული ორგანოს მიერ, რომლითაც შეიზღუდებოდა კომუნიკაციაში ჩარევა.

მოცემულ გარემოებებზე დაყრდნობით, სასამართლომ დაადგინა, რომ დირექტივის ძირითად უფლებებში ჩარევა არ არის საკმარისად შეზღუდული, რათა უზრუნველყოს ჩარევა იმ მოცულობით, რაც მკაცრად აუცილებელია.

Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,⁸² გადაწყვეტილებაში განიმარტა, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის მარეგულირებელი ეროვნული კანონმდებლობა უნდა შეიცავდეს მკაფიო წესებს მონაცემთა შენახვის მასშტაბსა და გამოყენების ფარგლებთან მიმართებით. კონკრეტულად, უნდა არსებობდეს ობიექტური კრიტერიუმი, რომლის მიხედვითაც დადგინდება კავშირი შესანახ მონაცემებსა და ლეგიტიმურ მიზანს შორის. ამ მიზნით, უნდა განისაზღვრონ პირები, რომელთაც შესაძლოა პირდაპირი/არაპირდაპირი კავშირი ჰქონდეთ სერიოზულ დანაშაულთან.

აღნიშნულ საქმეში, სასამართლომ იმსჯელა 2014 წლის მონაცემთა დაცვის და საგამომიებო რეგულირების აქტის 1-ლი ნაწილის კანონიერებაზე,⁸³ რომელიც ითვალისწინებდა სახელმწიფოს თანამდებობის პირის უფლებას მოეთხოვა სატელეკომუნიკაციო ოპერატორისთვის მნიშვნელოვანი საკომუნიკაციო მონაცემების შეგროვება. მოსარჩელები მიიჩნევდნენ, რომ 1-ლი ნაწილი ქარტიის მე-7 და მე-8 და ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის მოთხოვნებს არ შეესაბამებოდა.

სასამართლომ ყურადღება გაამახვილა სამართალდამცავი ორგანოების უფლებაზე პერსონალურ მონაცემებზე წვდომის თვალსაზრისით და აღნიშნა, რომ ორგანოების დაშვება უნდა მოხდეს იმ პირთა მონაცემებზე, რომლებთა მიმართაც არსებობს სერიოზული ეჭვი დანაშაულის დაგეგმვის, ჩადენის ან ასეთ დანაშაულში ნებისმიერი გზით მონაწილეობის შესახებ.

⁸² *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, CJEU, NC-203/15, C-698/15, 2016, § 109-111. ხელმისაწვდომია: <http://bit.do/eVBf7> (ბოლოს ნანახია: 20.06.2019).

⁸³ (DRIPA) – Data Retention and Investigatory Powers Act, 2014.

3.3. სად გადის ზღვარი კომუნიკაციის პატივისცემის უფლებასა და ეროვნულ უსაფრთხოებას შორის?

ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლო პრაქტიკის განხილვის შედეგად გამოიკვეთა, რომ ძირითად შემთხვევაში სახელმწიფოთა მიერ კომუნიკაციის კონტროლი ეროვნული უსაფრთხოების უზრუნველყოფის არგუმენტებით ხორციელდება. ამ თავის მიზანია კომუნიკაციის პატივისცემის უფლებასა და ეროვნულ უსაფრთხოებას შორის ბალანსის დაცვის საკითხებზე მსჯელობა.

შეერთებულ შტატებში 2001 წლის შემდეგ ეროვნული უსაფრთხოების სააგენტოში არსებობდა სპეციალური პროგრამა, რომელიც ცნობილი იყო „პრეზიდენტის სათვალთვალო პროგრამის“ სახელით.⁸⁴ ამ სისტემის შესაბამისად, ქვეყნის შიგნით ყოველგვარი საფუძვლის გარეშე ხორციელდებოდა ადამიანთა კომუნიკაციის კონტროლი ტერორიზმის საბაზით. სახელმწიფომ დაავალდებულა სატელეკომუნიკაციო კომპანიები, რომ გადაეცათ თითოეულ მომხმარებელზე საუბრის ჩანაწერები, რომლებიც მოიცავდა აბონენტის სახელს, მისამართს და სხვა მნიშვნელოვან პერსონალურ ინფორმაციას. გარდა ამისა, აქტიურად გამოიყენებოდა მოწყობილობები კომპანიებისგან პირთა კომუნიკაციის შესახებ ინფორმაციის მოსაპოვებლად. ამდენად, ადამიანის პირადი სივრცე აღარ არსებობდა და ამას საფუძვლად სწორედ ეროვნული უსაფრთხოება ედო.⁸⁵

მოცემულ ინტერესებს შორის ბალანსის⁸⁶ დაცვის დინამიკა სხვადასხვაგვარია, რაზეც გავლენას ახდენს ფუნდამენტური ინტერესების შინაარსობრივი ფარგლები. ეროვნული უსაფრთხოების ბუნება არასდროს არის განსაზღვრული და კონკრეტული. იგი დაკავშირებულია წინააღმდეგობრივ ინტერესებთან: პირები, საზოგადოება, სახელმწიფოს შიდა და გარე საფრთხეები. ამგვარად, ეროვნული უსაფრთხოების საკითხი არ არის სტატიკური ბუნების, განსაკუთრებით კიბერსივრცეში. ამის მსგავსად, კომპლექსურია პირადი ცხოვრების დაცვის უფლება. აქედან გამომდინარე, გასათვალისწინებელია დროის ელემენტი და საფრთხის აღქმადობა. ეს ეხება ომის ან კონფლიქტის პერიოდს, როდესაც გამოვლინდება სახელმწიფოს პოლიტიკური და სოციალური წესრიგის საფრთხე.⁸⁷

⁸⁴ President's Surveillance Program”.

⁸⁵ Laidey N. M., *Privacy vs. National Security: Where Do We Draw the Line?* World Academy of Science, Engineering and Technology International Journal of Law and Political Sciences vol:9, No:6, 2015, 2.

⁸⁶ პირადი ცხოვრება და ეროვნული უსაფრთხოება.

⁸⁷ Zaure, A., *Balance for Privacy, Freedom of Information and National Security*, University of Tartu (Estonia), Department of International Law, 2.

ადამიანის უფლებათა ევროპული სასამართლოს მიხედვით, სახელმწიფოს გარკვეულწილად აქვს ლეგიტიმური უფლება შეზღუდოს პირადი ცხოვრების ხელშეუხებლობა ეროვნული უსაფრთხოების დაცვის მოტივით. აქედან გამომდინარე, საფრთხის არსებობისას, სახელმწიფოს შესაბამის ორგანოებს აქვთ უფლებამოსილება, შეაგროვონ პირადი ინფორმაცია და უსაფრთხოების უზრუნველსაყოფად გამოიყენონ. მოცემულ შემთხვევაში, უნდა დაბალანსდეს სახელმწიფოს ინტერესი და შეზღუდვის ფორმა და ზომა, ამდენად, სახელმწიფოს ეს უფლება არ არის შეუზღუდავი.⁸⁸

ადამიანის უფლებათა ევროპული სასამართლოს მიდგომები მოწმობს, რომ უპირატესობა ეროვნულ უსაფრთხოებას იმ შემთხვევაში ენიჭება, როდესაც დაკმაყოფილებულია უფლების კანონიერი შეზღუდვის ტესტი: აუცილებლობა, ლეგიტიმურობა და პროპორციულობა.⁸⁹

ადამიანის უფლებებსა და ეროვნულ უსაფრთხოებას შორის მკაფიო საზღვრის გავლება სირთულეებთანაა დაკავშირებული, თუმცა მკაფიოდ გაწერილი კანონმდებლობით და კონკრეტული სიტუაციის ობიექტური შეფასებით, შესაძლებელია ბალანსის სწორად დაცვა.

4. სახელმწიფო უსაფრთხოების სამსახურების საქმიანობის კონტროლის მექანიზმები

უსაფრთხოების სამსახურებზე ზედამხედველობის საერთაშორისო და ევროპული სტანდარტები იყოფა მავალდებულებელ სამართლებრივ ინსტრუმენტებად და არამავალდებულებელ პრინციპებად ან რეკომენდაციებად. პირველ კატეგორიაში მოიაზრება დებულებები საერთაშორისო და რეგიონული ხელშეკრულებებიდან (ასევე, მნიშვნელოვანია მათი ინტერპრეტაცია შესაბამის სასამართლოთა ან ხელშეკრულების ორგანოთა მიერ). ხოლო, არამავალდებულებელ პრინციპში (რბილი სამართალი) მოიაზრება რეკომენდაციები, რეზოლუციები, განცხადებები და საანგარიშო მოხსენებები.⁹⁰

⁸⁸ „პირადი ცხოვრების ხელშეუხებლობის უფლება ადამიანის უფლებათა და ძირითად თავისუფლებათა კონვენციის მიხედვით.“ ხელმისაწვდომია: <http://bit.do/eTbCC> (ბოლოს ნანახია: 23.05.2019).

⁸⁹ იხ. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები შესაბამის საკითხზე: Chauvy and Others v. France, ECtHR, Appl. No. 64915/01, 2004 წლის 29 სექტემბერი, para. 70; Pfeifer v. Austria, ECtHR, Appl. No. 12556/03, 2007 წლის 15 ნოემბერი, Para. 35; Polanco Torres and Movilla Polanco v. Spain, ECtHR, Appl. No. 34147/06, 2010 წლის 21 სექტემბერი, Para. 40.

⁹⁰ საანგარიშო მოხსენებები შემდეგი წყაროებიდან: 1) გაერთიანებული ერების ინსტიტუტები, მათ შორის, გენერალური ასამბლეა და სპეციალური მანდატის მფლობელები; 2) ევროპის საბჭოს ინსტიტუტები, ვენეციის კომისიის, საპარლამენტო ასამბლეის (PACE) მომხსენებლების ჩათვლით (მათ შორის ადამიანის უფლებათა კომისარი); 3) ევროპის კავშირი; 4) ტრანსნაციონალური ინიციატივები სამოქალაქო საზოგადოების ხელმძღვანელობით.

თავის მხრივ, უსაფრთხოების სამსახურის კონტროლში მოიაზრება ნებართვის გაცემა უსაფრთხოების სამსახურებისთვის კონკრეტული ნაბიჯის გადასადგმელად. ზედამხედველობის მიზანია ძალაუფლების ბოროტად გამოყენების თავიდან არიდება და უფლებაში ჩარევის ლეგიტიმაცია.⁹¹

ინფორმაციის შეგროვების საფუძვლები უნდა იყოს კანონით განსაზღვრული. აუცილებელია შეიქმნას დამოუკიდებელი და ძლიერი საზედამხედველო სისტემა, რომლის მეშვეობითაც გაკონტროლდება კომუნიკაციაზე წვდომისთვის უფლებამოსილი ორგანოების საქმიანობა.⁹²

OECD-ის 2013 წლის სახელმძღვანელოში მითითებულია, რომ პერსონალური მონაცემები უნდა იყოს დაცული შესაბამისი უსაფრთხოების გარანტიებით უკანონო წვდომის, გამოყენებისა და გამჟღავნებისაგან.⁹³

გაეროს გენერალურმა ასამბლეამ მოუწოდა სახელმწიფოებს შეექმნათ ან შეენარჩუნებინათ დამოუკიდებელი, ეფექტიანი, შესაბამისი რესურსებით აღჭურვილი მიუკერძოებელი სასამართლო, ადმინისტრაციული ან/და საპარლამენტო საზედამხედველო მექანიზმები, რომლებიც უზრუნველყოფდა გამჭვირვალობას და ანგარიშვალდებულებას კომუნიკაციებზე თვალთვალისა და პერსონალურ მონაცემთა შეგროვებისას.⁹⁴

მაკონტროლებელი ორგანოს უფლებამოსილების ფარგლები შესაძლოა მოიცავდეს 3 ეტაპს: 1) საქმიანობის დასაწყებად ნებართვის გაცემა; 2) საქმიანობის განხორციელების პროცესი; 3) საქმიანობის დასრულების შემდგომი ეტაპი.⁹⁵

ვენეციის კომისიის ანგარიშისა და ზოგადი კვლევების შესაბამისად „გარე“ საზედამხედველო სისტემა უნდა შედგებოდეს შემდეგი ინსტიტუციებისგან: კონტროლი აღმასრულებელი ორგანოს მიერ; საპარლამენტო ზედამხედველობა; სასამართლო ორგანო; ექსპერტთა ორგანოები.⁹⁶

ევროპის საბჭოს ადამიანის უფლებათა კომისარმა ყურადღება გაამახვილა „შიდა კონტროლის“ მნიშვნელობაზე და აღნიშნა, რომ მხოლოდ „გარე

⁹¹ FRA (European Union Agency for Fundamental Rights), *Surveillance by intelligence services: fundamental rights safeguard and remedies in the EU, Volume I: Member States' legal frameworks*, 2017, p. 29.

⁹² Privacy, Data and Technology: *Human Rights Challenges in the Digital Age*, paper issued by the New Zealand Human Rights Commission, May 2018, p. 29.

⁹³ OECD (The Organisation for Economic Co-operation and Development) Guidelines, Security Safeguards Principle 11. ხელმისაწვდომია: <http://bit.do/eZWIn> (ბოლოს ნანახია: 15.07.2019).

⁹⁴ UN, General Assembly Resolution on the Right to Privacy in the Digital Age (19 December 2016).

⁹⁵ Privacy, Data and Technology: *Human Rights Challenges in the Digital Age*, paper issued by the New Zealand Human Rights Commission, May 2018, p. 29.

⁹⁶ FRA (European Union Agency for Fundamental Rights), *Surveillance by intelligence services: fundamental rights safeguard and remedies in the EU, Volume I: Member States' legal frameworks*, 2017, p. 29.

ზედამხედველობით“ მიზანი ვერ მიიღწევა, შესაბამისად, აუცილებელია უსაფრთხოების სამსახურის სისტემის შიგნით კონტროლის მექანიზმის არსებობა ადამიანის უფლებათა დაცვის უზრუნველსაყოფად.⁹⁷ დამატებით, ადამიანის უფლებათა კომისარმა წევრ სახელმწიფოებს მოუწოდა საზედამხედველო სისტემის პერიოდულად გადახედვისაკენ, რათა დარწმუნდნენ მის გამართულ მუშაობაში.⁹⁸

დამოუკიდებელი ზედამხედველობა წარმოადგენს მონაცემთა დაცვის არსებით კომპონენტს ევროპულ სისტემაში. ევროკავშირისა და ევროსაბჭოს ფარგლებში დამოუკიდებელი საზედამხედველო ორგანოს არსებობა შეუცვლელი კომპონენტია პირთა უფლებებისა და თავისუფლებების ეფექტიანი დაცვისთვის მათ პერსონალურ მონაცემთა დამუშავების თვალსაზრისით.

„პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 108-ე კონვენციის დამატებითი ოქმით საზედამხედველო ორგანოების შექმნა სავალდებულო გახდა. დოკუმენტის პირველი მუხლით მოცემულია დამოუკიდებელი საზედამხედველო ორგანოების სამართლებრივი მოწესრიგება, რომლის იმპლემენტირებაც უნდა მოახდინონ წევრმა სახელმწიფოებმა.⁹⁹ დამოუკიდებელი საზედამხედველო ორგანოს შექმნის აუცილებლობაზე ყურადღება გამახვილებულია პერსონალურ მონაცემთა დაცვის ზოგად რეგულაციაშიც.¹⁰⁰

5. პირადი კომუნიკაციის კონტროლი და პერსონალურ მონაცემთა დაცვის სტანდარტები საქართველოში

5.1. პერსონალურ მონაცემთა დაცვის მიმართულებით არსებული კანონმდებლობა და საქართველოს საერთაშორისო ვალდებულებები

საქართველოს კონსტიტუციით გარანტირებულია პირადი ცხოვრების ხელშეუხებლობა, პიროვნების განვითარება, ღირსების დაცვა და მოქალაქისთვის მის შესახებ არსებული ინფორმაციის გაცნობის უფლება, რომელიც სახელმწიფოს აკისრებს ვალდებულებას დაიცვას პირთან დაკავშირებული სხვადასხვა სახის ინფორმაცია.¹⁰¹ აღნიშნული ქმნის პერსონალურ მონაცემთა დაცვის კანონმდებლობის კონსტიტუციურ გარანტიას და საფუძველს.

⁹⁷ Council of Europe Commissioner for Human Rights, 2015, p. 8

⁹⁸ Ibid.

⁹⁹ სახელმძღვანელო: მონაცემთა დაცვის ევროპული სამართალი, გამომცემლობა - „იურისტების სამყარო“, გვ. 154.

¹⁰⁰ EU, GDPR – General Data Protection Regulation, 2018, Art. 51.

¹⁰¹ იხ. საქართველოს კონსტიტუციის მე-15, მე-12, მე-9 და მე-18 მუხლები, 23.03.2018.

კონსტიტუციით გარანტირებული უფლებების რეალიზებისთვის მნიშვნელოვანია მონაცემთა დამუშავება განხორციელდეს მხოლოდ კანონის შესაბამისად. ამ პროცესში, აუცილებელია პირმა იცოდეს, თუ როდის იქნება მის პირად ცხოვრებაში ჩარევა ლეგიტიმური და დაცვის რა საშუალებები არსებობს.¹⁰²

საქართველოს ზოგადი ადმინისტრაციული კოდექსი ითვალისწინებს პერსონალურ მონაცემთა დაცვას, რომელიც საჯარო ინფორმაციის ხელმისაწვდომობის შეზღუდვის ერთ-ერთი საფუძველია. საჯარო დაწესებულება ვალდებულია არ გაახმაუროს პირის პერსონალური მონაცემები ამ პირის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების ინტერესების დაცვა.¹⁰³

საქართველოში უშუალოდ პერსონალურ მონაცემთა დაცვის მარეგულირებელი საკანონმდებლო ბაზა 2011 წლის ბოლოს შეიქმნა და სრულად 2014 წლის 1-ლი ნოემბრიდან ამოქმედდა.¹⁰⁴

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი საერთაშორისო სტანდარტების შესაბამისად, ადგენს მონაცემთა დამუშავების პრინციპებს და განსაზღვრავს მონაცემთა დამუშავების სამართლებრივ საფუძვლებს.¹⁰⁵ კანონის მიზანია, პერსონალურ მონაცემთა დამუშავებისას ადამიანის უფლებათა და თავისუფლებათა, მათ შორის პირადი ცხოვრების ხელშეუხებლობის დაცვის უზრუნველყოფა.

საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ ადგენს საქართველოს ტერიტორიაზე ელექტრონული საკომუნიკაციო ქსელებით და საშუალებებით საქმიანობის სამართლებრივ და ეკონომიკურ საფუძვლებს.¹⁰⁶ აღნიშნულ კანონში გათვალისწინებულია პერსონალურ მონაცემთა დაცვის ძირითადი პრინციპები.¹⁰⁷

საქართველოს სისხლის სამართლის კოდექსის 175-ე მუხლი პერსონალურ მონაცემთა ხელყოფას დანაშაულად აღიარებს. ასევე, საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-7 მუხლის თანახმად: „პირს, რომელსაც ზიანი

¹⁰² თამარ ქალდანი, ნინო სარიშვილი, *პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში*, ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები, სტატიათა კრებული, რედ. კონსტანტინე კორკელია, 2016.

¹⁰³ იხ. საქართველოს ზოგადი ადმინისტრაციული კოდექსის 28-ე და 44-ე მუხლები.

¹⁰⁴ თამარ ქალდანი, ნინო სარიშვილი, *პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში*, ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები, სტატიათა კრებული, რედ. კონსტანტინე კორკელია, 2016.

¹⁰⁵ იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-4 და მე-5 მუხლები.

¹⁰⁶ იხ. საქართველოს კანონი ელექტრონული კომუნიკაციების შესახებ, 1-ლი მუხლი.

¹⁰⁷ Ibid., მე-19 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი, 24-ე მუხლი და 33-ე მუხლის მე-3 ნაწილი.

მიადგა მისი პირადი ცხოვრების შესახებ ცნობების/პერსონალური მონაცემების უკანონოდ გამჟღავნებით, აქვს საქართველოს კანონმდებლობით დადგენილი წესით ზიანის სრულად ანაზღაურების უფლება.

ოპერატიულ-სამძებრო საქმიანობის შესახებ საქართველოს კანონის თანახმად, ოპერატიულ-სამძებრო საქმიანობის ამსახველი მონაცემების, დოკუმენტებისა და წყაროების დადგენილი წესით გაცნობის უფლება აქვთ მხოლოდ ამ კანონით განსაზღვრულ პირებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად (პერსონალურ მონაცემთა დაცვის ინსპექტორს და მის მიერ უფლებამოსილ პირს).¹⁰⁸

პერსონალურ მონაცემთა დაცვაზე ზედამხედველობას ახორციელებს საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორი „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის შესაბამისად.

საქართველოსა და ევროკავშირის შორის გაფორმებული ასოცირების შეთანხმებით,¹⁰⁹ საქართველოს აქვს ნაკისრი ვალდებულებები მოახდინოს კანონმდებლობის ჰარმონიზება ევროკავშირის კანონმდებლობასთან. ვალდებულებებში მოიაზრება პერსონალურ მონაცემთა მიმართულებით ევროპული სტანდარტების დანერგვა. აქედან გამომდინარე, საქართველოს სამომავლო წევრობის საკითხი, სხვა თემებთან ერთად, პერსონალურ მონაცემთა დაცვის მიმართულებით მაღალი სტანდარტების დანერგვასაც უკავშირდება.¹¹⁰

5.2. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება და მისი შედეგები

2016 წლის 14 აპრილს, საკონსტიტუციო სასამართლოს მიერ მიღებული გადაწყვეტილებაში გაჟღერდა ყველა ის პრობლემური საკითხი, რამაც შეიძლება გამოიწვიოს ადამიანის უფლებებში გაუმართლებელი ჩარევა. გადაწყვეტილება შეეხებოდა თანამედროვე ტექნოლოგიების პირობებში ადამიანთა კომუნიკაციის პატივისცემის, პერსონალურ მონაცემთა დაცვის და სამართალდამცავი ორგანოების მხრიდან ადამიანის უფლებებში მართლზომიერი ჩარევის საკითხებს.

დავის საგანს წარმოადგენდა „ელექტრონული კომუნიკაციის შესახებ“ კანონის ნორმები, რომლებიც სახელმწიფო უსაფრთხოების სამსახურს ანიჭებდა უფლებამოსილებას, ჰქონოდა კავშირგაბმულობის და კომუნიკაციის ფიზიკური

¹⁰⁸ იხ. ოპერატიულ-სამძებრო საქმიანობის შესახებ საქართველოს კანონის მე-5 მუხლი.

¹⁰⁹ ასოცირების შესახებ შეთანხმება ერთის მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებსა და მეორეს მხრივ, საქართველოს შორის.

¹¹⁰ Ibid., მუხლი 14.

ხაზებიდან ინფორმაციის რეალურ დროში მოპოვების და ამ მიზნით სათანადო აპარატურის და პროგრამული უზრუნველყოფის საშუალებების განთავსების შესაძლებლობა.

მიღებული გადაწყვეტილების თანახმად, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა პირადი ცხოვრების უფლებაში ჩარევად იქნა მიჩნეული. აღინიშნა, რომ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ „მონაცემთა ერთობლიობა ქმნის შესაძლებლობას, უფლებამოსილ ორგანოებს ჰქონდეთ საკმარისი ინფორმაცია აბონენტის პირადი ცხოვრების ისეთი სფეროების შესახებ, როგორებიცაა: მათი ყოველდღიური ჩვევები, დროებითი ან მუდმივი ადგილსამყოფელი, ყოველწუთიერი გადაადგილება, საქმიანობა, სოციალური კავშირები, სოციალური გარემოცვა.“ შესაბამისად, განიმარტა, რომ წარმოდგენილი ინფორმაცია შეიძლება იძლეოდეს დეტალურ წარმოდგენას ადამიანის პირადი სივრცის არაერთ მნიშვნელოვან ასპექტზე, რაც იწვევს პირად ცხოვრებაში ინტენსიურ ჩარევას.

სასამართლომ არაკონსტიტუციურად ცნო ფარულ საგამომიებო მოქმედებებთან დაკავშირებული რამდენიმე დებულება, კონკრეტულად, ელექტრონული კომუნიკაციების შესახებ საქართველოს კანონის ის ნორმა, რომელიც შესაბამის ორგანოს ანიჭებდა უფლებამოსილებას ჰქონოდა კავშირგაბმულობის საშუალებებიდან ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობა.

სასამართლომ მიუთითა, რომ კანონმდებლობა არ შეიცავდა მკაფიო მითითებებს, თუ რა შემთხვევაში შეიძლება გამოიყენოს უფლებამოსილმა ორგანომ ტექნიკური საშუალებები კომუნიკაციაზე მეთვალყურეობის მიმართულებით პერსონალურ მონაცემთა დაცვის ინსპექტორის ჩართულობის გარეშე, რაც ზრდის პირადი ცხოვრების არამართლზომიერი შეზღუდვის საფრთხეს, რამდენადაც დიდია უსაფრთხოების სამსახურთა დისკრეცია.¹¹¹ ამისათვის, პარალელი გაივლო ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებაზე - *Roman Zakharov v. Russia*, რომელშიც სასამართლომ განმარტა, რომ მეთოდი, რომლითაც მოქმედებს ფარული მიყურადების სისტემა უსაფრთხოების სამსახურებსა და პოლიციას ანიჭებს ტექნიკურ შესაძლებლობას, გვერდი აუარონ ავტორიზაციის პროცედურას და კომუნიკაციის საშუალებებზე წვდომა განახორციელონ წინასწარი სასამართლო ნებართვის გარეშე.¹¹²

ამასთანავე, ქართული რეგულაციების არაკონსტიტუციურად ცნობა განაპირობა იმ გარემოებამ, რომ სახელმწიფო უსაფრთხოების სამსახურს, რომელიც

¹¹¹ Ibid., გვ. 61.

¹¹² *Roman Zakharov v. Russia*, ECtHR, Appl. No. 47143/06, 4 December 2015.

პასუხისმგებელია წარმატებული გამოძიების ჩატარებაზე, ჰქონდა კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობა, რაც ზრდიდა ადამიანის უფლებაში დაუსაბუთებელი ჩარევის რისკებს და ცდუნებას.¹¹³

სასამართლომ ყურადღება გაამახვილა „პროცესის დამაჯერებელი გამჭვირვალობისა და კონტროლის მექანიზმების“ აუცილებლობაზე, რაც საკანონმდებლო დონეზე საჭიროებდა დახვეწას. შესაბამისად, გამოიკვეთა ფარული ელექტრონული დაკვირვების ღონისძიებებზე ეფექტიანი ზედამხედველობის საჭიროება.

სასამართლოს მსჯელობა შეეხებოდა თუ რა ტიპის/შინაარსის ინფორმაციას ინახავს სახელმწიფო. „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის შესაბამისად, განიმარტა, რომ აღნიშნული ნორმა არ გულისხმობს უშუალოდ სატელეფონო საუბრების შინაარსზე წვდომას, თუმცა სახელმწიფო უსაფრთხოების სამსახურს ანიჭებს უფლებას: „გააკეთოს ასლი და შეინახოს ინფორმაცია იმასთან დაკავშირებით, ვინ ვის, როდის, რა ტექნიკური საშუალებით, რომელი ლოკაციიდან და როგორი ხანგრძლივობით დაუკავშირდა“.¹¹⁴

ასევე, განიმარტა, რომ: „მეტადატა წარმოადგენს ინფორმაციას მობილური სატელეფონო საშუალებების ადგილმდებარეობის, განხორციელებული თუ შემოსული ზარების, ღიად თუ ანონიმურად განხორციელებული მიებისა თუ სხვა ონლაინ ქმედებებთან დაკავშირებით“.¹¹⁵ სასამართლომ მიიჩნია, რომ მეტადატას ანალიზის შედეგად, შესაძლებელია დადგინდეს ინდივიდის ქცევა, სოციალური ურთიერთობები, პირადი მახასიათებლები, რაც კომუნიკაციის შინაარსთან ერთად ამ ინდივიდის შესახებ მნიშვნელოვან ინფორმაციას იძლევა.¹¹⁶

ხაზი გაესვა კომუნიკაციის შესახებ ინფორმაციის 2 წლით შენახვის საკითხსაც, რაც ადამიანებში იწვევს დაუცველობის განცდას. შესაბამისად, ასეთ პირობებში, სახელმწიფოს მიერ მაიდენტიფიცირებელი მონაცემების შენახვის ფაქტმა შესაძლოა მნიშვნელოვნად დააკორექტიროს პირთა კომუნიკაცია, რა პირობებშიც შეუძლებელია ადამიანის თავისუფალ განვითარებაზე საუბარი.¹¹⁷

გადაწყვეტილების თანახმად, ფარული საგამოძიებო განხორციელებისას სატელეფონო და ინტერნეტ კომუნიკაციაზე პირდაპირი წვდომა ისევე, როგორც

¹¹³ საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406.408 გადაწყვეტილება საქმეზე - საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ, გვ. 63.

¹¹⁴ Ibid., გვ. 71.

¹¹⁵ Ibid.

¹¹⁶ Ibid.

¹¹⁷ Ibid., გვ. 82.

მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის შესაძლებლობა არ უნდა ჰქონდეს პროფესიულად დაინტერესებულ საგამოძიებო ორგანოს. შესაბამისად, სახელმწიფო უსაფრთხოების სამსახურის მიერ სატელეფონო და ინტერნეტ კომუნიკაციაზე პირდაპირი წვდომის შესაძლებლობა არაკონსტიტუციურად იქნა ცნობილი.

სასამართლომ მიიჩნია, რომ სადავო ნორმები შესაძლებლობას აძლევს სახელმწიფო უსაფრთხოების სამსახურს, თანამედროვე ტექნოლოგიების გამოყენებით, მოიპოვოს პირადი ხასიათის ინფორმაცია განუსაზღვრელ პირთა წრის შესახებ, რაც ქმნის პირად ცხოვრებაში დაუსაბუთებელი ჩარევის მომეტებულ საფრთხეს.¹¹⁸

გამომდინარე იქიდან, რომ სასამართლომ ფარული მოსმენების არსებული წესი არაკონსტიტუციურად ცნო, საქართველოს პარლამენტს კანონის შესაცვლელი ვადა 2017 წლის 31 მარტამდე მისცა.

გადაწყვეტილების შესაბამისად, საქართველოს პარლამენტმა 2017 წლის 22 მარტს მიიღო ცვლილებები, რომლითაც ახლებურად მოწესრიგდა ფარული ელექტრონული თვალთვალის განმახორციელებელი ტექნიკური ინფრასტრუქტურის ორგანიზება.¹¹⁹ შეიცვალა პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამოსილებები, უფრო კონკრეტულად, ინსპექტორს აღარ აქვს ფარული საგამოძიებო მოქმედების განხორციელებაზე ელექტრონული თანხმობის გაცემის უფლება ე.წ. „ორგასაღებიანი სისტემის“ მეშვეობით. თუმცა, ინსპექტორს შეუწარმუნდა კონტროლის ელექტრონული სისტემით ზედამხედველობის უფლებამოსილება¹²⁰ და აქვს უფლება კონტროლის ელექტრონული სისტემით შეაჩეროს ფარული საგამოძიებო მოქმედება.¹²¹

ცვლილება შეეხო „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონსაც, რომლითაც უზენაეს სასამართლოს მიენიჭა სპეციალური სამსახურის შუამდგომლობის საფუძველზე ე.წ. სტრატეგიული მონიტორინგის განხორციელების შესახებ ბრძანების გაცემის უფლებამოსილება. ამასთან, კანონში გაჩნდა ე.წ. ზედამხედველი მოსამართლის ინსტიტუტი,¹²² რომელიც გასცემს ოპერატიულ-ტექნიკური ღონისძიების და ელექტრონული თვალთვალის ღონისძიების

¹¹⁸ საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება, № 1/1/625, 640. გვ. 84.

¹¹⁹ IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, *ფარული მიყურადების რეგულირება საქართველოში*, 2017.

¹²⁰ საქართველოს კანონი საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ, მუხლი 2.

¹²¹ საქართველოს სისხლის სამართლის საპროცესო კოდექსი, მუხლი 143⁶, ნაწილი 5.

¹²² განსაზღვრულია საქართველოს უზენაესი სასამართლოს თავმჯდომარის მიერ.

განხორციელების შესახებ ბრძანებას. ასევე, გააჩნია კონტროლის ფუნქციები, რომელსაც 2020 წლიდან განახორციელებს.¹²³

არასამთავრობო ორგანიზაციების კამპანიამ „ეს შენ გეხება,“ რომელიც აქტიურად მუშაობდა ფარული მიყურადების საკითხებზე, გააკრიტიკა ხელისუფლების მიერ წარმოდგენილი კანონპროექტი და მიიჩნია, რომ ცვლილებები საკონსტიტუციო სასამართლოს გადაწყვეტილებას ეწინააღმდეგებოდა. კონკრეტულად, კანონპროექტით გათვალისწინებული სტრუქტურული ერთეული - საჯარო სამართლის იურიდიული პირი კვლავ რჩებოდა სახელმწიფო უსაფრთხოების სამსახურის შემადგენლობაში და არ იყო საკმარისი დამოუკიდებლობის გარანტიებით აღჭურვილი.

სახალხო დამცველის აპარატმა გაიზიარა არასამთავრობო ორგანიზაციების პოზიცია და განაცხადა, რომ საქართველოს პარლამენტის მიერ 2017 წლის 22 მარტს მიღებული საკანონმდებლო ცვლილებები ეწინააღმდეგებოდა საკონსტიტუციო სასამართლოს გადაწყვეტილებას, გამომდინარე იქიდან, რომ ტექნიკური შესაძლებლობა კვლავ რჩებოდა სახელმწიფო უსაფრთხოების სამსახურის ხელში.

აღნიშნული გარემოებები იყო საკონსტიტუციო სასამართლოში მორიგი სარჩელის შეტანის საფუძველი. საკონსტიტუციო სასამართლოს მიმართა თითქმის სამასმა საქართველოს მოქალაქემ, პოლიტიკურმა პარტიებმა და სახალხო დამცველმა.¹²⁴

5.3. საქართველოში არსებული მდგომარეობა სახალხო დამცველის და პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშებზე დაყრდნობით

საქართველოს სახალხო დამცველი ზედამხედველობს საქართველოს ტერიტორიისა და მისი იურისდიქციის ფარგლებში ადამიანის უფლებების დაცვას,¹²⁵ ხოლო პერსონალურ მონაცემთა დაცვის ინსპექტორი,¹²⁶ ახორციელებს ზედამხედველობას უშუალოდ პერსონალურ მონაცემთა დაცვის მიმართულებით.

¹²³ IDFI - ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, *ფარული მიყურადების რეგულირება საქართველოში*, 2017.

¹²⁴ სარჩელის შესახებ დეტალური ინფორმაცია იხ. ნაშრომის თავში: *საქართველოში არსებული მდგომარეობა სახალხო დამცველის და პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშებზე დაყრდნობით*.

¹²⁵ იხ. საქართველოს ორგანული კანონი საქართველოს სახალხო დამცველის შესახებ, მე-2 მუხლი.

¹²⁶ საქართველოში 2013 წლის ივლისიდან ახორციელებს ზედამხედველობას პერსონალურ მონაცემთა დაცვაზე.

2018 წლის სახალხო დამცველის ანგარიშში¹²⁷ მითითება კეთდება სახალხო დამცველის მიერ 2017 წელს საკონსტიტუციო სასამართლოში შეტანილ სარჩელზე,¹²⁸ რომლითაც გასაჩივრებულია „საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის, საქართველოს სისხლის სამართლის საპროცესო კოდექსის, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმები, რომლებიც უკავშირდება ოპერატიულ-ტექნიკური სააგენტოს მიერ ფარული მეთვალყურეობის ღონისძიების განხორციელებას. გაკრიტიკებულია, რომ სააგენტო დარჩა კვლავ სახელმწიფო უსაფრთხოების სამსახურის დაქვემდებარებაში.

სახალხო დამცველი მიიჩნევს, რომ ფარული საგამოძიებო მოქმედებების განხორციელების მიზნით, პირად კომუნიკაციებზე წვდომა და კომუნიკაციის მონაწილეთა მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის შესაძლებლობა და ცენტრალური ბანკის შექმნის უფლებამოსილების მინიჭება არ უნდა ჰქონდეს პროფესიულად დაინტერესებულ ორგანოს. გარდა ამისა, აღნიშნულია, რომ სააგენტოს საქმიანობაზე არ ხორციელდება ეფექტიანი გარე კონტროლი, რაც წარმოშობს ფარული მეთვალყურეობის ღონისძიებების განხორციელების პროცესში თვითნებობის საფრთხეებს.

პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის ანგარიშის¹²⁹ შესაბამისად, შემცირებულია სამართალდამცავ სექტორში გამოვლენილი დარღვევების რაოდენობა, თუმცა, არსებობს საკითხები, რომლებიც კვლავ მოსაწესრიგებელია.

2017 წლის საკანონმდებლო ცვლილებების შედეგად, პერსონალურ მონაცემთა დაცვის ინსპექტორს მიენიჭა უფლებამოსილება, შეაჩეროს ფარული მიყურადებისა და ჩაწერის მიმდინარეობა. ანგარიშში აღნიშნულია, რომ შეჩერების მექანიზმი გამოყენებულ იქნა 96 განჩინების/დადგენილების შემთხვევაში.

გარდა ამისა, შესწავლილ იქნა სააგენტოს მიერ კომუნიკაციის რეალურ დროში მოპოვების შესაბამისი ტექნიკური შესაძლებლობების გამოყენებით ფარული საგამოძიებო მოქმედების - სატელეფონო კომუნიკაციის მიყურადებისა და

¹²⁷ საქართველოს სახალხო დამცველის ანგარიში საქართველოში ადამიანის უფლებათა და თავისუფლებათა დაცვის მდგომარეობის შესახებ, 2018 წელი. ხელმისაწვდომია: <http://bit.do/eVMT8> (ბოლოს ნანახია: 22.06.2019)

¹²⁸ 2019 წლის 22 ივნისის მონაცემებით, საქართველოს საკონსტიტუციო სასამართლომ დაასრულა საქმის არსებითი განხილვა, თუმცა გადაწყვეტილება არ არის ცნობილი.

¹²⁹ ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ, 2018.

დამუშავების და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების შედეგად მონაცემთა დამუშავების კანონიერება. მითითება გაკეთდა საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143⁹-ე მუხლზე, რომელიც ითვალისწინებს პროკურატურის ვალდებულებას ფარული საგამოძიებო მოქმედებების ჩატარების შემდეგ მოპოვებული მასალის შინაარსის და განადგურების შესახებ ინფორმაცია მიაწოდოს იმ პირს, რომლის მიმართაც ჩატარდა ფარული საგამოძიებო მოქმედება. პერსონალურ მონაცემთა დაცვის ინსპექტორის შემოწმების შედეგად, გამოვლინდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული პრინციპების და მონაცემთა უსაფრთხოების წესების დარღვევის რამდენიმე ფაქტი, რისთვისაც გაიცა შესაბამისი დავალებები/რეკომენდაციები.

საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის მიერ შესწავლილ იქნა ელექტრონული კომუნიკაციის კომპანიის მიერ სამართალდამცავი ორგანოებისთვის კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კანონდარღვევით გადაცემისა და ინსპექტორის ინფორმირების ვალდებულების შეუსრულებლობის ფაქტები. მაგალითად, სამართალდამცავმა ორგანომ ელექტრონული კომუნიკაციის კომპანიისგან განჩინების გარეშე მიიღო ინფორმაცია. ასევე გამოვლინდა ფაქტი, რომლის შესაბამისადაც კომპანია სამართალდამცავ ორგანოს მხოლოდ წერილის საფუძველზე აწვდიდა მონაცემებს.

აღნიშნულ ანგარიშებზე დაყრდნობით, შეიძლება ითქვას, რომ ადამიანის უფლებათა დაცვის თვალსაზრისით პროგრესი შეინიშნება, თუმცა, სამართალდამცავი ორგანოების სისტემაში ადამიანის უფლებათა დაცვის საკითხი კვლავ აქტუალურია, რადგან არსებობს ადამიანის პირად კომუნიკაციაში უკანონო ჩარევის და პერსონალურ მონაცემთა დაცვის პრინციპების უგულებელყოფის საფრთხე.

დასკვნა

სტატია ნათლად წარმოაჩენს, რომ თანამედროვე საკომუნიკაციო ტექნოლოგიების განვითარებასთან ერთად პირადი ცხოვრების, მიმოწერის, სატელეფონო და სხვა ტექნიკური საშუალებით საუბრისა და მიღებული შეტყობინებების ხელშეუხებლობის უფლებათა დაცვის საკითხი სულ უფრო მეტ აქტუალობას იძენს. საკომუნიკაციო საშუალებები ამარტივებს ადამიანის პირადი საუბრის კონტროლის შესაძლებლობას და, როგორც ვნახეთ, საკმაოდ დიდია ადამიანის უფლებებში არამართლზომიერი ჩარევის რისკი. შესაბამისად, ამ უფლებათა დოგმატიკა მუდმივ განვითარებას და დახვეწას საჭიროებს.

კომუნიკაციებზე გაუმართლებელი ფარული მეთვალყურეობის თავიდან აცილების მიზნით, ტექნოლოგიურ პროგრესთან ერთად აუცილებელია ეფექტიანი სტანდარტების შემუშავება და დანერგვა ეროვნულ და საერთაშორისო დონეზე. გამოიკვეთა, რომ პირადი კომუნიკაციის შესახებ ინფორმაციის მოპოვებამ შეიძლება ზიანი მიაყენოს როგორც ინდივიდის, ისე სახელმწიფოს ინტერესებს საერთაშორისო სამართლის ძირითადი პრინციპების შესაბამისად.

გამოვლინდა, რომ სახელმწიფო უსაფრთხოების სამსახურები ეროვნული უსაფრთხოების დაცვის უზრუნველსაყოფად ახორციელებენ ადამიანის უფლებაში ჩარევას. აქედან გამომდინარე, განსაკუთრებით მნიშვნელოვანია შემოწმდეს ადამიანის პირადი ცხოვრების დაცულობის უფლებაში მართლზომიერი ჩარევის ტესტი.

სტატიაში გამოვლენილი გამოწვევების საპასუხოდ და ადამიანის უფლებათა ეფექტიანი დაცვის მიზნით, პირადი კომუნიკაციის მონიტორინგის განხორციელებისას მიზანშეწონილია შემდეგი რეკომენდაციების გათვალისწინება:

- მაქსიმალურად იქნას მხედველობაში მიღებული ადამიანის უფლებები და პირად ინფორმაციათა სენსიტიურობა;
- პირადი ცხოვრების დაცულობის უფლებაში ჩარევამდე შემოწმდეს მართლზომიერების ტესტი;
- თუ არ არსებობს საფუძვლიანი ეჭვი, რომ საფრთხე შეექმნება სახელმწიფოებრივ ინტერესებს, არ განხორციელდეს მიმოწერაზე ფარული მეთვალყურეობა;
- მაქსიმალურად გაკონტროლდეს სამართალდამცავი ორგანოების საქმიანობა, როგორც შიდა, ისე გარე კონტროლის მექანიზმის საშუალებით;
- მაქსიმალურად იქნას დაცული პერსონალურ მონაცემთა დაცვის პრინციპები და განისაზღვროს კომუნიკაციის შესახებ მოპოვებული ინფორმაციის შენახვის და განადგურების ვადები;
- სახელმწიფოებმა ეროვნულ დონეზე დანერგონ საერთაშორისო სტანდარტები და სხვადასხვა ქვეყნის საუკეთესო პრაქტიკა;
- პერსონალური მონაცემები დამუშავდეს მხოლოდ იმ მოცულობით, რაც აუცილებელია კონკრეტული მიზნის მისაღწევად.