ავტორის სტილი დაცულია

სსიპ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

იურიდიული ფაკულტეტი

სამართლის სადოქტორო პროგრამა

თამარი გეგეშიძე

თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება და გამოყენება სისხლის სამართლის პროცესში

სამართლის დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარმოდგენილი დისერტაცია

სამეცნიერო ხელმძღვანელი:

გიორგი თუმანიშვილი, სამართლის დოქტორი, ასოცირებული პროფესორი

თბილისი

2021

აბსტრაქტი

თანამედროვე ტექნოლოგიების განვითარების მასშტაბებიდან გამომდინარე, ელექტრონული კომუნიკაციის .საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების თემატიკამ ცენტრალური მნიშვნელობა შეიძინა სისხლის სამართლის პროცესში.

აღსანიშნავია, რომ 2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით ფარული მეთვალყურეობის სფეროში საქართველოს კანონმდებლობაში ძირეული ცვლილებები განხორციელდა, რომლითაც კერძო კომუნიკაციის შემზღუდველი ღონისძიებები „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონიდან სისხლის სამართლის საპროცესო კოდექსში ფარული საგამოძიებო მოქმედებების სახით იქნა გადატანილი. მიუხედავად განხორციელებული ნოვაციებისა, არსებულ კანონმდებლობაში კვლავ რჩება არაერთი პრობლემატური ასპექტი, როგორც კონსტიტუციურ-სამართლებრივ, ასევე საერთაშორისო მოთხოვნებთან შესაბამისობის თვალსაზრისით. ამასთანავე, მოცემული თემის მნიშვნელობას განსაკუთრებით გაუსვა ხაზი კომუნიკაციის რეალურ დროში მოპოვების მარეგულირებელ კანონმდებლობასთან დაკავშირებით საქართველოს საკონსტიტუციო სასამართლოში მიმდინარე დავებმა.

ნიშანდობლივია, რომ ევროკავშირთან ასოცირების ხელშეკრულებიდან გამომდინარე, საქართველოს ერთ-ერთ ვალდებულებას წარმოადგენს პერსონალურ მონაცემთა მაღალ დონეზე დაცვა ევროკავშირის, ევროპის საბჭოსა და სხვა საერთაშორისო სამართლებრივი დოკუმენტების შესაბამისად. ამის გათვალისწინებით, ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მარეგულირებელი კანონმდებლობის საერთაშორისო სტანდარტების შესაბამისად რეგულირება საქართველოსთვის განსაკუთრებით მნიშვნელოვანია.

აღნიშნულიდან გამომდინარე, ნაშრომის მიზანს წარმოადგენს სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ სატელეფონო და ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების ფარულ საგამოძიებო მოქმედებებთან, ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვასთან/სისხლის სამართლის პროცესში გამოყენებასთან დაკავშირებული კანონმდებლობის ანალიზი, არსებული

პრობლემური საკითხების წარმოჩენა/განხილვა, საერთაშორისო და კონსტიტუციურ-სამართლებრივ სტანდარტებთან შესაბამისობის შეფასება და შესაბამისი სარეკომენდაციო წინადადებების შემუშავება.

ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული კანონმდებლობა სიახლეს წარმოადგენს ქართულ რეალობაში, რის გამოც მწირია გამოცდილება ამ მიმართულებით. აღნიშნულის გათვალისწინებით, თემის ერთ-ერთ დანიშნულებას საკვლევ თემასთან დაკავშირებით თეორიული საკითხების დამუშავება განეკუთვნება, რაც განხორციელებულია საერთაშორისო სტანდარტებისა და საუკეთესო უცხოური პრაქტიკის განხილვის გზით.

კვლევის მიზნებისათვის ძირითადად გამოყენებულია კვლევის ისტორიული, ფორმალურ-ლოგიკური, ნორმატიულ-დოგმატური და შედარებით-სამართლებრივი მეთოდები.

აღსანიშნავია, რომ კვლევა წარმოადგენს ნოვაციას სამეცნიერო თვალსაზრისით; მასში განხილულია საკითხები, რომლებიც საქართველოში მეცნიერულად არ არის სათანადოდ დამუშავებული, კერძოდ, სამეცნიერო კუთხით სიახლეს განეკუთვნება ინტერნეტკომუნიკაციის რეალურ დროში მოპოვებასა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა/გამოყენების საკითხების კვლევა; ხოლო სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიების შემთხვევაში სამეცნიერო ნოვაციას განეკუთვნება აღნიშნული ღონისძიების მარეგულირებელი ქართული კანონმდებლობის ევროპულ და სხვა საერთაშორისო სტანდარტებთან შესაბამისობის კონტექსტში კვლევა და შეფასება.

ნაშრომი შედგება 7 თავისგან. პირველი თავი შესავალია, რომელშიც წარმოდგენილია კვლევის აქტუალურობა, საგანი, მიზნები, მეთოდები. მეორე თავი ეთმობა სისხლის სამართლის პროცესში ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების შესაძლებლობების განვითარებას და მასთან დაკავშირებულ გამოწვევებს; მე-3 თავში განხილულია თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების ტექნიკური შესაძლებლობები; მე-4 თავში წარმოდგენილია კონსტიტუციურ-სამართლებრივი სტანდარტები ამ სფეროში; მე-5 თავში კი ფუნდამენტურად არის განხილული საკვლევ თემატიკასთან დაკავშირებული საერთაშორისო სტანდარტები; მე-6 თავი უკვე ეთმობა ამ სფეროს მარეგულირებელი ქართული კანონმდებლობის სიღრმისეულ

კვლევას, ანალიზს, საერთაშორისო და კონსტიტუციურ-სამართლებრივ სტანდარტებთან შესაბამისობის ჭრილში განხილვას, ქართულ კანონმდებლობაში არსებული პრობლემატური ასპექტების წარმოჩენას და შესაბამისი სარეკომენდაციო წინადადებების შემუშავებას. საბოლოოდ, დასკვნაში წარმოდგენილია კვლევის შედეგების შეჯამება და ძირითადი მოსაზრებები.

Abstract

Considering the scale of recent technological developments, the issues related to obtaining information from the means of electronic communications and its use in criminal proceedings have acquired critical importance.

Significant amendments have been made into Georgian legislation concerning the secret surveillance under August 1, 2014 legislative package, by which the actions restricting privacy of communications were moved from the Law of Georgia on "Operative Investigatory Activities" to the Criminal Procedural Code of Georgia in the form of secret investigative actions. Regardless of this novelty, current legislation still has many gaps in terms of compliance with constitutional and international standards.

It is noteworthy, that one of the obligations of Georgia under Association Agreement is protection of personal data at a higher level in conformity with EU, Council of Europe and other international legal documents. Therefore, it is extremely important for Georgia to regulate obtaining of information through means of electronic communication in compliance with international standards.

Considering abovementioned, the main goal of this work is to analyze the legislation related to secret investigative actions for obtaining telephone and internet communications in real time established in sub-paragraphs ''a'' and ''b'' of the article 143[1] of the Criminal Code of Georgia, as well as legal provisions regarding retention/use of electronic communication identification data in criminal proceedings; to raise/discuss current problems, evaluate the compliance of Georgian regulations with international and constitutional-legal standards and elaborate relevant recommendations.

As the legislation related to secret investigative actions is a novelty in Georgia and there is a lack of experience, one of the objectives of the thesis is to analyze theoretical issues with

regard to the research topic by discussing international standards and the best international practice.

For the purposes of this study, the historical, formal-logical, normative-dogmatic and comparative-legal methods were applied.

This research can be deemed as a scientific novelty, because it's referring to issues which are not properly processed in Georgia from scientific point of view, such as issues related to obtaining internet communications in real time and retention/use of electronic communication identification data. As regards telephone communications, analyzing relevant Georgian legislation in compliance with European and other internation standards can be deemed as scientific novelty.

The thesis consists of 7 chapters. The first chapter is an introduction, where the significance of the topic, thesis subject, goals and methodology of the survey are outlined. The second chapter is dedicated to the development of capabilities of obtaining information from the electronic means of communications in criminal proceedings and related challenges. Chapter 3 reviews the technical capacity for obtaining information from the modern electronic means of communication. Chapter 4 presents the constitutional-legal standards in this area. Chapter 5 provides thorough review of international standards related to the research topic. Chapter 6 is dedicated to in-depth study of Georgian legislation regulating the sphere, its analysis against constitutional and international legal standards, highlighting problematic aspects and elaboration of relevant recommendations. The conclusive part summarizes the research results and main considerations.

ს ა რ ჩ ე ვ ი

გამოყენებული შემოკლებანი

ქართულ ენაზე:

ასოცირების შეთანხმება - ასოცირების შესახებ შეთანხმება ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის

ა.შ. - ასე შემდეგ

გაერო - გაერთიანებული ერების ორგანიზაცია

გვ. - გვერდი

ევროკავშირი - ევროპული კავშირი

ევროპული სასამართლო - ადამიანის უფლებათა ევროპული სასამართლო

ევროსაბჭო - ევროპის საბჭო

ე.წ. - ეგრეთ წოდებული

იხ. - იხილეთ

მაგ. - მაგალითად

რედ. - გამოცემის რედაქტორი

ინსპექტორი - სახელმწიფო ინსპექტორი

ინსპექტორის სამსახური - სახელმწიფო ინსპექტორის სამსახური

კონვენცია - ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია

სააგენტო - საჯარო სამართლის იურიდიული პირი - ოპერატიულ-ტექნიკური სააგენტო

სსიპ - საჯარო სამართლის იურიდიული პირი

სსკ- სისხლის სამართლის კოდექსი

სსსკ - სისხლის სამართლის საპროცესო კოდექსი

სხვ. - სხვა

თბ. - თბილისი

ინგლისურ ენაზე:

CCPR - Covenant on Civil and Political Rights

CJEU – Court of Justice of the European Union

City U. H.K. L. Rev. – City University of Hong Kong Law Review

CSLI - Cell Site Location Information

Ed. – Edited

Eds. – Editors

ECtHR -European Court of Human Rights

ERA - Academy of European Law

EU – European Union

GCHQ - Government Communications Headquarters

Geo. Wash. L. Rev - The George Washington Law Review

GPS - The Global Positioning System

GSM - The Global System for Mobile Communications

IDFI - Institute for Development of Freedom of Information

IMEI - International Mobile Equipment Identity

IMSI - International Mobile Subscriber Identity

IP – Internet Protocol

NSA – National Security Agency

Ser. - Series

UN – Unites Nations

URLs -Uniform Resource Locator

US – United States

Utrecht L. Rev. – Utrecht Law Review

VoIP _ Voice over IP

Vol. – Volume

გერმანულ ენაზე:

Abs. - Absatz

BVerfG - Bundesverfassungsgericht

DGStZ - Deutsch-Georgische Strafrechtszeitschrift

StPO - Strafprozessordnung

ZStW - Zeitschrift für die gesamte Strafrechtswissenschaft

I. შესავალი

კვლევის აქტუალურობა და საგანი: თანამედროვე ტექნოლოგიები მსოფლიოს ნებისმიერი წერტილიდან ინფორმაციის გაცვლის უპრეცენდენტო შესაძლებლობებს გვთავაზობს. კომპიუტერული ტექნოლოგიებისა და ელექტრონული საკომუნიკაციო საშუალებების დახვეწის შედეგად ელექტრონულ კავშირგაბმულობის ქსელები და მოწყობილობები იძლევიან დროის უმოკლეს მონაკვეთში დედამიწის ნებისმიერი წერტილიდან დიდ მანძილზე ნებისმიერი სახის ინფორმაციის გადაცემის, გავრცელების ან მიღების შესაძლებლობას. ტექნოლოგიური პროგრესის კვალდაკვალ ვითარდება სახელმწიფოს ტექნიკური შესაძლებლობებიც ფარული მეთვალყურეობის სფეროში. დღესდღეობით სახელმწიფოები ინტენსიური, მიზანმიმართული და ფართომასშტაბიანი ფარული თვალთვალის ისეთ მძლავრ შესაძლებლობებს ფლობენ, როგორც არასდროს,[1] რაც თავის მხრივ, საფრთხის ქვეშ აყენებს კერძო პირთა პირადი ცხოვრების ინტერესებს.

ელექტრონული კომუნიკაციების საშუალებებიდან ინფორმაციის მოპოვება და სისხლის სამართლის პროცესში გამოყენება საქართველოს კონსტიტუციის მე-15 მუხლით უზრუნველყოფილ პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებებში განსაკუთრებით სერიოზულ ჩარევას წარმოადგენს. ამასთან, პირადი ცხოვრების უფლება არაერთი საერთაშორისო სამართლებრივი აქტით განმტკიცებული ფუნდამენტური გარანტიაა, როგორიცაა, მაგალითად, გაეროს ადამიანის უფლებათა საყოველთაო დეკლარაცია (მუხლი 12), სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტი (მუხლი 17), ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია (შემდგომში - კონვენცია) (მუხლი 8) და სხვა.

თანამედროვე ტექნოლოგიებიდან მომდინარე საფრთხეების გათვალისწინებით, პირადი ცხოვრების დაცვის საკითხმა გლობალური მნიშვნელობა შეიძინა. საერთაშორისო დონეზე მწვავედ დგას პირადი ცხოვრების უფლების დაცვის

[1] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 10, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> [05.06.2020]

პრობლემატიკა კომუნიკაციის მონიტორინგის მიმართულებით[2]. გაეროს, ევროსაბჭოს თუ ევროკავშირის მასშტაბით აქტიურად განიხილება ციფრულ ეპოქაში პირადი ცხოვრების დაცვასთან დაკავშირებული ასპექტები[3].

მიუხედავად იმისა, რომ პირადი ცხოვრების ხელშეუხებლობა ერთ-ერთი ფუნდამენტური გარანტიაა, ის მაინც არ მიეკუთვნება აბსოლუტურად დაცულ სფეროს და სახელმწიფოს შეუძლია მასში გამონაკლის შემთხვევებში მნიშვნელოვანი საზოგადოებრივი ინტერესების გათვალისწინებით ჩაერიოს.[4] დანაშაულთან, განსაკუთრებით კი ორგანიზებულ დანაშაულთან ბრძოლის ინტერესები შეუცვლელს ხდის ფარული თვალთვალის გამოყენებას გამოძიების მიზნებისათვის. ბუნებრივია, სახელმწიფოს უნდა გააჩნდეს ბერკეტი, ტერორიზმიდან და სხვა მძიმე დანაშაულებიდან მომდინარე საფრთხეების გასანეიტრალებლად გამოიყენოს ფარული მეთვალყურეობის ღონისძიებები, მაგრამ მათი გამოყენება მხოლოდ საგამონაკლისო შემთხვევებში დაიშვება, იმ პირობით, რომ აღნიშნული ღონისძიება ლეგიტიმური მიზნის [სახელმწიფო უსაფრთხოების დაცვის, დანაშაულის ან უწესრიგობის თავიდან აცილების] მიღწევის პროპორციული და აუცილებელი საშუალებაა.[5]

ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება და სისხლის სამართლის პროცესში გამოყენება ერთ-ერთ იმ საკითხს განეკუთვნება, როდესაც განსაკუთრებით თვალსაჩინოა ღირებულებათა კონფლიქტი დანაშაულის გახსნის საჯარო და ინდივიდის უფლებების დაცვის კერძო ინტერესს შორის. თავისთავად ამ ორივე ინტერესის მნიშვნელობა ღირებულებათა ამ კონფლიქტს განსაკუთრებულ აქტუალურობას სძენს. ამასთან, სახელმწიფოს მხრიდან პრიორიტეტების სწორად და სამართლიანად გადაწყვეტა, კერძო და საჯარო

---

[2] General Assembly, United Nations, Resolution on "The Right to Privacy in The Digital Age", 21.01.2013, <https://undocs.org/A/RES/68/167> [05.06.2020].

[3] იქვე; Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 21 (ბმული იხ. პირველ გვერდზე); Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Committee of Ministers, 11.06.2013, <https://www.garanteprivacy.it/documents/10160/2603116/Declaration+of+the+Committee.pdf> [05.06.2020]; Case NC-293/12 and C-594/12, Digital Rights Ireland ltd and Seitlinger and others, [2014], Court of Justice, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice.

[4] *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი, ზოგადი ნაწილის მიმოხილვა, თბ., 2014, 274.

[5] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 48.

ინტერესების გონივრული დაბალანსება არსებითად დამოკიდებულია „ყოველი კონკრეტული უფლების შინაარსისა და ფარგლების ადეკვატურ საკანონმდებლო განსაზღვრაზე“[6]. მოცემულ შემთხვევაშიც, ღირებულებათა ამ კონფლიქტის მოგვარება შესაძლებელია გონივრულად დაბალანსებული სისტემის შექმნის გზით, რაც არც თუ ისე მარტივ ამოცანას წარმოადგენს სისხლის სამართლის პროცესში.

ნიშანდობლივია, რომ ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და გამოყენების თემატიკამ განსაკუთრებული აქტუალურობა შეიძინა საქართველოში. ამ თვალსაზრისით აღსანიშნავია, რომ რამდენიმე წლის წინ, ე.წ. „უკანონო მოსმენების“ საკითხი საქართველოში მთელი სიმძაფრით წამოიჭრა. 2014 წლის 1 აგვისტოს საქართველოს პარლამენტმა მიიღო ახალი საკანონმდებლო ცვლილებათა პაკეტი, რომლითაც კერძო კომუნიკაციის ხელშეუხებლობის შემზღუდველი ღონისძიებები „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონიდან სისხლის სამართლის საპროცესო კოდექსში (შემდგომში - სსსკ) ფარული საგამოძიებო მოქმედებების სახით იქნა გადატანილი. მიუხედავად იმისა, რომ ახალმა კანონმდებლობამ გაცილებით მეტი გარანტია გაითვალისწინა, მოცემული საკითხი მუდმივ აქტუალურობას ინარჩუნებს, რასაც ასევე ადასტურებს ამ თემის გარშემო საქართველოს საკონსტიტუციო სასამართლოში არსებული დავებიც, კერძოდ, საქართველოს საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით ინტერნეტურთიერთობის მონიტორინგთან,[7] ისევე როგორც სატელეფონო კომუნიკაციის ფარულ მიყურადებასა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირებასთან დაკავშირებული გარკვეული მნიშვნელოვანი დებულებები კონსტიტუციურ-სამართლებრივ სტანდარტთან შეუსაბამოდ მიიჩნია.[8]

[6] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 2 ივლისის N1/2/384 გადაწყვეტილება, II-5.

[7] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება. აღნიშნულ გადაწყვეტილებაში საქართველოს საკონსტიტუციო სასამართლომ იმსჯელა საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით (სატელეფონო კომუნიკაციის ფარული მიყურადება) და ამავე მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებზე. გადაწყვეტილებაში 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების ღონისძიება მოხსენებულია, როგორც „ინტერნეტკომუნიკაციის მონიტორინგი“, იგივე „ინტერნეტურთიერთობის მონიტორინგი“.

[8] იქვე.

აღნიშნული გადაწყვეტილების შესრულების მიზნით, ქართულ კანონმდებლობაში 2017 წლის 22 მარტს გარკვეული ცვლილებები განხორციელდა, თუმცა დღევანდელი მდგომარეობით კვლავ მიმდინარეობს დავა საკონსტიტუციო სასამართლოში. მითითებული დავის ფარგლებში მოსარჩელეები მიიჩნევენ, რომ კანონმდებლობაში განხორციელებული ცვლილებები ვერ პასუხობს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით დადგენილ მოთხოვნებს.[9]

აღნიშნულის გათვალისწინებით წინამდებარე კვლევის საგანს სატელეფონო და ინტერნეტკომუნიკაციების რეალურ დროში მოპოვებასთან დაკავშირებული ფარული საგამოძიებო მოქმედებების, ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვისა და სისხლის სამართლის პროცესში გამოყენების საკითხების შესწავლა და ანალიზი წარმოადგენს. ეს სწორედ ის საკითხებია, რომლებმაც ასეთი აქტუალურობა და მნიშვნელობა შეიძინა ქართულ რეალობაში.

ამდენად, კვლევის ფარგლებში საუბარი იქნება 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ ღონისძიებებზე. „ა“ ქვეპუნქტი განსაზღვრავს „სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის“ ღონისძიებას, ხოლო „ბ“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას მიეკუთვნება - „ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებებთან, კომპიუტერულ ქსელებთან, სახაზო კომუნიკაციებთან და სასადგურე აპარატურასთან მიერთებით), კომპიუტერული სისტემიდან (როგორც უშუალოდ, ისე დისტანციურად) და ამ მიზნით კომპიუტერულ სისტემაში შესაბამისი პროგრამული უზრუნველყოფის საშუალებების ინსტალაცია“.

კვლევა ასევე დაეთმობა უფლებამოსილი სახელმწიფო ორგანოს (სსიპ ოპერატიულ-ტექნიკური სააგენტოს (შემდგომში - სააგენტო)) მიერ კავშირგაბმულობის არხში არსებული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირების/შენახვის და საგამოძიებო ორგანოების მიერ აღნიშნულ მონაცემებზე წვდომის საკითხებს სსსკ-ის 136-ე მუხლის (დოკუმენტის ან ინფორმაციის გამოთხოვა) შესაბამისად. ამასთან, კვლევის მიზანს არ წარმოადგენს

[9] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.

სსსკ-ის 136-ე მუხლით რეგულირებული ყველა სამართლებრივი ურთიერთობის განხილვა, არამედ კვლევის ფარგლებში აღნიშნულ მუხლთან მიმართებით საუბარი იქნება მხოლოდ საგამოძიებო ორგანოების მიერ სააგენტოდან/ელექტრონული კომუნიკაციის კომპანიიდან კომუნიკაციის მაიდენტიფიცირებელი მონაცემების (მეტადატა) გამოთხოვის საკითხზე.

აღსანიშნავია, რომ „ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონში მოცემულია „ფარული მეთვალყურეობის ღონისძიებების“ ჩამონათვალი, რომელიც სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ღონისძიებების გარდა, ასევე მოიცავს ამავე მუხლით გათვალისწინებულ ზოგიერთ სხვა ფარულ საგამოძიებო მოქმედებას, ასევე „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონის მე-9 მუხლის მე-3 პუნქტით გათვალისწინებული ელექტრონული თვალთვალის ღონისძიებებსა და ამავე კანონით გათვალისწინებულ სტრატეგიული მონიტორინგის ღონისძიებას და ინდივიდუალური მონიტორინგის ღონისძიებას;[10] თუმცა მოცემული კვლევის მიზნებისათვის როდესაც საუბარია „ფარული მეთვალყურეობის ღონისძიებებზე“, მოიაზრება მხოლოდ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებები.

თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენების კონტექსტში კვლევა ეხება ისეთ საკითხებს, როგორიცაა მაგალითად, მოპოვებული ინფორმაციის გადარჩევა გამოძიებისათვის ღირებულების თვალსაზრისით, ინფორმაციის განადგურება, შენახვა, სხვა სახელმწიფო ორგანოსათვის გადაცემა, მოპოვებული მონაცემების გამოყენება „შემთხვევით პირებთან მიმართებით“ და სხვა. ამასთანავე, კვლევის საგანს არ წარმოადგენს განსახილველი ღონისძიებების შედეგად მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში მტკიცებულებად დასაშვებობასთან დაკავშირებული საკითხები.

ზოგადად, ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების/გამოყენების უფლებამოსილება შეიძლება არსებობდეს როგორც სისხლის

[10] „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ“ ქვეპუნქტი, <matsne.gov.ge> 27/03/2017.

სამართლებრივ, ასევე საპოლიციო და უშიშროების სფეროებში.[11] ქართულ სამართალში გათვალისწინებულია კომუნიკაციის მონიტორინგის ღონისძიებების გამოყენების სისხლის საპროცესო და კონტრდაზვერვითი რეგულირება.[12] ამასთან, ნაშრომის თემატიკას წარმოადგენს ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების/გამოყენების საკითხი მხოლოდ სისხლის საპროცესო სამართალში.

განსახილველი ღონისძიებები მრავალ პრობლემატურ ასპექტთან არის დაკავშირებული. საქართველოს საკონსტიტუციო სასამართლოში მიმდინარე დავებმა ამ თვალსაზრისით არაერთი მნიშვნელოვანი საკითხი წარმოაჩინა, როგორიცაა მაგალითად, სახელმწიფო ხელისუფლების ორგანოების მხრიდან კომუნიკაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის კონსტიტუციურობა და გარე კონტროლის მექანიზმები ამ უფლებამოსილების განხორციელებაზე, სააგენტოს[13] მიერ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების ელექტრონული კომუნიკაციის კომპანიებისგან კოპირების შესაძლებლობის კონსტიტუციასთან მიმართება და სხვა;

კვლევის ერთ-ერთ ძირითად ასპექტს სატელეფონო კომუნიკაციის ფარული მიყურადების, ისევე როგორც ინტერნეტურთიერთობის მონიტორინგისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირების პროცესზე ზედამხედველობის მექანიზმების ეფექტიანობა განეკუთვნება. ამ თვალსაზრისით კვლევაში დასმულ ერთ-ერთ პრობლემურ საკითხს ინტერნეტკომუნიკაციების მონიტორინგის ღონისძიებაზე კონტროლის მექანიზმები წარმოადგენს; ასევე პრობლემატურ საკითხად არის გამოკვეთილი ფარული საგამოძიებო მოქმედებების აღსრულების მთელ პროცესზე სათანადო კონტროლის

---

[11] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 31.

[12] დანაშაულის გამოძიების სექტორში ფარული საგამოძიებო მოქმედება გამოიყენება სსსკ-ით დადგენილი წესით, მას შემდეგ რაც დაიწყება გამოძიება ან/და სისხლის სამართლებრივი დევნა სსსკ-ით სპეციალურად განსაზღვრულ დანაშაულებთან დაკავშირებით; რაც შეეხება კონტრდაზვერვითი მიზნებისათვის ფარული მეთვალყურეობის უფლებამოსილებას, სამართლებრივ საფუძველს ქმნის "კონტრდაზვერვითი საქმიანობის შესახებ საქართველოს კანონი".

[13] სააგენტო წარმოადგენს სახელმწიფო უსაფრთხოების სამსახურის სტრუქტურული ერთეულის - ოპერატიულ-ტექნიკური დეპარტამენტის უფლებამონაცვლეს. 2017 წლის 22 მარტამდე არსებული კანონმდებლობით ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირების უფლებამოსილებით აღჭურვილი იყო ოპერატიულ-ტექნიკური დეპარტამენტი.

ბერკეტების ნაკლებობაც. ამასთანავე, ზედამხედველობის სისტემის კონტექსტში საკვლევ თემატიკას და ამავდროულად, თემის ერთ-ერთ ცენტრალურ ასპექტს განეკუთვნება როგორც გარე კონტროლის მექანიზმების ეფექტიანობის შეფასება და მაკონტროლებელი ორგანოს - სახელმწიფო ინსპექტორის (შემდგომში - ინსპექტორი) უფლებამოსილებები, ასევე სასამართლოს ზედამხედველობა.

კვლევის საგანს ასევე მიეკუთვნება ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული პრობლემატური ასპექტების გაანალიზება ისეთ საკითხებთან დაკავშირებით, როგორიცაა მოპოვებული ინფორმაციის გადარჩევის, შენახვის, განადგურების, სხვა პირებისათვის გადაცემის წესების რეგულირება, ასევე სსსკ-ის 143^7 მუხლით უზრუნველყოფილი მინიმუმამდე დაყვანის მოთხოვნის პრაქტიკაში განხორციელების საკითხი, მათ შორის, ადვოკატსა და კლიენტს შორის განხორციელებული ადვოკატის პროფესიულ საქმიანობას მიკუთვნებული ინფორმაციის დაცვა და სხვ. მნიშვნელოვანი ყურადღება დაეთმობა აგრეთვე პირადი ცხოვრების ინტიმური სფეროს დაცვის სამართლებრივ გარანტიებს და სსსკ-ში შესაბამისი რეგულაციების გათვალისწინების აუცილებლობას.

ერთ-ერთი მნიშვნელოვანი ასპექტი უკავშირდება ასევე სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კავშირგაბმულობის არხიდან/კომპიუტერული სისტემიდან ინფორმაციის მოპოვების ღონისძიების საკანონმდებლო განსაზღვრულობის პრობლემატიკას და ამ თვალსაზრისით 143^1 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტის ზოგად ფორმულირებას.

ასევე ერთ-ერთ ცენტრალურ საკითხად არის წარმოჩენილი „ე.წ დავირუსების ტექნიკის“ გამოყენებით ინტერნეტურთიერთობის მონიტორინგის განხორციელების პრაქტიკა. როგორც საკონსტიტუციო სასამართლოში გამოიკვეთა, სწორედ ეს ღონისძიება გამოიყენება ინტერნეტკომუნიკაციების რეალურ დროში მოპოვების მიზნით,[14] თუმცა ამ თვალსაზრისით ერთი მხრივ, ბუნდოვანია რა შინაარსის ღონისძიება იგულისხმება ამ „ტექნიკის“ ქვეშ, ხოლო მეორე მხრივ, ქართული კანონმდებლობა არ შეიცავს სპეციალურ რეგულირებას და უფლების დაცვის საიმედო გარანტიებს ამ თვალსაზრისით.

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

კვლევის მიზანი: საერთაშორისო დონეზე პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის განვითარების და უფლების დაცვის ინსტრუმენტების გაძლიერების ღონისძიებები აქტიურად მიმდინარეობს.[15] მნიშვნელოვანია, საქართველომ, თავის მხრივ, ფეხი აუწყოს ევროპაში მიმდინარე პროცესებს. აღნიშნული განსაკუთრებით აქტუალურია საქართველოში მიმდინარე ევროინტეგრაციისკენ სწრაფვის პროცესიდან გამომდინარე, რომლის ფარგლებშიც დადებული ასოცირების ხელშეკრულებიდან გამომდინარე, პერსონალურ მონაცემთა დაცვა აღნიშნული შეთანხმების I დანართში მითითებული ევროკავშირის, ევროსაბჭოს თუ სხვა საერთაშორისო სტანდარტების მიხედვით, საქართველოს ერთ-ერთ ვალდებულებას წარმოადგენს. აქედან გამომდინარე, საქართველოსთვის ძალიან მნიშვნელოვანია ფარული მეთვალყურეობის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან შესაბამისობაში მოყვანა. ამ ინტერესის გათვალისწინებით, წინამდებარე ნაშრომი წარმოადგენს მცდელობას, გაანალიზებულ იქნეს კომუნიკაციის რეალურ დროში მოპოვებასთან დაკავშირებული ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა/გამოყენების საკითხთან დაკავშირებული პრობლემატიკა, მოხდეს ქართული რეგულაციების საერთაშორისო სტანდარტებთან შესაბამისობის შეფასება და ქართული კანონმდებლობის საერთაშორისო მოთხოვნებთან შესაბამისობაში მოყვანის მიზნით შესაბამისი სარეკომენდაციო წინადადებების შემუშავება.

კვლევის ერთ-ერთ მთავარ დანიშნულებად დასახულია ასევე ქართული რეგულაციების საქართველოს საკონსტიტუციო სასამართლოს მიერ დადგენილ მოთხოვნებთან შესაბამისობის დადგენა. ამ თვალსაზრისით, ნაშრომის ერთ-ერთ ცენტრალურ მიზანს წარმოადგენს, პასუხი გაეცეს კითხვას, თუ რამდენად პასუხობს საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილების შესრულების მიზნით კანონმდებლობაში განხორციელებული

[15] იხ. მაგალითად, EU General Data Protection Regulation (EU) 2016/679 (GDPR); <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [12.06.2020]; EU Data Protection Directive for Police and Criminal Justice Authorities (EU) 2016/680 („Police Directive“), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680> [12.06.2020]; ევროპის საბჭოს კონვენცია „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ 08/11/2001; კონვენციის დამატებითი ოქმი ზედამხედველობით ორგანოებთან და მონაცემთა ტრანსსასაზღვრო გადადინებასთან დაკავშირებით, 01/07/2004.

ცვლილებები ამავე გადაწყვეტილებით დადგენილ კონსტიტუციურ-სამართლებრივ სტანდარტებს.

გასათვალისწინებელია, რომ ფარული საგამოძიებო მოქმედებების მომწესრიგებელი კანონმდებლობა საკმაოდ ახალია საქართველოსთვის და მასთან დაკავშირებული პრაქტიკული გამოცდილებაც მწირია; ამასთანავე, სსსკ შეიცავს არაერთ ზოგად ცნებას და დებულებას, როგორიცაა მაგალითად, თანაზომიერების პრინციპი, მათ შორის, ფარული საგამოძიებო მოქმედება, როგორც უკიდურესი საშუალება, მინიმუმამდე დაყვანის მოთხოვნა და სხვ. აღნიშნულიდან გამომდინარე, ნაშრომის ერთ-ერთ დანიშნულებას განეკუთვნება საერთაშორისო სტანდარტებისა და საუკეთესო უცხოური გამოცდილების განხილვის გზით, ქართულ კანონმდებლობაში გათვალისწინებული ცნებების განმარტებისა და შესაბამისი სამართლებრივი დებულებების სწორად ინტერპრეტირების/პრაქტიკაში გამოყენებისათვის შესაბამისი თეორიული საკითხების დამუშავება.

საბოლოო ჯამში, საერთაშორისო სტანდარტებისა და საუკეთესო უცხოური პრაქტიკის (ძირითადად - აშშ, გერმანია) გათვალისწინებით ნაშრომში წარმოდგენილია სარეკომენდაციო წინადადებები ქართულ კანონმდებლობაში არსებული პრობლემატური ასპექტების გადაჭრის მიზნით.

კვლევის მეთოდოლოგიური საფუძველი: ნაშრომის მიზნებისათვის ძირითადად გამოყენებულია კვლევის ისტორიული, ფორმალურ-ლოგიკური, ნორმატიულ-დოგმატური და შედარებით-სამართლებრივი მეთოდები.

დისერტაციის სტრუქტურის მოკლე აღწერა: დისერტაცია შედგება 7 თავისგან. აქედან პირველი თავი შესავალია; მე-2 თავი ეხება ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების შესაძლებლობებს სისხლის სამართლის პროცესში და მასთან დაკავშირებულ გამოწვევებს. ამ თავის მიზანს წარმოადგენს, დაინტერესებულ პირებს შეექმნათ წარმოდგენა ფარული მეთვალყურეობის ღონისძიებებთან დაკავშირებული ზოგადი საკითხების შესახებ და ამავდროულად, მომზადდეს შესაბამისი საფუძველი, კვლევის თემატიკას მიკუთვნებული ღონისძიებების ნაშრომის შემდგომ თავებში სიღრმისეულად განხილვისა და ანალიზისთვის.

ნაშრომის მე-3 თავი ეთმობა თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის ფარულად მოპოვების ტექნიკურ შესაძლებლობებს.

მოცემული თავით გათვალისწინებული ტექნიკური ასპექტები მჭიდრო კავშირშია ნაშრომის შემდგომ ნაწილში განსახილველ სამართლებრივ საკითხებთან, უფრო მეტიც, ხშირად ინფორმაციის მოპოვების ტექნიკური შესაძლებლობები განსაზღვრავს სწორედ მასზე წვდომის სამართლებრივ გზებს; ამასთანავე, მოცემული თავის მიზანი არ არის ნაშრომის თემატიკასთან დაკავშირებული ტექნიკური ასპექტების სიღრმისეული კვლევა, არამედ ეს საკითხები წარმოდგენილი იქნება მხოლოდ იმ მოცულობით, რაც ფარული მეთვალყურეობის ღონისძიებების არსის გააზრებისა და შემდგომი სამართლებრივი ასპექტების სრულფასოვნად დამუშავების მიზნით არის აუცილებელი.

ნაშრომის მე-4 თავში წარმოდგენილია კონსტიტუციურ-სამართლებრივი სტანდარტები ფარულ საგამოძიებო მოქმედებებთან მიმართებით, მათ შორის, პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებების დაცვის კონსტიტუციურ-სამართლებრივი ჩარჩოები და აღნიშნულ უფლებებში ჩარევის წინაპირობები.

მე-5 თავში განხილულია ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების სფეროში არსებული საერთაშორისო სტანდარტები. ამ კონტექსტში წარმოდგენილია ადამიანის უფლებათა ევროპული სასამართლოსა და ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკაში ჩამოყალიბებული მოთხოვნები, ისევე როგორც გაეროს დონეზე და სხვადასხვა საერთაშორისო დოკუმენტებში შემუშავებული მიდგომები ფარულ საგამოძიებო მოქმედებებთან დაკავშირებულ ძირითად საკითხებზე.

ნაშრომის მე-6 თავი უკვე ეთმობა ელექტრონული კომუნიკაციების საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებულ ქართულ კანონმდებლობას. ამ თავში გაანალიზებულია საკვლევ თემატიკასთან დაკავშირებული ეროვნული რეგულაციები ევროპული სტანდარტების, კონსტიტუციურ-სამართლებრივი ჩარჩოებისა და საუკეთესო უცხოური გამოცდილების ჭრილში; დასმულია პრობლემატური საკითხები და შეფასებულია მათი მიმართება საერთაშორისო და კონსტიტუციურ სამართლებრივ მოთხოვნებთან; ამავდროულად, წარმოდგენილია პრობლემატური საკითხების გადაჭრის ავტორისეული ხედვა და სარეკომენდაციო წინადადებები ქართული კანონმდებლობის სრულყოფის მიზნით.

ნაშრომის მე-7 თავში - დასკვნაში შეჯამებულია კვლევის შედეგები, ძირითადი მოსაზრებები განხილულ საკითხებთან დაკავშირებით და სარეკომენდაციო წინადადებები.

II. ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების შესაძლებლობები სისხლის სამართლის პროცესში და მასთან დაკავშირებული გამოწვევები

1. ელექტრონული კომუნიკაციის საშუალებები და კერძო კომუნიკაციის მოპოვების შესაძლებლობები სისხლის სამართლის პროცესში (ზოგადი მიმოხილვა)

1.1. ძირითადი ცნებები ქართული კანონმდებლობის მიხედვით

საინფორმაციო ტექნოლოგიების განვითარებამ კომუნიკაციის ახალი საშუალებები დაამკვიდრა ყოველდღიურ ცხოვრებაში, საკმაოდ ხელმისაწვდომი გახდა ინფორმაციის მოპოვება, ხოლო პოტენციური ზიანი – განუსაზღვრელი[16]. ელექტრონული საშუალებების განვითარების პარალელურად კომუნიკაციის ფორმათა ჩამონათვალი სისტემატურად იზრდება. ადამიანები თავიანთ პირად ინტერესებსა და მოსაზრებებს სულ უფრო მეტად ანდობენ თანამედროვე ტექნოლოგიებს, თუმცა ინოვაციების პარალელურად იზრდება სახელმწიფოს ცდუნებაც, მიიღოს, გააანალიზოს და გამოიყენოს პერსონალური ინფორმაცია განსხვავებული მიზნებით. თავისთავად, აღნიშნული ქმედებები შესაძლებელია ყოველთვის არ მოდიოდეს წინააღმდეგობაში ადამიანის ძირითად უფლებებთან, თუმცა აუცილებელია მათი ზედმიწევნითი და სწორი რეგულირება[17].

აღსანიშნავია, რომ „კომუნიკაცია“ წარმოდგება ლათინური სიტყვიდან „communicare“ (ერთად კეთება, გაზიარება)[18] და ნიშნავს ინდივიდებს შორის ინფორმაციის გაცვლას ნებისმიერი სახით.[19] კომუნიკაციის მონიტორინგი შეიძლება განიმარტოს როგორც საკომუნიკაციო ქსელების საშუალებით გადაცემულ ან წარმოშობილ ინფორმაციაზე დაკვირვება, გადაჭერა, შეგროვება და შენახვა.[20]

---

[16] *ფაფიაშვილი ლ.* პირადი ცხოვრების ხელშეუხებლობა პირადი ჩხრეკისას მობილურ ტელეფონებთან მიმართებით, საკონსტიტუციო სამართლის მიმოხილვა VIII, 2015, 81, იხ. ციტირება: Savin A. EU Internet Law, Edward Elgar Publishing, 2013, 190.

[17] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-26.

[18] *Cobley P., Schulz P.J.,* Introduction, წიგნში: Theories and Models of Communication, (ed.), Berlin/Boston, 2013, 1.

[19] <https://www.merriam-webster.com/dictionary/communication> [10.06.2020].

[20] Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 3 (ბმული იხ. პირველ გვერდზე).

დანაშაულის გამოძიების მიზნებისათვის ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების/გამოყენების წესი და პროცედურა განსაზღვრულია სსსკ-ით, რომლის XVI[1] თავი არეგულირებს ფარული საგამოძიებო მოქმედებების განხორციელებასა და მოპოვებული ინფორმაციის გამოყენებასთან დაკავშირებულ სტანდარტებს. ამასთან, სსსკ-ის 143[1] მუხლი განსაზღვრავს ფარული საგამოძიებო მოქმედებების სახეებს. სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული სატელეფონო კომუნიკაციის ფარული მიყურადება/ჩაწერის ფარული საგამოძიებო მოქმედება „თავისი შინაარსით, გულისხმობს სახელმწიფო უფლებამოსილი ორგანოს მიერ სატელეფონო საუბრების ფარული მიყურადებისა და ჩაწერის (სატელეფონო მოსმენების) განხორციელების შესაძლებლობას, ხოლო ამავე ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიება - სახელმწიფოს მიერ ნებისმიერი ინფორმაციის მოხსნას და ფიქსაციას ყველა კავშირგაბმულობის საშუალებებიდან, კომპიუტერული ქსელებიდან, კომპიუტერული სისტემიდან. რაც ფაქტობრივად გულისხმობს როგორც ინტერნეტურთიერთობის მონიტორინგს, ისე კომპიუტერულ სისტემებში არსებულ, შექმნილ/შენახულ ინფორმაციაზე ხელმისაწვდომობის უზრუნველყოფას.“[21]

წინამდებარე ქვეთავის მიზანს წარმოადგენს საქართველოს კანონმდებლობით გათვალისწინებული იმ ძირითადი ცნებების და ტერმინების მიმოხილვა და განმარტება, რომლებიც დაკავშირებულია ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება/გამოყენების საკითხთან. კვლევის ფარგლებში განსახილველი საგამოძიებო მოქმედებები - სატელეფონო კომუნიკაციის ფარული მიყურადება/ჩაწერა, ასევე ინტერნეტკომუნიკაციის რეალურ დროში მოპოვება, ისევე როგორც კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ბაზების კოპირება და სამართალდამცავი ორგანოების მიერ გამოყენება დაკავშირებულია არაერთ ტექნიკურ ასპექტთან და ცნებასთან, აქედან გამომდინარე, იმისათვის, რათა უკეთ იქნეს გააზრებული, თუ რა საგამოძიებო მოქმედებებზე გვაქვს საუბარი და რას გულისხმობს თითოეული მათგანი შინაარსობრივად, აუცილებელია საქართველოს

[21] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, II-37.

კანონმდებლობით გათვალისწინებული ამ ღონისძიებებთან დაკავშირებული ტერმინების განმარტება.

ელექტრონული კომუნიკაციის საშუალებებთან დაკავშირებული რიგი საკითხები, მათ შორის, ელექტრონული საკომუნიკაციო ქსელების, იგივე ელექტრო-კავშირგაბმულობის ქსელების ცნება მოცემულია „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონში. აღნიშნული კანონის მე-2 მუხლის „ყ“ ქვეპუნქტის მიხედვით, ელექტრონულ საკომუნიკაციო ქსელებს მიეკუთვნება „გამომახებებისა და სხვადასხვა საინფორმაციო სიგნალების ელექტრონული დამუშავების, დამისამართების (კომუტაციის), გატარების და გადაცემის ტექნოლოგიური სისტემა, რომელიც მოიცავს სადენიან (მათ შორის, ოპტიკურბოჭკოვან), თანამგზავრულ, რადიოსიხშირულ ან ოპტიკურ აღჭურვილობას, სხვა ტექნოლოგიურ საშუალებებს და საოპერაციო ტექნიკურ რესურსებს, მათ შორის, ფიქსირებული (არხული და პაკეტური კომუტაციის, მათ შორის, ინტერნეტის) და მობილური კომუნიკაციების, ციფრული მაუწყებლობის, საეთერო და საკაბელო ქსელებს.“ მაშასადამე, ელექტრონულ საკომუნიკაციო ქსელებში იგულისხმება მრავალი განსხვავებული მოწყობილობისა და ტექნოლოგიური საშუალების ურთიერთკავშირი, რომელთა შორისაც მოიაზრება ყოველდღიურ ცხოვრებაში ფართოდ დამკვიდრებული ისეთი საკომუნიკაციო საშუალებები, როგორიცაა მობილური ტელეფონი, კომპიუტერი, ელექტრონული პლანშეტები და სხვა. ეს მოწყობილობები და ტექნოლოგიური საშუალებები უპრეცედენტოდ ხელმისაწვდომს ხდის სწრაფი კომუნიკაციის ისეთ შესაძლებლობებს, როგორებიცაა სატელეფონო GSM კომუნიკაცია, სხვადასხვა აპლიკაციები თუ ვებ-გვერდები, მაგალითად, Facebook, Messenger, Skype, Whatsapp, Viber, Gmail და სხვა მრავალი. აღნიშნული პროდუქტები თავდაპირველად განსხვავდებოდა ერთმანეთისგან ფუნქციურად და ტექნოლოგიურად, თუმცა თანამედროვე ტექნოლოგიების ხელმისაწვდომობამ საშუალება მისცა შემქმნელებს იმ დონეზე განევითარებინათ პროდუქცია, რომ ზემოთ ჩამოთვლილი და კიდევ სხვა მრავალი პროდუქტი თითქმის მსგავს სერვისებს სთავაზობს მომხმარებლებს, ესენია ინტერნეტ ტელეფონი (VoIP), ვიდეოზარი, ტექსტური და ხმოვანი შეტყობინებები, ფოტო/ვიდეო მონაცემების გაზიარება და ა.შ.

როგორც უკვე აღინიშნა პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებები საქართველოს კონსტიტუციის მე-15 მუხლით დაცულ

ფუნდამენტურ ღირებულებებს წარმოადგენენ, რომელთა შეზღუდვაც დასაშვებია ამავე მუხლით დადგენილი მკაცრი წინაპირობების არსებობისას. კომუნიკაციის ხელშეუხებლობის უფლება დაცულია ასევე სსსკ-ის მე-7 მუხლით, კერძოდ, უზრუნველყოფილია ნებისმიერი სახის მონაცემების ხელშეუხებლობა, რომელთა გადაცემა, შენახვა და გენერირება ხდება კავშირგაბმულობის საშუალების (მობილური და კაბელური ტელეფონები, ტელეგრაფი და სხვა), ან კომპიუტერული სისტემის მეშვეობით.[22]

პირადი ცხოვრების უფლების დაცვის ქვეშ ექცევა როგორც უშუალოდ კომუნიკაციის შინაარსი, ასევე კომუნიკაციის მაიდენტიფიცირებელი მონაცემები.[23] შინაარსობრივ მონაცემებს მიეკუთვნება მაგალითად, სატელეფონო კომუნიკაციის შინაარსი, ელექტრონული ფოსტით გაგზავნილი და მიღებული შეტყობინებები, ინტერნეტ ტელეფონის საუბრის შინაარსი, ინტერნეტ აპლიკაციების და სოციალური ქსელების მეშვეობით გაცვლილი ტექსტური, ხმოვანი და სხვა ციფრული ფორმატის შეტყობინებები, გაგზავნილი და მიღებული ფაილები და სხვ. მაიდენტიფიცირებელ მონაცემებს - იგივე მეტადატას განეკუთვნება ინფორმაცია, რომელიც წარმოშობილი ან დამუშავებულია კომუნიკაციის განხორციელების შედეგად.[24] ეს მონაცემები შესაძლებელს ხდის იდენტიფიცირებულ იქნეს კომუნიკაციის წყარო და დანიშნულება, კომუნიკაციის თარიღი, დრო, ხანგრძლივობა და ტიპი, მომხმარებლის საკომუნიკაციო აღჭურვილობა, დადგინდეს მობილური საკომუნიკაციო აღჭურვილობის ადგილმდებარეობა. აღნიშნულ მონაცემებს მიეკუთვნება, მათ შორის, მომხმარებლის ვინაობა და მისამართი, სატელეფონო ზარის ინიციატორის და ადრესატის ტელეფონის ნომრები და IP მისამართი ინტერნეტ სერვისების შემთხვევაში.[25]

სსსკ ითვალისწინებს ძირითად ცნებებს როგორც სატელეფონო კომუნიკაციის ფარული მიყურადების, ასევე კავშირგაბმულობის არხიდან/კომპიუტერული

[22] იქვე.

[23] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, II-92, 93. იხ. ასევე Case NC-293/12 and C-594/12, Digital Rights Ireland ltd and Seitlinger and others, [2014], Court of Justice, 34. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98-100.

[24] *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No 2, 2015, 54.

[25] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98.

სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის საგამოძიებო მოქმედებებთან მიმართებით, კერძოდ, მე-3 მუხლის 33-ე და 34-ე ნაწილების თანახმად, „ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან“ განმარტებულია როგორც „შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ ელექტრონული კავშირიდან (ელექტრონული ფოსტა), კავშირგაბმულობის ქსელიდან, სატელეკომუნიკაციო ან საინფორმაციო სისტემიდან მიმდინარე, გადაცემული, მიღებული, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით“ (სსსკ-ის მე-3 მუხლის 33-ე ნაწილი), ხოლო „ინფორმაციის მოხსნა და ფიქსაცია კომპიუტერული სისტემიდან“ - როგორც „შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ კომპიუტერული სისტემიდან გადაცემული, მიღებული, აგრეთვე კომპიუტერულ სისტემაში მიმდინარე, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით“ (სსსკ-ის მე-3 მუხლის 34-ე ნაწილი).

სსსკ-ის მე-3 მუხლის 27-ე ნაწილი განმარტავს ასევე „კომპიუტერული სისტემის“ ცნებას - „ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს“. ამ კატეგორიას, მათ შორის, მიეკუთვნება პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური ტელეფონი (სსსკ-ის მე-3 მუხლის 27-ე ნაწილი); ხოლო „კომპიუტერულ მონაცემებს“ წარმოადგენს „კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას“ (სსსკ-ის მე-3 მუხლის 28-ე ნაწილი).

სსსკ-ის მე-3 მუხლის 36-ე ნაწილი ასევე ითვალისწინებს „სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის“ ცნებას - მოცემულ ღონისძიებას განეკუთვნება „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის შესაბამისად ავტორიზებული პირის საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით განხორციელებული სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა“ (სსსკ-ის მე-3 მუხლის 36-ე ნაწილი). ამასთან, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ვ“ ქვეპუნქტის თანახმად, „ავტორიზებულ პირს“ წარმოადგენს

„საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ რეგისტრირებული ნებისმიერი სამეწარმეო პირი, აგრეთვე ნებისმიერი არასამეწარმეო იურიდიული პირი, რომელიც ახორციელებს ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფას (ელექტრონული საკომუნიკაციო ქსელის ოპერატორი) ან/და ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას (ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელი)“. ხოლო ამავე მუხლის „ჰ[18]“ ქვეპუნქტით „საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელი“ განმარტებულია როგორც „ელექტრონული საკომუნიკაციო ქსელების ერთიანი სისტემა, რომელიც განკუთვნილია მომხმარებლისთვის საზოგადოებისათვის შეუზღუდავად ხელმისაწვდომი, საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მისაწოდებლად“. აღსანიშნავია, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ფორმულირება სსსკ-ში 2017 წლის 22 მარტის ცვლილებებით ახლებურად ჩამოყალიბდა, კერძოდ, განხორციელებული ცვლილებების თანახმად, მანამდე არსებული ტერმინი „სატელეფონო საუბარი“ შეიცვალა ტერმინით „სატელეფონო კომუნიკაცია“, რითაც დაზუსტდა და სრულყოფილად განისაზღვრა აღნიშნული საგამოძიებო მოქმედების ფარგლებში მოსაპოვებელი ინფორმაციის სახეობა, კერძოდ, „კომუნიკაცია“ უფრო ფართო ტერმინია, ვიდრე „საუბარი“ და მოიცავს ვერბალური და არავერბალური ფორმით აზრთა გაცვლას. ამდენად, 2017 წლის 22 მარტის საკანონმდებლო ცვლილებებით ტერმინი „კომუნიკაციის“ შემოტანით სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ღონისძიების შედეგად მოსაპოვებელი ინფორმაციის ცნება გაფართოვდა.

ამდენად, მოცემულ ქვეთავში განხილული იქნა, თუ რას გულისხმობს ელექტრონული საკომუნიკაციო ქსელები, რომლითაც გადაიცემა ელექტრონული კომუნიკაციები, ასევე რა მოიაზრება კომუნიკაციის მაიდენტიფიცირებელ და შინაარსობრივ მონაცემებში, როგორ განიმარტება ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან/კომპიუტერული სისტემიდან, ისევე როგორც კომპიუტერული სისტემა და კომპიუტერული მონაცემი, აგრეთვე განმარტებულ იქნა საქართველოს კანონმდებლობის მიხედვით, რას გულისხმობს სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა, საერთო სარგებლობის

ელექტრონული საკომუნიკაციო ქსელები, რომლითაც ხორციელდება სატელეფონო კომუნიკაცია. ნაშრომის მომდევნო, შესაბამის თავებში უკვე საუბარი იქნება განსახილველ ღონისძიებებთან დაკავშირებულ სამართლებრივ საკითხებზე.

1.2. სახელმწიფოს ტექნიკური შესაძლებლობების განვითარება ფარული მეთვალყურეობის სფეროში (საერთაშორისო გამოცდილების მიმოხილვა)

ტელეფონის გამოჩენამ არსებითად შეცვალა კერძო პირებს შორის კომუნიკაციის საშუალებები. ტელეფონი იქცა ყოველდღიური კომუნიკაციის არსებით ნაწილად.[26] ფიქსირებული სატელეფონო ქსელებიდან მობილურ კავშირგაბმულობაზე გადასვლამ და საკომუნიკაციო სერვისებზე ფასის შემცირებამ გამოიწვია ტელეფონის მოხმარების მკვეთრი მატება.[27] ამასთან, ინტერნეტის მეშვეობით ხელმისაწვდომი გახდა კომუნიკაციის სხვადასხვა საშუალებები და აპლიკაციები. აღნიშნულმა მიღწევებმა გააუმჯობესა კავშირი მსოფლიოს მასშტაბით, გაამარტივა ინფორმაციის და იდეების გაცვლა გლობალურ დონეზე და გააძლიერა ეკონომიკური პროგრესისა და სოციალური ცვლილებების შესაძლებლობები.[28]

აღსანიშნავია, რომ მე-20 საუკუნის განმავლობაში ტექნოლოგიური ინოვაციების გამო შეიცვალა კომუნიკაციის მონიტორინგის ხასიათი და შედეგები.[29] ტელეფონის აქტიურმა მოხმარებამ დღის წესრიგში დააყენა სატელეფონო კომუნიკაციის მონიტორინგის გამოყენება, რომელიც გულისხმობდა სატელეფონო ხაზზე მოსასმენი მოწყობილობის დამონტაჟებას სატელეფონო საუბრების ფარული მიყურადების მიზნით.[30] თუმცა 90-იან წლებში ციფრული გადამრთველების და ოპტიკურ-ბოჭკოვანი ტექნოლოგიის გამოჩენის გამო სახელმწიფოებმა დახვეწეს მიყურადების ტექნოლოგიები[31]. შედეგად, თანამედროვე სატელეფონო ქსელები დისტანციურად ხელმისაწვდომი და კონტროლირებადია.[32]

---

[26] *Solove D. J., Schwartz P. M.*, Privacy, Information, and Technology, 2nd ed., 2008, 85.
[27] იქვე.
[28] იქვე.
[29] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 5 (ბმული იხ. პირველ გვერდზე).
[30] იქვე.
[31] იქვე.
[32] იქვე.

ტექნოლოგიურმა მიღწევებმა განაპირობა, რომ სახელმწიფოს მხრიდან ელექტრონული თვალთვალის ეფექტიანობა უკვე აღარ არის შეზღუდული რაიმე ფარგლებით ან ხანგრძლივობით[33]. თანამედროვე ტექნოლოგიების ფასის შემცირებამ აღმოფხვრა ელექტრონული მეთვალყურეობის ფინანსური და პრაქტიკული სირთულეები.[34] აღსანიშნავია ისიც, რომ დღესდღეობით ინტერნეტ ქსელების, ასევე მობილური და ფიქსირებული სატელეფონო ქსელების შემთხვევაში ფარული მეთვალყურეობა ტექნიკური თვალსაზრისით შეიძლება განხორციელდეს საკომუნიკაციო სერვისების მიმწოდებელი კომპანიების დახმარებით ან მათ გარეშე.[35]

ნიშანდობლივია, რომ კომუნიკაციის მონიტორინგის ღირებულება მნიშვნელოვნად არის გაზრდილი. საზოგადოების სოციალური აქტივობების უმეტესობა თანამედროვე საკომუნიკაციო ინფრასტრუქტურის საშუალებით ხორციელდება. მაგალითად, თუკი პირს თან აქვს მობილური ტელეფონი, შესაბამისი სერვისის პროვაიდერი ფლობს ინფორმაციას მისი ადგილმდებარეობის შესახებ; ოჯახის წევრებთან, მეგობრებთან და თანამშრომლებთან სოციალური კავშირების უფრო და უფრო დიდი ნაწილი აღირიცხება ელექტრონულად და ინახება კომუნიკაციის ჩანაწერის სახით.[36] ამასთან, თუკი კომუნიკაციის მაიდენტიფიცირებელი მონაცემები ადრე დაბალი ღირებულების ინფორმაციად ითვლებოდა, დღესდღეობით წარმოადგენს ინფორმაციას ყველა იმ პირის შესახებ, რომელსაც ვიცნობთ, ყველა იმ ადგილის შესახებ, რომელსაც ვსტუმრობთ, ყველა იმ საკითხის შესახებ, რომელსაც ინტერნეტის საშუალებით ვეცნობით და იმ ინტერნეტრესურსის შესახებ, რომლის მიმართაც დაინტერესებას გამოვხატავთ.[37] ელექტრონულ კომუნიკაციას შეუძლია გამოავლინოს ყველაზე ინტიმური და

---

[33] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 3, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc> [05.06.2020].

[34] იქვე.

[35] <https://privacyinternational.org/explainer/1309/communications-surveillance> [05.06.2020].

[36] *Hosein G., Palow C. W.,* Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, Ohio State Law Journal, Vol.74, No6, 1077, <https://kb.osu.edu/bitstream/handle/1811/71608/OSLJ_V74N6_1071.pdf> [12.06.2020] იხ. ციტირება: *Viktor Mayer-Schonberger & Kenneth Cukier*, Big Data: A Revolution That Will Transform How We Live, Work and Think 151 (2013).

[37] *Hosein G., Palow C. W.,* Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, Ohio State Law Journal, Vol.74, No6, 1077, <https://kb.osu.edu/bitstream/handle/1811/71608/OSLJ_V74N6_1071.pdf> [12.06.2020].

სენსიტიური დეტალები პიროვნების შესახებ, მათ შორის, მისი წარსული და სამომავლო საქმიანობა. შესაბამისად, კომუნიკაციებს დიდი მტკიცებულებითი ღირებულება გააჩნია.[38]

2. ძირითადი რისკები სისხლის სამართლის პროცესში გამოყენების მიზნით ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებით

როგორც უკვე აღინიშნა, ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება და სისხლის სამართლის პროცესში გამოყენება პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებებში განსაკუთრებით სერიოზულ ჩარევას წარმოადგენს. ეს უფლება ერთ-ერთი თვალსაჩინოა იმ უფლებებს შორის, რომელთა შინაარსის განსაზღვრისას, ხელისუფლება დემოკრატიული და პოლიციური სახელმწიფოების ზღვარზე გადის.[39] საქართველოს კონსტიტუციის მე-15 მუხლით დაცულია კომუნიკაციის თავისუფლება, რაც გულისხმობს კომუნიკაციის დაცვას გარეშე პირთა არასასურველი მონაწილეობისგან.[40] სსსკ-ით ასევე გარანტირებულია კერძო კომუნიკაციის ხელშეუხებლობის უფლება (მუხლი 7). „სსსკ-ის მე-7 მუხლი იცავს ნებისმიერი საშუალებით განხორციელებული კერძო კომუნიკაციის ხელშეუხებლობას, რაც გულისხმობს სატელეფონო, ვერბალურ, წერილობით კომუნიკაციას და კომუნიკაციას ჟესტიკულაციის მეშვეობით.“[41]

ფარული მეთვალყურეობის სფეროში სახელმწიფოს მხრიდან მასშტაბურმა და შეუზღუდავმა ტექნიკურმა შესაძლებლობებმა გამოწვევების წინაშე დააყენა პირადი ცხოვრების დაცვის სფერო. საერთაშორისო დოკუმენტებში ხაზგასმულია ფარული მეთვალყურეობის სფეროს მარეგულირებელი კანონმდებლობის დახვეწის, თანაზომიერების პრინციპის დაცვის, დეტალური და განჭვრეტადი სამართლებრივი რეგულაციების და უფლების დაცვის ადეკვატური გარანტიების უზრუნველყოფის

---

[38] Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 4 (ბმული იხ. პირველ გვერდზე).

[39] იხ. საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის 1/3/407 გადაწყვეტილება, II-8.

[40] *კობახიძე ი.,* მუხლი 20 - პირადი ცხოვრების და პირადი კომუნიკაციის ხელშეუვალობა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 181. წიგნში მოხსენიებულია საქართველოს კონსტიტუციის ძველი რედაქციის 20-ე მუხლი.

[41] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 66.

აუცილებლობა.[42] ევროპული სასამართლოს შეხედულებით, საიდუმლო სამსახურები შეიძლება ლეგიტიმურად ფუნქციონირებდნენ დემოკრატიულ საზოგადოებაში, ამავდროულად, მოქალაქეთა საიდუმლო თვალთვალის უფლებამოსილება, კონვენციის თანახმად, დასაშვებია მხოლოდ იმ შემთხვევებში, როდესაც იგი მკაცრად აუცილებელია დემოკრატიული ინსტიტუტების დაცვის მიზნით.[43]

თანამედროვე ტექნოლოგიების საშუალებით მოპოვებულ ინფორმაციას შეუძლია გამოავლინოს სენსიტიური პერსონალური მონაცემები, როგორიცაა ფინანსური მდგომარეობის, ჯანმრთელობის, პოლიტიკური და რელიგიური შეხედულებებისა და სექსუალური ცხოვრების შესახებ[44]. ეს ინფორმაცია, ერთად აღებული, შესაძლოა გამოყენებულ იქნეს პიროვნების „დეტალური და ინტიმური პროფილის“ შესაქმნელად.[45] ინფორმაციულ ეპოქაში პერსონალურ მონაცემთა დამუშავება, რომელსაც თან არ ახლავს აუცილებელი გარანტიები და უსაფრთხოების ზომები, შესაძლოა დღის წესრიგში აყენებდეს ადამიანის უფლებების დარღვევის საკითხებს.[46] ევროპის საბჭოს მინისტრთა კომიტეტის განმარტებით, კანონმდებლობა, რომელიც ფართომასშტაბიანი ელექტრონული მეთვალყურეობის შესაძლებლობას იძლევა, შესაძლოა წინააღმდეგობაში მოდიოდეს პირადი ცხოვრების პატივისცემის უფლებასთან[47]. პიროვნებებზე დაკვირვების ასეთმა შესაძლებლობებმა და პრაქტიკამ კი შეიძლება მსუსხავი ეფექტი იქონიოს პირის მონაწილეობაზე სოციალურ, კულტურულ და პოლიტიკურ ცხოვრებაში და გრძელვადიან პერსპექტივაში დააზიანოს დემოკრატიული ღირებულებები.[48]

აღსანიშნავია, რომ საქართველოს საკონსტიტუციო სასამართლომ, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემების

---

[42] იხ. მაგალითად, General Assembly, United Nations, Resolution on “The Right to Privacy in The Digital Age”, 21.01.2013 (ბმული იხ. მე-2 გვერდზე).
Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 21 (ბმული იხ. პირველ გვერდზე).

[43] *კილკელი უ.,* პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის განხორციელება, გზამკვლევი, *(რედ.),* ევროპის საბჭო, თბ., 2005, 117-118.

[44] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Committee of Ministers, 11.06.2013, (ბმული იხ. მე-2 გვერდზე).

[45] იქვე.

[46] იქვე.

[47] იქვე.

[48] იქვე.

კოპირების/შენახვის მარეგულირებელი კანონმდებლობის შეფასებისას განმარტა, რომ „ამ მონაცემების სახელმწიფო უსაფრთხოების სამსახურის მიერ კოპირება/შენახვის თავად ფაქტი, არის ერთგვარად მსუსხავი ეფექტის მქონე, ადამიანებისთვის, რადგან მათ იციან, რომ სახელმწიფო ფლობს და ხანგრძლივი ვადით (2 წლით) ინახავს თითოეულის პერსონალური ხასიათის/შინაარსის ამსახველ მნიშვნელოვან ინფორმაციას“[49]. ხანგრძლივი ვადით ამ ინფორმაციის შენახვა საკმარისი და ეფექტიანი კონტროლის არასებობის პირობებში „თავისთავად ზრდის ალბათობას და ინტენსივობას ამ თვალსაზრისით დაუცველობის შეგრძნებისა[50]. ამდენად, ასეთ პირობებში, სახელმწიფოს მიერ მაიდენტიფიცირებელი მონაცემების შენახვის ფაქტმა შესაძლოა მნიშვნელოვნად დააკორექტიროს მათი კომუნიკაცია, ცალკეულ შემთხვევაში კონკრეტულ პირებთან კონკრეტულ ურთიერთობაზე უარის თქმის ჩათვლით“[51].

აღსანიშნავია, რომ თანამედროვე ტექნოლოგიების მოდერნიზების ტემპი გაცილებით მაღალია, ვიდრე თავად კანონმდებლობის. ეს გასაგებიცაა, ვინაიდან რთული წარმოსადგენია, კანონმდებლობა როდესმე დაეწიოს ინფორმაციული ტექნოლოგიების განვითარების მასშტაბებსა და სისწრაფეს. თანამედროვე ელექტრონული კომუნიკაციის საშუალებების ტექნიკური შესაძლებლობები და ინფორმაციის მოპოვების რესურსი მუდმივად ვითარდება, მაგალითად, თუკი რამდენიმე ათწლეულის წინ კომუნიკაციის მონიტორინგის ძირითად ფორმას სატელეფონო კომუნიკაციის ფარული მიყურადება წარმოადგენდა, დღეს ხელმისაწვდომია კერძო კომუნიკაციის მოპოვების მრავალფეროვანი და უფრო მძლავრი ტექნიკური შესაძლებლობები, როგორიცაა, მაგალითად, კომპიუტერულ სისტემაში ფარული შეღწევა (Hacking), რომელიც კომპიუტერულ სისტემაში შენახულ და კავშირგაბმულობის არხით გადაცემულ ნებისმიერ ინფორმაციულ რესურსზე წვდომის შესაძლებლობას იძლევა. ამდენად, ამ ფაქტორის გათვალისწინება მეტად მნიშვნელოვანია ციფრულ ეპოქაში პირადი ცხოვრების უფლების დაცვის კონტექსტში.

[49] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-113.
[50] იქვე.
[51] იქვე.

3. ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვება/გამოყენებასთან დაკავშირებული ქართული კანონმდებლობის მოკლე ისტორიული მიმოხილვა

3.1. ფარული მეთვალყურეობის ღონისძიებების წარმოშობა საკანონმდებლო დონეზე

„ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონი წარმოადგენს პირველ სამართლებრივ აქტს დამოუკიდებელი საქართველოს ისტორიაში, რომლითაც წარმოიშვა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების ღონისძიებების რეგულირების საკანონმდებლო საფუძველი. აღნიშნული კანონი მიღებული იქნა 1999 წლის 30 აპრილს და ამოქმედდა 1999 წლის 15 მაისიდან. კანონის განმარტებითი ბარათის მიხედვით, „საქართველოში იმ დრომდე არ არსებობდა არავითარი საკანონმდებლო ბაზა, რომელიც მოაწესრიგებდა ოპერატიულ-სამძებრო საქმიანობას. როგორც ადრეულ საბჭოთა პერიოდში, საქართველოში ეს უაღრესად რთული და ფაქიზი სფერო სამართალდაცვითი საქმიანობის კვლავ უწყებრივი ნორმატიული აქტებით რეგულირდებოდა. ამასთან, ეს აქტები მკაცრად გასაიდუმლოებული იყო და უმეტესობა ჯერ კიდევ სსრ კავშირის დროს იყო მიღებული.“[52] „სსრ კავშირის დაშლის შემდეგ ყოფილ მოკავშირე რესპუბლიკებში მკაცრად გასაიდუმლოებული უწყებრივი ნორმატიული აქტების ნაცვლად, რომლებითაც წესრიგდებოდა ოპერატიულ-სამძებრო საქმიანობა, იქმნება საკანონმდებლო აქტები, რომლებშიც გათვალისწინებულია კანონიერების დაცვის სამართლებრივი მექანიზმები (საპროკურორო ზედამხედველობა, სასამართლო კონტროლი და ა.შ)“, - აღნიშნულია კანონპროექტის განმარტებით ბარათში.[53]

მოცემული კანონით განისაზღვრა ოპერატიულ-სამძებრო საქმიანობის ცნება, პრინციპები, ამოცანები, სამართლებრივი-საფუძვლები, ოპერატიულ-სამძებრო ღონისძიების ჩატარების წესი, პირობები და სხვა საკითხები. კანონის თანახმად, „ოპერატიულ-სამძებრო საქმიანობა არის ამ კანონით დადგენილი სახელმწიფო ორგანოების სპეციალური სამსახურების მიერ თავიანთი კომპეტენციის ფარგლებში ღია თუ ფარული მეთოდით ჩატარებული ღონისძიებების სისტემა, რომლის მიზანია

[52] განმარტებითი ბარათი კანონპროექტზე „ოპერატიულ-სამძებრო საქმიანობის შესახებ“.
[53] იქვე.

ადამიანის უფლებებისა და თავისუფლებების, იურიდიული პირის უფლებების, საზოგადოებრივი უშიშროების დაცვა დანაშაულებრივი და სხვა მართლსაწინააღმდეგო ხელყოფისაგან.“[54] კანონმა ასევე გაითვალისწინა ოპერატიულ-სამძებრო ღონისძიების ცნება, რომელიც განისაზღვრა როგორც „ამ კანონით დადგენილი წესით უფლებამოსილი სახელმწიფო ორგანოს ან თანამდებობის პირის მოქმედება, რომელიც თავისი კომპეტენციის ფარგლებში უზრუნველყოფს ამ კანონის გათვალისწინებულ ამოცანათა შესრულებას“ (კანონის მე-7 მუხლის პირველი პუნქტი). ასევე დადგინდა ოპერატიულ-სამძებრო ღონისძიებათა ჩამონათვალი, რომელთა შორისაც დასახელდა „მოსამართლის ბრძანებით სატელეფონო საუბრების ფარული მიყურადება და ჩაწერა, ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებებთან, კომპიუტერულ ქსელებთან, სახაზო კომუნიკაციებთან და სასადგურო აპარატურასთან მიერთებით), საფოსტო-სატელეგრაფო გზავნილთა კონტროლი (გარდა დიპლომატიური ფოსტისა).“[55]

3.2 ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მარეგულირებელი ღონისძიებები „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონის მიხედვით

2014 წლის 1 აგვისტომდე მოქმედი კანონმდებლობით ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებული ღონისძიებები რეგულირდებოდა „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონით - როგორც უკვე აღინიშნა, ამავე კანონის მე-7 მუხლის მე-2 პუნქტის „თ“ ქვეპუნქტში გაერთიანებული იყო როგორც სატელეფონო საუბრის ფარული მიყურადების, ასევე კავშირგაბმულობის არხიდან და კომპიუტერული სისტემიდან ინფორმაციის მოპოვების ღონისძიებები - „მოსამართლის ბრძანებით სატელეფონო საუბრის ფარული მიყურადება და ჩაწერა; ინფორმაცის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებებთან,

[54] „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონის 1999 წლის 30 აპრილის რედაქციის პირველი მუხლის პირველი პუნქტი („ოპერატიულ-სამძებრო საქმიანობის“ ცნება დღეს მოქმედ რედაქციაშიც იგივე სახით არის ჩამოყალიბებული), სსმ, 14(21), 30/04/1999.

[55] „ოპერატიულ-სამძებრო საქმიანობის შესახებ” საქართველოს კანონის 1999 წლის 30 აპრილის რედაქციის მე-7 მუხლის მე-2 პუნქტის „თ“ ქვეპუნქტი, სსმ, 14(21), 30/04/1999.

კომპიუტერულ ქსელებთან, სახაზო კომუნიკაციებთან და სასადგურო აპარატურასთან მიერთებით), კომპიუტერული სისტემიდან (როგორც უშუალოდ, ისე დისტანციურად) და ამ მიზნით კომპიუტერულ სისტემაში შესაბამისი პროგრამული უზრუნველყოფის საშუალებების ინსტალაცია;[56] ამავე პუნქტი ასევე ითვალისწინებდა საფოსტო-სატელეგრაფო გზავნილთა (გარდა დიპლომატიური ფოსტისა) კონტროლის ღონისძიებას.

მითითებული მუხლი „თ“ ქვეპუნქტში მოცემული ღონისძიების ჩატარების მატერიალურ წინაპირობად განსაზღვრავდა მოსამართლის ბრძანებას, რომელსაც პროკურორის მოტივირებული შუამდგომლობის საფუძველზე გასცემდა რაიონული (საქალაქო) სასამართლოს მოსამართლე გამოძიების ადგილის ან განაჩენის გამოტანის ადგილის მიხედვით.[57] ამავე მუხლი ასევე ითვალისწინებდა დასახელებული ოპერატიულ-სამძებრო ღონისძიებების ჩატარების შესაძლებლობას მოსამართლის ბრძანების გარეშე გადაუდებელი აუცილებლობისას, რომელიც ექვემდებარებოდა სასამართლოს post factum კონტროლს.[58]

სატელეფონო და სხვა სახის ტექნიკური საშუალებით წარმოებულ კომუნიკაციის შემზღუდველ ღონისძიებებზე წინასწარი სასამართლო კონტროლის აუცილებლობა „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონის „მნიშვნელოვან ფასეულობად“ ითვლებოდა,[59] თუმცა სამეცნიერო ლიტერატურაში გამოთქმული შეხედულების მიხედვით, სადავოა, რამდენად ქმედითი შეიძლებოდა ყოფილიყო სასამართლო კონტროლი სატელეფონო საუბრის ფარული მიყურადებისა და ჩაწერის მკაცრად საიდუმლო ხასიათიდან გამომდინარე.[60]

რაც შეეხება აღნიშნულ ღონისძიებათა განხორციელების საფუძველს, ამავე კანონის მე-9 მუხლის მე-2 პუნქტის მიხედვით, ისეთი ოპერატიულ-სამძებრო ღონისძიების ჩატარება, რომელიც ზღუდავდა კანონით გარანტირებული სატელეფონო და სხვა სახის ტექნიკური საშუალებებით წარმოებული შეტყობინების საიდუმლოებას, დაიშვებოდა მხოლოდ მოსამართლის ბრძანებით და პროკურორის

---

[56] „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონი 2014 წლის 31 აგვისტოს მოქმედი რედაქციის მიხედვით; მე-7 მუხლის მე-2 პუნქტის „თ“ ქვეპუნქტი, სსმ, 14(21), 30/04/1999.

[57] იქვე. მე-7 მუხლის მე-3 პუნქტი.

[58] იქვე. მე-7 მუხლის მე-4 პუნქტი.

[59] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 232.

[60] იქვე.

დადგენილებით, არამართლზომიერ მოქმედებათა მსხვერპლის წერილობითი განცხადების საფუძველზე ან თუ სახეზე იყო ისეთი მართლსაწინააღმდეგო ქმედების მონაცემები, რომლისთვისაც სასჯელის სახით კანონი ითვალისწინებდა თავისუფლების აღკვეთას 2 წელზე მეტი ვადით.[61] შესაბამისად, მართალია ეს პუნქტი ზღუდავდა ღონისძიების ჩატარების საფუძვლებს მხოლოდ იმ დანაშაულთა წრით, რომელიც ითვალისწინებდა თავისუფლების აღკვეთას 2 წელზე მეტი ვადით, თუმცა ეს საფუძველი იყო ალტერნატიული ხასიათის და დანაშაულთა წრის შეზღუდვის მოთხოვნა არ ატარებდა სავალდებულო ხასიათს, როდესაც არსებობდა „არამართლზომიერ მოქმედებათა მსხვერპლის წერილობითი განცხადება“.

კერძო კომუნიკაციის შემზღუდველ ღონისძიებებთან მიმართებით „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ კანონის ერთ-ერთ სუსტ მხარედ შეიძლება მიჩნეულ იქნეს ამ ღონისძიებათა პირველად ვადასთან დაკავშირებული რეგულაციის არარსებობა.[62] მართალია ეს საკითხი პრაქტიკით დარეგულირებული იყო და განისაზღვრებოდა 30 დღით,[63] თუმცა საკანონმდებლო კუთხით ამ საკითხს აკლდა განსაზღვრულობა.

საბოლოო ჯამში, შეიძლება ითქვას, რომ 2014 წლის 1 აგვისტომდე სატელეფონო საუბრის ფარული მიყურადების, ისევე როგორც ინტერნეტურთიერთობის მონიტორინგის ღონისძიებები წარმოადგენდა ოპერატიულ-სამძებრო ღონისძიებებს და რეგულირდებოდა „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონით. აღსანიშნავია ისიც, რომ ეს კანონი ვერ გამოირჩეოდა ადამიანის უფლებების დაცვის მაღალი სტანდარტებით ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების/გამოყენების მიმართულებით[64] და არაერთი დებულება გამხდარა საქართველოს საკონსტიტუციო სასამართლოს მსჯელობისა და

---

[61] „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონი 2014 წლის 31 აგვისტოს მოქმედი რედაქციის მე-9 მუხლის მე-2 პუნქტი, სსმ, 14(21), 30/04/1999.

[62] აღნიშნულ საკითხთან დაკავშირებით იხ. *უსენაშვილი ჯ.* პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციის პრობლემა სასამართლოს კონტროლს დაქვემდებარებული ოპერატიულ-სამძებრო ღონისძიებების წარმოებისას, „სამართლის ჟურნალი“, №2, 2012, 100.

[63] იქვე. 99-100.

[64] *გეგეშიძე. თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება – ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №2, 2017, 45,
<http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].

არაკონსტიტუციურად ცნობის საგანი. აღნიშნული კანონის „მთელი რიგი ნორმების საერთაშორისო სტანდარტებთან შეუსაბამობა“ დასახელდა სწორედ 2014 წელს ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული მასშტაბური ცვლილებების ერთ-ერთ მიზეზად.[65]

3.3. ფარული საგამოძიებო მოქმედებები 2009 წლის 9 ოქტომბრის სისხლის სამართლის საპროცესო კოდექსის მიხედვით

2009 წლის 9 ოქტომბერს მიღებულ იქნა საქართველოს სისხლის სამართლის საპროცესო კოდექსი, რომელმაც ძალადაკარგულად გამოაცხადა 1998 წლის 20 თებერვლის სისხლის სამართლის საპროცესო კოდექსი. ახალი კოდექსის ამოქმედების თარიღად განისაზღვრა 2010 წლის 1 ოქტომბერი (გარდა ცალკეული მუხლებისა). კოდექსის XVI თავი დაეთმო ფარულ საგამოძიებო მოქმედებებს, ხოლო 136-ე მუხლით გათვალისწინებულ იქნა ფარულ საგამოძიებო მოქმედებათა სახეები, მათ შორის, ამავე მუხლის პირველი ნაწილის „დ“ ქვეპუნქტმა დაარეგულირა სატელეფონო და ინტერნეტკომუნიკაციის მოპოვების საპროცესო ღონისძიებები, რომლებიც შემდეგნაირი ფორმულირებით ჩამოყალიბდა - „ტექნიკური საშუალებით განხორციელებული კომუნიკაციის ფარული მიყურადება და ჩაწერა, კავშირგაბმულობის არხიდან (კავშირგაბმულობის საშუალებასთან, კომპიუტერულ ქსელთან, სახაზო კომუნიკაციასთან და სასადგურო აპარატურასთან მიერთებით) ინფორმაციის მოხსნა და ფიქსაცია.“[66]

აღსანიშნავია, რომ 136-ე მუხლის პირველი ნაწილის „დ“ ქვეპუნქტით გათვალისწინებული ღონისძიების ჩატარების აუცილებელ პირობად განისაზღვრა სასამართლოს განჩინება (გარდა გადაუდებელი აუცილებლობის შემთხვევისა). ამასთან, დადგინდა ფარული საგამოძიებო მოქმედების ჩასატარებლად აუცილებელი მტკიცებულებითი სტანდარტი - „დასაბუთებული ვარაუდი“ დანაშაულის ჩადენის შესახებ. ასევე გათვალისწინებულ იქნა ფარული საგამოძიებო მოქმედების ჩატარების

[65] განმარტებითი ბარათი „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ საქართველოს კანონის პროექტზე, <https://info.parliament.ge/#law-drafting/1317> [10.06.2020].

[66] სსსკ-ის 2009 წლის 9 ოქტომბრის რედაქციის 136-ე მუხლის პირველი ნაწილის „დ“ ქვეპუნქტი, სსმ, 31, 09/10/2009.

პირველადი 30 დღემდე ვადა და განისაზღვრა ამ ვადის გაგრძელების შესაძლებლობაც.[67]

სსსკ-ის 138-ე მუხლით დარეგულირდა ფარული საგამოძიებო მოქმედების ჩატარების ზოგადი წესი - პროკურორის შუამდგომლობის განხილვის პროცედურა, სასამართლოს განჩინების რეკვიზიტები, ფარული საგამოძიებო მოქმედების შეწყვეტის საფუძვლები და სხვ.

აღსანიშნავია, რომ სსსკ-მა გაითვალისწინა ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნა, რაც მოცემული ცვლილებების ერთ-ერთ ნოვაციას წარმოადგენდა. მინიმუმამდე დაყვანის პრინციპით განისაზღვრა ფარული საგამოძიებო მოქმედების ჩამტარებელი პირის ვალდებულება, მაქსიმალურად შეეზღუდა იმ კომუნიკაციისა და პირის მონიტორინგი, რომელსაც გამოძიებასთან კავშირი არ ჰქონდა. ასევე გათვალისწინებულ იქნა ცალკეული პროფესიის/საქმიანობის პირთა „კანონით დაცულ საქმიანობას“ მიკუთვნებული კომუნიკაციის დაცვის მოთხოვნაც.[68]

ერთ-ერთ სიახლეს წარმოადგენდა ასევე ფარული საგამოძიებო მოქმედების განჩინების რეესტრთან დაკავშირებული დანაწესი, რომლის მიხედვითაც სასამართლოში უნდა შემდგარიყო ფარული საგამოძიებო მოქმედების განჩინების რეესტრი, რომელშიც განჩინების გამომტან სასამართლოს შეჰქონდა ინფორმაცია, ვინ, როდის, ვისი შუამდგომლობით, ვის მიმართ და რა ვადით გამოიტანა განჩინება, ასევე სისხლის სამართლის საქმის ნომერი.[69]

გარდა აღნიშნულისა, კოდექსის გარდამავალი და დასკვნითი დებულებების მიხედვით, ამ კოდექსის ნორმები ფარული საგამოძიებო მოქმედებების შესახებ უნდა ამოქმედებულიყო 2011 წლის 1 აპრილიდან. მთავრობას ეთხოვა, რომ 2011 წლის 1 იანვრამდე პარლამენტისთვის განსახილველად წარედგინა „ფარული საგამოძიებო მოქმედებების შესახებ“ საქართველოს კანონის პროექტი, რომლის ამოქმედებისთანავე ძალადაკარგულად უნდა გამოცხადებულიყო საპროცესო კოდექსის დებულებები ფარული საგამოძიებო მოქმედებების შესახებ.[70]

---

[67] სსსკ-ის 2009 წლის 9 ოქტომბრის რედაქციის 137-ე მუხლის მე-2 ნაწილი, 138-ე მუხლის პირველი და მე-4 ნაწილები, სსმ, 31, 09/10/2009.

[68] სსსკ-ის 2009 წლის 9 ოქტომბრის რედაქციის 140-ე მუხლი, სსმ, 31, 09/10/2009.

[69] სსსკ-ის 2009 წლის 9 ოქტომბრის რედაქციის 143-ე მუხლი, სსმ, 31, 09/10/2009.

[70] სსსკ-ის 2009 წლის 9 ოქტომბრის რედაქციის 333-ე მუხლის მე-4 პუნქტი, სსმ, 31, 09/10/2009.

მიუხედავად კანონმდებლის ინიციატივისა, ოპერატიულ-სამძებრო ღონისძიებები სსსკ-ის რეგულირების ფარგლებში მოექცია, ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული ზემოთ ხსენებული დებულებები არ ამოქმედებულა - 2010 წლის 24 სექტემბრის კანონით სსსკ-ში განხორციელებული ცვლილებების შედეგად, ამოღებულ იქნა ფარული საგამოძიებო მოქმედებების თავი და სსსკ-ის 136-ე-138-ე მუხლები დაიკავა „კომპიუტერულ მონაცემებთან დაკავშირებულმა საგამოძიებო მოქმედებებმა.“[71]

3.4. 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებათა პაკეტი ფარული საგამოძიებო მოქმედებების შესახებ

2014 წლის 1 აგვისტოს საქართველოს პარლამენტის მიერ მიღებულ იქნა საკანონმდებლო ცვლილებათა პაკეტი, რომლითაც არსებითად შეიცვალა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და გამოყენების მარეგულირებელი კანონმდებლობა. პროექტის ძირითადი არსი სასამართლოს ნებართვას დაქვემდებარებული პირადი ცხოვრების უფლების შემზღუდველი ოპერატიულ-სამძებრო ღონისძიებების „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონიდან სსსკ-ში გადატანაში მდგომარეობდა. შედეგად, სსსკ-ს დაემატა XVI[1] თავი - „ფარული საგამოძიებო მოქმედებები“ და აღნიშნული ოპერატიულ-სამძებრო ღონისძიებები ფარული საგამოძიებო მოქმედების სახით ჩამოყალიბდა. „ცვლილებების შემუშავებისას განსაკუთრებული ყურადღება ეთმობა ისეთი სახის ღონისძიებების განხორციელების პროცესის სამართლებრივ ჩარჩოებში მოქცევას, რომლებიც თავისი შინაარსით ადამიანის კონსტიტუციურ უფლებათა შეზღუდვის მომეტებულ შესაძლებლობას შეიცავს. ამ მიზნით, „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონით გათვალისწინებული ცალკეული ღონისძიებები, რომელთა განხორციელების დროსაც საკმაოდ დიდია ადამიანის კონსტიტუციურ უფლებათა შეზღუდვის ხარისხი და რომელთა განხორციელება, „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს მოქმედი კანონის თანახმად, სასამართლოს ნებართვას საჭიროებს,

[71] „საქართველოს სისხლის სამართლის საპროცესო კოდექსში დამატებებისა და ცვლილებების შეტანის შესახებ“ საქართველოს კანონი, სსმ, 50, 24/09/2010.

გადადის სისხლის სამართლის საპროცესო კოდექსის რეგულირების სფეროში და უზრუნველყოფილია სათანადო პროცესუალური გარანტიებით, მათ შორის, მაღალი ხარისხის სასამართლო კონტროლით და ამ ღონისძიებათა შედეგების გასაჩივრების ეფექტიანი მექანიზმებით“ - აღნიშნულია „საქართველოს სისხლის სამართლის საპროცესო კოდექსში“ ცვლილების შეტანის თაობაზე“ საქართველოს კანონის პროექტის განმარტებით ბარათში.[72]

ამდენად, საკანონმდებლო ცვლილებების მიზნად ადამიანის კონსტიტუციური უფლებების დასაცავად უკეთესი გარანტიების შექმნა, „პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის ეფექტური მექანიზმის ჩამოყალიბება“ დასახელდა.[73] კანონპროექტის განმარტებითი ბარათიდან გამომდინარე, ოპერატიულ-სამძებრო ღონისძიებების სისხლის სამართლის პროცესში გადატანის დანიშნულებაც ამ ღონისძიებებზე საპროცესო კოდექსით გათვალისწინებული პროცედურული გარანტიების გავრცელება წარმოადგენდა.[74]

აღსანიშნავია, რომ სხვადასხვა ქვეყნის სამართლებრივ სისტემებში ოპერატიულ-სამძებრო საქმიანობის საკანონმდებლო რეგულირების ორი ძირითადი მოდელი არსებობს.[75] ისინი პირობითად მოიხსენიება პოსტსაბჭოურ და დასავლეთევროპულ მოდელებად.[76] დასავლეთ ევროპის ზოგიერთ ქვეყანაში (მათ შორის, გერმანია) ოპერატიულ-სამძებრო საქმიანობა განიხილება სისხლის სამართლის საპროცესო კოდექსით დარეგულირებულ, ჩვეულებრივ საგამოძიებო მოქმედებად; ხოლო პოსტსაბჭოური ქვეყნების სამართლებრივი მოდელების შემთხვევაში (მაგ., აზერბაიჯანი) აღნიშნული საქმიანობა რეგულირდება დამოუკიდებელი ნორმატიული აქტებით.[77]

ამდენად, საქართველოს კანონმდებელმა 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებებით უარი თქვა ცალკეული მომეტებულად უფლებაშემზღუდველი და

---

[72] „საქართველოს სისხლის სამართლის საპროცესო კოდექსში“ ცვლილების შეტანის თაობაზე“ საქართველოს კანონის პროექტის განმარტებითი ბარათი, <https://info.parliament.ge/#law-drafting/24>, [12.06.2020].

[73] იქვე.

[74] იქვე.

[75] *უსენაშვილი ჯ.* პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციის პრობლემა სასამართლოს კონტროლს დაქვემდებარებული ოპერატიულ-სამძებრო ღონისძიებების წარმოებისას, სამართლის ჟურნალი, №2, 2012, 87.

[76] იქვე.

[77] იქვე.

ინტენსიური ოპერატიულ-სამძებრო ღონისძიებების ცალკე აქტით რეგულირების პრაქტიკაზე და აღნიშნული ღონისძიებები დაუქვემდებარა სისხლის სამართლის პროცესის რეგულირების სფეროს, რითაც აღნიშნული საქმიანობა მოექცა მეტი კონტროლის რეჟიმისა და გარანტიების ქვეშ.

3.5. შეჯამება

ამდენად, კერძო პირებს შორის ურთიერთობა უფრო და უფრო ინაცვლებს სირტუალურ სივრცეში, რის გამოც ელექტრონული კომუნიკაციის საშუალებებით გადაცემული ინფორმაცია მაღალი სენსიტიურობით ხასიათდება. თანამედროვე ტექნოლოგიების განვითარებამ განაპირობა, რომ სახელმწიფოს შესაძლებლობები ფარული თვალთვალის მიმართულებით თითქმის შეუზღუდავია; ელექტრონული საკომუნიკაციო საშუალებების განვითარების ფონზე, ბუნებრივია, დანაშაულის ჩადენასთან, დაგეგმვასა თუ მომზადებასთან დაკავშირებულმა კომუნიკაციამაც ელექტრონული სახე მიიღო, რაც თავის მხრივ, აისახება კომუნიკაციის მონიტორინგის ღონისძიებების საგამოძიებო ღირებულების გაზრდაზე; ყოველივე აღნიშნული დღის წესრიგში აყენებს ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების და სისხლის სამართლის პროცესში გამოყენების შესაძლებლობების ზედმიწევნით, დეტალურად და ადამიანის უფლებების განუხრელ დაცვაზე ორიენტირებული სახით რეგლამენტაციის აუცილებლობას.

აღსანიშნავია, რომ მოქმედი კანონმდებლობა განსაზღვრავს ძირითად ცნებებს და ტერმინებს სატელეფონო და ინტერნეტკომუნიკაციის მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებების შესახებ, განმარტავს თუ რა ტიპის ღონისძიებები მოიაზრება ამ საგამოძიებო მოქმედებების ქვეშ, რას გულისხმობს ელექტრონული ქსელები, კომპიუტერული მონაცემები და ა.შ.

როგორც გამოიკვეთა, სატელეფონო კომუნიკაციის ფარულ მიყურადებას და ინტერნეტურთიერთობის მონიტორინგს ფარული საგამოძიებო მოქმედებების სახით განვითარების დიდი ისტორია არ გააჩნია, ვინაიდან 2014 წლის 1 აგვისტომდე ეს ღონისძიებები „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონით რეგულირდებოდა; აღსანიშნავია ისიც, რომ მითითებული კანონი არ გამოირჩეოდა ადამიანის უფლებების დაცვის საიმედო გარანტიებით და ევროპულ სტანდარტებზე ორიენტირებული მიდგომით.

ნიშანდობლივია, რომ ჯერ კიდევ 2009 წელს სსსკ-ის მიღებასთან ერთად გადაიდგა გარკვეული ნაბიჯები კერძო კომუნიკაციის შემზღუდველი ღონისძიებების სისხლის სამართლის პროცესში რეგულირების მიზნით, თუმცა იმ დროს სსსკ-ში გათვალისწინებული ფარული საგამოძიებო მოქმედებების თავი არ ამოქმედებულა. ამ სფეროს მოწესრიგების კუთხით ფუნდამენტური ცვლილებები 2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით განხორციელდა, რომლის შედეგადაც სსსკ-ში ფარული საგამოძიებო მოქმედებების რეგულირების გზით კანონმდებელმა გაითვალისწინება გაცილებით მეტი გარანტია და ადამიანის უფლებების დაცვის ხელშესახები ბერკეტები ამ სფეროს რეგულირების თვალსაზრისით.

III. თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის ფარულად მოპოვების ტექნიკური შესაძლებლობები

წინამდებარე თავის მიზანს წარმოადგენს თანამედროვე ელექტრონული კომუნიკაციის საშუალებების წარმოშობისა და განვითარების შესახებ გარკვეული ინფორმაციის მიწოდება მკითხველისათვის, სატელეფონო და ინტერნეტკომუნიკაციის სფეროში არსებული ძირითადი საკომუნიკაციო საშუალებების წარმოჩენა, ასევე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მეთოდების განხილვა. აღნიშნული ემსახურება სისხლის სამართლის პროცესში ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებული შესაძლებლობების უკეთ გააზრებასა და ნაშრომის თემატიკასთან დაკავშირებული საგამოძიებო მოქმედებების არსის უკეთ გაგებას. ნიშანდობლივია, რომ ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების ტექნიკურ ასპექტებთან მჭიდროდაა დაკავშირებული პროცესუალური მიზნებით მათზე წვდომის სამართლებრივი საკითხები - ხშირად ინფორმაციის შეგროვებასთან დაკავშირებული ტექნიკური საკითხები განსაზღვრავს სწორედ, თუ რა მეთოდით უნდა იქნეს ეს ინფორმაცია საპროცესო სამართლებრივი თვალსაზრისით მოპოვებული, მაგალითად, თუკი ინფორმაცია დაშიფრული სახით გადაიცემა (მაგ. ინტერნეტსივრცეში), სამართლებრივი თვალსაზრისით ამ ინფორმაციაზე წვდომის შესაძლებლობები შესაძლოა განსხვავებული იყოს. ამდენად, ნაშრომის ფარგლებში განსახილველი სამართლებრივი საკითხების უკეთ გააზრება შეუძლებელია იმ ძირითადი ტექნიკური ასპექტების წარმოჩენის გარეშე, რომლებიც მჭიდრო კავშირშია საკვლევ თემატიკასთან.

მოცემულ ქვეთავში საუბარი იქნება ასევე იმ ინფორმაციებზე, რომლებიც გადაიცემა ელექტრონულ საკომუნიკაციო ქსელში, კერძოდ, შინაარსობრივ და კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე, რომელზე წვდომაც ხორციელდება სისხლის სამართლის პროცესში. ნიშანდობლივია, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვა/მოპოვებასთან მიმართებით ჩამოყალიბებულია მნიშვნელოვანი კონსტიტუციურ-სამართლებრივი და საერთაშორისო სტანდარტები, რომლებიც ნაშრომის შემდეგ თავებში იქნება დეტალურად გაანალიზებული. ამდენად, ამ საკითხების უკეთ გააზრების მიზნით,

მნიშვნელოვანია ნათლად იქნეს წარმოჩენილი აღნიშნულ მონაცემთა ცნებასა და შინაარსთან დაკავშირებული ასპექტები.

1. თანამედროვე ელექტრონული კომუნიკაციის საშუალებები

1.1. მობილური კავშირგაბმულობა

ტელეფონი და სატელეფონო კომუნიკაცია ყოველდღიური ცხოვრების უმნიშვნელოვანეს ნაწილს წარმოადგენს. სატელეფონო ქსელები იყოფა ორი ტიპის კავშირგაბმულობად: ფიქსირებული და მობილური[78]. ფიქსირებული სატელეფონო ქსელები ემსახურება სტაციონალური ტელეფონების კავშირგაბმულობას[79].

აღსანიშნავია, რომ თანამედროვე კომუნიკაციების ეპოქაში დომინანტი ადგილი მობილურ კავშირგაბმულობას უჭირავს.[80] სწრაფმა ტექნოლოგიურმა განვითარებამ ფუნდამენტური ცვლილებები გამოიწვია სატელეფონო სამყაროში. მობილური ტელეფონი იმდენად პრაქტიკული აღმოჩნდა, რომ საქალაქო ტელეფონების როლი დროთა განმავლობაში შემცირდა.[81]

თანამედროვე მობილური ტელეფონი მოიხსენიება როგორც „ჭკვიანი ტელეფონი“, ანუ „სმარტფონი“. აღნიშნული განპირობებულია იმით, მობილური კავშირგაბმულობისა და კომპიუტერული ტექნოლოგიების სწრაფი განვითარების შედეგად მოხდა ამ ორი ტექნოლოგიის შერწყმა.[82] ამ ცვლილების შედეგად, მობილური ტელეფონები დღესდღეობით მცირე მოცულობის კომპიუტერულ სისტემას წარმოადგენენ.[83] გარდა ტრადიციული სატელეფონო სერვისებისა, თანამედროვე მობილური ტელეფონი გვთავაზობს ისეთ შესაძლებლობებს, როგორებიცაა ელექტრონული მეილის მიღება/გაგზავნა, ინტერნეტ ტელეფონი (VoIP), სხვადასხვა აპლიკაციების გადმოწერა და ინსტალირება, ინტერნეტთან წვდომა, მაგალითად, სოციალური ქსელებით და ონლაინ ჩატებით სარგებლობა და სხვა.

---

[78] <https://privacyinternational.org/explainer/1640/phone-monitoring> [15.06.2020].
[79] იქვე.
[80] იქვე.
[81] <https://theconversation.com/rise-and-fall-of-the-landline-143-years-of-telephones-becoming-more-accessible-and-smart-113295> [15.06.2020].
[82] <https://searchmobilecomputing.techtarget.com/definition/smartphone> [15.06.2020].
[83] *Clough J.,* Principles of Cybercrime, New York, 2010, 135.

1.2. ინტერნეტი და ინტერნეტკავშირგაბმულობა

ინტერნეტი წარმოადგენს დიდ საერთაშორისო კომპიუტერულ სისტემას, რომელიც აერთიანებს კომპიუტერულ ქსელებს[84]. ესაა „ქსელების ქსელი“, სადაც ქსელში ჩართულ კომპიუტერს წვდომის უფლების შემთხვევაში საშუალება აქვს მიიღოს ინფორმაცია ნებისმიერი სხვა კომპიუტერიდან, რაც ასევე გულისხმობს უშუალოდ კომპიუტერის მომხმარებლებს შორის კომუნიკაციას.[85]

აღსანიშნავია, რომ ინტერნეტმა ფუნდამენტური ცვლილებები შეიტანა საზოგადოების ცხოვრების წესში.[86] დიდი მოცულობის ინფორმაციის მთელი მსოფლიოს მასშტაბით სწრაფად და ნაკლები ხარჯებით გავრცელების გზით ინტერნეტმა გარდაქმნა კომუნიკაციის არსებული შესაძლებლობები.[87] ელექტრონული ფოსტა, მოკლე ტექსტური შეტყობინებები, ონლაინ ჩატები საქმიანი და პირადი კომუნიკაციის თანდათან უფრო მოთხოვნადი საშუალება ხდება.[88] ინტერნეტი იქცა დიდ მანძილზე სატელეფონო ზარების განხორციელების მთავარ საშუალებად. ინტერნეტი გვთავაზობს მრავალფეროვან სერვისებს და კომუნიკაციის განსხვავებულ შესაძლებლობებს, რომელთა შორის აღსანიშნავია, მაგალითად, ელექტრონული ფოსტა, ონლაინ ფორუმები, სწრაფი შეტყობინების სერვისი, ინტერნეტ ტელეფონები და სხვა მრავალი.

2. ელექტრონული საკომუნიკაციო ქსელით გადაცემული ინფორმაციები

2.1. კომუნიკაციის შინაარსის შესახებ ინფორმაცია

კერძო პირებს შორის კომუნიკაციისას ელექტრონული საკომუნიკაციო ქსელების საშუალებით გადაეცემა როგორც კომუნიკაციის შინაარსი, ასევე კომუნიკაციის მაიდენტიფიცირებელი მონაცემები. ფარული მეთვალყურეობის ფარგლებში სახელმწიფო ხელისუფლების ორგანოებს წვდომის საშუალება აქვთ ორივე აღნიშნული ტიპის ინფორმაციაზე.

---

[84] <https://searchwindevelopment.techtarget.com/definition/Internet> [15.06.2020].

[85] იქვე.

[86] *Wright J.,* Necessary and Inherent Limits to Internet Surveillance, Internet Policy Review,Vol.2, No. 3, 2013, 1.

[87] *Clough J.,* Principles of Cybercrime, New York, 2010, 135.

[88] იქვე.

კომუნიკაციის შინაარსის და მაიდენტიფიცირებელი ინფორმაციის დიფერენციაციას აშშ-ის სამოსამართლო სამართალში, მაგალითად, საფუძვლად უდევს „კონვერტის“ პრინციპი - კონვერტში მოთავსებული წერილი შეიცავს შინაარსობრივ ინფორმაციას, ხოლო კონვერტზე აღნიშნული მონაცემები, რომლებიც აუცილებელია მის გასაგზავნად, მაგალითად, ადრესატის მისამართი, არის "მაიდენტიფიცირებელი მონაცემები (მეტადატა)."[89] ამდენად, კომუნიკაციის მაიდენტიფიცირებელი მონაცემები წარმოადგენს ინფორმაციას იმის შესახებ, თუ კონკრეტულად ვისთან, როდის, რა საშუალებით, სად და რა ხანგრძლივობით შედგა კომუნიკაცია.[90] ხოლო კომუნიკაციის შინაარსს მიეკუთვნება უშუალოდ სატელეფონო საუბარი და ტელეფონის მეშვეობით გაცვლილი მოკლე ტესტური შეტყობინებების შინაარსი, ელექტრონული ფოსტით გაგზავნილი და მიღებული შეტყობინებების ტექსტი, ინტერნეტაპლიკაციებისა და სოციალური ქსელების მეშვეობით გაცვლილი ტექსტური, ხმოვანი და ფოტო/აუდიო ფორმატის შეტყობინებები, გაგზავნილი და მიღებული დოკუმენტები და სხვ. შინაარსობრივი ინფორმაცია არის მონაცემთა ისეთი სახე, რომლის გადაცემა კომუნიკაციის მიზანს წარმოადგენს; ამავდროულად, აუცილებელია, რომ კომუნიკაცია შედგეს ადამიანებს შორის.[91] ამდენად, კომუნიკაციის შინაარსი წარმოადგენს ორ ან მეტ პირს შორის გაცვლილ ტექსტურ, ხმოვან ან ფოტო/აუდიო ინფორმაციას.

აღსანიშნავია, რომ კომუნიკაციის შინაარსსა და მაიდენტიფიცირებელ მონაცემებს შორის განსხვავება ასევე საკანონმდებლო დონეზე არის გათვალისწინებული, კერძოდ, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი ერთმანეთისგან განასხვავებს კომუნიკაციის შინაარსს და მის

---

[89] Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 8-9, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf> [15.06.2020].
იხ. ასევე: *Solove D.J., Rotenberg M., Schwartz P. M. Privacy*, Information, and Technology, New York, 2006, 100. აღსანიშნავია, რომ აშშ-ის სამოსამართლო სამართალში მეტადატა მოიხსენიება როგორც "Envelope information".

[90] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, 30.

[91] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 33-34.

მაიდენტიფიცირებელ მონაცემებს.[92] ასევე, განმარტავს კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცნებას.

2.2. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები

როგორც უკვე აღინიშნა, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებს, იგივე „მეტადატას“ განეკუთვნება ინფორმაცია, რომელიც წარმოშობილი ან დამუშავებულია კომუნიკაციის განხორციელების შედეგად.[93] ამდენად „მეტადატა“ შეიძლება მოიცავდეს ტრაფიკის შესახებ მონაცემებს, ადგილმდებარეობის შესახებ ინფორმაციას, ასევე კომუნიკაციის წყაროს მაიდენტიფიცირებელ მონაცემებს.

“ტრაფიკის მონაცემებს” მიეკუთვნება ინფორმაცია, რომელიც დამუშავებულია ელექტრონულ საკომუნიკაციო ქსელში კომუნიკაციის გადაცემის ან ბილინგის მიზნებისათვის.[94] ხოლო “ადგილმდებარეობის შესახებ“ ინფორმაცია წარმოადგენს ელექტრონულ საკომუნიკაციო ქსელში დამუშავებულ ნებისმიერ ინფორმაციას, რომელიც მიუთითებს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელის მომხმარებლის საკომუნიკაციო აღჭურვილობის გეოგრაფიულ ლოკაციას.“[95]

აღსანიშნავია, რომ „ინტერნეტტრაფიკის მონაცემები“ ასევე განმარტებულია „კომპიუტერული დანაშაულის შესახებ“ 2001 წლის 23 ნოემბრის კონვენციით, კერძოდ, მითითებული კონვენცია ამ მონაცემებს მიაკუთვნებს „კომუნიკაციებთან დაკავშირებულ და კომპიუტერული სისტემის მიერ გენერირებულ ნებისმიერ კომპიუტერულ მონაცემს, რომელიც კომუნიკაციათა ჯაჭვის ნაწილია, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს.“[96]

---

[92] „ელექტრონული კომუნიკაციების შესახებ” საქართველოს კანონის 8[1] მუხლი ცალ-ცალკე გამოყოფს კომუნიკაციის შინაარსს და მის მაიდენტიფიცირებელ მონაცემებს, სსმ, 26, 02/06/2005.

[93] *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No.2, 2015, 54.

[94] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).
<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058> [15.06.2020].

[95] იქვე.

[96] კონვენცია კომპიუტერული დანაშაულის შესახებ, ევროპის საბჭო, 23/11/2001.

კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცნება ასევე გათვალისწინებულია საქართველოს კანონმდებლობით, კერძოდ, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ჰ[62]“ ქვეპუნქტის შესაბამისად, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებს წარმოადგენს: „მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები.“[97] შესაბამისად, საქართველოს კანონმდებლობით განსაზღვრული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცნება აერთიანებს მომხმარებლის მაიდენტიფიცირებელ მონაცემებს, ტრაფიკისა და ადგილმდებარეობის შესახებ ინფორმაციას.

მეტადატა წარმოადგენს ინფორმაციას იმასთან დაკავშირებით, თუ ვინ (კომუნიკაციის მხარეები), როდის, რა ხანგრძლივობით, რა სიხშირით დაუკავშირდა ერთმანეთს, ასევე კომუნიკაციის ტიპის (მაგალითად, სატელეფონო ზარი, ელექტრონული ფოსტა), ადგილის და გამოყენებული მოწყობილობის (ფიქსირებული ტელეფონი, სმარტფონი და სხვ.) შესახებ.[98]

აღსანიშნავია, რომ არაერთი ქვეყნის კანონმდებლობა ავალდებულებს ელექტრონული სერვისის მიმწოდებლებს, შეინახონ მომხმარებლების ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემები სამართალდამცავი ორგანოების ხელმისაწვდომობის მიზნებისათვის.[99] ელექტრონული კომუნიკაციის კომპანიების

[97] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ჰ[62]“ ქვეპუნქტი, სსმ, 26, 02/06/2005.

[98] *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, , Vol. 3, No.2, 2015, 54.

[99] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9 (ბმული იხ. მე-19 გვერდზე).

მიერ მეტადატის სავალდებულო შენახვა გათვალისწინებულია ევროკავშირის არაერთი წევრი ქვეყნის კანონმდებლობით.[100]

ინტერნეტკომუნიკაციებთან მიმართებით კომუნიკაციის მაიდენტიფიცირებელ მონაცემს წარმოადგენს, მაგალითად, ინტერნეტ პროტოკოლის მისამართი (IP მისამართი), ელექტრონული ფოსტის გაგზავნა-მიღებასთან დაკავშირებული მონაცემები, ინტერნეტთან წვდომის შესახებ ინფორმაცია, ადგილმდებარეობის შესახებ მონაცემები[101] და სხვ. რაც შეეხება სატელეფონო სერვისებს, მეტადატას განეკუთვნება, მაგალითად, ზარის ინიციატორის და ადრესატის ტელეფონის ნომრები, მობილური აღჭურვილობის საერთაშორისო იდენტიფიკატორი (IMEI), მობილურის მომხმარებლის საერთაშორისო იდენტიფიკატორი (IMSI), ზარის დაწყებისა და დასრულების თარიღი და დრო, ადგილმდებარეობის შესახებ მონაცემები და სხვ.

როგორც უკვე აღინიშნა, ინტერნეტსერვისების შემთხვევაში მეტადატას მიეკუთვნება, მაგალითად, ინტერნეტ პროტოკოლის (IP) მისამართი. ეროვნული რეგულაციები მეტადატის სავალდებულო შენახვასთან დაკავშირებით ავალდებულებს სერვისის მიმწოდებლებს, შეინახონ ინტერნეტ პროტოკოლის მისამართის შესახებ ინფორმაცია მისი მფლობელის დადგენის მიზნით.[102]

IP მისამართი წარმოადგენს ინტერნეტთან დაკავშირებული ნებისმიერი მოწყობილობის უნიკალურ ნომერს, რომელიც მოწყობილობებს ერთმანეთთან დაკავშირების შესაძლებლობას აძლევს.[103] ცალკე აღებული IP მისამართი იძლევა გარკვეული გარემოებების დადგენის შესაძლებლობას, როგორიცაა კონკრეტული ინტერნეტ სერვისის მომწოდებელი და ზოგადი ადგილმდებარეობა (როგორც წესი, აღნიშნული ინტერნეტ სერვისის მიმწოდებლის ლოკაცია)[104]. შესაბამისად, IP მისამართების უმრავლესობამ დაინტერესებულ პირი შეიძლება დააყენოს ინტერნეტ სერვისის მიმწოდებლის და არა კონკრეტული მოწყობილობის კვალზე.[105] თუმცა

---

[100] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgement, 2017, 4, <https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf> [15.06.2020].

[101] *Kerr O.S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 384.

[102] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 18 (ბმული იხ. პირველ გვერდზე).

[103] Benedik v. Slovenia; [2018], ECtHR. 96.

[104] იქვე.

[105] იქვე.

აღნიშნული ინტერნეტ სერვისის მიმწოდებელი კომპანიის მეშვეობით სამართალდამცავ ორგანოს შეუძლია დაადგინოს პირის ვინაობა და კონკრეტული მისამართი.[106]

IP მისამართი შეიძლება მჭიდროდ იყოს დაკავშირებული კომუნიკაციის შინაარსობრივ მონაცემებთან და შეუძლია გამოავლინოს პირის ონლაინ აქტივობის შესახებ მნიშვნელოვანი ინფორმაცია, მათ შორის, სენსიტიური დეტალები მისი ინტერესების, შეხედულებებისა და ინტიმური ცხოვრების წესის შესახებ.[107] გაეროს სპეციალური მომხსენებელი 2013 წლის 17 აპრილის ანგარიშში ყურადღებას ამახვილებს IP მისამართის განსაკუთრებულ ინფორმაციულ ღირებულებაზე და აღნიშნავს, რომ ეს მონაცემი შესაძლოა გამოყენებულ იქნეს მისი მფლობელის ვინაობის და ადგილმდებარეობის დასადგენად და მის მიერ ინტერნეტ სივრცეში განხორციელებული ქმედებების თვალთვალის მიზნებისათვის.[108] IP მისამართის ინფორმაციულ ღირებულებასა და მნიშვნელობაზე დიდი ყურადღებაა გამახვილებული სამეცნიერო ლიტერატურაშიც. ამ მონაცემის საფუძველზე შესაძლებელია დადგინდეს პირის ონლაინ აქტივობებთან დაკავშირებული საკმაოდ სენსიტიური ინფორმაცია[109]. IP მისამართის ცოდნის შემთხვევაში, შესაძლებელია მაგალითად, სამართალდამცავმა ორგანომ შეიტყოს იმ კომპანიების ჩამონათვალი, სადაც პირი ონლაინ ყიდვა-გაყიდვას ახორციელებს, პოლიტიკური ორგანიზაციები, რომლებითაც ინტერესდება, ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაცია და ა.შ.[110] აღნიშნული, შესაძლებელია კონკრეტული ელექტრონული კომუნიკაციის კომპანიის მეშვეობით. ამდენად, IP მისამართით შეიძლება გამოვლინდეს ონლაინ სერვისები, სადაც პირი არის დარეგისტრირებული, ორგანიზაციებთან კავშირები და პერსონალური ინტერესები, გამომახებული ვებგვერდების საფუძველზე.[111]

---

[106] იქვე.
[107] Benedik v. Slovenia; [2018], ECtHR, 109.
[108] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 18 (ბმული იხ. პირველ გვერდზე).
[109] *Solove D. J.,* Reconstructing Electronic Surveillance Law, Geo. Wash. L. Rev, Vol.72, 2004, 1287.
[110] იქვე.
[111] *Forcese C.*, Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Initiatives, წიგნში: Law, Privacy and Surveillance in Canada in the Post-Snowden Era, *Geist M., (ed.),* 2015, 130.

იურიდიულ ლიტერატურაში გამოთქმული მოსაზრების თანახმად, IP მისამართი განეკუთვნება ტრაფიკის მონაცემს, მაგრამ უფრო რთული სიტუაციაა URL (Uniform Resource Locator) და ონლაინ ძიების მონაცემების შემთხვევაში - სამეცნიერო ლიტერატურაში აქტიურად განიხილება საკითხი იმის შესახებ, აღნიშნული მონაცემი მიეკუთვნება შინაარსობრივ თუ ტრაფიკის ინფორმაციას.[112] აღსანიშნავია, რომ URL წარმოადგენს ინტერნეტსივრცეში კონკრეტული ინფორმაციის ადგილმდებარეობის განმსაზღვრელს. როდესაც პირი ინტერნეტში იძახებს რაიმე ინფორმაციას, ის იძახებს მის URL-ს[113]. URL ასევე შეიცავს ონლაინ ძიების შესახებ ინფორმაციას[114]. კონკრეტულ ვებგვერდზე სტუმრობის შესახებ მონაცემი იძლევა პირის მიერ აღნიშნულ ვებგვერდზე განთავსებული კონკრეტული შინაარსის გაცნობის შესახებ ინფორმაციას, კერძოდ, კონკრეტული დოკუმენტის მისამართით - URL, საიტის IP მისამართისგან განსხვავებით, შესაძლებელია იდენტიფიცირებულ იქნეს ვებ-გვერდზე პირის მიერ ნანახი კონკრეტული დოკუმენტი და შესაბამისად, გამოვლინდეს პირის ინტერნეტ აქტივობის შესახებ მეტი ინფორმაცია.[115]

სამეცნიერო ლიტერატურაში გამოხატული შეხედულების მიხედვით, ძალიან რთულ საკითხს წარმოადგენს, თუ რამდენად შეიცავს URL შინაარსობრივ ინფორმაციას,[116] ვინაიდან შინაარსობრივ და ტრაფიკის მონაცემებს შორის განსხვავება ხშირად არ არის ცალსახა და ნათელი.[117] აღნიშნული განპირობებულია იმით, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემებს პირის საქმიანობის შესახებ საკმაოდ ბევრი დეტალის გამოვლენა შეუძლია, ხშირად იმაზე მეტის, ვიდრე თავად კომუნიკაციის შინაარსს.[118]

---

[112] *Clough J.,* Principles of Cybercrime, New York, 2010, 153; *Zigerell L. J.,* Maintaining the Technological Neutrality of the Fourth Amendment, წიგნში: Privacy in the Digital Age, 21st – Century Challenges to the Fourth Amendments, *Lind N., S., Rankin E., Praeger (eds.),* California, 2015, Vol. 2, 554-557.

[113] *Solove D.J., Schwartz P.,* Information Privacy Law, 5th Edition, New York, 2015, 405-406.

[114] იქვე.

[115] იქვე.

[116] *Kerr, O. S.* Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, Northwestern University Law Review, 2003, Vol. 97, No.2, 645.

[117] *Solove D. J.,* Reconstructing Electronic Surveillance Law, Geo. Wash. L. Rev, Vol.72, 2004, 1287.

[118] იქვე.

3. ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მეთოდები

3.1. ინფორმაციის მოპოვება სატელეფონო კავშირგაბმულობიდან

როგორც უკვე აღინიშნა, კომუნიკაციის მონიტორინგის ტექნოლოგია მუდმივად ვითარდება და უფრო და უფრო მეტი ინფორმაციის მოპოვების პოტენციალი გააჩნია. კომუნიკაციის მონიტორინგი დღეს უკვე აღარ არის შეზღუდული სატელეფონო ხაზზე სპეციალური "მოსასმენი მოწყობილობის" („crocodile clip") ფიზიკურად დამაგრებით, როგორც ეს ფიქსირებული სატელეფონო ქსელის შემთხვევაში ხდებოდა.[119] აღსანიშნავია, რომ ფიქსირებული სატელეფონო ქსელის „მოსმენა" გულისხმობს ინფორმაციის „გადაჭერას", როდესაც ეს ინფორმაცია გადაეცემა საერთო სარგებლობის ფიქსირებული სატელეფონო ქსელის მეშვეობით[120]. ისტორიული თვალსაზრისით ამ საშუალებით წარმოებული კომუნიკაციის მონიტორინგი ხდებოდა სადენზე მოსასმენი მოწყობილობის დამაგრებით.[121] ფიქსირებული სატელეფონო ქსელის მონიტორინგის თანამედროვე ტექნოლოგიებიც ძირითადად ამავე პრინციპით - სატელეფონო ქსელზე შესაბამისი მოწყობილობის მოთავსებით ფუნქციონირებს.[122] აღნიშნულისგან განსხვავებით, თანამედროვე მობილური საკომუნიკაციო ქსელების მონიტორინგი, როგორც წესი, აბსოლუტურად განსხვავებული ტექნოლოგიის გამოყენებით ხორციელდება.

ქვემოთ განვიხილავთ მობილური კომუნიკაციის შინაარსის და კომუნიკაციის მაიდენტიფიცირებელი მონაცემების (მათ შორის, ადგილმდებარეობის შესახებ მონაცემების) მოპოვების გავრცელებულ საშუალებებს.

ამასთან, მოცემული ქვეთავის მიზანი არ არის კომუნიკაციის მოპოვების მხოლოდ იმ შესაძლებლობების განხილვა, რომლებიც საქართველოს კანონმდებლობით არის გათვალისწინებული, არამედ ზოგადად, საერთაშორისო გამოცდილების გათვალისწინებით, სატელეფონო და ინტერნეტკომუნიკაციის

---

[119] <https://privacyinternational.org/explainer/1309/communications-surveillance> [05.06.2020].
[120] იქვე.
[121] იქვე.
[122] იქვე.

მონიტორინგის სფეროში გავრცელებული ზოგიერთი ძირითადი ტექნიკური საშუალებების წარმოჩენა.

3.1.1. პირის ადგილმდებარეობის დადგენა მობილური ტელეფონის საშუალებით

მობილური ტელეფონის ადგილმდებარეობის დადგენის ერთ-ერთ საშუალებას მიეკუთვნება სატელეფონო ანძის ადგილმდებარეობის შესახებ მონაცემი (Cell Site Location Information - CSLI).[123] CSLI წარმოადგენს ჩანაწერს, რომელიც აერთიანებს კონკრეტული სატელეფონო ანძის (რომელსაც დროის მოცემულ მონაკვეთში დაუკავშირდა მობილური ტელეფონი) ადგილმდებარეობის შესახებ ინფორმაციას და ამ პროცესთან დაკავშირებულ ტექნიკურ მონაცემებს.[124] ამ ინფორმაციის საშუალებით შესაძლებელია დადგინდეს სად იყო მობილური აპარატი, როგორ მოხვდა კონკრეტულ ტერიტორიაზე და რა ვადით იმყოფებოდა ამ ადგილას.[125] ყოველ ჯერზე, როდესაც მომხმარებელი ახორციელებს ან ღებულობს ზარს, ან აგზავნის მოკლე ტექსტურ შეტყობინებას მობილური ტელეფონის საშუალებით, კომუნიკაცია მყარდება მობილურ აპარატსა და უახლოეს სატელეფონო ანძას შორის[126]. თუ მომხმარებელი შეიცვლის ადგილმდებარეობას ზარის განმავლობაში, ზარი უწყვეტად გადამისამართდება უახლოეს ანძასთან.[127] ასევე, მობილური ტელეფონის გამართულად მუშაობისთვის მობილური აპარატი პერიოდულად ახდენს იდენტიფიცირებას და რეგისტრაციას უახლოეს სატელეფონო ანძასთან, რომელიც, როგორც წესი, სიგნალის ყველაზე ძლიერი მიმწოდებელია[128]. აღნიშნული ხდება იმისთვის, რომ მობილური ქსელის ოპერატორმა ზუსტად იცოდეს, რა მიმართულებით გადაამისამართოს შემომავალი სატელეფონო ზარი.[129]

როდესაც მობილური აპარატი უკავშირდება სატელეფონო ანძას, მომხმარებლის ტელეფონის ნომერთან ერთად აგზავნის სხვა მონაცემებსაც, მათ შორის, მობილური

---

[123] *Pell S. K.,* Location Tracking, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 47.
[124] https://www.eff.org/criminaldefender/cell-site-location [15.06.2020].
[125] *Gray D.* The Fourth Amendment in an Age of Surveillance, Cambridge, 2017, 27.
[126] *Pell S. K.,* Location Tracking, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 48.
[127] იქვე.
[128] იქვე.
[129] იქვე.

აღჭურვილობის საერთაშორისო იდენტიფიკატორს (IMEI). მობილური კავშირგაბმულობის ოპერატორი აფიქსირებს რომელი მობილური აპარატი დაუკავშირდა ქსელს, როდის და რომელი სატელეფონო ანძის საშუალებით, რათა შეძლოს მომხმარებლისთვის სერვისის საფასურის დაანგარიშება.[130]

მობილური ოპერატორები ინახავენ აღნიშნულ მონაცემებს სხვადასხვა მიზნებით (მაგ. გადასახადების დაანგარიშების) და ვადით.[131] თუმცა აღსანიშნავია, რომ ბევრ ქვეყანაში მოქმედებს ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების სავალდებულო შენახვასთან დაკავშირებული დებულებები[132]. ასეთ შემთხვევაში სერვისის მიმწოდებელი ვალდებულია გარკვეული ვადით შეინახოს ასეთი მონაცემები სამართალდამცავი ორგანოების მიერ ხელმისაწვდომობის მიზნებისათვის.[133] ამ მონაცემებს მიეკუთვნება, მათ შორის, მობილური აღჭურვილობის ადგილმდებარეობის შესახებ ინფორმაციაც. ამდენად, ამ მონაცემების გამოთხოვა შესაძლებელია სამართალდამცავი ორგანოების მიერ დანაშაულის გამოძიების მიზნებისათვის.

აღსანიშნავია, რომ საქართველოს კანონმდებლობა ასევე ითვალისწინებს უფლებამოსილი სახელმწიფო ორგანოდან (სააგენტოდან), ასევე ელექტრონული კომუნიკაციის კომპანიისგან ადგილმდებარეობის შესახებ მონაცემთა გამოთხოვის შესაძლებლობას. აღნიშნულის სამართლებრივ საფუძველს ქმნის სსსკ-ის 136-ე მუხლი, კერძოდ, ადგილმდებარეობის შესახებ ინფორმაციაზე, როგორც კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ერთ-ერთ კატეგორიაზე, წვდომა შეიძლება განხორციელდეს იმ სამართლებრივი ჩარჩოს ფარგლებში, რაც გათვალისწინებულია ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების მოპოვებისთვის, ამდენად, აღნიშნული ინფორმაციის მოპოვება შესაძლებელია სსსკ-ის 136-ე მუხლით გათვალისწინებული მკაცრი წინაპირობების

---

[130] *Bloom R. M., Clark W. T.,* Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and The Need for Fourth Amendment Protection, The Journal of Criminal Law & Crimininology, Vol.106, No.2, 173, იხ, ციტირება: *O'Malley,* supra note 37, at 23.

[131] *Pell S. K.,* Location Tracking, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 48.

[132] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9 (ბმული იხ. მე-19 გვერდზე).

[133] იქვე.

არსებობისას და ამავე მუხლით დადგენილი წესით, რაზეც უფრო დეტალურად ნაშრომის შესაბამის თავში იქნება საუბარი.

3.1.2. სატელეფონო კომუნიკაციის ფარული მიყურადება

ერთ-ერთ ყველაზე ცნობილ მობილურ საკომუნიკაციო ქსელს წარმოადგენს GSM ქსელი (გლობალური სისტემა მობილური კომუნიკაციებისთვის)[134]. GSM ქსელში შესაძლებელია იმ ინფორმაციის მიყურადება, რომელიც გადაიცემა მობილური ტელეფონიდან იმ სატელეფონო ანძასთან, რომელსაც უკავშირდება ტელეფონი.[135]

ტელეკომუნიკაციის „გადაჭერასთან" დაკავშირებით გარკვეულ სტანდარტებს ადგენს ევროკავშირის პარლამენტისა და საბჭოს 1995 წლის 17 იანვრის რეზოლუცია „ტელეკომუნიკაციის კანონიერი მოსმენის თაობაზე."[136] აღნიშნული რეზოლუცია ემსახურება სატელეკომუნიკაციო მონიტორინგის სფეროში სამართალდამცავი ორგანოების საჭიროებების და სატელეკომუნიკაციო ქსელის ოპერატორის/სერვისის მიმწოდებლის მოვალეობების დადგენას.

რეზოლუცია ეხება როგორც „ტელეკომუნიკაციის" შინაარსის, ასევე სატელეფონო ზართან დაკავშირებული მონაცემების მოპოვებას (call associated data) და განსაზღვრავს, თუ რა სახის შესაძლებლობებით უნდა იყვნენ უზრუნველყოფილი სამართალდამცავი ორგანოები სატელეკომუნიკაციო მონიტორინგის სფეროში და შესაბამისად - ქსელის ოპერატორების/სერვისის მიმწოდებლების ვალდებულებას, დაეხმარონ სამართალდამცავ ორგანოებს სასამართლოს ნებართვით გათვალისწინებული ინფორმაციის მოპოვებაში.[137] რეზოლუციის მიხედვით, სამართალდამცავ ორგანოებს ესაჭიროებათ ტელეკომუნიკაციის შინაარსის მიმდინარე რეჟიმში მიღების შესაძლებლობა. ასევე მიმდინარე რეჟიმში უნდა იქნეს უზრუნველყოფილი სატელეფონო ზართან დაკავშირებული მონაცემების (ზარის ინიციატორის და ადრესატის ტელეფონის ნომრები, კავშირის დრო, ხანგრძლივობა და ა.შ.) მიღების შესაძლებლობა (თუკი ეს უკანასკნელი არ არის შესაძლებელი,

---

[134] <https://privacyinternational.org/explainer/1640/phone-monitoring> [05.06.2020].

[135] იქვე.

[136] Council Resolution of 17 January 1995 On the Lawful Interception of Telecommunications, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104> [15.06.2020].

[137] იქვე.

მონაცემები სამართალდამცავ ორგანოს უნდა მიეწოდოს დაუყოვნებლივ ღონისძიების შეწყვეტისას).

ამდენად, აღნიშნული რეზოლუცია განსაზღვრავს სტანდარტებს სატელეკომუნიკაციო მოსმენების სფეროში და მათ შორის, რაც ყველაზე მნიშვნელოვანია, ქსელის ოპერატორების/მომსახურების მიმწოდებლის ვალდებულებას, ითანამშრომლონ საგამოძიებო ორგანოებთან ამ მიმართულებით.

აღსანიშნავია, რომ განასხვავებენ სატელეფონო კომუნიკაციის ფარული მიყურადების ორ მოდელს - აშშ-ში და დასავლეთ ევროპულ სახელმწიფოებში მოქმედი სისტემის მიხედვით, „კანონიერი მოსმენის“ ჩატარების მიზნით შესაბამისი სახელმწიფო ორგანო სატელეფონო და ინტერნეტ სერვისის მიმწოდებელ კომპანიას წარუდგენს სასამართლოს ნებართვას, რის შემდეგაც „მონაცემთა გადაჭერის“ ტექნიკური აღსრულების პროცესს ახორციელებს აღნიშნული სერვისის მიმწოდებელი და მოთხოვნილ ინფორმაციას აწვდის სახელმწიფო ორგანოს.[138] ამრიგად, ასეთი სისტემის პირობებში სახელმწიფოს არ აქვს უშუალო წვდომა კავშირგაბმულობის საშუალებებზე, მონაცემთა მოპოვებას ახორციელებს თავად ელექტრონული კომუნიკაციის კომპანია და უზრუნველყოფს მონაცემთა მიმდინარე რეჟიმში მიწოდებას საგამოძიებო ორგანოებისათვის. ასეთი სისტემა არის სწორედ ასახული ევროკავშირის ზემოთაღნიშნულ რეზოლუციაში.

თუმცა არსებობს განსხვავებული მოდელიც, სადაც სახელმწიფოს შესაბამის ორგანოებს უშუალო წვდომა აქვთ კომუნიკაციის არხებზე, მაგალითად, ასეთ სისტემას მიეკუთვნება რუსეთში მოქმედი “SORM” (ოპერატიულ-სამძებრო ღონისძიებების სისტემა),[139] რომელიც დაინერგა 1990-იან წლებში და ითვალისწინებს არქიტექტურას, რომლის საშუალებითაც სამართალდამცავ და უშიშროების ორგანოებს აქვთ კომუნიკაციებზე (სატელეფონო კომუნიკაციის შინაარსი, სატელეფონო და ინტერნეტკომუნიკაციებთან დაკავშირებული მეტადატა) პირდაპირი წვდომის შესაძლებლობა, სატელეფონო და ინტერნეტ სერვისების

[138] <https://privacyinternational.org/blog/1296/lawful-interception-russian-approach> [15.06.2020].

[139] Privacy International, Submission to the UN Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression: Study on Telecommunications and Internet Access Sector, 2016, 3 <https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/PrivacyInternational.pdf> [17.06.2020].

მიმწოდებელი კომპანიების ჩართულობის გარეშე.[140] ასეთი მოდელი ასევე მოქმედებს ცენტრალური აზიის ზოგიერთ ქვეყანაში.[141]

აღსანიშნავია, რომ ასეთი სისტემის პირობებში კავშირგაბმულობის ქსელი იმგვარად არის კონფიგურირებული, რომ გამოირიცხოს სატელეფონო და ინტერნეტსერვისების მიმწოდებელი კომპანიების ჩართულობა ღონისძიების აღსრულების პროცესში[142]. ამდენად, სერვისის მიმწოდებელი არ არის ინფორმირებული მომხმარებლის კომუნიკაციის „გადაჭერის“ ფაქტის შესახებ[143].

მსგავსი სისტემა არის აწყობილი საქართველოს შემთხვევაშიც, კერძოდ, მოქმედი კანონმდებლობის შესაბამისად, სააგენტოს, რომლის საქმიანობა რეგულირდება „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონით, გააჩნია კავშირგაბმულობის არხებთან პირდაპირი მიერთების ტექნიკური შესაძლებლობა, რისთვისაც შეუძლია გამოიყენოს ელექტრონული კომუნიკაციის კომპანიის ქსელური ან/და სასადგურე ინფრასტრუქტურა, კერძოდ, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის 8^1 მუხლის პირველი პუნქტის შესაბამისად, სააგენტოს უფლება აქვს, „ჰქონდეს ელექტრონული კომუნიკაციის კომპანიის ინფრასტრუქტურის მეშვეობით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების რეალურ დროში მოპოვების სტაციონარული ან ნახევრად სტაციონარული ტექნიკური შესაძლებლობა და ამ მიზნით:

ა) საჭიროების შემთხვევაში, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე უსასყიდლოდ განათავსოს/დაამონტაჟოს მართლზომიერი გადაჭერის მენეჯმენტის სისტემა ან/და მასთან დაკავშირებული/მისი ფუნქციონირებისთვის აუცილებელი აპარატურა და პროგრამული უზრუნველყოფის საშუალებები;

ბ) ელექტრონული კომუნიკაციის კომპანიას მოსთხოვოს, იქონიოს მისი ინფრასტრუქტურის მეშვეობით გადაცემული კომუნიკაციის შინაარსის და მისი

---

[140] <https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/> [17.06.2020].

[141] Privacy International, Submission to the UN Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression: Study on Telecommunications and Internet Access Sector, 2016, 3 <https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/PrivacyInternational.pdf> [17.06.2020].

[142] იქვე, 5.

[143] იქვე.

მაიდენტიფიცირებელი მონაცემების უფლებამოსილი ორგანოს მონიტორინგის სისტემისთვის რეალურ დროში მიწოდების სტაციონარული ტექნიკური შესაძლებლობა კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ტექნიკური შესაძლებლობით განსაზღვრული არქიტექტურისა და ინტერფეისების შესაბამისად.“[144]

საყურადღებოა, რომ უშიშროებისა და სამართალდამცავი ორგანოების მიერ კავშირგაბმულობის არხებთან პირდაპირი მიერთების ტექნიკური შესაძლებლობის პირადი ცხოვრების უფლებასთან შესაბამისობის თაობაზე ჩამოყალიბებულია ევროპული სასამართლოს სტანდარტები; ამასთან, ეს საკითხი საქართველოს საკონსტიტუციო სასამართლოს შეფასების საგანიც გახდა და შესაბამისი კონსტიტუციურ-სამართლებრივი ჩარჩოებიც შემუშავდა. აქედან გამომდინარე, აღნიშნული ასპექტების სიღრმისეულ გააზრებას კვლევაში მნიშვნელოვანი ყურადღება დაეთმობა.

3.2. ინტერნეტით გადაცემული კომუნიკაციის მოპოვების მეთოდები

3.2.1. ზოგადი მიმოხილვა

მართალია ინტერნეტკომუნიკაციის მოპოვებასთან დაკავშირებული ცალკეული დეტალები არ არის გასაჯაროებული, მაგრამ დღეს გაცილებით მეტი ინფორმაცია არის ხელმისაწვდომი სახელმწიფოების მიერ ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებული შესაძლებლობების შესახებ, ვიდრე ეს ახლო წარსულში იყო. საერთაშორისო დონეზე არსებულ სხვადასხვა წყაროებში განხილულია სამართალდამცავი ორგანოების მიერ კომუნიკაციის შინაარსისა და მისი მაიდენტიფიცირებელი მონაცემების მოპოვების მიზნით გამოყენებული ძირითადი შესაძლებლობები. მაგალითად, გაეროს სპეციალური მომხსენებლის 2013 წლის 17 აპრილის ანგარიშში გამოყოფილია კერძო კომუნიკაციის მოპოვების რამდენიმე ტექნიკური შესაძლებლობა[145]. აღნიშნული ანგარიშის მიხედვით, სახელმწიფოებს კერძო კომუნიკაციის მონიტორინგის სხვადასხვა ტექნიკურ საშუალებაზე

[144] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის 8^1 მუხლის პირველი პუნქტი, სსმ, 26, 02/06/2005.

[145] Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 10 (ბმული იხ. პირველ გვერდზე).

მიუწვდებათ ხელი, მაგალითად, კონკრეტულ ლოკაციასთან ან პიროვნებასთან მიმართებით ინტერნეტ კაბელზე სპეციალური მოწყობილობის დამაგრების გზით შესაძლებელია პიროვნების ონლაინ აქტივობების თვალთვალი, მათ შორის, ინფორმაციის მოპოვება იმასთან დაკავშირებით, თუ რომელ ვებგვერდებს სტუმრობს მომხმარებელი.[146] კონკრეტული ადრესატების მიმართ გამიზნული ფარული მეთვალყურეობის პარალელურად, ზოგიერთი სახელმწიფო ინტერნეტ და სატელეფონო კომუნიკაციის მასობრივი/ტოტალური მონიტორინგის ტექნიკურ შესაძლებლობებს ფლობს[147], ელექტრონული კომუნიკაციის გამტარ ოპტიკურ-ბოჭკოვან კაბელებზე სპეციალური მოწყობილობების დამონტაჟების საშუალებით, შესაძლებელია სატელეფონო და ონლაინ კომუნიკაციის თითქმის სრული კონტროლის მოპოვება.[148]

აღსანიშნავია ასევე, რომ სულ რაღაც რამდენიმე წლის წინ ე.წ. „სნოუდენის ამბებებმა“ (Snowden Revelations) გამოააშკარავა ზოგიერთი სახელმწიფოს მიერ სატელეფონო და ინტერნეტკომუნიკაციის მასობრივი მონიტორინგის პრაქტიკა. აშშ-ის ეროვნული უსაფრთხოების სააგენტოს (NSA) ყოფილი თანამშრომლის - ედვარდ სნოუდენის მიერ გამჟღავნებულმა სხვადასხვა დოკუმენტებმა სააშკარაოზე გამოიტანა პირადი ხასიათის ინფორმაციის მასობრივი მონიტორინგის პროგრამები, რომლებიც ხორციელდებოდა აშშ-ის ეროვნული უსაფრთხოების სააგენტოსა და დიდი ბრიტანეთის კომუნიკაციის სამთავრობო შტაბების (GCHQ) მიერ და რომლის ფარგლებშიც მსოფლიოს მასშტაბით მილიონობით ადამიანის კომუნიკაციის შინაარსი და მაიდენტიფიცირებელი მონაცემები კონტროლდებოდა[149]. მაგალითად, ინფორმაციამ გამოჟონა დიდი ბრიტანეთის კომუნიკაციის სამთავრობო შტაბების მიერ წყალქვეშა ოპტიკურ-ბოჭკოვანი სადენების მონიტორინგთან (Tapping) დაკავშირებით.[150] გარდა ამისა, როგორც გაირკვა, აშშ-ის ეროვნული უშიშროების

---

[146] იქვე, 10-11.
[147] იქვე, 11.
[148] იქვე.
[149] <https://privacyinternational.org/feature/827/how-bulk-interception-works> [17.06.2020].
[150] სნოუდენის მიერ გამჟღავნებული დოკუმენტები მიუთითებდა, რომ დიდი ბრიტანეთის ხელისუფლებამ შესაბამის კომერციულ კომპანიებთან თანამშრომლობით მოახდინა აღნიშნულ სადენებზე გადაცემული მონაცემების გადაჭერა იხ. <https://privacyinternational.org/feature/827/how-bulk-interception-works> [17.06.2020]. როგორც ცნობილია, ეს მონაცემები მოიცავდა სატელეფონო ზარებს, ელექტრონული ფოსტის შინაარსს, Facebook-ზე შეყვანილ მონაცემებს და მომხმარებლის მიერ

სააგენტო ასევე ახორციელებდა წყალქვეშა ოპტიკურ-ბოჭკოვანი სადენების მონიტორინგს.[151]

ამდენად, როგორც ვხედავთ, დღესდღეობით კერძო პირების შესახებ ინფორმაციის მოპოვების მძლავრი და მრავალფეროვანი შესაძლებლობები არსებობს; როგორც ირკვევა, ზოგიერთ სახელმწიფოს გააჩნია ტექნიკური რესურსიც და გამოცდილებაც მსგავსი მასშტაბური ხასიათის ფარული თვალთვალის მიმართულებით. ქვემოთ განხილული იქნება ინტერნეტით გადაცემული ინფორმაციის მოპოვების კონკრეტული შესაძლებლობები, რომლებიც საერთაშორისო პრაქტიკის გათვალისწინებით, ფართოდ გამოყენებადი და აპრობირებულია.

3.2.2. „კომპიუტერულ სისტემაში ფარული შეღწევა," როგორც ინფორმაციის მოპოვების მეთოდი სისხლის სამართლის პროცესში

საერთაშორისო დონეზე არსებულ დოკუმენტებსა თუ სამეცნიერო წრეებში მწვავე დისკუსიისა და განხილვის ქვეშ მოექცა სამართალდამცავი ორგანოების მიერ „კომპიუტერულ სისტემაში ფარული შეღწევის" მეთოდის (hacking) გამოყენებით ინფორმაციის მოპოვების პრაქტიკა[152]. როგორც ცნობილია, აღნიშნული ღონისძიება არაერთი ქვეყნის სამართალდამცავი ორგანოების მიერ გამოიყენება დანაშაულის გამოძიების მიზნებისათვის.[153]

თავის მხრივ, „კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიების განმარტება საკმაოდ რთულია, ვინაიდან ეს ტერმინი ღონისძიებათა ფართო სპექტრს

ვებგვერდებზე სტუმრობის ისტორიას; იხ. <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> [17.06.2020].

[151] <https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/> [17.06.2020].

[152] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 121-122.

[153] *Gutheil M., Liger Q., Heetman A., Eager J.* (Optimity Advisors), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs), Policy Department for Citizens' Rights and Constitutional Affairs, 2017, 42-43, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [17.06.2020]; *Petersen J.K.,* Handbook of Surveillance Technologies, 3rd edition, 2012, 982, 987; Landau S., Surveillance or Security? The Risks Posed by New Wiretapping Technologies, 2013, 133; *Winter L.B.,* Remote Computer Searches Under Spanish Law: The Proportionality Principle and The Protection of Privacy, ZStW, Vol.129, No 1, 2017, 211-212.

მოიცავს."[154] მაგალითად, ერთ-ერთი წამყვანი უფლებათა დამცველი ორგანიზაციის განმარტებით, ამ მეთოდით შესაძლებელია კომპიუტერულ სისტემაზე დისტანციურად წვდომა და პოტენციურად ხელმისაწვდომია სისტემაში შენახული ნებისმიერი მონაცემი.[155] ასევე შესაძლებელია კომუნიკაციის მონიტორინგი რეალურ დროში.[156] გერმანიის ფედერალური საკონსტიტუციო სასამართლო 2008 წლის 27 თებერვლის გადაწყვეტილებაში, რომელიც ეხებოდა სწორედ საინფორმაციო-ტექნოლოგიურ სისტემაში ფარულად შეღწევის ღონისძიების კონსტიტუციურობას, განმარტავს, რომ ინფორმაციულ სისტემაში ფარული შეღწევა არის ტექნიკური პროცესი, რომელიც იყენებს მაგალითად, სისტემის უსაფრთხოების სისუსტეებს ან ხორციელდება ვირუსული პროგრამის გამოყენებით, ამ მეთოდით შესაძლებელია სისტემის გამოყენების კონტროლი, შენახულ მონაცემებზე წვდომა ან სისტემაზე კონტროლის მოპოვება დისტანციურად.[157]

აღსანიშნავია, რომ კომპიუტერულ სისტემაში ფარული შეღწევის შესაძლებლობის გამოყენების პრაქტიკას მნიშვნელოვანი ყურადღება დაეთმო გაეროს სპეციალური მომხსენებლის ზემოთაღნიშნულ ანგარიშში. ანგარიშში ხაზგასმულია, რომ „ე.წ. ტროიანი (ჯაშუში პროგრამა)" წარმოადგენს სერიოზულ გამოწვევას ელექტრონულ კომუნიკაციებზე ფარული თვალთვალის ტრადიციული ფორმებისთვის, სცდება აქამდე არსებული სამართლებრივი რეგულირების ფარგლებს და ადამიანის უფლებების დაცვის თვალსაზრისით განსაკუთრებით შემზღუდველ ხასიათს ატარებს.[158] მაგალითისთვის, "ტროიანის" გამოყენების გზით არამარტო კომპიუტერულ სისტემაზე წვდომაა შესაძლებელი, არამედ მასში არსებული ინფორმაციის შეცვლაც (შემთხვევით ან გამიზნულად)[159].

---

[154] Encryption and Anonymity follow-up report, Special Rapporteur On The Promotion and Protection of The Right to Freedom of Opinion and Expression, 2018, 7, <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, [17.06.2020].

[155] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 8, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020].

[156] იქვე.

[157] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07.

[158] Report of the Special Rapporteur On the Promotion and Protection of the Right to Freedom of Opinion and Expression, 17.04.2013, 10 (ბმული იხ. პირველ გვერდზე).

[159] იქვე.

კომპიუტერულ სისტემაში ფარული შეღწევა შესაძლებელია სხვადასხვა გზებით განხორციელდეს[160]. აღნიშნული მეთოდი მოიცავს ღონისძიებების ფართო სპექტრს და ნებისმიერი კონკრეტული მიზნის მიღწევის უამრავი ტექნიკური საშუალება არსებობს.[161] ამ ღონისძიების ერთ-ერთი უფრო ცნობადი სახე - „ტროიანი“, მაგალითად, შეიძლება გამოყენებულ იქნეს მომხმარებლის საავტორიზაციო მონაცემების (ვებგვერდზე, ბლოგებზე, სოციალურ ქსელებში) მოსაპოვებლად, სხვადასხვა ტიპის „ვირუსის“ ინსტალაციისთვის, დავირუსებულ კომპიუტერულ სისტემაში განხორციელებული აქტივობების თვალთვალის მიზნებისათვის და ა.შ.[162] კომპიუტერულ სისტემაში ვირუსული პროგრამის (Malware), ძირითადად - „ტროიანის“, ინსტალაციის შემთხვევაში, პროგრამის მიხედვით ან იმის გათვალისწინებით თუ რა დავალებებს იღებს პროგრამა მაკონტროლებელი პირისგან, შესაძლოა დაინსტალირდეს keystrokes logger (პროგრამა, რომელიც იწერს კომპიუტერული მოწყობილობის კლავიატურაზე აკრეფილ ინფორმაციას), მოხდეს კომუნიკაციის რეალურ დროში მონიტორინგი, Skype-ის ან სხვა VoIP ტექნოლოგიაზე დაფუძნებული პროგრამის საშუალებით განხორციელებული კომუნიკაციის მოპოვება ან თუნდაც ვებ კამერის ან მიკროფონის აქტივაცია.[163]

როგორც უკვე აღინიშნა, ვირუსული პროგრამის ერთ-ერთ სახეს წარმოადგენს keystroke logging. keystroke logging (keylogger) წარმოადგენს პროგრამას, რომელიც ინსტალირდება შესაბამის კომპიუტერულ სისტემაში და შეუძლია ჩაიწეროს კომპიუტერული სისტემის კლავიატურაზე აკრეფილი ნებისმიერი ასო, სიმბოლო და რიცხვი. აღნიშნული პროგრამის საშუალებით შესაძლებელია მაგალითად, მესინჯერის აპლიკაციებში კომუნიკაციისას და ელექტრონული ფოსტის გაგზავნის დროს აკრეფილი ტექსტის ჩაწერა, ასევე პაროლებისა და კოდების მოპოვება[164].

---

[160] *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 88-89, < http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020].

[161] Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf> [17.06.2020].

[162] *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 88-89, < http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020].

[163] *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 90, < http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020].

[164] <https://www.webopedia.com/TERM/K/keylogger.html> [17.06.2020].

სამეცნიერო ლიტერატურაში keystroke logging პირად ცხოვრებაში ჩარევის საკმაოდ ინტენსიურ მეთოდად განიხილება.[165] პირის მიერ კომპიუტერის კლავიატურაზე აკრეფილი ტექსტების წაკითხვის გზით სახელმწიფო ორგანოს შეიძლება მიეცეს შესაძლებლობა, გააკონტროლოს ინდივიდის ფიქრები/ნააზრევი[166]. ამ მეთოდით შესაბამის პირს შეუძლია გაეცნოს ინდივიდის ჯერ კიდევ ჩამოუყალიბებელ აზრებსა და იდეებს, რომელთა გამჟღავნებას, კომპიუტერში შენახვას ან სამომავლოდ რაიმე ფორმით შენარჩუნებას პირი შესაძლოა არც აპირებდეს[167], ასევე გაეცნოს ინდივიდის ისეთ ფიქრებს, რომლის უარყოფასაც ის მისი აკრეფვის მომენტშივე ახდენს.[168]

3.2.3. ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელთან შენახულ ინფორმაციაზე წვდომა

დღესდღეობით ინტერნეტსივრცეში სულ უფრო იზრდება კომუნიკაციის დაშიფვრის გამოყენების პრაქტიკა. დაშიფვრა სტანდარტული და აუცილებელი საშუალებაც კი გახდა, რომელიც უზრუნველყოფს ერთის მხრივ, მონაცემთა უსაფრთხოებას, მეორეს მხრივ, კი კერძო პირებს შორის კომუნიკაციის დაცვას გარეშე პირთა ხელმისაწვდომობისგან. ინტერნეტსივრცეში დაშიფვრის ფართო მასშტაბებით გავრცელება არსებით ზეგავლენას ახდენს სახელმწიფოს მიერ ინფორმაციის მოპოვების შესაძლებლობებზე.[169] იქედან გამომდინარე, რომ ძირითადი აპლიკაციების და სოციალური ქსელების მეშვეობით წარმოებული კომუნიკაცია ინტერნეტსივრცეში დაშიფრული სახით გადაიცემა, ადგილობრივი ოპერატორები (ინტერნეტ სერვისის მიმწოდებლები) მოკლებული არიან აღნიშნული ინფორმაციის წაკითხვის შესაძლებლობას.[170] შესაბამისად, ამ ინფორმაციაზე წვდომის აპრობირებულ მეთოდს წარმოადგენს მისი გამოთხოვა უშუალოდ ვებსერვისების ან აპლიკაციების მწარმოებელი კომპანიებისგან (Facebook, Instagram და სხვ.). ამასთან, დაშიფვრის

[165] *Solove D.J., Schwartz P.*, Information Privacy Law, 5th Edition, New York, 2015, 396, იხ. ციტირება: *Raymond K.,* Think Twice Before You Type, 163 N.J. L.J. 747 (Feb. 19, 2001).
[166] იქვე.
[167] იქვე.
[168] იქვე.
[169] *Swire. P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 203.
[170] იქვე. 202.

სხვადასხვა სახეები არსებობს, ზოგიერთი სერვისის მიმწოდებელი, როგორიცაა მაგალითად, Google ან Dropbox, ახორციელებს მონაცემების შენახვას დაშიფრული სახით და განშიფვრის ტექნიკურ შესაძლებლობას თვითონ ფლობს[171]. ასეთი ინფორმაციის მოპოვება შესაძლებელია აღნიშნული სერვისის მიმწოდებლის მეშვეობით.[172] სხვა ტიპის დაშიფვრის შემთხვევაში (End-to-end დაშიფვრა) კომუნიკაციის განშიფვრის ტექნიკური შესაძლებლობა (დაშიფვრის „გასაღები“) გააჩნიათ მხოლოდ კომუნიკაციის მხარეებს თავიანთ კომპიუტერებში ან სმარტფონებში და შესაბამისად, კომუნიკაციის შინაარსი სერვისის მიმწოდებლისთვისაც არ არის ხელმისაწვდომი.[173] აღსანიშნავია, რომ End-to-end მეთოდით დაშიფრული კომუნიკაციის მოპოვება სამართალდამცავი ორგანოებისათვის საკმაოდ პრობლემურია, იმ მარტივი მიზეზით, რომ კომუნიკაციის შინაარსი სერვისის მიმწოდებლისთვისაც არ არის ხელმისაწვდომი, რადგან კომუნიკაციის განშიფვრის ტექნიკური შესაძლებლობა არ გააჩნია[174]. შესაბამისად, დაშიფვრის აღნიშნული ტიპი მნიშვნელოვან მექანიზმს წარმოადგენს კერძო კომუნიკაციის დაცვის თვალსაზრისით.

აღსანიშნავია, რომ როგორც წესი, დაშიფვრა იცავს მხოლოდ კომუნიკაციის შინაარსს და არა მის მაიდენტიფიცირებელ მონაცემებს, როგორიცაა მაგალითად, ინტერნეტპროტოკოლის მისამართი (IP მისამართი).[175] ასევე დაუშიფრავი სახით შეიძლება იყოს ხელმისაწვდომი ინფორმაცია იმის შესახებ, თუ რა ვებგვერდებს ეწვია მომხმარებელი.[176]

საკომუნიკაციო ტექნოლოგიების ინფრასტრუქტურა და სერვისები დღესდღეობით, ძირითადად, კერძო კომპანიების ხელთაა, შესაბამისად, ისინი

---

[171] *Corn G.S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 334.

[172] იქვე.

[173] იქვე, 335.

[174] *Swire. P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202.

[175] Report of the Special Rapporteur On The Promotion and Protection of The Right to Freedom of Opinion and Expression, 22.05.2015, 4 (ბმული იხ. პირველ გვერდზე).

[176] Encryption and Anonymity follow-up report, Special Rapporteur On The Promotion and Protection of The Right to Freedom of Opinion and Expression, 2018, 18 (ბმული იხ. 51-ე გვერდზე).

უზარმაზარ ინფორმაციულ რესურსს ფლობენ[177]. ამასთან, ვინაიდან ელექტრონული ინფორმაციის გადინება არ არის შეზღუდული სახელმწიფოს ეროვნული საზღვრებით, მონაცემები შეიძლება ინახებოდეს ტრანსნაციონალურ დონეზე და არა იმ ქვეყანაში, სადაც მოხდა მისი შეგროვება ან სადაც იმყოფება მონაცემთა სუბიექტი[178]. სერვის მიმწოდებელთან შენახული ინფორმაციის გამოთხოვა შესაძლოა განხორციელდეს სერვისის მიმწოდებლისადმი პირდაპირი მიმართვის გზით ან იმ სახელმწიფოს სამართალდამცავ ორგანოებთან საერთაშორისო თანამშრომლობის მეშვეობით, რომლის იურისდიქციაშიც იმყოფება შესაბამისი სერვისის მიმწოდებელი.[179] ტრანსნაციონალური მოთხოვნები მონაცემთა „ნებაყოფლობით“ გადაცემის მიზნით საერთაშორისო დონეზე სტანდარტული პროცედურაა[180]. ამ გზით სახელმწიფოს შეუძლია თავი დააღწიოს საერთაშორისო თანამშრომლობის ფორმალიზებულ პროცესს.[181] თუმცა ინფორმაციის გამოთხოვა პირდაპირ სერვისის მიმწოდებლისგან შესაძლოა მრავალ პრაქტიკულ სირთულესთან იყოს დაკავშირებული, როდესაც სერვისის მიმწოდებელი იმყოფება უცხო სახელმწიფოს იურისდიქციის ქვეშ. აღსანიშნავია, რომ კერძო კომპანიებსა და სხვა ქვეყნის სამართალდამცავ ორგანოებს შორის თანამშრომლობა საერთაშორისო დონეზე ერთ-ერთ აქტუალურ თემას წარმოადგენს. ეს საკითხი, განსაკუთრებით მწვავედ დგას ევროპული ქვეყნების შემთხვევაში, ვინაიდან ძირითადი საკომუნიკაციო კომპანიები აშშ-ში არიან დაფუძნებული. მოთხოვნის გამგზავნი სახელმწიფო ბუნებრივია არ ფლობს სამართლებრივ ბერკეტს, აიძულოს უცხო იურისდიქციაში დაფუძნებული კომპანია, მასთან ითანამშრომლოს და მიაწოდოს სასურველი ინფორმაცია[182]. შესაბამისად, ეს თანამშრომლობა, პრაქტიკაში, როგორც წესი, ნებაყოფლობით საწყისებზე ხორციელდება.[183]

ამრიგად, სერვისის მიმწოდებლებისგან ინფორმაციის მოპოვება, როდესაც ის ფლობს კომუნიკაციაზე წვდომის ტექნიკურ შესაძლებლობას, პრაქტიკული

[177] *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 126.
[178] იქვე.
[179] იქვე.
[180] იქვე. 130.
[181] იქვე.
[182] იქვე. 130-131.
[183] იქვე.

თვალსაზრისით ძალიან ეფექტიან და ამავე დროს ფართოდ აპრობირებულ მეთოდს წარმოადგენს, თუმცა ეს საშუალებაც შესაძლოა დაკავშირებული იყოს ზემოთაღნიშნულ პრაქტიკულ სირთულეებთან ან უცხო სახელმწიფოს სამართალდამცავ ორგანოებთან საერთაშორისო თანამშრომლობის შედარებით გახანგრძლივებულმა და ფორმალურმა პროცედურამ გარკვეული დისკომფორტი შეუქმნას მომთხოვნი სახელმწიფოს კომპეტენტურ უწყებებს.

როგორც ვხედავთ, გამოძიების მიზნებისათვის ინტერნეტკომუნიკაციის მოპოვების სხვადასხვა გზები არსებობს. სისხლის სამართლის პროცესში ინტერნეტით განხორციელებული კომუნიკაციის მოპოვების ძირითადი სამართლებრივი შესაძლებლობების უკეთ გააზრების მიზნით, ინფორმაციის რეალურ დროში მოპოვების შესაძლებლობების პარალელურად, წინამდებარე ქვეთავში განხილულ იქნა ვებსერვისებისა და აპლიკაციების მწარმოებელი კომპანიებისგან მათთან შენახული ინფორმაციის გამოთხოვის საკითხებიც.

4. შეჯამება

ამდენად, ელექტრონულ საკომუნიკაციო ქსელში გადაცემულ გამოძიებისათვის საინტერესო ინფორმაციას წარმოადგენს როგორც შინაარსობრივი მონაცემები, ასევე მეტადატა. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები აერთიანებს კომუნიკაციის ტრაფიკის შესახებ ინფორმაციას, ადგილმდებარეობის შესახებ მონაცემებს, კომუნიკაციის წყაროს მაიდენტიფიცირებელ მონაცემებს; შესაბამისად, მეტადატა მიეკუთვნება ინფორმაციას იმასთან დაკავშირებით, თუ ვინ, როდის, რა ხანგრძლივობით, რა სიხშირით დაუკავშირდა ერთმანეთს, ასევე კომუნიკაციის ტიპის, ადგილის და გამოყენებული მოწყობილობის შესახებ. არაერთი ქვეყნის ეროვნული სამართლით და მათ შორის, ქართული კანონმდებლობით, არის გათვალისწინებული ელექტრონული კომუნიკაციის კომპანიების მიერ მეტადატას სავალდებულო შენახვასთან დაკავშირებული რეგულაციები.

აღსანიშნავია, რომ სამართალდამცავ ორგანოებს სატელეფონო და ინტერნეტკომუნიკაციაზე წვდომის სხვადასხვა შესაძლებლობებზე მიუწვდებათ ხელი, რომელთა შორის უნდა გამოიყოს ადგილმდებარეობის შესახებ მონაცემების გამოთხოვა სერვისის მიმწოდებელი კომპანიებისგან, სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა, ინტერნეტკომუნიკაციის მოპოვება კომპიუტერულ

სისტემაში ფარული შეღწევის გზით, ინტერნეტ სერვისის მიმწოდებელთან არსებული მონაცემების გამოთხოვა. ინფორმაციაზე წვდომის სამართლებრივი შესაძლებლობები განსახვავებული შეიძლება იყოს იმისდა მიხედვით, თუ რა ფორმით არსებობს ინფორმაცია, მაგ. თანამედროვე ინტერნეტსივრცეში მონაცემები ხშირ შემთხვევაში დაშიფრული სახით გადაიცემა; ამიტომ აღნიშნულ ინფორმაციაზე რეალურ დროში წვდომის მიზნებისათვის ერთ-ერთ ყველაზე ეფექტიან მეთოდს კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება წარმოადგენს; ამასთან, სერვისის მიმწოდებელთან შენახულ ინფორმაციაზე წვდომა შესაძლოა განხორციელდეს მონაცემების ამ კომპანიისგან გამოთხოვის საშუალებით. თითოეული ეს უფლებამოსილება სსსკ-ის ფარგლებში სხვადასხვა სამართლებრივი საშუალებებით (ნორმებით) რეგულირდება, თუმცა კვლევის ფარგლებში ინტერესის ობიექტს წარმოადგენს კომუნიკაციის რეალურ დროში მოპოვების შესაძლებლობების სამართლებრივი რეგლამენტაცია და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა, მათ შორის, ადგილმდებარეობის შესახებ ინფორმაციის შენახვის/ხელმისაწვდომობის საკითხები.

IV. საქართველოს კონსტიტუციით დადგენილი სტანდარტები ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების ღონისძიებებთან მიმართებით

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩატარება ადამიანის ფუნდამენტური უფლებების სერიოზულ შეზღუდვას წარმოადგენს, კერძოდ, ასეთ შემთხვევაში ადგილი აქვს საქართველოს კონსტიტუციით განმტკიცებულ პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის (მუხლი 15) და პიროვნების თავისუფალი განვითარების უფლებებით (მუხლი 12) დაცულ სფეროებში ჩარევას.

1. პიროვნების თავისუფალი განვითარების უფლება

საქართველოს კონსტიტუციის მე-12 მუხლით უზრუნველყოფილი პიროვნების თავისუფალი განვითარების უფლება ადამიანის ხელშეუვალი უფლებაა, რომლის ძალითაც თითოეულ პიროვნებას საშუალება ეძლევა მონაწილეობა მიიღოს, თავისი წვლილი შეიტანოს და ისარგებლოს ეკონომიკური, სოციალური, კულტურული და პოლიტიკური განვითარებით, რომელშიც ადამიანის უფლებების და ძირითადი თავისუფლებების რეალიზაცია შეიძლება განხორციელდეს[184]. პიროვნების თავისუფალი განვითარების უფლება უნდა გავიგოთ როგორც ადამიანის ღირსების უფლების კონკრეტიზაცია, რადგან ადამიანის ღირსების დაცვის პრინციპი პიროვნების თავისუფალი განვითარების უფლების აღიარებას მოითხოვს.[185]

აღსანიშნავია, რომ პიროვნების თავისუფალი განვითარების უფლება კონსტიტუციით განმტკიცებული ყველაზე ზოგადი ხასიათის ძირითადი უფლებაა[186]. იგი აერთიანებს ადამიანის არაერთ უფლებასა და თავისუფლებას, რომლებიც პიროვნების თავისუფალი განვითარების რეალიზაციის საშუალებებად შეიძლება წარმოვიდგინოთ, მაგალითად: პირადი და ოჯახური ცხოვრება, გამოხატვის, ინფორმაციის მიღების, გაერთიანებების შექმნისა და მასში მონაწილეობის უფლება, ინტელექტუალური შემოქმედების, საკუთარი შეხედულებით პროფესიის არჩევისა

---

[184] *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, 2013, 90, იხ. ციტირება: Declaration 41/128 of 4 December 1986 on the Right to Development, UN General Assembly.

[185] *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი, ზოგადი ნაწილის მიმოხილვა, თბ., 2014, 274.

[186] *დემეტრაშვილი/კობახიძე,* კონსტიტუციური სამართალი, თბ., 2014, 85.

თუ საქმიანობის თავისუფლებების უფლება და სხვა, რომელთა განხორციელების გარეშე შეუძლებელია პიროვნების თავისუფალი განვითარების რეალიზაცია.[187] ამდენად, საქართველოს კონსტიტუციის მე-12 მუხლი მოიცავს ყველა იმ უფლებას თუ ინტერესს, რომელიც განაპირობებს პიროვნების თავისუფალი განვითარების შესაძლებლობას.[188]

პიროვნების თავისუფალი განვითარების უფლება, დაცვის სფეროების მიხედვით, ორ ძირითად უფლებას აერთიანებს. ესენია: ზოგადი პიროვნული უფლება (რომელიც ადამიანის პირადი და ინტიმური ცხოვრების სფეროს მოიცავს) და საქმიანობის საყოველთაო თავისუფლება (რომელიც პიროვნების არსებობისა და საქმიანობის ყველა დანარჩენ სფეროზე ვრცელდება).[189] თავის მხრივ, ზოგადი პიროვნული უფლება შინაარსობრივად მეტად მოცულობითია და რამდენიმე კონკრეტული უფლების საფუძველს წარმოადგენს.[190] ფაქტობრივად, ზოგადი პიროვნული უფლების ცნება მოიცავს მთელ რიგ უფლებებს, რომლებიც აკონკრეტებენ პიროვნების თავისუფალი განვითარების უფლებას ადამიანის ცხოვრებისა და საქმიანობის სხვადასხვა სფეროების მიხედვით.[191] ზოგადი პიროვნული უფლება მოიცავს თვითგამორკვევის უფლებას, პირადი ცხოვრების უფლებას, თვითგამოსახვის უფლებას და ფიზიკურ ხელშეუხებლობას.[192] კვლევის შინაარსიდან გამომდინარე, ამ უფლებათა შორის, საინტერესოა, უფრო დეტალურად იქნეს განხილული პირადი ცხოვრების უფლება.

1.1. პირადი ცხოვრების უფლება და „სფეროთა თეორია"

პირადი ცხოვრების უფლებიდან გამომდინარე, ყოველ ადამიანს აქვს უფლება, თავად განსაზღვროს პირადი ცხოვრების გარესამყაროსთან ურთიერთობის

---

[187] *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 89.

[188] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-16.

[189] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ.,2008, 96-97, *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 91.

[190] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 105.

[191] იქვე.

[192] *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 92.

ფარგლები, მოსწყდეს საზოგადოებას და დარჩეს საკუთარ თავთან მარტო.[193] როგორც საქართველოს საკონსტიტუციო სასამართლომ განმარტა, „უფლება პრივატულ სფეროზე, პირად სივრცეზე, მოიცავს ადამიანის თავისუფლების შემდეგ გამოხატულებებს: განმარტოების უფლებას (უფლებას, დარჩეს მარტო), უფლებას, თავად განსაზღვროს გარესამყაროსთან, საზოგადოებასთან ურთიერთობის ფორმა, დრო, ინტენსივობა, გააკეთოს არჩევანი ნებისმიერ საკითხზე, რომელიც ეხება პირადად მას, ნებისმიერი შინაარსისა და სახის ურთიერთობებს მისთვის სასურველ პირებთან სხვებისაგან დამოუკიდებლად, მათი ინფორმირების გარეშე და მათგან თავისუფალ პირობებში.“[194] აღსანიშნავია, რომ პირადი ცხოვრების უფლება საკონსტიტუციო სასამართლომ სწორედ პიროვნების თავისუფალ განვითარებასთან და ადამიანის ღირსებასთან მჭიდრო კონტექსტში განმარტა.[195]

საქართველოს საკონსტიტუციო სასამართლოს განმარტებით, კონსტიტუციის მე-16 მუხლი [ძველი რედაქციით][196] მოიცავს პირადი ცხოვრების, ადამიანის პირადი სივრცის ხელშეუხებლობის ყველა ასპექტს[197]. ის, ერთი მხრივ, წარმოადგენს საფუძველს და ზოგად ნორმას კონსტიტუციის მე-20 მუხლით [ძველი რედაქციით][198] დაცული სფეროსთვის, ხოლო, მეორე მხრივ, დამატებით გარანტიას პირადი ცხოვრების ყველა იმ კომპონენტისთვის, რომელიც სპეციალურად არ არის რეგულირებული კონსტიტუციის კონკრეტული მუხლით[199]. საკონსტიტუციო სასამართლოს განმარტებით, პირადი ცხოვრების ხელშეუხებლობის კონსტიტუციური დაცვის ფარგლების გააზრების კონტექსტში, საქართველოს კონსტიტუციის მე-20 მუხლი [ძველი რედაქციით] შეიძლება ჩაითვალოს მე-16 მუხლით [ძველი

---

[193] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 112.

[194] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-10.

[195] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-18.

[196] საუბარია საქართველოს კონსტიტუციის ძველი რედაქციით მე-16 მუხლით უზრუნველყოფილ პიროვნების თავისუფალი განვითარების უფლებაზე, რომელიც დღეს კონსტიტუციის მე-12 მუხლით არის განმტკიცებული.

[197] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-21.

[198] საუბარია საქართველოს კონსტიტუციის ძველი რედაქციით მე-20 მუხლით უზრუნველყოფილ პირადი ცხოვრების ხელშეუხებლობის უფლებაზე, რომელსაც დღეს იცავს კონსტიტუციის მე-15 მუხლი.

[199] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-21.

რედაქციით] დაცული სფეროსთვის სპეციალურ ნორმად იმ გაგებით, რომ ის არეგულირებს პიროვნების განვითარების ერთ-ერთ უმნიშვნელოვანეს სფეროს.[200]

როგორც საქართველოს საკონსტიტუციო სასამართლო აღნიშნავს, "ზოგადად, პირადი ცხოვრება გულისხმობს ინდივიდის ცხოვრებისა და განვითარების კერძო სფეროს. უფლება პირად ცხოვრებაზე კი, ერთი მხრივ, ნიშნავს ინდივიდის შესაძლებლობას, პირადად, საკუთარი შეხედულებისამებრ, დამოუკიდებლად შექმნას და განავითაროს თავისი კერძო ცხოვრება, ხოლო, მეორე მხრივ, იყოს დაცული და უზრუნველყოფილი მის კერძო სფეროში სახელმწიფოს, ისევე როგორც ნებისმიერი სხვა პირების ჩარევისგან..."[201]

პირადი ცხოვრების სფერო - ეს არის ურთიერთდამოკიდებულება ოჯახში, - ურთიერთობა და კავშირები სხვა ადამიანებთან; პირადი დღიურების, წერილების, ჩანაწერების შინაარსი; ცხოვრების წესი და ადამიანის არსებობის ყველა სხვა გარემოება, რომელსაც თვითონ არ თვლის საჭიროდ ან შესაძლებლად გაახმაუროს; ასევე გარემოებები, რომლებიც კონფიდენციალური ხასიათისაა.[202]

აღსანიშნავია, რომ პირადი ცხოვრების უფლებასთან დაკავშირებით განვითარდა ე.წ. „სფეროთა თეორია", რომლის თანახმად, პიროვნების პირადი ცხოვრება იყოფა სამ სფეროდ: 1) ინტიმური სფერო; 2) კერძო სფერო; 3) სოციალური და საჯარო სფეროები).[203] ზოგადი პიროვნული უფლებიდან გამომდინარე, პირადი ცხოვრების უფლება ე.წ. „სფეროთა თეორიის" საფუძველზე იცავს ყოველ ადამიანს პირად ცხოვრებაში არასასურველი ჩარევებისაგან.[204] განსხვავებულია პირადი ცხოვრების დაცვის სტანდარტი იმისდა მიხედვით, თუ რომელ სფეროში ჩარევას აქვს ადგილი.[205]

1.1.1. ინტიმური სფერო

პირადი ცხოვრების ინტიმური სფერო არის ადამიანის პიროვნულობის არსებითი და ცენტრალური ნაწილი და სარგებლობს აბსოლუტური დაცვით.[206] ეს

---

[200] იქვე.

[201] საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-4.

[202] *აქუბარდია ი.,* წიგნში: სისხლის სამართლის პროცესი (ზოგადი ნაწილის ცალკეული ინსტიტუტები), *(რედ.),* თბ., 2009, 143.

[203] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 113.

[204] იქვე. 112.

[205] *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 95.

[206] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 113.

სფერო წარმოადგენს ზოგადი პიროვნული უფლების არსს და მისი განკარგვა შეუძლია მხოლოდ ინდივიდს.[207] მასში იგულისხმება სექსუალური ცხოვრება, ადამიანის ფარული ფიზიკური ან სხვაგვარი ნაკლი, ჩვევა, ან რაიმე თავისებურება, პირადი დღიური ან სხვაგვარი ჩანაწერები, ფოტოსურათები, აღსარების დროს განდობილი ფაქტები თუ განწყობილებები, ადვოკატისათვის მიცემული ინფორმაცია და განმარტებები, ნოტარიუსისათვის გამჟღავნებული ნება-სურვილი, სამედიცინო გამოკვლევის შედეგები და სხვ.[208] ამ სფეროს მიკუთვნებული ინფორმაციის საჯაროდ გავრცელება მხოლოდ პიროვნების ნება-სურვილის ან თანხმობის საფუძველზეა დასაშვები.[209]

ნიშანდობლივია, რომ ინტიმური სფეროს განსაკუთრებული დაცვის აუცილებლობაზე ყურადღებას ამახვილებს ასევე საქართველოს საკონსტიტუციო სასამართლო, კერძოდ, სასამართლოს შეხედულებით, „პირადი ცხოვრების ძირითადი სფერო - ადამიანის ინტიმური, სექსუალური ურთიერთობები, ოჯახური ცხოვრება, მისი ჩვევები, მოძღვრისთვის აღსარებისას მინდობილი ინფორმაცია, სამედიცინო გამოკვლევების შედეგები, ადამიანის ემოციები და გრძნობები, მათი პრივატულ სფეროში გამოხატვის ფორმები უნდა იყოს განსაკუთრებულად დაცული სახელმწიფოსა და ნებისმიერი მესამე პირის ზედამხედველობისგან“[210].

1.1.2. კერძო სფერო

კერძო სფერო მოიცავს ინტიმური სფეროს ფარგლებს გარეთ ადამიანის პირად ცხოვრებას, განსაკუთრებით, შიდა ოჯახურ ცხოვრებას. ინტიმური სფეროსგან განსხვავებით, კერძო სფერო არ არის აბსოლუტურად დაცული, თუმცა მასში ჩარევა დაიშვება მკაცრი წინაპირობების დაცვისას და თანაზომიერების პრინციპის შესაბამისად.[211] ამ სფეროს მიეკუთვნება პირის ოჯახური ცხოვრება, ოჯახის წევრებთან და უახლოეს ნათესავებთან დაკავშირებული ურთიერთობები, საცხოვრებელი ადგილი, კავშირები უცხოეთთან, შემოსავლებისა და ქონების საკითხები,

---

[207] იქვე.

[208] *გოცირიძე. ე.,* მუხლი 16 - პიროვნების თავისუფალი განვითარების უფლება, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 95.

[209] იქვე.

[210] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-12.

[211] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 114.

ჯანმრთელობის მდგომარეობა, რელიგიას თუ სხვა მსოფლმხედველურ ჯგუფებთან ურთიერთობის საკითხები და სხვა.[212]

1.1.3. სოციალური და საჯარო სფეროები

სოციალური და საჯარო სფეროები არის ადამიანის ცხოვრებისა და საქმიანობის ისეთი სფეროები, რომლებშიც მოქმედება მიმდინარეობს ინტიმურ და კერძო სფეროთა ფარგლებს გარეთ, ნაწილობრივ შეზღუდული ან შეუზღუდავი საჯაროობის პირობებში.[213] ამ სფეროებში ადამიანები არ არიან აბსოლუტურად დაუცველნი, მაგრამ ასეთ შემთხვევაში უპირატესობა ენიჭება საზოგადოების ლეგიტიმურ ინტერესს პირის ზოგად პიროვნულ უფლებასთან შედარებით.[214] განსაკუთრებით ეს ეხება საჯარო სფეროს, სადაც, როგორც წესი, არ არსებობს რაიმე შეზღუდვა ინფორმაციის გავრცელებასთან დაკავშირებით.[215] შედარებით უფრო მაღალი დაცვის ხარისხით სარგებლობს სოციალური სფერო - ინდივიდის სოციალური და არა უშუალოდ საჯარო სფეროს მიკუთვნებული პროფესიული გარემო.[216] ასეთ შემთხვევაში პირს გააჩნია თმენის ვალდებულება მასთან დაკავშირებით გავრცელებული ინფორმაციის მიმართ, თუკი არსებობს საზოგადოების განსაკუთრებული და ლეგიტიმური ინტერესი, სხვა შემთხვევაში საკითხი უნდა გადაწყდეს დაპირისპირებულ ინტერესთა აწონ-დაწონვის საფუძველზე.[217]

2. პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებები

2.1. პირადი ცხოვრების უფლების დაცვის კონსტიტუციურ - სამართლებრივი სტანდარტები

პირადი ცხოვრების უფლებას საქართველოს კონსტიტუციაში ეძღვნება მე-15 მუხლი, რომელიც განამტკიცებს პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებებს. აღნიშნული მუხლის თანახმად:

[212] იქვე.
[213] იქვე. 115-116.
[214] იქვე. 116.
[215] იქვე.
[216] იქვე.
[217] იქვე. 116-117.

„1. ადამიანის პირადი და ოჯახური ცხოვრება ხელშეუხებელია. ამ უფლების შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით.

2. ადამიანის პირადი სივრცე და კომუნიკაცია ხელშეუხებელია. არავის აქვს უფლება შევიდეს საცხოვრებელ ან სხვა მფლობელობაში მფლობელი პირის ნების საწინააღმდეგოდ, აგრეთვე ჩაატაროს ჩხრეკა. ამ უფლებათა შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით, სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას. გადაუდებელი აუცილებლობისას უფლების შეზღუდვის შესახებ არაუგვიანეს 24 საათისა უნდა ეცნობოს სასამართლოს, რომელიც შეზღუდვის კანონიერებას ადასტურებს მიმართვიდან არაუგვიანეს 24 საათისა.“*[218]*

მოცემული მუხლით აღიარებული უფლებების კონსტიტუციურ-სამართლებრივი განმტკიცება საქართველოში პირველად 1921 წლის კონსტიტუციით განხორციელდა. პირველი რესპუბლიკის კონსტიტუცია განამტკიცებდა ამ უფლებებს შემდეგი შინაარსით: „ყოველი მოქალაქის ბინა შეუვალია: მხოლოდ სასამართლოს დადგენილებით შეიძლება მისი გაჩხრეკა კანონით გათვალისწინებულ შემთხვევაში. კერძო მიწერ-მოწერა ხელშეუხებელია. მისი ამოხმა და გადასინჯვა შეიძლება მხოლოდ სასამართლოს დადგენილებით” (28-ე და 29-ე მუხლები).[219] პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებები დაცული იყო ასევე საბჭოთა საქართველოს 1937 და 1978 წლის კონსტიტუციებით.[220] ამასთან, 1995 წლის საკონსტიტუციო რეფორმის საფუძველზე, საქართველოს მოქმედი კონსტიტუციით განმტკიცებულ იქნა პირადი ცხოვრებისა და პირადი ჩანაწერის ხელშეუხებლობის, წერილობითი, ტექნიკური საშუალებებით და ვერბალური ფორმით დამყარებული კომუნიკაციის თავისუფლებისა და საცხოვრებელი და სხვა მფლობელობის

[218] საქართველოს კონსტიტუციის მე-15 მუხლი, საქართველოს პარლამენტის უწყებები, 31-33, 24/08/1995.
[219] *კობახიძე ი.,* მუხლი 20 - პირადი ცხოვრების და პირადი კომუნიკაციის ხელშეუვალობა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 178.
[220] იქვე.

ხელშეუხებლობის უფლებები, როგორც ადამიანის საყოველთაოდ აღიარებული ძირითადი უფლებები და თავისუფლებები და უშუალოდ მოქმედი სამართალი[221].

პირადი ცხოვრების უფლებით დაცული სფერო უფრო დეტალურად განხილულ იქნა პიროვნების თავისუფალი განვითარების უფლებაზე საუბრისას, ამიტომ ქვემოთ წარმოდგენილი იქნება ამ უფლების მხოლოდ მოკლე მიმოხილვა და ძირითადი ყურადღება გამახვილდება მისი უფლებრივი კომპონენტის - კომუნიკაციის ხელშეუხებლობის უფლებაზე, ისევე როგორც - მე-15 მუხლით დაცულ სფეროში ჩარევის სამართლებრივ საფუძვლებსა და მისი შეზღუდვის კონსტიტუციურ-სამართლებრივ სტანდარტებზე.

როგორც უკვე აღინიშნა, ადამიანის პირადი ცხოვრების ძირითადი უფლება პიროვნების თავისუფალი განვითარების უფლების შინაარსობრივი კომპონენტია, რომელიც მოიცავს ინდივიდის ცხოვრების ინტიმურ, კერძო და სოციალურ სფეროებს.[222] მე-15 მუხლი არის სპეციალური ნორმა (lex specialis) მე-12 მუხლის მიმართ[223]. შესაბამისად, პირადი ცხოვრების უფლების ნებისმიერი შეზღუდვა უნდა შეფასდეს მე-15 მუხლის მოთხოვნების შესაბამისად[224]. მე-15 მუხლით აღიარებული სხვა უფლებები კი განიხილება სპეციალურ უფლებებად პირადი ცხოვრების ძირითადი უფლების მიმართ.[225]

მე-15 მუხლით აღიარებული ძირითადი უფლებები დაცულია როგორც ნეგატიური (status negativus), ისე პოზიტიური (status positivus) თვალსაზრისით.[226] „ერთი მხრივ, არსებობს სახელმწიფოს პოზიტიური ვალდებულება, უზრუნველყოს პირადი ცხოვრების პატივისცემა და ამ უფლებით ეფექტიანი სარგებლობა, რაც, პირველ რიგში, გულისხმობს პიროვნების თავისუფალი განვითარების ხელშემშლელი გარემოებების, შეზღუდვების უგულებელყოფას, აღკვეთას. მეორე მხრივ, სახელმწიფოს აქვს ნეგატიური ვალდებულება, არ ჩაერიოს ამ უფლებით[227]

---

[221] იქვე.

[222] *კობახიძე ი.,* მუხლი 20 - პირადი ცხოვრების და პირადი კომუნიკაციის ხელშეუვალობა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, 2013, 180.

[223] იქვე.

[224] იქვე.

[225] *იქვე;* წიგნში მოხსენიებულია კონსტიტუციის ძველი რედაქციის მე-16 და მე-20 მუხლები.

[226] იქვე.

[227] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-12. მოცემულ გადაწყვეტილებაში ნახსენებია საქართველოს კონსტიტუციის ძველი რედაქციის მე-20 მუხლი.

სარგებლობაში და, შესაბამისად, უზრუნველყოს პიროვნების დაცვა, მის პირად ცხოვრებაში სახელმწიფო ხელისუფლების ორგანოების ან თანამდებობის პირების მხრიდან თვითნებური ჩარევისაგან."[228]

პირადი ცხოვრების უფლების ფარგლების განსაზღვრისას გამოიყენება „გონივრული მოლოდინის ტესტი"[229] - პირს არ გააჩნია მიზეზი იფიქროს, რომ თვალყურს ადევნებენ[230]. მაგალითად, პირი შეიძლება ლეგიტიმურად ვარაუდობდეს, რომ მისი სამსახურებრივი სატელეფონო ხაზი არ ისმინება, თუ ამის შესახებ მას არ მიუღია ფორმალური გაფრთხილება[231]. ხელშეუხებლობის დარღვევას ადგილი არ აქვს, თუ პირის მოლოდინი მის პირად ცხოვრებას მიკუთვნებული ინფორმაციის დაცულობის შესახებ სუბიექტური და არაგონივრულია.[232]

2.2. კომუნიკაციის ხელშეუხებლობის უფლება

კომუნიკაციის ხელშეუხებლობის უფლებით დაცულია ადამიანების როგორც ზეპირი, ისე წერილობითი (მაგალითად, sms-ის შეტყობინებანი) ურთიერთობა ტელეფონის, ფაქსის, ინტერნეტის, ელექტრონული ფოსტის, პეიჯერებისა და ნებისმიერი სხვა ტექნიკური საშუალების გამოყენებით.[233]

აღსანიშნავია, რომ საქართველოს კონსტიტუციის ძველი რედაქციის (2018 წლის 23 მარტის ცვლილებებამდე) მიხედვით, პირადი ცხოვრების უფლება უზრუნველყოფილი იყო მე-20 მუხლით, რომელიც იცავდა „სატელეფონო და სხვა სახით ტექნიკური საშუალებებით საუბარს", ისევე როგორც „სხვა ტექნიკური საშუალებებით მიღებულ შეტყობინებებს". საქართველოს კონსტიტუციის მე-20 მუხლით (კონსტიტუციის ძველი რედაქცია) დაცულ სფეროზე საუბრისას საქართველოს საკონსტიტუციო სასამართლომ „სატელეფონო და სხვა სახის ტექნიკური საშუალებებით საუბარი" განმარტა, როგორც „ადამიანების (ორი ან მეტი

---

[228] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-4.

[229] პირადი ცხოვრების უფლების დაცვის „გონივრული მოლოდინის" დოქტრინა აშშ-ში სამოსამართლო სამართალში დამკვიდრებულ იქნა საქმეზე Katz v. United States, (1967), 389 U.S. 347.

[230] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 63.

[231] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 63, იხ. ციტირება: Halford v UK, [1997], ECtHR, Reports of Judgments and Decisions 1997-III, 42; Kopp v Switzerland, [1998], ECtHR, Reports 1998-II.

[232] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 63.

[233] *კუბლაშვილი კ.,* ძირითადი უფლებები, თბ., 2008, 158.

პირის) კომუნიკაცია ტელეფონის ან ვერბალური კომუნიკაციისთვის განკუთვნილი ინტერნეტპროგრამების გამოყენებით.“[234] ხოლო „ტექნიკური საშუალებებით მიღებული შეტყობინებების“ ხელშეუხებლობის უფლებით დაცულ სფეროს მიაკუთვნა „კომუნიკაცია ტელეფონის, ფაქსის, ელექტრონული ფოსტის, შესაბამისი ინტერნეტპროგრამების და სხვა ტექნიკური საშუალებების გამოყენებით.“[235]

კონსტიტუციის მოქმედი რედაქციის მე-15 მუხლი, უკვე აღარ ახდენს კომუნიკაციის დიფერენცირებას „სატელეფონო“ ან „სხვა ტექნიკური საშუალებების“ მიხედვით და იყენებს ერთიან ცნებას - „კომუნიკაციას“, რომელიც აერთიანებს ყველა სახის კომუნიკაციას, ნებისმიერი ტიპის ტექნიკური საშუალებების გამოყენებით. ამასთან, კონსტიტუციით დაცულია როგორც სადენიანი, ისე უსადენო ელექტრონული საკომუნიკაციო სისტემებით დამყარებული კომუნიკაცია.[236]

„კონსტიტუციის მიზანი არის, დაიცვას პირებს შორის ნებისმიერი საშუალებით საუბრისა და მიმოწერის შესაძლებლობა. ამ უფლების უზრუნველყოფის ფარგლებში სახელმწიფოს ზოგადად ეკრძალება, გაეცნოს სატელეფონო და სხვა სახის ტექნიკური საშუალებით წარმოებული საუბრებისა და შეტყობინებების შინაარსს, აგრეთვე დააწესოს კონტროლი, ვისთან და რა ინტენსივობით შედგა ასეთი ურთიერთობები.“[237] საკონსტიტუციო სასამართლოს განმარტებით, „დემოკრატიული საზოგადოების არსებობა და განვითარება წარმოუდგენელია, შეუძლებელია ინფორმაციის თავისუფლების, აზრთა გაცვლისა და ადამიანების ნებისმიერ სფეროში თავისუფალი კომუნიკაციის გარანტირებული შესაძლებლობის გარეშე. ... ადამიანებს აქვთ უფლება, მათთვის სასურველი ან საჭირო ინფორმაცია მიაწოდონ მხოლოდ კონკრეტულ პირს (პირებს), ანუ აქვთ უფლება, აირჩიონ თემები, ინტერესები და პირთა წრე, ვისთანაც ამ თემებზე კომუნიკაცია სურთ...“[238].

კონსტიტუციით დაცულია არამარტო კომუნიკაციის შინაარსი, არამედ მისი მაიდენტიფიცირებელი მონაცემებიც - კომუნიკაციის ხელშეუხებლობის უფლება ასევე მოიაზრებს „ადამიანების იმ არჩევანის ანონიმურობასაც, კონკრეტულად

[234] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, II-23.
[235] იქვე.
[236] იქვე.
[237] საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-6.
[238] საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 24 ოქტომბრის N1/2/519 გადაწყვეტილება, II-6.

ვისთან, როდის, რა საშუალებით, სად და რა ხანგრძლივობით ექნებათ კომუნიკაცია“[239] (კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დეტალური განმარტება იხ. ზემოთ).

ამასთან, დაცვის სფეროში ხვდება მხოლოდ კონფიდენციალურად დამყარებული ურთიერთობა და არა იმგვარი კომუნიკაცია, რომელიც საყოველთაოდ ხელმისაწვდომი წყაროების საშუალებით მყარდება და პირთა განუსაზღვრელი წრისკენ არის მიმართული (მაგალითად, კომუნიკაცია რადიოს და ტელევიზიის საშუალებით).[240] ამდენად, პიროვნულ უფლებაში ჩარევას არ ექნება ადგილი, როდესაც სახელმწიფო ხელისუფლების ორგანო ინტერნეტში არსებულ კომუნიკაციის შინაარსს მოიპოვებს ყველასთვის ხელმისაწვდომი წყაროების მეშვეობით. მაგალითად, გამოიძახებს ყველასთვის ხელმისაწვდომ ვებ-გვერდს, ხდება ყველასათვის ხელმისაწვდომი ელექტრონული მეილის გამომწერი, ან აკონტროლებს „ღია ჩატს“ (open chat room).[241] მიუხედავად აღნიშნულისა, გერმანიის საკონსტიტუციო სასამართლოს შეხედულებით, პირადი ცხოვრების უფლებაში ჩარევის საკითხი შეიძლება წამოიჭრას ისეთ შემთხვევაში, როდესაც სახელმწიფო ორგანოების მიერ ხდება საზოგადოდ ღია წყაროებიდან მოპოვებული ინფორმაციის შეგნებულად შეკრება, შეგროვება, სხვა მონაცემებთან ურთიერთკავშირში შეფასება და ამ ქმედებებით საფრთხე ექმნება პირის ზოგად პიროვნულ უფლებას[242]. სასამართლოს განმარტებით, ასეთ ქმედებებს სჭირდება შესაბამისი საფუძველი.[243]

კომუნიკაციის ხელშეუხებლობის უფლებით დაცული არიან როგორც ფიზიკური, ისე იურიდიული პირები.[244] აღნიშნული უფლება იცავს ბრალდებულებსა და მსჯავრდებულებსაც პატიმრობისა და თავისუფლების აღკვეთის აღმასრულებელი დაწესებულებების თავისებურებების გათვალისწინებით[245]. დაცული არიან საჯარო მოსამსახურეებიც (მაგალითად, ძირითადი უფლების შეზღუდვად განიხილება

[239] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, II-25.

[240] *კობახიძე ი.,* მუხლი 20 - პირადი ცხოვრების და პირადი კომუნიკაციის ხელშეუვალობა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 185.

[241] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07, 308.

[242] იქვე. 309.

[243] იქვე.

[244] *კობახიძე ი.,* მუხლი 20 - პირადი ცხოვრების და პირადი კომუნიკაციის ხელშეუვალობა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 185.

[245] იქვე.

სატელეფონო ზარების აღრიცხვა და გადამოწმება სამსახურებრივი ტელეფონით არასათანადო სარგებლობის თავიდან ასაცილებლად).[246]

გარდა აღნიშნულისა, საუბრისა და შეტყობინებების ხელშეუხებლობის უფლებებით დაცულია კომუნიკაციის ორივე მხარე მათ ერთობლიობაში[247]. შესაბამისად, ჩარევა დაცვის სფეროში არ ხორციელდება იმ შემთხვევაში, როდესაც ერთ-ერთი პარტნიორი აძლევს საჯარო ხელისუფლებას საუბრის ფარული მიყურადების ან კომუნიკაციის შინაარსის გაცნობის უფლებას.[248] გასათვალისწინებელია, რომ ჩარევის გამართლების შეფასებისას, განსაზღვრული მნიშვნელობა ენიჭება კომუნიკაციის პარტნიორთა ვინაობას (მაგალითად, ადვოკატთან, მოძღვართან კომუნიკაცია).[249] ამდენად, პირადი ცხოვრების უფლება არ იცავს პირს კომუნიკაციის მეორე მხარის მიერ ინფორმაციის გასაჯაროებისგან, მაგალითად, თუ მოსაუბრე აღმოჩნდება ინფორმატორი/კონფიდენტი ან პროცესის მწარმოებელ ორგანოს მიაწვდის ინფორმაციას შემდგარი კომუნიკაციის ფაქტის ან/და შინაარსის შესახებ.[250] კომუნიკაციის დროს მხარეები თავად კისრულობენ კომუნიკაციის ფაქტთან დაკავშირებული ინფორმაციის არადანიშნულებისამებრ/მოტყუებით გამოყენების რისკს.[251]

2.3. ჩარევის საფუძვლები პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებებში

როგორც უკვე აღინიშნა, საქართველოს კონსტიტუციის მე-15 მუხლით დაცული პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებები არ მიეკუთვნება აბსოლუტურად დაცულ სფეროს. პირადი ცხოვრების ხელშეუხებლობის უფლება შეიძლება შეიზღუდოს დემოკრატიულ სახელმწიფოში აუცილებელი, კონსტიტუციით გათვალისწინებული ლეგიტიმური მიზნების მისაღწევად, ამასთან

[246] იქვე.
[247] იქვე. 186.
[248] იქვე.
[249] იქვე.
[250] *ფაფიაშვილი ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 64.
[251] იქვე.

იმ პირობის სავალდებულო დაცვით, რომ უფლებაში ჩარევა ლეგიტიმური მიზნების მიღწევისთვის აუცილებელი და პროპორციული გზით მოხდება.[252]

მე-15 მუხლი ადგენს ამ უფლებაში ჩარევის საფუძვლებს, კერძოდ, „კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით, სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას. გადაუდებელი აუცილებლობისას უფლების შეზღუდვის შესახებ არაუგვიანეს 24 საათისა უნდა ეცნობოს სასამართლოს, რომელიც შეზღუდვის კანონიერებას ადასტურებს მიმართვიდან არაუგვიანეს 24 საათისა“.

როგორც უკვე აღინიშნა, სსსკ-ის 143[1] მუხლის პირველი ნაწილით გათვალისწინებული სატელეფონო საუბრის ფარული მიყურადების და კავშირგაბმულობის არხიდან/კომპიუტერული სისტემიდან ინფორმაციის მოხსნისა და ფიქსაციის ფარული საგამოძიებო მოქმედებები პირადი ცხოვრების ხელშეუხებლობის უფლებაში განსაკუთრებით მნიშვნელოვან ჩარევას წარმოადგენს.

„ზოგადად, ადამიანებზე ფარული დაკვირვება პოლიციური სახელმწიფოსთვისაა დამახასიათებელი. იმავდროულად, ქვეყნის კონსტიტუციური წყობის, სახელმწიფო და ეროვნული უსაფრთხოების, საზოგადოებრივი წესრიგის დაცვა, დანაშაულის თავიდან აცილება, რაც საბოლოო ჯამში, ემსახურება ადამიანთა უფლებების ეფექტურ დაცვას, დემოკრატიული და სამართლებრივი სახელმწიფოს ვალდებულებაა. ზუსტად ამ საჯარო ინტერესების უზრუნველყოფას ემსახურება დასახელებული უფლების შეზღუდვა.“[253]

საკონსტიტუციო სასამართლოს შეხედულებით, „ნებისმიერი დემოკრატიული სახელმწიფოს ვალდებულებაა, მიიღოს ყველა შესაძლო ზომა, რათა აღიკვეთოს სერიოზული საფრთხეები, რომლებმაც შეიძლება დემოკრატიული ინსტიტუტების დესტაბილიზაცია გამოიწვიონ. ამიტომ ამ საფრთხეებთან ბრძოლისთვის, სახელმწიფოს უნდა ჰქონდეს, მათ შორის იმის შესაძლებლობაც, რომ განახორციელოს

[252] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება, II - 29.

[253] საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-8.

ფარული კონტროლი, თვალთვალი პირებზე (პირთა ჯგუფზე) რომელთაგანაც ეს საფრთხეები მომდინარეობს. ასეთ დროს, ზუსტად უფლებაში ჩარევის ფარული ხასიათი უზრუნველყოფს საჯარო ინტერესის დაცვის ეფექტურობას.“[254]

იმავდროულად, სახელმწიფოს არ აქვს უფლება, სერიოზულ საფრთხესთან ბრძოლის მოტივით მიიღოს ნებისმიერი ზომები, რომლებსაც ის შესაბამისად და ადეკვატურად მიიჩნევს[255]. უფლებაში ჩარევა, მისი ფარული ხასიათიდან გამომდინარე, აჩენს უფლებამოსილების გადამეტების, ბოროტად გამოყენების რისკს, რასაც შესაძლოა საზიანო შედეგები მოჰყვეს მთლიანად დემოკრატიული საზოგადოებისთვის[256]. შესაბამისად, კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევა შეიძლება იყოს გამართლებული მხოლოდ მაშინ, თუ კანონმდებლობა უზრუნველყოფილი იქნება ძალაუფლების ბოროტად გამოყენებისაგან დაცვის ეფექტური მექანიზმებით.[257]

კონსტიტუციის მე-15 მუხლი განსაზღვრავს მასში მოცემული უფლების როგორც მატერიალურ შინაარსს, ისე უფლების შეზღუდვის ფორმალურ გარანტიებს.[258] უფლებაში ჩარევის მატერიალურ წინაპირობად გათვალისწინებულია სასამართლოს გადაწყვეტილება. მოსამართლის განჩინების სავალდებულო პირობა ემსახურება უფლებაში ჩარევის კონკრეტული ღონისძიების „წინასწარი კონტროლის უზრუნველყოფას დამოუკიდებელი და ნეიტრალური ინსტანციის მიერ.“[259] აღნიშნული, პირველ რიგში, მიზნად ისახავს სახელმწიფოს ხელისუფლების მხრიდან უფლებამოსილების თავიდან აცილებას.[260] „იმავდროულად, თავისთავად სასამართლო გადაწყვეტილების არსებობა აპრიორი უფლებაში თანაზომიერ ჩარევას არ გულისხმობს. იმისათვის, რომ უზრუნველყოფილი იყოს სასამართლო

[254] იქვე, II-9.
[255] იქვე.
[256] იქვე.
[257] იქვე.
[258] საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 24 ოქტომბრის N1/2/519 გადაწყვეტილება, II-12. საკონსტიტუციო სასამართლოს გადაწყვეტილებაში საუბარია კონსტიტუციის ძველი რედაქციის მე-20 მუხლზე.
[259] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-24.
[260] იქვე.

გადაწყვეტილების საფუძველზე უფლების პროპორციული შეზღუდვა, გადამწყვეტი მნიშვნელობა აქვს შესაბამისი საკანონმდებლო გარანტიების შექმნას.“[261]

რაც შეეხება უფლების შეზღუდვის ალტერნატიულ საფუძველს - გადაუდებელ აუცილებლობას, საკონსტიტუციო სასამართლოს განმარტებით, „გადაუდებელი აუცილებლობა“ გულისხმობს ისეთ შემთხვევებს, როდესაც თანაზომიერების პრინციპზე დაყრდნობით, კონსტიტუციით გათვალისწინებული საჯარო ინტერესის მიღწევა, რეალურად არსებული ობიექტური მიზეზების გამო, შეუძლებელია კერძო ინტერესების დაუყოვნებლივი, მყისიერი შეზღუდვის გარეშე. ამასთან, ძალზე მკაფიო, ნათელი და ცალსახა უნდა იყოს, რომ კონსტიტუციის ფარგლებში საჯარო ინტერესის სხვაგვარად დაცვის მცირედი ალბათობაც არ არსებობს. გადაუდებლობა მიუთითებს დროის სიმცირეზე, რაც უფლების შესაზღუდად მოსამართლის ბრძანების მოპოვების საშუალებას არ იძლევა და საჭიროებს დაუყოვნებლივ მოქმედებას.“[262]

აღსანიშნავია, რომ 2017 წლის 10 ოქტომბრის ცვლილებებით საქართველოს კონსტიტუციის გადასინჯვის შედეგად, კონსტიტუციის ახალი რედაქციის მე-15 მუხლი, წინა რედაქციის მე-20 მუხლისგან განსხვავებით, უკვე კონსტიტუციურ დონეზე არეგულირებს გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული კომუნიკაციის ხელშეუხებლობის უფლების შემზღუდველი ღონისძიებების შემდგომი სასამართლო კონტროლის მოთხოვნას, ვადას (არაუგვიანეს 24 საათი) და სასამართლოს მიერ გადაწყვეტილების მიღების მაქსიმალურ ხანგრძლივობას (არაუგვიანეს 24 საათი).

კონსტიტუციის მე-15 მუხლით უზრუნველყოფილ უფლებებში ჩარევის შეფასების კონსტიტუციურობის საზომს თანაზომიერების და განსაზღვრულობის პრინციპები წარმოადგენენ.

მართალია თანაზომიერების პრინციპი, კონსტიტუციაში სახელდებით მოხსენებული არ არის, მაგრამ „ადამიანის უფლებათა შეზღუდვის მართლზომიერების შეფასების კონსტიტუციურ კრიტერიუმს წარმოადგენს, სწორედ ამიტომ კონსტიტუციური კონტროლისთვის არსებითი მნიშვნელობა აქვს.“[263] „თანა-

[261] იქვე.
[262] იქვე, II-26.
[263] საქართველოს საკონსტიტუციო სასამართლოს 2006 წლის 15 დეკემბრის N1/3/393,397 გადაწყვეტილება, I.

ზომიერების პრინციპი სამართლებრივი სახელმწიფოს იდეიდან მომდინარეობს და მისი ძირითადი დატვირთვა არის ადამიანის უფლებების შეზღუდვისას სახელმწიფოსთვის ფარგლების განსაზღვრა“[264]. „ის უზრუნველყოფს თავისუფლებისა და მისი შეზღუდვის ერთგვარ გაწონასწორებულ, თანაზომიერ დამოკიდებულებას და კრძალავს ადამიანის უფლებების იმაზე მეტად შეზღუდვას, რაც აუცილებელია დემოკრატიულ საზოგადოებაში.“[265] თანაზომიერების პრინციპი მოითხოვს, რომ უფლების შემზღუდველი საკანონმდებლო რეგულირება წარმოადგენდეს „ღირებული, ლეგიტიმური მიზნის მიღწევის გამოსადეგ და აუცილებელ საშუალებას,“[266] ამავდროულად უფლების შეზღუდვის ინტენსივობა მისაღწევი მიზნის პროპორციული, თანაზომიერი საშუალება უნდა იყოს[267]. „დაუშვებელია ლეგიტიმური მიზნის მიღწევა განხორციელდეს ადამიანის უფლების მომეტებული შეზღუდვის ხარჯზე.“[268]

როგორც საკონსტიტუციო სასამართლო აღნიშნავს, პირადი ცხოვრების უფლების შეზღუდვა უნდა იძლეოდეს დასახული ლეგიტიმური მიზნის მიღწევის რეალურ შანსებს[269]. ამასთან, ჩარევა პირად ცხოვრებაში უნდა იყოს აბსოლუტურად აუცილებელი, როდესაც სხვა ნაკლებმზღუდველი ღონისძიებების გამოყენება უშედეგოა ან უკავშირდება განსაკუთრებულ ძალისხმევას.[270]

თანაზომიერების პრინციპის ანალოგიურად, საქართველოს კონსტიტუცია არც „განჭვრეტადობის პრინციპზე“ აკეთებს პირდაპირ დათქმას, თუმცა „კანონის ხარისხის მოთხოვნა“ სამართლებრივი სახელმწიფოს ქმედითობის უზრუნველყოფის არსებითი გარანტიაა, ამიტომაც თავისთავად გამომდინარეობს სამართლებრივი სახელმწიფოს იდეიდან და ამდენად, მყარი კონსტიტუციური საფუძველი აქვს.[271] განსაზღვრულობის პრინციპის თანახმად, საჯარო ხელისუფლების აქტის შინაარსი

---

[264] იქვე.
[265] იქვე.
[266] *ფირცხალაშვილი ა.,* მუხლი 21 - საკუთრების უფლება; მემკვიდრეობის უფლება; საკუთრების ჩამორთმევა, წიგნში: საქართველოს კონსტიტუციის კომენტარი, თბ., 2013, 217.
[267] იქვე.
[268] იქვე.
[269] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-32.
[270] იქვე.
[271] *ერემაძე ქ.* წიგნში: საქართველოს საკონსტიტუციო სამართალი, თბ., 2017, 44-45.

მკაფიოდ და ნათლად განსაზღვრული, ჩარევის შედეგი კი - იოლად განჭვრეტადი უნდა იყოს.[272]

საქართველოს საკონსტიტუციო სასამართლოს განმარტებით, „კანონად“ შეიძლება ჩაითვალოს საკანონმდებლო საქმიანობის მხოლოდ ის პროდუქტი, რომელიც პასუხობს კანონის ხარისხის მოთხოვნებს“[273]. „ეს უკანასკნელი კი გულისხმობს კანონის შესაბამისობას სამართლის უზენაესობისა და სამართლებრივი უსაფრთხოების პრინციპებთან“[274]. „ამ პრინციპების რეალური დაცვისთვის პრაქტიკული და გადამწყვეტი მნიშვნელობა აქვს კანონის ხელმისაწვდომობასა და განჭვრეტადობას. კანონის ხარისხი მოითხოვს, რომ საკანონმდებლო რეგულაცია იყოს იმდენად მკაფიო, რომ პირმა, რომლის უფლებაში ჩარევაც ხდება, შეძლოს სამართლებრივი მდგომარეობის ადეკვატურად შეცნობა და საკუთარი ქმედების შესაბამისად წარმართვა.“[275] გასათვალისწინებელია, რომ კომუნიკაციის ხელშეუხებლობის უფლების შემზღუდველი ფარული საგამოძიებო მოქმედებების მომწესრიგებელი ნორმების მიმართ ხელმისაწვდომობასა და განჭვრეტადობასთან დაკავშირებით მოთხოვნები, ზოგადად, გაცილებით მკაცრია, ვიდრე ჩვეულებრივ ამა თუ იმ ნორმის კონსტიტუციურობის შეფასებისას, რაც განპირობებულია სხვადასხვა ფაქტორებით, მაგ., უფლებაში ჩარევის ფარული ხასიათით, პირის მიერ შესაძლებლობის არ ქონით, მონაწილეობა მიიღოს მის მიმართ კონკრეტული ღონისძიების ჩატარების საკითხის გადაწყვეტაში, „მესამე პირების“ ინტერესების ადეკვატური დაცვის სირთულით[276]. საქართველოს საკონსტიტუციო სასამართლო აღნიშნავს, რომ „დაცული სფეროს განსაკუთრებულობა და უფლებაში ჩარევის ფორმა განაპირობებს კანონისადმი დამატებით მოთხოვნებსაც: ... მოცემულ შემთხვევაში კანონის სიზუსტე, განჭვრეტადობა და ხელმისაწვდომობა მოიცავს იმ აუცილებელ პირობასაც, რომ უფლების შეზღუდვაზე უფლებამოსილი პირების დასაშვები მოქმედების ფარგლები იყოს კონკრეტული, გასაგები, მკაფიო ... “[277].

---

[272] *დემეტრაშვილი/კობახიძე,* კონსტიტუციური სამართალი, თბ., 2014, 93.

[273] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-11.

[274] იქვე.

[275] იქვე.

[276] *ტუღუში თ., ბურჯანაძე გ., მშვენიერაძე გ., გოცირიძე გ., მენაბდე ვ.,* ადამიანის უფლებები და საქართველოს საკონსტიტუციო სასამართლოს სამართალწარმოების პრაქტიკა, თბ., 2013, 203.

[277] საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის N1/3/407 გადაწყვეტილება, II-14.

საქართველოს კონსტიტუცია ადგენს პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევის ლეგიტიმურ მიზნებს. მე-15 მუხლის მიხედვით, ამ უფლებათა შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით.

აღსანიშნავია, რომ კონსტიტუციის დღეს არსებული რედაქცია, წინა რედაქციისგან განსხვავებით, პირადი ცხოვრების უფლებისა და კომუნიკაციის ხელშეუხებლობის უფლებებში ჩარევის საფუძვლებთან მიმართებით განსხვავებულ სამართლებრივ რეჟიმებს აწესებს, კერძოდ, პირადი ცხოვრების უფლების შეზღუდვა, მე-15 მუხლის პირველი პუნქტის შესაბამისად, დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით. ხოლო კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევისათვის, გარდა ზემოთ აღნიშნული ლეგიტიმური მიზნებისა, სავალდებულოა ასევე სასამართლოს გადაწყვეტილების ან კანონით გათვალისწინებული გადაუდებელი აუცილებლობის არსებობა[278].

3. შეჯამება

საბოლოო ჯამში, შეიძლება ითქვას, რომ საქართველოს კონსტიტუცია ადგენს კომუნიკაციის ხელშეუხებლობის უფლების შემზღუდველი ფარული საგამოძიებო მოქმედებების კონსტიტუციურ-სამართლებრივ ჩარჩოებს და უფლებაში ჩარევის ფორმალურ/მატერიალურ წინაპირობებს. თავის მხრივ, კანონმდებლის ვალდებულებაა, ააწყოს დაბალანსებული სისტემა საჯარო და კერძო ინტერესების სამართლიანი, გონივრული ჰარმონიზაციის მიზნით. სწორედ კანონმდებლობამ უნდა უზრუნველყოს სათანადო, ადეკვატური გარანტიები უფლების ბოროტად გამოყენების წინააღმდეგ, აუცილებელი პირობები აღნიშნულ ღონისძიებათა რეგულირების დროს თანაზომიერებისა და განსაზღვრულობის პრინციპების უზრუნველსაყოფად.

[278] აღნიშნულ საკითხთან დაკავშირებით იხ. ასევე *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 290.

ამდენად, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედებების, ისევე როგორც კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის/კოპირების და სსსკ-ის 136-ე მუხლის საფუძველზე გამოთხოვის საკითხის მარეგულირებელი კანონმდებლობის განხილვისას უნდა შეფასდეს, რამდენად უზრუნველყოფს აღნიშნული სამართლებრივი დებულებები ადამიანის უფლებების დაცვის საკმარის მექანიზმებს, რამდენად პასუხობს ამ სფეროში დადგენილ კონსტიტუციურ-სამართლებრივ სტანდარტებს.

V. საერთაშორისო სტანდარტები ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების სფეროში

1. „პირადი ცხოვრებისა“ და „მიმოწერის“ ცნებები ევროპული სასამართლოს პრაქტიკის მიხედვით

ევროპული სასამართლოს პრაქტიკის მიხედვით, პირადი ცხოვრება ფართო ცნებაა და არ ექვემდებარება ამომწურავ განმარტებას[279]. საქმეში ნიმიტცი გერმანიის წინააღმდეგ (Niemietz v. Germany), სასამართლომ განაცხადა, რომ „არ თვლის შესაძლებლად ან აუცილებლად, ამომწურავად განსაზღვროს პირადი ცხოვრების კონცეფცია. თუმცა ძალზე შეზღუდული იქნებოდა ამ კონცეფციის შემოფარგვლა „შიდა წრით“, რომელშიც ინდივიდი შეიძლება მის მიერ არჩეული პირადი ცხოვრებით ცხოვრობდეს და მისგან გამორიცხავდეს გარესამყაროს, რომელიც არ შედის ამ წრეში. პირადი ცხოვრების პატივისცემა ასევე უნდა მოიცავდეს, გარკვეულ ფარგლებში, სხვა ადამიანებთან ურთიერთობის დამყარებისა და განვითარების უფლებას.“[280] სასამართლოს განმარტებით, კონვენციის მე-8 მუხლი განამტკიცებს „პირადი ცხოვრების უფლებას ფართო გაგებით“, რაც ასევე მოიცავს „პირადი სოციალური ცხოვრების“ უფლებასაც, რაც წარმოადგენს ინდივიდის შესაძლებლობას, განავითაროს თავისი „სოციალური იდენტობა“. ამ კონტექსტში მოცემული უფლება განამტკიცებს პირის შესაძლებლობას, სხვა პირებთან დაამყაროს და განავითაროს ურთიერთობები.[281]

ევროპული სასამართლოს პრეცედენტული სამართალი ცხადყოფს, რომ სამსახურებრივი დაწესებულებებიდან, ისევე როგორც საცხოვრებელი ადგილიდან კომუნიკაცია ექცევა „პირადი ცხოვრებისა“ და „მიმოწერის“ უფლების ქვეშ კონვენციის მე-8 მუხლის მიზნებისათვის.[282] იმის დასადგენად, თუ რამდენად ექვემდებარება „პირადი ცხოვრებისა“ და „მიმოწერის“ ცნებები გამოყენებას, ევროპულმა სასამართლომ რამდენიმე შემთხვევაში განიხილა, თუ რამდენად გააჩნდათ

---

[279] Costello-Roberts v. the United Kingdom, [1993], ECtHR, (Series A) 36.

[280] *კორკელია კ.,* პირადი ცხოვრების, მიმოწერისა და საცხოვრებლის ხელშეუხებლობის უფლებები საქართველოს კონსტიტუციის მიხედვით, ქართული სამართლის მიმოხილვა 7/2004-1, 80, იხ. ციტირება: Niemietz v. Germany, [1992], ECtHR, (Series A).

[281] Bigaeva v. Greece, [2009], ECtHR, 22; Özpınar v. Turkey, [2010], ECtHR, 45.

[282] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08.2019, 32, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [18.06.2020].

ინდივიდებს თავიანთი „პირადი ცხოვრების დაცვის გონივრული მოლოდინი.“[283] ამ კონტექსტში სასამართლომ აღნიშნა, რომ „პირადი ცხოვრების დაცვის გონივრული მოლოდინი“ მნიშვნელოვან, თუმცა არა „აუცილებლად გადამწყვეტ“ ფაქტორს წარმოადგენს.[284]

ევროპული სასამართლოს პრაქტიკის თანახმად, ტერმინი „მიმოწერა“ მოიცავს მათ შორის, სატელეფონო საუბარს ოჯახის წევრებთან ან სხვა პირებთან, სატელეფონო საუბრებს კერძო ან სამსახურებრივი შენობებიდან, სასჯელაღსრულების დაწესებულებიდან, ასევე ამ სატელეფონო საუბრებთან დაკავშირებული ინფორმაციის (თარიღი, ხანგრძლივობა, აკრეფილი სატელეფონო ნომრები) მოპოვებას.[285] ასევე კონვენციის მე-8 მუხლით დაცულ სფეროში ექცევა ელექტრონული ფოსტა[286], ინტერნეტის გამოყენება[287], კომპიუტერულ სერვერებზე შენახული მონაცემები, მათ შორის, მყარ დისკებზე[288]. მე-8 მუხლით დაცულია ასევე ელექტრონული კომუნიკაციის შედარებით მოძველებული ფორმებით მიმოწერა, როგორიცაა, ტელეგრაფი, პეიჯერები.[289]

ამდენად, ვინაიდან XXI საუკუნეში კომუნიკაციის მეთოდები ბევრად უფრო სრულყოფილი გახდა და სწრაფად ვითარდება, ევროპულმა სასამართლომ მიზანშეწონილად მიიჩნია, მიმოწერის/კომუნიკაციის კონცეფცია ისე განემარტა, რომ ამ უკანასკნელმა ფეხი აუწყოს ტექნოლოგიების განვითარებას, რომლებმაც საფუძველი ჩაუყარა კომუნიკაციის ახალ მეთოდებს, როგორებიცაა: ელექტრონული ფოსტა, სოციალური ქსელები და ა.შ. ამასთანავე, უფლებაში ჩარევისაგან

[283] იქვე.
[284] *Stalla-Bourdillon S., Phillips J., Ryan M.D.*, Privacy vs. Security, Springer, 2014, 24, იხ. ციტირება: Köpke v Germany, [2010], ECtHR.
[285] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08. 2019, 85, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [18.06.2020].
[286] Copland v. the United Kingdom, [2007], ECtHR 2007-I, 41;
[287] Bărbulescu v. Romania, [2017], ECtHR, 72, 74. Copland v. the United Kingdom, [2007], ECtHR 2007-I, 41-42.
[288] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08. 2019, 89 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [18.06.2020].
[289] იქვე.

სამართლებრივი დაცვის ხარისხი შეიძლება განსხვავდებოდეს გამოყენებული კომუნიკაციის ტიპის მიხედვით.[290]

2. ძირითადი პრინციპები ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების ღონისძიებებთან მიმართებით

პირადი ცხოვრების დაცვის მიზნით აუცილებელია მოცემული სფეროს მარეგულირებელი კანონმდებლობა უზრუნველყოფდეს უფლების დაცვის სათანადო გარანტიებს. საერთაშორისო დონეზე შემუშავებულია ის ფუნდამენტური პრინციპები, რომლებსაც უნდა აკმაყოფილებდეს ფარული მეთვალყურეობის ღონისძიებების მარეგულირებელი ნორმები, კერძოდ, აღნიშნული ღონისძიება გათვალისწინებული უნდა იყოს ეროვნულ კანონმდებლობაში, პასუხობდეს კანონის ხარისხის მოთხოვნებს, უნდა იყოს აუცილებელი დემოკრატიულ საზოგადოებაში კონკრეტული ლეგიტიმური მიზნის მისაღწევად და წარმოადგენდეს აღნიშნული მიზნის მისაღწევ ყველაზე ნაკლებად ინტენსიურ საშუალებას.[291] ევროპული სასამართლოს პრაქტიკის მიხედვით, პირადი ცხოვრების უფლების ეფექტიანი დაცვა საჭიროებს ადეკვატურ სამართლებრივ ჩარჩოს და უფლებაში ჩარევას უკავშირებს კანონიერებისა და „დემოკრატიულ საზოგადოებაში აუცილებლობის“ მკაცრ ტესტებს.[292]

2.1. კანონიერების პრინციპი

კანონიერების პრინციპი ადამიანის უფლებების დაცვის საერთაშორისო ინსტრუმენტებისა და მთლიანად კანონის უზენაესობის ფუნდამენტური ასპექტი და სახელმწიფოს მხრიდან თვითნებობის საწინააღმდეგო არსებითი გარანტიაა.

---

[290] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, 197, <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [18.06.2020].

[291] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9 (ბმული იხ. მე-19 გვერდზე); EU Data Protection Directive for Police and Criminal Justice Authorities (EU) 2016/680 („Police Directive“) (ბმული იხ. მე-8 გვერდზე).

[292] *Psychogiopoulou E.,* The European Couts of Human Rights, Privacy and Data Protection in the Digital Era, წიგნში: Court, Privacy and Data Protection in The Digital Environment, *Brkan M., Psychogiopoulou E. (eds.),* Cheltenham, UK, 2017, 60.

აღნიშნული პრინციპიდან გამომდინარე, ადამიანის უფლების ნებისმიერი შეზღუდვა უნდა იყოს კანონით გათვალისწინებული.[293]

სამოქალაქო და პოლიტიკური უფლებების შესახებ პაქტის მიხედვით, კანონიერების პრინციპი მჭიდროდაა დაკავშირებული „უფლების თვითნებური შეზღუდვის“ კონცეფციასთან". მაგალითად, პაქტის მე-17 მუხლის შესაბამისად, დაუშვებელია პირის პირად, ოჯახურ ცხოვრებასა და კორესპოდენციის ხელშეუხებლობის უფლებაში თვითნებური ან უკანონო ჩარევა.[294] ამასთან, გაეროს ადამიანის უფლებათა კომიტეტი „უფლების თვითნებურად შეზღუდვას“ შემდეგნაირად განმარტავს: „თვითნებობის კონცეფცია ემსახურება იმას, რომ უფლებაში ჩარევა, თუნდაც - კანონით გათვალისწინებული, შეესაბამებოდეს პაქტის მიზნებს, დებულებებს და ნებისმიერ შემთხვევაში იყოს გონივრული კონკრეტულ სიტუაციაში.“[295] ხოლო „გონივრულობის“ აღნიშნული ცნება გაეროს ადამიანის უფლებათა კომიტეტმა შემდეგი შინაარსით განმარტა - „პირადი ცხოვრების უფლებაში ნებისმიერი ჩარევა უნდა იყოს დასახული მიზნის პროპორციული და ამავდროულად, აუცილებელი საქმის კონკრეტული გარემოებებიდან გამომდინარე.“[296]

პირადი ცხოვრების უფლებაში ნებისმიერი ჩარევა დასაშვებია კანონმდებლობის საფუძველზე, რომელიც არის საჯაროდ ხელმისაწვდომი და საკმარისად სიცხადით ფორმულირებული.[297] ადამიანის უფლებების საკითხებში გაეროს სპეციალური მომხსენებელი აღნიშნავს, რომ სამოქალაქო და პოლიტიკური უფლებების შესახებ პაქტის მე-17 მუხლით დაცულ პირადი ცხოვრების უფლებაში ნებისმიერი ჩარევა უნდა იყოს გათვალისწინებული კანონით, რომელიც იქნება საკმარისად ხელმისაწვდომი, ნათელი და განჭვრეტადი, რათა მოქალაქეებს შეეძლოთ ფარული

---

[293] Necessary and Proportionate, International Principles on The Application of Human Rights to Communications Surveillance, 2014, <https://necessaryandproportionate.org/text> [15.06.2020].

[294] Article 17, International Covenant on Civil and Political Rights, 16/12/1966.

[295] CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 08/04/1988, <https://www.refworld.org/docid/453883f922.html> [18.06.2020].

[296] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 7 (ბმული იხ. მე-19 გვერდზე).

[297] Report of the Special Rapporteur On The Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 28.12.2009, 21 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement> [18.06.2020].

მეთვალყურეობის ჩატარებაზე უფლებამოსილი ორგანოსა და მის განსახორციელებლად საჭირო გარემოებების განსაზღვრა.[298]

ანალოგიური მოთხოვნებია გაჟღერებული კანონიერების პრინციპთან დაკავშირებით ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაში.[299] ევროპული სასამართლოს პრეცედენტული სამართლის მიხედვით, კანონიერების პრინციპი აერთიანებს ორ ასპექტს – სამართლებრივი საფუძვლის არსებობას კანონმდებლობაში და ასეთი საფუძვლის „ხარისხს", რომელიც თავის თავში მოიცავს კანონის ხელმისაწვდომობისა და განჭვრეტადობის მოთხოვნებს.[300]

2.1.1. კანონის ხელმისაწვდომობის კრიტერიუმი

ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების კონტექსტში „კანონის ხარისხის" მოთხოვნის აუცილებელ ელემენტს წარმოადგენს მარეგულირებელი კანონმდებლობის საჯაროდ ხელმისაწვდომობა[301]. აღნიშნული, ჩვეულებრივ, მიიღწევა სამართლებრივი რეგულაციების საჯაროდ გამოქვეყნების გზით.[302]

საიდუმლო რეგულაციები და კანონის საიდუმლო ინტერპრეტაციები, თუნდაც სასამართლოს მიერ განხორციელებული, არ აკმაყოფილებს „კანონისთვის" აუცილებელ „ხარისხის" მოთხოვნებს[303]. კომუნიკაციის მონიტორინგის ღონისძიებების ფარულ ხასიათს თან ახლავს დისკრეციის თვითნებურად განხორციელების მეტი რისკი, რომელიც თავის მხრივ, მოითხოვს მეტ კონკრეტიკას აღნიშნული დისკრეციის სამართლებრივი რეგულირებისას და დამატებითი ზედამხედველობის ბერკეტებს.[304]

კანონის ხელმისაწვდომობის კრიტერიუმი იქნა შეფასებული ევროპული სასამართლოს დიდი პალატის მიერ მაგალითად, საქმეში ზახაროვი რუსეთის

---

[298] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 8 (ბმული იხ. მე-19 გვერდზე).

[299] Kennedy v. United Kingdom, [2010] ECtHR, 151; Roman Zakharov v. Russia, [2015] ECtHR, 228.

[300] იქვე.

[301] Rotaru v. Romania, [2000], ECHR 2000-V, 54; Leander v. Sweden, [1987] ECtHR, (Ser. A.), 52-53.

[302] იქვე.

[303] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 10 (ბმული იხ. მე-19 გვერდზე).

[304] იქვე.

წინააღმდეგ (Zakharov v. Russia)[305]. ამ საქმეში კომუნიკაციის მინისტრის ბრძანება, რომელიც განსაზღვრავდა ტექნიკურ მოთხოვნებს სერვისის მიმწოდებლების მიერ დასაინსტალირებელ კომუნიკაციის მონიტორინგის მოწყობილობასთან დაკავშირებით, არ ყოფილა ოფიციალური წესით გამოქვეყნებული, რადგან მიჩნეულ იქნა ტექნიკური ხასიათის მქონედ[306]. ევროპული სასამართლოს შეხედულებით, ამ დოკუმენტს შეეძლო გავლენა მოეხდინა აბონენტების პირადი ცხოვრების ინტერესებზე, რადგან რუსეთში დამკვიდრებული სისტემის მიხედვით, მონიტორინგის მოწყობილობის საშუალებით უზრუნველყოფილი იყო სამართალდამცავი ორგანოების პირდაპირი წვდომა ყველა სახის მობილურ სატელეფონო კომუნიკაციაზე და არ აღირიცხებოდა სამართალდამცავი ორგანოების მიერ ინიცირებული სატელეფონო კომუნიკაციის ფარული მიყურადების შესახებ ინფორმაცია. აქედან გამომდინარე, სასამართლომ ამ დოკუმენტის საჯაროდ ხელმისაწვდომობა აუცილებლად მიიჩნია. მიუხედავად აღნიშნულისა, „კანონის ხელმისაწვდომობის“ კრიტერიუმის დარღვევა არ დადგინდა, რადგან აღნიშნული დააბალანსა მისი სხვა გზებით ხელმისაწვდომობის შესაძლებლობამ, კერძოდ, მოცემული დოკუმენტი გამოქვეყნდა კომუნიკაციის სამინისტროს ოფიციალურ ჟურნალში. მართალია აღნიშნულ ჟურნალში გამოქვეყნებული ბრძანება ხელმისაწვდომი იყო მხოლოდ პირთა შეზღუდულ წრისათვის - კომუნიკაციის სპეციალისტებისთვის, მაგრამ გადამწყვეტი როლი ითამაშა იმ ფაქტმა, რომ ბრძანებაზე წვდომა საზოგადოებას შეეძლო კერძო ონლაინ სამართლებრივი ბაზის მეშვეობით.[307]

2.1.2. კანონის განჭვრეტადობის კრიტერიუმი

კანონის განჭვრეტადობის კრიტერიუმი ფარული მეთვალყურეობის სფეროში სახელმწიფო ორგანოების თვითნებობის საწინააღმდეგო უმნიშვნელოვანეს გარანტიას წარმოადგენს. კანონი საკმარისი სიცხადით არის ფორმულირებული, თუკი პირს,

[305] Roman Zakharov v. Russia, [2015] ECtHR.
[306] იქვე. 240.
[307] იქვე. 241-242.

რომელსაც ის ეხება, შეუძლია (საჭიროების შემთხვევაში შესაბამისი კონსულტაციის გზით) საკუთარი ქმედებების მის შესაბამისად წარმართვა.[308]

ევროპულ სასამართლოს არაერთ საქმეზე აღუნიშნავს, რომ „კანონის განჭვრეტადობა“ ფარული მეთვალყურეობის ღონისძიებების კონტექსტში არ არის ანალოგიური შინაარსის, როგორც სხვა მრავალ სფეროში[309]. ამ კონკრეტულ საკითხთან მიმართებაში „კანონის განჭვრეტადობა“ არ გულისხმობს პირის შესაძლებლობას, წინასწარ განსაზღვროს, როდის შეიძლება დაექვემდებაროს სამართალდამცავი ორგანოების მხრიდან თვალთვალს და თავისი ქმედებაც აღნიშნულის შესაბამისად წარმართოს[310]. მიუხედავად ამისა, აღმასრულებელი ხელისუფლების საქმიანობის საიდუმლო რეჟიმში განხორციელების გამო თვითნებობის რისკი თვალსაჩინოა. შესაბამისად, აუცილებელია „ნათელი, დეტალური ნორმების“ არსებობა, განსაკუთრებით იმ პირობებში, როდესაც ტექნოლოგია, რომელიც ფარული მეთვალყურეობის ღონისძიების განხორციელების შესაძლებლობას იძლევა, მუდმივად იხვეწება.[311] „ეროვნული კანონმდებლობა უნდა იყოს საკმარისად მკაფიო, რათა მოქალაქეებს მიეცეთ ადეკვატური მითითება იმ გარემოებებისა და პირობების შესახებ, რომელთა არსებობისას სახელმწიფო ხელისუფლების ორგანოები უფლებამოსილნი არიან, გამოიყენონ აღნიშნული ღონისძიებები.“[312] ქმედების ფარული ხასიათი განსაკუთრებით პრობლემურია მისი კონტროლის თვალსაზრისით.[313] ევროპული სასამართლოს განმარტებით, ვინაიდან ამ ღონისძიებების პრაქტიკაში აღსრულება არ არის მისი ადრესატებისა და მთლიანად საზოგადოებისთვის საჯარო, კანონის უზენაესობის პრინციპის საწინააღმდეგო იქნებოდა აღმასრულებელი ხელისუფლებისთვის ან თუნდაც სასამართლოსთვის

[308] Doerga v. The Netherlands, [2004], ECtHR, 50.

[309] Roman Zakharov v. Russia, [2015] ECtHR. 229; Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Leander v. Sweden, [1987], ECtHR, (Ser. A.), 51; Huvig v. France, 24 April 1990, § 29, Series A no. 176-B; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 93.

[310] იქვე.

[311] Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Leander v. Sweden, [1987], ECtHR, (Ser. A.), 51; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46. Huvig v. France, [1990], ECtHR, (Ser. A.), 32. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75; Kruslin v. France, [1990], ECtHR, (Ser. A.), 33.

[312] Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Roman Zakharov v. Russia, [2015] ECtHR, 229.

[313] *ტრექსელი შ.,* ადამიანის უფლებები სისხლის სამართლის პროცესში, *(რედ.),* თბ., 2009, 568.

შეუზღუდავი დისკრეციის მინიჭება[314]. შესაბამისად, თვითნებობის საწინააღმდეგო გარანტიების უზრუნველსაყოფად კანონმდებლობით „საკმარისი სიცხადით“ უნდა დარეგულირდეს აღნიშნული დისკრეციის ფარგლები და მისი განხორციელების წესი.[315]

ევროპულ სასამართლოს კომუნიკაციის მონიტორინგთან დაკავშირებულ თავის პრეცედენტულ სამართალში დადგენილი აქვს ის მინიმალური გარანტიები, რომლებსაც უნდა აკმაყოფილებდეს კონვენციის წევრი სახელმწიფოს კანონმდებლობა[316], ესენია: დანაშაულების კატეგორია, რომელთა შემთხვევაშიც დასაშვებია კომუნიკაციის მონიტორინგის ღონისძიების განხორციელება; პირთა წრე, რომელთა მიმართაც დაიშვება ამ ღონისძიების გამოყენება; ღონისძიების მაქსიმალური ხანგრძლივობა; მონაცემების გამოკვლევის, შენახვისა და გამოყენების პროცედურა; უსაფრთხოების ზომები, რომლებიც გამოყენებულ უნდა იქნეს აღნიშნული მონაცემების სხვა პირთათვის გადაცემის დროს; გარემოებები, როდესაც მოპოვებული ჩანაწერები უნდა იქნეს წაშლილი ან განადგურებული.[317]

კანონის საჯაროდ ხელმისაწვდომობისა და სამართლებრივი სიცხადის მოთხოვნების დარღვევა დაადგინა ევროპულმა სასამართლომ მაგალითად, საქმეზე ლიბერთი და სხვები დიდი ბრიტანეთის წინააღმდეგ (Liberty and others v. United Kingdom)[318]. მოცემულ საქმეში სასამართლომ მიიჩნია, რომ ბრიტანეთის კანონმდებლობა აღმასრულებელ ხელისუფლებას (უშიშროების ორგანოებს) ანიჭებდა პრაქტიკულად შეუზღუდავ შესაძლებლობებს დიდი ბრიტანეთის ფარგლებს გარეთ გამავალ/საზღვარგარეთიდან ბრიტანეთში შემომავალ კომუნიკაციის მონიტორინგთან დაკავშირებით, კერძოდ, იმ დროს მოქმედი კანონმდებლობის მიხედვით, ნებისმიერი ადამიანი, რომელიც რაიმე სახის ტელეკომუნიკაციას აგზავნიდა/იღებდა ბრიტანეთის ფარგლებს გარეთ კონკრეტულ პერიოდში, შესაძლებელია მოქცეულიყო კომუნიკაციის მონიტორინგის ქვეშ. ბრიტანეთის

[314] Roman Zakharov v. Russia, [2015] ECtHR, 230.

[315] იქვე.

[316] Roman Zakharov v. Russia, [2015] ECtHR, 231; Szabo and Vissy v. Hungary, [2016] ECtHR 56; Huvig v. France, [1990], ECtHR, (Ser. A.), 34; Amman v. Switzerland, [2000], ECHR 2000-II, 56-58; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46; Prado Bugallo v. Spain, [2003], ECtHR 30; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 95.

[317] იქვე.

[318] Liberty and others v. United Kingdom, , [2008], ECtHR.

კანონმდებლობის მიხედვით, სახელმწიფო მდივანი ტელეკომუნიკაციის მონიტორინგის ბრძანების გამოცემის დროს უზრუნველყოფდა „ისეთი ზომების“ გატარებას, რომლებსაც მიიჩნევდა საჭიროდ, რათა კომუნიკაცია, რომლებსაც არ ეხებოდა ნებართვა, არ ყოფილიყო გამოკვლეული, ხოლო მასალები, რომლებიც ექცეოდა ნებართვის ქვეშ, გამოკვლეულიყო მხოლოდ იმ ფარგლებით, რაც აუცილებლობას წარმოადგენდა. ამასთან, მოპოვებული მასალების „შერჩევის პროცედურა, მათი გამოკვლევის, გამჟღავნების და შენახვის მიზნით“, რეგულირდებოდა მხოლოდ შიდა რეგულაციებით/ინსტრუქციებით, რომლებიც არ იყო საჯაროდ ხელმისაწვდომი. მიუხედავად აღნიშნულისა, სასამართლოს განმარტებით „ზომები“, რომლებიც სახელმწიფო მდივანს უნდა გაეტარებინა მასალების შერჩევის კონტექსტში მათი გამოკვლევის მიზნით, არ რეგულირდებოდა კანონმდებლობით ან საზოგადოებისათვის ხელმისაწვდომი სხვა ფორმით, რის გამოც სასამართლომ მიიჩნია, რომ კომუნიკაციის მონიტორინგის შედეგად მოპოვებული მასალის შერჩევის პროცედურა მისი გამოკვლევის, გამჟღავნების, შენახვის და განადგურების მიზნით, არ აკმაყოფილებდა სამართლებრივი სიცხადის და კანონის ხელმისაწვდომობის მოთხოვნებს[319].

კანონის განჭვრეტადობის კრიტერიუმთან დაკავშირებით ანალოგიური შინაარსის მოთხოვნებია გაჟღერებული გაეროს დონეზეც[320]. პირადი ცხოვრების უფლების ზოგად კომენტარში გაეროს ადამიანის უფლებების კომიტეტი აღნიშნავს, რომ კანონმდებლობა, რომელიც კერძო კომუნიკაციის ხელშეუხებლობის უფლებაში ჩარევის შესაძლებლობას იძლევა, დეტალურად უნდა განსაზღვრავდეს გარემოებებს, რომელთა შემთხვევაშიც დასაშვებია ამგვარი ჩარევა.[321] ამასთან, გამოხატვის თავისუფლებასთან დაკავშირებით გაეროს და ინტერამერიკული კომისიის სპეციალური მომხსენებლების ერთობლივ ანგარიშში ხაზგასმულია, რომ „პერსონალური მონაცემების გადაჭერა, მოპოვება და გამოყენება, ისევე როგორც მონაცემთა სუბიექტის მიერ ამ მონაცემებზე წვდომის შეზღუდვის შემთხვევები, უნდა იყოს მკაფიოდ რეგულირებული კანონში უფლებაში თვითნებური ან/და უნებართვო

[319] იქვე. 64-70.
[320] CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 08/04/1988, (ბმული იხ. მე-80 გვერდზე).
[321] იქვე.

ჩარევისგან პირის დაცვის მიზნით[322]. კანონმა უნდა დააწესოს შეზღუდვები ფარული მეთვალყურეობის ღონისძიებების ხასიათთან, ფარგლებთან და ხანგრძლივობასთან დაკავშირებით, ასევე უნდა განსაზღვროს მისი ჩატარების საფუძვლები, ორგანოები, რომლებიც პასუხისმგებელი არიან ნებართვის გაცემაზე, ღონისძიების აღსრულებასა და მონიტორინგზე, ასევე ამ ღონისძიებათა გასაჩივრების სამართლებრივი ბერკეტები"[323].

2.2. უფლებაში ჩარევის ლეგიტიმური მიზანი

პირადი ცხოვრების ხელშეუხებლობის უფლებაში ნებისმიერი ჩარევა უნდა ემსახურებოდეს მნიშვნელოვანი სამართლებრივი ინტერესის დაცვას, რომელიც „აუცილებელია დემოკრატიულ საზოგადოებაში."[324] „ლეგიტიმური მიზნის" ელემენტის მიხედვით, ნებისმიერი მიზანი ვერ გაამართლებს კონსტიტუციური უფლების შეზღუდვას. მიზნები, რომლებსაც შეუძლია ეს როლი შეასრულოს, უკავშირდება იმ ძირითად ღირებულებებს, რომლებზედაც საზოგადოება დგას.[325] კონსტიტუციურ დემოკრატიულ წყობილებაში ეს ღირებულებები წარმოადგენს დემოკრატიულ ღირებულებებს.[326]

კონვენციის მე-8 (2) მუხლის მიხედვით, პირადი ცხოვრების უფლების შეზღუდვა დასაშვებია ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების, ქვეყნის ეკონომიკური კეთილდღეობის, დანაშაულის ან უწესრიგობის თავიდან აცილების, ჯანმრთელობის ან მორალის დაცვის, ან სხვათა უფლებებისა და თავისუფლებების დაცვის მიზნით.[327] მართალია „ლეგიტიმური მიზნის ტესტი," როგორც წესი, არ არის გადამწყვეტი მნიშვნელობის ევროპული სასამართლოს მიერ ფარულ მეთვალყურეობასთან დაკავშირებული საქმეების ბედის გადაწყვეტისას, მაგრამ ეს

[322] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration On Surveillance Programs and Their Impact on Freedom of Expression, 21/06/2013, <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1>[18.06.2020].

[323] იქვე.

[324] Necessary and Proportionate, International Principles on The Application of Human Rights to Communications Surveillance, 2014, <https://necessaryandproportionate.org/text> [15.06.2020].

[325] *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 245-246. წიგნში „ლეგიტიმური მიზნის" ელემენტი მოხსენიებულია როგორც "Proper Purpose".

[326] იქვე.

[327] ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია, მუხლი 8, 04/11/1950.

პრინციპი სასამართლოს მიერ გამოიყენება ყოველდღიურ ცხოვრებაში თანამედროვე ტექნოლოგიების „დაშვების ზღვარის“ დასადგენად და იმის გასარკვევად, ამ ტექნოლოგიების გამოყენება რამდენად შეესაბამება კონვენციის მე-8 მუხლს,[328] მაგალითად, საქმეში პეკი გაერთიანებული სამეფოს წინააღმდეგ (Peck v. United Kingdom), ევროპულმა სასამართლომ ხაზი გაუსვა CCTV სისტემის (ვიდეომეთვალყურეობის სისტემა) გამოსადეგობას და ამ საშუალების მნიშვნელოვან როლს დანაშაულის წინააღმდეგ ბრძოლაში.[329]

ევროპული სასამართლოს პრაქტიკაში სახელმწიფოები „იშვიათად აწყდებიან რაიმე სირთულეს „ლეგიტიმური მიზნის“ კომპონენტის დემონსტრირების დროს,“[330] რაც ძირითადად განპირობებულია იმით, რომ სასამართლო უფრო მეტად კონცენტრირებულია ეროვნული კანონმდებლობით გათვალისწინებული ფარული მეთვალყურეობის მთლიანი რეჟიმის და არა ინდივიდუალურ შემთხვევაში გამოყენებული კონკრეტული ღონისძიების შეფასებაზე.[331] ამასთან, სასამართლოს მიერ ზოგადად აღიარებულია, რომ ფარული თვალთვალის უფლებამოსილების გამოყენება დანაშაულის გამოძიების მიზნებისათვის დასაშვებია,[332] ხოლო რამდენად გააჩნია ფარულ საგამოძიებო მოქმედებას „კონკრეტული/მიზანმიმართული“ ხასიათი, ეს უკვე სხვა ტესტის - „თანაზომიერების“ ქვეშ განსახილველ საკითხს წარმოადგენს.[333]

2.3. თანაზომიერების პრინციპი

კონსტიტუციური უფლების შეზღუდვა დემოკრატიულ საზოგადოებაში აუცილებელი ინტერესის დაცვის მოტივით მოითხოვს ურთიერთდაპირისპირებული ინტერესების შეფასებას და ეს შეფასება თანაზომიერების პრინციპის საფუძველზე

---

[328] *Galletta A., Hert P.D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht Law Review, 2014, Vol. 10, No 1, 68.

[329] *Galletta A., Hert P.D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht Law Review, 2014, Vol. 10, No 1, 68. იხ. ციტირება: Peck v the United Kingdom, [2003] ECHR.

[330] Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 19, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf>[15.06.2020].

[331] იქვე.

[332] იხ. მაგალითად, Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.).

[333] Necessary and Proportionate & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 19, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf>[15.06.2020].

უნდა განხორციელდეს.[334] შესაბამისად, უფლების შეზღუდვა უნდა იყოს თანაზომიერი და ემსახურებოდეს შესაფერის მიზანს. შეზღუდვის საშუალება უნდა იყოს რაციონალური და აუცილებელი. კონსტიტუციური უფლების შეზღუდვის შედეგად მიყენებული ზიანი არ უნდა აღემატებოდეს შეზღუდვის შედეგად მიღებულ სარგებელს („თანაზომიერება ვიწრო გაგებით“).[335] ზოგიერთი ავტორი თანაზომიერების პრინციპს განმარტავს, როგორც "წესების ერთობლიობას, რომელიც განსაზღვრავს უფლების შეზღუდვის აუცილებელ და საკმარის პირობებს",[336] ხოლო ზოგიერთი - როგორც პრინციპს, რომელიც ზღუდავს სახელმწიფოს უფლებამოსილებას."[337] შესაბამისად, აღნიშნული პრინციპი ასრულებს ორმაგ როლს: იცავს ფუნდამენტურ უფლებას და უზრუნველყოფს მასში ჩარევის საფუძვლიანობას.[338]

როგორც წესი, იურიდიულ ლიტერატურასა და სამოსამართლო პრაქტიკაში „თანაზომიერების პრინციპის“ სამ ელემენტს გამოყოფენ, ესენია: 1) აუცილებლობა; 2) შესაფერისობა; 3) „თანაზომიერება ვიწრო გაგებით“ ("Proportionality stricto sensu")[339], თუმცა ზოგიერთი მეცნიერი, მაგალითად, ბარაკი (Barak), აღნიშნული ცნების ქვეშ მოიაზრებს ასევე „ლეგიტიმური მიზნის“ კომპონენტსაც.[340]

თანაზომიერება წარმოადგენს სახელმძღვანელო პრინციპს, თუ როგორ უნდა განხორციელდეს ფარული მეთვალყურეობის ღონისძიება პრაქტიკული

---

[334] *Barak A.*, Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 133, იხ. ციტირება: S. v. Makwanyane, 1995 (3) SA 391 § 104.

[335] *Barak A.*, Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 140.

[336] *Milaj J.,* Privacy, Surveillance, and The Proportionality Principle: The Need for A Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No 3, 2016, 117, იხ. ციტირება: *Barak A.*, Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 3.

[337] *Milaj J.,* Privacy, Surveillance, and The Proportionality Principle: The Need for A Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No 3, 2016, 117, იხ. ციტირება: *Jans, J. H., R. de Lange, S. Prechal, R. Widdershoven, J.H.*, 2007, Europeanisation of Public Law, Groningen: Europa Law Publishing.

[338] *Milaj J.,* Privacy, Surveillance, and The Proportionality Principle: The Need for A Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No 3, 2016, 117.

[339] იქვე. 119. *Tranberg C. B.,* Proportionality and Data Protection in The Case Law of The European Court of Justice, International Data Privacy Law, 2011, Vol. 1, No. 4, 239-240; *Cohen-Eliya M., Porat I.,* American balancing and German proportionality: The Historical Origins, International Journal of Constitutional Law, Vol 8, No 2, 2010, 267, <https://academic.oup.com/icon/article/8/2/263/699991> [18.06.2020].

[340] *Barak A.*, Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 131, 245-247.

თვალსაზრისით.[341] კონსტიტუციური უფლების შეზღუდვისას აღნიშნული პრინციპი ხელისუფლების სამივე შტოს სახელმძღვანელო მოთხოვნას წარმოადგენს - ამ პრინციპით იზღუდება როგორც საკანონმდებლო, ასევე აღმასრულებელი და სასამართლო ხელისუფლება.[342]

აღსანიშნავია, რომ თანაზომიერების ცნება გერმანიის სასამართლო პრაქტიკაში ჩამოყალიბდა და შემდგომში გასცდა გერმანიის ფარგლებს[343]. თანაზომიერების დოქტრინა დაინერგა ასევე ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტულ სამართალში[344], ისევე როგორც ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკაში. ევროკავშირის სამართლში თანაზომიერების პრინციპი განმტკიცებულია ფუნდამენტური უფლებების ქარტიის 52(1) მუხლით, როგორც აღნიშნული ქარტიით უზრუნველყოფილი უფლებების შეზღუდვის საფუძველი.[345]

შესაფერისობის ტესტი - კონსტიტუციური უფლების შემზღუდველი ღონისძიების შესაფერისობა თანაზომიერების პრინციპის ერთ-ერთ სავალდებულო კომპონენტს წარმოადგენს. ნებისმიერი ფარული საგამოძიებო მოქმედება მისაღწევი მიზნის შესაფერისი და ადეკვატური საშუალება უნდა იყოს[346]. როგორც მინიმუმ, ასეთ ღონისძიებას უნდა გააჩნდეს დასახული მიზნის მიღწევის შესაძლებლობა.[347] გერმანიის ფედერალური საკონსტიტუციო სასამართლოს განმარტებით, შესაფერისობის ტესტი არ მოითხოვს, რომ ნორმის მიზანი ყოველ კონკრეტულ შემთხვევაში რეალურად განხორციელდეს, არამედ საკმარისია მისი მიღწევა გაადვილდეს.[348]

---

[341] *Taylor N.,* To Find the Needle Do You need the Whole Haystack? Global Surveillance and Principled Regulation, The International Journal of Human Rights, Vol. 18, No 1, 2014, 57.

[342] *Barak A.*, Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 379-381.

[343] იქვე. 178-185.

[344] *Somody B., Szabo M., D., Szekely I.,* Moving Away from The Security–Privacy Trade-off: The Use of the Test of Proportionality in Decision Support, წიგნში: Surveillance, Privacy and Security, Citizens' Perspectives, *Friedewald M., Burgess J. P., Čas J., Bellanova R., Peissl W., (eds),* London/New York, 2017, 158.

[345] Charter of Fundamental Rights of The European Union, article 52(1), <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [18.06.2020].

[346] *Rodríguez K,* A Principled Fight Against Surveillance", Global information Society Watch, Communications Surveillance in the Digital Age, Edited by *Finlay A.* APC and Hivos, 2014, 15 (11-16) <https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf> [18.06.2020].

[347] იქვე.

[348] BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08, 207.

მსგავსი მოთხოვნაა გაჟღერებული ასევე ადამიანის უფლებების დარგში გაეროს უმაღლესი კომისრის ანგარიშში „პირადი ცხოვრების უფლება ციფრულ ეპოქაში“[349]. უმაღლესი კომისარი აღნიშნავს, რომ პირადი ცხოვრების უფლების შემზღუდველ ღონისძიებას უნდა გააჩნდეს დასახული ლეგიტიმური მიზნის (მაგალითად, ეროვნული უსაფრთხოების დაცვის) მიღწევის შესაძლებლობა[350]. ორგანოს, რომელსაც სურს ასეთი უფლებაშემზღუდველი ზომის გამოყენება, ეკისრება მტკიცების ტვირთი, აჩვენოს, რომ შეზღუდვა ნამდვილად კავშირშია ლეგიტიმურ მიზანთან[351]. გარდა აღნიშნულისა, პირადი ცხოვრების სფეროში ნებისმიერი ჩარევა „აზრს არ უნდა უკარგავდეს თავად უფლებას” და თანხვედრაში უნდა იყოს სხვა ძირითად უფლებებთან.[352]

ვენეციის კომისიის შეხედულებით, საგამოძიებო ორგანოს უნდა გააჩნდეს საკმარისი მიზეზები, ივარაუდოს, რომ ფარული მეთვალყურეობის ღონისძიების მეშვეობით შესაძლებელია გამოძიებისათვის მნიშვნელოვანი ინფორმაციის მოპოვება[353]. მოსაპოვებელი ინფორმაციის „გამოსადეგობა“ თანაზომიერების ზოგადი პრინციპის ერთ-ერთ მოთხოვნას წარმოადგენს[354]. ამასთან, არ არის აუცილებელი, საგამოძიებო ორგანო დარწმუნებული იყოს ინფორმაციის გამოსადეგობაში, არამედ საკმარისია, აჩვენოს გარკვეული „ალბათობა“ იმისა, მოცემული ღონისძიების შედეგად ასეთი ინფორმაცია იქნება მოპოვებული[355]. მიუხედავად ამისა, ნემისმიერი ასეთი მტკიცება გამყარებული უნდა იყოს რაიმე „ფაქტობრივი გარემოებით და მტკიცებულებით.”[356]

ამდენად, „შესაფერისობის ტესტი“ არ მოითხოვს განსახორციელებელი ღონისძიების უპირობო წარმატებულობის შესაძლებლობას, არამედ შეიძლება ითქვას, რომ უფრო ახლოს დგას კანადურ კონცეფციასთან, რაც განსახორციელებელი

---

[349] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 8 (ბმული იხ. მე-19 გვერდზე).
[350] იქვე.
[351] იქვე.
[352] იქვე.
[353] European Commission for Democracy Throgh Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 14, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].
[354] იქვე.
[355] იქვე.
[356] იქვე.

ღონისძიების მიზანთან „რაციონალური კავშირის“ მოთხოვნაში მდგომარეობს[357], თუმცა ამავდროულად, „შესაფერისობის ტესტი“ უფრო მკაცრია ვიდრე კანადური მიდგომა და არ კმაყოფილდება მხოლოდ მიზანთან ღონისძიების ლოგიკურ კავშირში არსებობით, არამედ მოითხოვს, რომ საგამოძიებო მოქმედება იყოს „ეფექტიანი“ საშუალება ლეგიტიმური მიზნის მისაღწევად.[358] ღონისძიება, რომელსაც საერთოდ არ გააჩნია დასახული მიზნის მიღწევის შესაძლებლობა, ან რომელიც აშკარად წარუმატებელია მის მისაღწევად, ვერ ჩაითვლება „შესაფერის“, „პროპორციულ“ საშუალებად.[359]

აუცილებლობის ტესტი - თანაზომიერების პრინციპის კიდევ ერთ შემადგენელ ელემენტს სუბსიდიარულობის პრინციპი, იგივე აუცილებლობის ტესტი წარმოადგენს. ის ასევე მოხსენებულია, როგორც „ნაკლებად უფლებაშემზღუდველი საშუალებების“ ტესტი.[360] აღნიშნული პრინციპის თანახმად, კანონი ზღუდავს ფუნდამენტურ უფლებას იმ ხარისხით, რაც აუცილებელია, მხოლოდ იმ შემთხვევაში, როდესაც კანონმდებელი მის ხელთ არსებული რამდენიმე ალტერნატიული საშუალებიდან ირჩევს ყველაზე ნაკლებად მზღუდავ საშუალებას[361]. შესაბამისად, კანონმდებელმა უფლების შეზღუდვის საშუალების შერჩევისას, პირველ რიგში, უნდა განიხილოს ყველაზე მსუბუქი და შემდეგ უფრო მკაცრი საშუალებები, სანამ არ შეარჩევს ისეთს, როდესაც ლეგიტიმური მიზნის მისაღწევად უფრო მკაცრი ზომის გამოყენება უკვე აღარ არის აუცილებელი.[362] კანონით გათვალისწინებული საშუალება აკმაყოფილებს აუცილებლობის მოთხოვნას, თუკი არ არსებობს სხვა ჰიპოთეტური ალტერნატივა, რომელიც უფლებისთვის ნაკლებად ზიანის მომტანი და ამავდროულად მიზნის მიღწევის თანაბრად წარმატებული საშუალება იქნებოდა.[363]

---

[357] Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 21, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf> [15.06.2020].

[358] იქვე.

[359] იქვე.

[360] *Michaelsen C.,* The Proportionality Principle, Counter-Terrorism Laws and Human Rights: A German-Australian Comparison, City U. H.K. L. Rev. 19, 2010, 30.

[361] *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, Cambridge University Press, 2012, 317.

[362] Barak A. Proportionality - Constitutional Rights and their Limitations, Cambridge, Cambridge University Press, 2012, 317, იხ. ციტირება: CA 6821/93 United Mizrahi Bank Ltd. v. Migdal Cooperative Village [1995] IsrLR 1.

[363] *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, Cambridge University Press, 2012, 317.

ამასთან, აუცილებლობის ტესტი არ მოითხოვს სხვა ისეთი საშუალების გამოყენებას, რომლითაც უფლების შეზღუდვა მინიმალური ან თუნდაც უფრო ნაკლები იქნება, თუკი აღნიშნული საშუალებით ლეგიტიმური მიზნის მიღწევა შეუძლებელია იმ ხარისხით, როგორითაც კანონმდებლის მიერ არჩეული საშუალებით.[364] ამდენად, ეს პრინციპი სახელმწიფოსგან მოითხოვს, რომ ადამიანის ძირითადი უფლება არ შეიზღუდოს იმაზე მეტად, ვიდრე დასახული ლეგიტიმური მიზნის მისაღწევად არის აუცილებელი.[365]

ამ ტესტის შესაბამისად, ფარული მეთვალყურეობის ღონისძიების გამოყენება შეუსაბამო იქნება აუცილებლობის მოთხოვნასთან, თუკი ხელმისაწვდომია სხვა, უფრო ნაკლებად უფლებაშემზღუდველი ღონისძიება ან მისი გამოყენების შესაძლებლობა არ არის ამოწურული.[366] აღნიშნული პრინციპი მიზნად ისახავს ტელეკომუნიკაციის ფარული მიყურადების ღონისძიებები გამოიყენონ მხოლოდ ისეთი საქმის გარემოებების გამოძიებისთვის, რომლის დროსაც ჩვეულებრივი, ღია საგამოძიებო მოქმედებები წარუმატებელი იქნება.[367]

თანაზომიერება ვიწრო გაგებით - თანაზომიერების პრინციპის ყველაზე მნიშვნელოვან ელემენტს წარმოადგენს „თანაზომიერება ვიწრო გაგებით". ამ ტესტის თანახმად, იმისათვის, რათა კონსტიტუციური უფლების შეზღუდვა გამართლებულად ჩაითვალოს, შესაფერისი ურთიერთდამოკიდებულება უნდა არსებობდეს შეზღუდვის შედეგად მისაღწევ სიკეთესა და დამდგარ ზიანს შორის.[368]

ყოველთვის, როდესაც დღის წესრიგში დგას კონფლიქტური ინტერესების დაბალანსების საკითხი - იზღუდება კონსტიტუციური უფლება რაიმე სამართლებრივი აქტით, დაბალანსების ტესტი მოითხოვს, რომ სასწორის პინის ერთ მხარეს განხილულ იქნეს: 1) ლეგიტიმური მიზანი, რომლის მიღწევასაც ემსახურება

---

[364] იქვე, 321.

[365] *Michaelsen C.,* The Proportionality Principle, Counter-Terrorism Laws and Human Rights: A German-Australian Comparison, 2 City U. H.K. L. Rev. 19, 2010, 30.

[366] *Rodríguez K.,* Principled Fight Against Surveillance, Global information Society Watch, Communications Surveillance in the Digital Age, *Finlay A. APC and Hivos (eds.),* 2014, 15, <https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf> [18.06.2020]. Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 21 (ბმული იხ. პირველ გვერდზე).

[367] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 125 იხ. ციტირება: *Albrecht/ Dorsch/ Krüpe,* Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, 2003, S. 20.

[368] *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 340.

კონსტიტუციური უფლების შემზღუდველი ნორმა; 2) სარგებელი, რომელსაც ემსახურება მოცემული ნორმა და 3) ალბათობა იმისა, რომ ეს სარგებელი რეალურად მიიღწევა, ხოლო მეორე მხარეს - 1) შეზღუდული კონსტიტუციური უფლება; 2) ზიანი, რომელიც თან სდევს ამ შეზღუდვას და 3) ალბათობა იმისა, რომ ეს ზიანი რეალურად დადგება.[369] ამდენად, ეს ტესტი მოითხოვს კონსტიტუციური უფლების შეზღუდვის შედეგად მიღებული სარგებელისა და გამოწვეული ზიანის დაბალანსებას.[370]

თანაზომიერების ამ ელემენტის თანახმად, ძირითადი უფლების შემზღუდველი ღონისძიებები უნდა შეესაბამებოდეს დანაშაულის სიმძიმესა და დანაშაულის შესახებ არსებული ეჭვის ხარისხს.[371]

თანაზომიერების პრინციპიდან გამომდინარე, რაც უფრო მაღალია კონკრეტული ტიპის ფარული საგამოძიებო მოქმედების შედეგად უფლების შეზღუდვის ინტენსივობა და კონფიდენციალურობის ლეგიტიმური მოლოდინის ხელყოფა, მით უფრო მკაცრი მოთხოვნები უნდა იქნეს ღონისძიების მიმართ გათვალისწინებული.[372] ფარული მეთვალყურეობის ღონისძიებები შეიძლება განხორციელდეს მხოლოდ საკმარისად წონადი სამართლებრივი ინტერესების დაცვის მოტივით.[373] გერმანიის ფედერალური საკონსტიტუციო სასამართლო, მაგალითად, ფარული მეთვალყურეობის ღონისძიებების საფუძვლების შემდეგნაირ კლასიფიკაციას განიხილავს - სისხლის სამართლის დანაშაულის გამოძიების მიზნებისათვის საცხოვრებლის შიგნით ფარული საგამოძიებო მოქმედებები შეიძლება განხორციელდეს მხოლოდ განსაკუთრებით მძიმე დანაშაულების შემთხვევაში; ტელეკომუნიკაციის მონიტორინგი და პრევენციულად შენახული ტრაფიკის მონაცემების გამოყენება დასაშვებია მხოლოდ მძიმე დანაშაულების შემთხვევაში, ხოლო GPS ადგილმდებარეობის განსაზღვრის გლობალური სისტემის (The Global Positioning System - GPS) მეშვეობით ადგილმდებარეობის შესახებ მონაცემების

---

[369] უფრო ვრცლად იხ. *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012, 348-363.

[370] იქვე. 340.

[371] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 101, იხ. ციტირება: BVerfGE 35, 382, 410; 63, 131, 144; Meyer-Goßner, StPO, Einleitung, Rn. 20; Pfeiffer in: Karlsruher Kommentar, StPO, Einleitung Rn. 30; *Talaska* Der Richtervorbehalt, 2007, S. 45; *Goring, in Mangoldt/Klein/Starck,* Bonner Grundgesetz, 2005, Art. 13 Abs. 2, Rn. 89.

[372] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, 105.

[373] იქვე. 106

მოპოვება – კანონმდებლობით განსაზღვრული საკმაო მნიშვნელობის მქონე დანაშაულების შემთხვევაში.[374] შესაბამისად, რაც უფრო ინტენსიურია ფარული საგამოძიებო მოქმედება, მით უფრო მნიშვნელოვანი უნდა იყოს საჯარო ინტერესი, რომლის დაცვასაც ის ემსახურება. აღნიშნულის საილუსტრაციოდ ასევე გამოდგება გერმანიის ფედერალური საკონსტიტუციო სასამართლოს 2008 წლის 27 თებერვლის გადაწყვეტილებაც, რომლითაც სასამართლომ მიიჩნია, რომ საინფორმაციო-ტექნოლოგიურ სისტემაში ფარულ შეღწევას, როგორც უაღრესად ინტენსიურ ღონისძიებას, შეიძლება საფუძვლად დაედოს მხოლოდ განსაკუთრებით მნიშვნელოვანი სამართლებრივი სიკეთის მიმართ კონკრეტული საფრთხე[375]. ასეთ სამართლებრივ სიკეთედ სასამართლომ მიიჩნია ჯანმრთელობა, სიცოცხლე, თავისუფლება ან ისეთი საჯარო ინტერესები, რომელთა მიმართ საფრთხე გავლენას ახდენს სახელმწიფოს ან კაცობრიობის არსებობის საფუძვლებზე.[376]

2.3.1 ცალკეული ასპექტები თანაზომიერების პრინციპიდან გამომდინარე

თანაზომიერების პრინციპის თანახმად, ფარული მეთვალყურეობის ნებისმიერი მეთოდის გამოყენებისას უნდა შეფასდეს მოსაპოვებელი ინფორმაციის სენსიტიურობა და დაცულ უფლებაში ჩარევის ინტენსივობა. აღნიშნული მოითხოვს კუმულაციურად მინიმუმ შემდეგი გარემოებების შეფასებას: არსებობს მაღალი ალბათობა იმისა, რომ მძიმე დანაშაული განხორციელდება ან განხორციელდა; არსებობს მაღალი ალბათობა, რომ მძიმე დანაშაულის გამოძიების მიზნებისათვის რელევანტური მტკიცებულება იქნება მოპოვებული; სხვა ნაკლებად უფლებაშემზღუდველი საშუალებების გამოყენების შესაძლებლობა ამოწურულია ან უშედეგო იქნება, შედეგად გამოსაყენებელი საშუალება წარმოადგენს ყველაზე უფრო ნაკლებად ინტენსიურს; მონაცემები, რომელზეც განხორციელდა წვდომა, შემოიფარგლება მხოლოდ მძიმე დანაშაულის გამოძიებისათვის რელევანტური ინფორმაციით, ხოლო ნებისმიერი მოპოვებული ინფორმაცია, რომელიც არ არის კავშირში მძიმე დანაშაულთან არ იქნება შენახული, არამედ განადგურდება; ინფორმაციათან წვდომა ექნება მხოლოდ კონკრეტულ უფლებამოსილ ორგანოს და აღნიშნული ინფორმაცია გამოყენებული

[374] იქვე. 107
[375] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07.
[376] იქვე.

იქნება მხოლოდ იმ მიზნით და ხანგრძლივობით, რომელიც ღონისძიების ჩატარების ნებართვაში არის აღნიშნული; თავად ღონისძიება და გამოყენებული ტექნიკური საშუალებები ძირს არ უთხრის პირადი ცხოვრების უფლების არსს .[377]

თანაზომიერების პრინციპის მიხედვით, საჯარო და კერძო ინტერესების დაბალანსება შესაფერისი პროცედურული გარანტიებით უნდა განხორციელდეს.[378] სწორედ თანაზომიერების პრინციპიდან გამომდინარეობს სხვადასხვა პროცედურული მოთხოვნების გათვალისწინების აუცილებლობა ფარულ საგამოძიებო მოქმედებებთან დაკავშირებულ კანონმდებლობაში,[379] მაგალითად, ღონისძიების ჩატარებაზე ნებართვის გაცემა დამოუკიდებელი ორგანოს მიერ, საზედამხედველო მექანიზმები, შეტყობინების ვალდებულება და სხვა.[380] ასევე შესაფერისობის, აუცილებლობისა და თანაზომიერების კონტექსტში განიხილება ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული ისეთი პროცედურული გარანტიები, როგორიცაა, მაგალითად, მოთხოვნები ფარული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე შუამდგომლობის და სასამართლოს განჩინების მიმართ, მტკიცებულებითი სტანდარტი, განგრძობადი სასამართლო კონტროლი.[381] თანაზომიერების კონტექსტში ფასდება ასევე ღონისძიების ფარგლები - ფარული მეთვალყურეობის ღონისძიება მიმართული უნდა იყოს კონკრეტული ადრესატის წინააღმდეგ; ამ პრინციპიდან გამომდინარეობს ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნაც.[382]

დღესდღეობით, ფარული მეთვალყურეობა სხვადასხვა თანამედროვე ტექნოლოგიების გამოყენებით ხორციელდება. ამ ტექნიკური საშუალებების მახასიათებლებს რელევანტური მნიშვნელობა ენიჭება ფარული თვალთვალის ღონისძიების აუცილებლობისა და პროპორციულობის შეფასებისას. ინტენსიური

---

[377] Necessary and Proportionate, International Principles on The Application of Human Rights to Communications Surveillance, 2014, <https://necessaryandproportionate.org/text> [15.06.2020].

[378] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07, 117.

[379] იქვე.

[380] იქვე, 134, 136.

[381] Access Now, Universal Implementation Guide for The International Principles on The Application of Human Rights to Communication Surveillance, 2015, <https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf> [17.06.2020].

[382] *Dempsey J., X.; Gate F., H.,* Recommendations for Government and Industry, წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.),* Oxford, 2017, 428.

ფარული მეთვალყურეობის ტექნოლოგიების გამოყენება აუცილებლად შეიძლება მიჩნეულ იქნეს მხოლოდ მაშინ, როდესაც ფარული თვალთვალის სხვა ნაკლებად ინტენსიური ზომები არაეფექტიანი იქნება.[383] „ვიწრო გაგებით პროპორციულობის“ მოთხოვნის (დაბალანსების ტესტი) კონტექსტში, საჯარო და პირადი ცხოვრების ინტერესების დაბალანსების დროს მნიშვნელობა ენიჭება გამოყენებული ტექნიკური საშუალებების მახასიათებლებსაც[384]. ამ თვალსაზრისით სხვადასხვა საკითხებს უნდა მიექცეს ყურადღება, მაგალითად, გამოყენებული ტექნიკური საშუალება რამდენად არის დაკავშირებული სხვა ტექნოლოგიურ საშუალებასთან, ვის აქვს წვდომა მოპოვებულ ინფორმაციაზე, რა ხანგრძლივობით იქნა გამოყენებული ფარული მეთვალყურეობის ტექნიკური საშუალებები.[385] იურიდიულ ლიტერატურაში გამოთქმული მოსაზრების თანახმად, გამოყენებული ტექნიკური საშუალებების შესაძლებლობა უფლებაში ჩარევის ინტენსივობის კუთხით თანაზომიერების შეფასების მნიშვნელოვან საზომს წარმოადგენს.[386]

თანაზომიერების პრინციპი განსაკუთრებულ მნიშვნელობას იძენს „მასობრივი მონიტორინგის“ ღონისძიებების კონტექსტში. ასეთი ღონისძიებები მოიაზრებს კომუნიკაციის შინაარსის ან/და მაიდენტიფიცირებელი მონაცემების ტოტალურ მონიტორინგს მიზანმიმართული ხასიათის ან „გონივრული ეჭვის“ გარეშე.[387] მაგალითად, საქმეში S და მარპერი გაერთიანებული სამეფროს წინააღმდეგ (S and Marper), ადამიანის უფლებათა ევროპული სასამართლოს დიდმა პალატამ მიიჩნია, რომ დნმ-ის მონაცემების „მასობრივი, ბლანკეტური“ შენახვა წარმოადგენდა იმ პირთა პირად ცხოვრებაში „არათანაზომიერ ჩარევას“, რომელთა მონაცემების შენახვასაც ჰქონდა ადგილი[388]. სასამართლომ განსაკუთრებული მნიშვნელობა მიანიჭა იმ ფაქტს,

---

[383] *Somody B., Szabo M., D., Szekely I.,* Moving Away from The Security–Privacy Trade-off: The Use of The Test of Proportionality in Decision Support, წიგნში: Surveillance, Privacy and Security, Citizens' Perspectives, Friedewald M., Burgess J. P., Čas J., Bellanova R., Peissl W. (eds.), London, New York, 2017, 166.

[384] იქვე.

[385] იქვე.

[386] *Milaj J.,* Privacy, Surveillance, and The Proportionality Principle: The Need for A Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No 3, 2016, 115-116; *Milaj. J.,* Invalidation Data Retention Directive – Extending the Proportionality Test, Computer Law & Security Review, 31, 2015, 612-613.

[387] Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 21, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf> [15.06.2020].

[388] S and Marper v. United Kingdom, [2008], ECtHR.

რომ მონაცემები ინახებოდა განურჩევლად დანაშაულის ხასიათის ან სიმძიმისა, რომელთან დაკავშირებითაც არსებობდა პირის მიმართ ეჭვი.[389]

კომუნიკაციის მაიდენტიფიცირებელი მონაცემების „მასობრივი“, „ტოტალური“ შენახვის კონტექსტში ერთ-ერთ უმნიშვნელოვანეს საქმეს წარმოადგენს „სეიტლინგერი და სხვები ირლანდიის წინააღმდეგ“, სადაც ევროკავშირის მართლმსაჯულების სასამართლომ „მონაცემთა შენახვის შესახებ“ ევროკავშირის პარლამენტისა და საბჭოს 2006 წლის 15 მარტის N2006/24/EC დირექტივით გათვალისწინებული ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვის მარეგულირებელი ნორმები არათანაზომიერად მიიჩნია[390]. მართალია აღნიშნული დირექტივით გათვალისწინებული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა განპირობებული იყო მძიმე დანაშაულთან ბრძოლის ლეგიტიმური მიზნით, მაგრამ სასამართლოს გადაწყვეტილებას საფუძვლად დაედო ის ფაქტი, რომ კომუნიკაციის მაიდენტიფიცირებელი მონაცემის მასობრივი, ბლანკეტური შენახვა - „ნებისმიერი მონაცემის, ნებისმიერი პირის შესახებ და ასევე ნებისმიერი საშუალების გამოყენებით, ყოველგვარი დიფერენციაციის, შეზღუდვის და გამონაკლისის გარეშე“, - იწვევდა მთელი ევროპული მოსახლეობის პირად ცხოვრებაში ჩარევას, მათ შორის, ისეთი პირების, რომელთან დაკავშირებითაც არ არსებობდა ეჭვის საფუძველი, რომ თუნდაც არაპირდაპირი კავშირი ჰქონდათ მძიმე დანაშაულთან.[391]

თანაზომიერების პრინციპთან შესაბამისობის კონტექსტში უნდა შეფასდეს ასევე შემთხვევა, როდესაც ადგილი აქვს ერთი პირის მიმართ რამდენიმე საგამოძიებო მოქმედების, მათ შორის, ფარული საგამოძიებო მოქმედების, განხორციელებას. გერმანიის ფედერალური სასამართლოს განმარტებით, სხვადასხვა საგამოძიებო ღონისძიების ერთობლივი განხორციელება „პიროვნების სრული პროფილის” შესაქმნელად, შესაძლოა, უკვე თავისთავად არ აკმაყოფილებდეს თანაზომიერების პრინციპის კრიტერიუმებს.[392] ამ დროს ადგილი აქვს პირის ე.წ. „ტოტალურ

[389] იქვე.
[390] Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice.
[391] იქვე, 58.
[392] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 108-109, იხ. ციტირება: BGH, NStZ 2001, 386, 388 f.

შესწავლას", რომლის დროსაც ირღვევა ინდივიდის პირადი ცხოვრების ძირითადი სფეროს ხელშეუხებლობა.[393]

აღსანიშნავია, რომ საქმეში უზუნი გერმანიის წინააღმდეგ (Uzun v. Germany), ევროპული სასამართლოს მიერ შეფასებულ იქნა ერთი და იმავე პირის მიმართ სხვადასხვა უწყებების მიერ ერთდროულად რამდენიმე ფარული საგამოძიებო მოქმედების ჩატარების საკითხი.[394] ამ საქმეში განმცხადებლის მიმართ გამოყენებულ იქნა მისი გადაადგილების მონიტორინგის ღონისძიება ავტომანქანაზე დამაგრებული GPS ტექნოლოგიის საშუალებით, ასევე ამ საგამოძიებო მოქმედების განხორციელებამდე მის მიმართ ჩატარებულ იქნა ერთდროულად თითქმის ერთი და იმავე ფარული საგამოძიებო მოქმედებები ორი სხვადასხვა საგამოძიებო უწყების მიერ. თუმცა ამ საქმეში სასამართლომ იმსჯელა მხოლოდ GPS ტექნოლოგიის გამოყენებით განმცხადებლის გადაადგილების მონიტორინგის ღონისძიების კონვენციის მე-8 მუხლთან შესაბამისობაზე, იქედან გამომდინარე, რომ სწორედ ეს ღონისძიება გახადა სადავოდ განმცხადებელმა[395].

სასამართლომ ორი სხვადასხვა უწყების მიერ განმცხადებლის მიმართ ერთი და იმავე ფარული მეთვალყურეობის ღონისძიებების გამოყენების ფაქტი პირადი ცხოვრების უფლებაში მომეტებულად მძიმე ჩარევის ფორმად შეაფასა, იმ არგუმენტზე დაყრდნობით, რომ ამ შემთხვევაში პირადი ხასიათის ინფორმაციაზე წვდომა უფრო მეტ პირს აქვს[396]. სასამართლოს განმარტებით, ასეთ პირობებში, მიმდინარე ფარული საგამოძიებო მოქმედებების პარალელურად, GPS ტექნოლოგიის გამოყენებით პირის გადაადგილების მონიტორინგი საჭიროებდა ჩატარების უფრო მყარ საფუძვლებს. მიუხედავად ამისა, სასამართლომ ხაზი გაუსვა იმ გარემოებას, რომ GPS-ის გამოყენებით ავტომანქანის გადაადგილების მონიტორინგი განხორციელდა შედარებით ხანმოკლე დროის განმავლობაში (3 თვე), ამასთან, განმცხადებლის ვიზუალური მეთვალყურეობა ხორციელდებოდა მხოლოდ შაბათ-კვირას და ასევე მხოლოდ მაშინ, როდესაც ამ მანქანით გადაადგილდებოდა. შესაბამისად, მიიჩნია,

[393] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 108-109, იხ. ციტირება: *Steinmetz,* NStZ 2001, 344, 345; *Talaska,* Der Richtervorbehalt, 2007, S. 47.

[394] Uzun v. Germany, [2015], ECtHR.

[395] იქვე.

[396] იქვე, 77-80.

რომ განმცხადებლის მისამართით არ განხორციელებულა „სრული“ და „ტოტალური შესწავლა“[397]. სასამართლომ ასევე არსებითი მნიშვნელობა მიანიჭა იმ ფაქტს, რომ მოცემულ შემთხვევაში გამოძიება მიმდინარეობდა განსაკუთრებული სიმძიმის დანაშაულებთან დაკავშირებით, კერძოდ, დაბობმბვის გზით პოლიტიკოსების და სამოქალაქო პირების მკვლელობის მცდელობის რამდენიმე ეპიზოდთან დაკავშირებით[398]. ამავდროულად, ასევე მხედველობაში მიიღო ის გარემოება, რომ GPS ტექნოლოგიის გამოყენებით პირის გადაადგილების მონიტორინგის განხორციელებამდე თავდაპირველ ეტაპზე გამოყენებულ იქნა უფრო ნაკლებად ინტენსიური საგამოძიებო მოქმედებები, თუმცა აღნიშნული წარუმატებელი აღმოჩნდა. ყოველივე აღნიშნულის გათვალისწინებით, დადგინდა, რომ GPS-ის მეშვეობით განმცხადებლის გადაადგილების მონიტორინგის ღონისძიება წარმოადგენდა ლეგიტიმური მიზნის მიღწევის პროპორციულ საშუალებას.[399]

დასკვნის სახით მოცემულ საკითხთან დაკავშირებით შეიძლება ითქვას, რომ როდესაც ერთდროულად გამოიყენება რამდენიმე ფარული საგამოძიებო მოქმედება, თანაზომიერების საკითხის გადასაწყვეტად მნიშვნელოვანია, თუ რამდენად ხდება პიროვნების „ტოტალური“, “სრულფასოვანი“ შესწავლა ფარული მეთვალყურეობის შედეგად.[400] გერმანიის ფედერალური საკონსტიტუციო სასამართლოს გადაწყვეტილებიდან გამომდინარე, სახელმწიფო ორგანოების მიერ პირის „სრულყოფილი პერსონალური პროფილის“ შედგენა, რომელიც ავლენს პირის „კუმულაციური საქმიანობის დეტალებს”, წინააღმდეგობაში მოდის პირადი ცხოვრების უფლებასთან.[401] უზუნის საქმიდან გამომდინარე, შეიძლება ითქვას, რომ ყურადღება ექცევა ასევე ისეთ გარემოებებს, როგორიცაა, მაგალითად, დანაშაულის სიმძიმე, ღონისძიების ხანგრძლივობა, რაც უფლებაში ჩარევის ინტენსივობის განმსაზღვრელია, სხვა ნაკლებად მძიმე ღონისძიების გამოყენების ფაქტი.

---

[397] იქვე.
[398] იქვე.
[399] იქვე.
[400] აღნიშნულ საკითხთან დაკავშირებით იხ. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 108-109.
[401] *Jacoby N.,* Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States, Georgia Journal of International and Comparative Law, Vol. 35, No.3, 2007, 483.

2.3.2. თანაზომიერების პრინციპი ევროპული სასამართლოს პრაქტიკაში

მართალია თანაზომიერების პრინციპი არ არის კონვენციაში სახელდებით მოხსენიებული, მაგრამ პირადი ცხოვრების უფლებაში ჩარევის შეფასებისას ევროპული სასამართლოს ერთ-ერთი ძირითადი საზომი და ხშირ შემთხვევაში გადამწყვეტი ფაქტორია.[402] აღსანიშნავია, ისიც, რომ "თანაზომიერების" ამომწურავი დეფინიცია სასამართლოს პრაქტიკაში არ არის ჩამოყალიბებული და ის საკმაოდ კომპლექსური ცნებაა.[403] თანაზომიერების მოთხოვნას და მის შემადგენელ ელემენტებს ევროპული სასამართლო „დემოკრატიულ საზოგადოებაში აუცილებლობის" ტესტის ქვეშ განიხილავს - ევროპული სასამართლოს პრეცედენტული სამართლის მიხედვით, კონვენციის მე-8 მუხლით უზრუნველყოფილი პირადი ცხოვრების უფლებაში ჩარევა უნდა იყოს "აუცილებელი დემოკრატიულ საზოგადოებაში."[404] ჩარევა ჩაითვლება "დემოკრატიულ საზოგადოებაში აუცილებლად", როდესაც ემსახურება ლეგიტიმურ მიზანს, გამოწვეულია „გადაუდებელი სოციალური საჭიროებით", პროპორციულია მისაღწევი ლეგიტიმური მიზნის და ეროვნული კანონმდებლობით გათვალისწინებული ჩარევის საფუძვლები საკმარისი და რელევანტურია.[405] კონვენციის მე-10 მუხლის კონტექსტში ევროპულმა სასამართლომ აღნიშნა, რომ „აუცილებლობა" არ არის „გარდაუვალის" სინონიმი, თუმცა არც ისეთი მოქნილი მნიშვნელობის მატარებელია როგორც „დასაშვები", „სასარგებლო", „გონივრული" ან თუნდაც „სასურველი", არამედ უნდა პასუხობდეს „მწვავე სოციალურ საჭიროებას."[406]

როგორც უკვე აღინიშნა, თანაზომიერების პრინციპის ძირითადი ასპექტი კონფლიქტური ინტერესების დაბალანსებაში მდგომარეობს. საქმეში S და მარპერი გაერთიანებული სამეფოს წინააღმდეგ (S and Marper v. United Kingdom) ევროპულმა სასამართლომ აღნიშნა, რომ კონვენციის მე-8 მუხლის დაცული სფერო

[402] *Galetta A., Hert P. D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht law review, Vol. 10, No 1, 2014, 70.

[403] იქვე.

[404] *Hert P. D.,* Balancing Security and Liberty within The European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11, Utrecht L. Rev. Vol. 1, No 1, 2005, 80, 91-92.

[405] იქვე. 91-92.

[406] იქვე. 91.

„გაუმართლებლად შესუსტდება", თუკი თანამედროვე ტექნოლოგიური საშუალებები სისხლის სამართლის მართლმსაჯულების სისტემაში დაშვებული იქნება „ნებისმიერ ხარჯზე", მათი ფართო გამოყენებით მიღებული სარგებლისა და პირადი ცხოვრების ინტერესის სამართლიანი დაბალანსების გარეშე.[407] საჯარო და კერძო ინტერესების დაბალანსების პროცესში ეროვნულ ორგანოებს მინიჭებული აქვთ მიხედულობის გარკვეული ფარგლები[408]. ასეთი დისკრეციის ზღვარი დამოკიდებულია სხვადასხვა ფაქტორებზე, მათ შორის, კონვენციით გათვალისწინებული უფლების ხასიათზე, ინდივიდისთვის მის მნიშვნელობაზე, ჩარევის ხარისხსა და მისაღწევ ლეგიტიმურ მიზანზე[409]. დისკრეციის ფარგლები უფრო ვიწროა, როდესაც საქმე ეხება უფლებას, რომლით სარგებლობაც გადამწყვეტია ინდივიდისთვის ძირითადი უფლებებით ეფექტიანი სარგებლობის თვალსაზრისით.[410]

საქმეში კლასი გერმანიის წინააღმდეგ (Klass v. Germany) დადგენილი სტანდარტის მიხედვით, „მოქალაქეთა საიდუმლო თვალთვალის უფლებამოსილება დასაშვებია მხოლოდ იმ შემთხვევებში, როდესაც იგი მკაცრად აუცილებელია დემოკრატიული ინსტიტუტების დაცვის მიზნით."[411] მაგალითად, ამავე საქმეში ევროპულმა სასამართლომ მიიჩნია, რომ ტერორიზმი და ჯაშუშობის დახვეწილი ფორმები წარმოადგენს სერიოზულ საფრთხეს დემოკრატიული წყობილებისთვის და შესაბამისად, ამართლებს ფარული მეთვალყურეობის ღონისძიებების გამოყენების საჭიროებას.[412]

საქმეში საბო და ვისი უნგრეთის წინააღმდეგ (Dzabo Vissy v. Hungary), ევროპულმა სასამართლომ მინიშნება გააკეთა კლასის საქმეში გამოყენებულ „მკაცრი აუცილებლობის ტესტზე" და აღნიშნა, რომ ერთი შეხედვით, ხსენებული ტერმინი - „მკაცრი აუცილებლობა" თითქოს უნდა წარმოადგენდეს „დემოკრატიულ საზოგადოებაში აუცილებლობის" მოთხოვნისგან განსხვავებულ ტესტს, თუმცა ფარული მეთვალყურეობის შედეგად პირადი ცხოვრების სფეროში ჩარევის

[407] S and Marper v. United Kingdom, [2008], ECtHR, 112.
[408] იქვე, 101-102.
[409] იქვე.
[410] იქვე.
[411] *კილკელი უ.,* პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის განხორციელება, გზამკვლევი, *(რედ.),* ევროპის საბჭო, თბ., 2005, 117-118.
[412] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.).

განსაკუთრებული ხასიათიდან და ფარული თვალთვალის ტექნოლოგიების დამახასიათებელი უფლების შეზღუდვის მაღალი პოტენციალიდან გამომდინარე, „დემოკრატიულ საზოგადოებაში აუცილებლობის“ ტესტი უნდა იქნეს ინტერპრეტირებული როგორც „მკაცრი აუცილებლობის“ მნიშვნელობის მატარებელი შემდეგ კონტექსტში: „მკაცრად აუცილებელი“ უნდა იყოს ერთის მხრივ, ზოგადად დემოკრატიული საფუძვლების უზრუნველსაყოფად, ხოლო მეორე მხრივ, კონკრეტულ სიტუაციაში სასიცოცხლო მნიშვნელობის ინფორმაციის მოპოვების მიზნით.[413]

იურიდიულ ლიტერატურაში გამოთქმული მოსაზრების თანახმად, თანაზომიერების პრინციპის განსაზღვრის დროს ევროპული სასამართლო განსაკუთრებულ ყურადღებას უთმობს განხორციელებული ღონისძიების ხასიათს (მისი მასშტაბი, ზოგადია თუ აბსოლუტური, მისი საზიანო შედეგები, უფლების ბოროტად გამოყენების პოტენციალი), შეეძლო თუ არა სახელმწიფოს უფრო ნაკლებად ინტენსიური ზომების გატარება, ხომ არ აქვს ადგილი ისეთი პირის მონაწილეობას, რომლის შემთხვევაშიც უფლების შეზღუდვა უფრო მძიმე ხასიათისაა და რამდენად არსებობს საქმეში გარანტიები, რომლებსაც შეუძლია უფლების შეზღუდვის კომპენსირება.[414]

აღსანიშნავია, რომ იურიდიულ ლიტერატურაში კრიტიკა არის გამოთქმული იმასთან დაკავშირებით, რომ ევროპულ სასამართლოს არ აქვს შემუშავებული „კარგად ჩამოყალიბებული პრაქტიკა“ „დემოკრატიულ საზოგადოებაში აუცილებლობის“ ტესტთან მიმართებით.[415] მიუხედავად იმისა, რომ სასამართლოს პრეცედენტული სამართალი ასრულებს მნიშვნელოვან სახელმძღვანელო როლს ამ მოთხოვნის დასადგენად, ზოგიერთი ავტორი აღნიშნავს, რომ “აუცილებლობის ტესტის“ შინაარსი

[413] Szabo and Vissy v. Hungary, [2016] ECtHR, 73.

[414] *Hert P. D.,* Balancing Security and Liberty within The European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11, Utrecht L. Rev. Vol. 1, No 1, 2005, 80, იხ. ციტირება: *M. Delmas-Marty*, The European Convention for the Protection of Human Rights, Dordrecht, 1992, 71.

[415] *Hert P. D.,* Balancing Security and Liberty within The European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11, Utrecht L. Rev., Vol. 1, No 1, 2005, 92.

მაინც „ბუნდოვან“ და „განუსაზღვრელ“ ცნებად რჩება.[416] აღნიშნული ახსნილია იმ გარემოებით, რომ არ არსებობს მკაფიოდ ჩამოყალიბებული, ფიქსირებული ბალანსი ინტერესთა შორის კონვენციის მე-8 მუხლთან მიმართებით და ამასთან, წესები და გამონაკლისები არ არის წინასწარ განსაზღვრული.[417] ასევე გამოთქმულია მოსაზრება იმასთან დაკავშირებით, რომ სასამართლოს პრაქტიკაში საკმარისად არ არის განვითარებული სუბსიდიარულობის პრინციპი [ნაკლებად შემზღუდველი საშუალებების ტესტი] - ძირითად შემთხვევაში მე-8 მუხლთან დაკავშირებულ საქმეებში სასამართლო არ ეყრდნობა ამ კრიტერიუმს.[418] თუმცა, აღსანიშნავია, რომ ბოლოდროინდელ საქმეებში სუბსიდიარულობის პრინციპს დიდი ყურადღება დაეთმო ევროპული სასამართლოს პრაქტიკაში.[419]

თანაზომიერების პრინციპიდან გამომდინარეობს, რომ საკანონმდებლო დონეზე ფუნქციონირებდეს სისტემა, რომელიც უზრუნველყოფს ფარული საგამოძიებო მოქმედებების გამოყენებას მხოლოდ მკაცრად აუცილებელ შემთხვევებსა და შესაფერისი პროცედურული გარანტიების პირობებში. ამასთან, ფარული მეთვალყურეობის ღონისძიების თანაზომიერება ყოველ კონკრეტულ შემთხვევაში უნდა შეფასდეს საქმის ინდივიდუალური გარემოებებიდან გამომდინარე.[420]

„დემოკრატიულ საზოგადოებაში აუცილებლობის“ ტესტის განმარტებასთან დაკავშირებით ევროპული სასამართლოს მიერ დადგენილი პრაქტიკის თანახმად, საჯარო და კერძო ინტერესების დაბალანსების პროცესში სახელმწიფოები სარგებლობენ მიხედულობის გარკვეული ფარგლებით, ეროვნული ინტერესების

---

[416] *Galetta A., Hert P. D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht L. Rev., Vol. 10, No 1, 2014, 67, იხ. ციტირება: *S. Greer,* The exceptions to Articles 8 to 11 of the European Convention of Human Rights, 1997 *Human Rights Files*, no.15, Council of Europe Publishing. აღნიშნულ საკითხთან დაკავშირებით იხ. ასევე *Murphy, M. H.,* The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases, 3(2) Irish Journal of Legal Studies, 2013, 75.

[417] *Galetta A., Hert P. D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht L. Rev., Vol. 10, No 1, 2014, 67.

[418] *Hert P. D.,* Balancing Security and Liberty within The European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11, Utrecht L. Rev., Vol. 1, No 1, 2005, 93.

[419] იხ. მაგალითად, Dragojević v. Croatia, [2015], ECtHR, Liblik and others v. Estonia, [2019], ECtHR, Matanović v. Croatia, [2017], ECtHR, Mustafa Sezgin Tanrikulu v. Turkey, [2017], ECtHR.

[420] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 9 (ბმული იხ. მე-80 გვერდზე).

დაცვის მიზნით აირჩიონ გარკვეული ღონისძიება[421]. თუმცა ეროვნული ორგანოებისათვის მინიჭებული დისკრეციის ეს ზღვარი ექვემდებარება ევროპული სასამართლოს მხრიდან ზედამხედველობას[422]. იქედან გამომდინარე, რომ ფარული მეთვალყურეობის სისტემას დემოკრატიის დაცვის მოტივით შეუძლია თავადვე გამოუთხაროს ძირი დემოკრატიულ საფუძვლებს, აუცილებელია ევროპული სასამართლო დარწმუნდეს, რომ შიდა კანონმდებლობით უზრუნველყოფილია თვითნებობისგან დაცვის საკმარისი და ეფექტიანი გარანტიები[423]. ამ თვალსაზრისით შეფასების დროს მხედველობაში მიიღება საქმის ყველა გარემოება, როგორიცაა, მაგალითად, „სავარაუდო ღონისძიების ხასიათი, ხანგრძლივობა და ფარგლები, მისი ჩატარების საფუძვლები, მის ჩატარებაზე ნებართვის გამცემი, განმახორციელებელი და ზედამხედველობაზე კომპეტენტური ორგანოები და გასაჩივრების საშუალებები.“[424]

ქვემოთ განხილული იქნება თანაზომიერების პრინციპის შეფასების მიზნით რელევანტური თითოეული ეს კონკრეტული პროცედურული გარანტია ევროპული სასამართლოს პრაქტიკისა და სხვა საერთაშორისო სტანდარტების მიხედვით.

2.4. შეჯამება

კომუნიკაციის მონიტორინგის ღონისძიებების ფარული ხასიათი ხელისუფლების ორგანოთა მხრიდან უფლებამოსილების ბოროტად გამოყენების მეტ რისკთანაა დაკავშირებული, რაც თავის მხრივ, დღის წესრიგში აყენებს ხელმისაწვდომობისა და სამართლებრივი სიცხადის მოთხოვნების დაცვის აუცილებლობას შესაბამისი საკითხების რეგულირების დროს. კანონის ხელმისაწვდომობის კრიტერიუმიდან გამომდინარე, აუცილებელია იმ სამართლებრივი აქტის საჯაროდ ხელმისაწვდომობა, რომელსაც შეუძლია გავლენა მოახდინოს ინდივიდების პირადი ცხოვრების ინტერესებზე. ხოლო კანონის განჭვრეტადობის კრიტერიუმის მიხედვით, ეროვნული კანონმდებლობა უნდა იყოს

[421] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49-50; Kennedy v. United Kingdom, [2010] ECtHR, 153; Roman Zakharov v. Russia, [2015] ECtHR, 232. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 106.

[422] იქვე.

[423] იქვე.

[424] იქვე.

საკმარისად ნათელი, რათა მოქალაქეებს, ჰქონდეთ მის შესაბამისად საკუთარი ქმედებების წარმართვის შესაძლებლობა. განჭვრეტადობის მოთხოვნის შესაბამისად, „საკმარისი სიცხადით“ უნდა განისაზღვროს აღმასრულებელი ხელისუფლების ორგანოების დისკრეციის ფარგლები და განხორციელების წესი.

თანაზომიერების პრინციპი წარმოადგენს სახელმძღვანელო ტესტს ფარული თვალთვალის უფლებამოსილების პრაქტიკაში განხორციელებლად. აღნიშნული პრინციპიდან გამომდინარე, ძირითად უფლებაში ნებისმიერი ჩარევა უნდა პასუხობდეს შესაფერისობის, აუცილებლობისა და ვიწრო გაგებით პროპორციულობის მოთხოვნებს. თანაზომიერების პრინციპიდან გამომდინარეობს სხვადასხვა პროცედურული გარანტიების გათვალისწინების აუცილებლობა ფარულ საგამოძიებო მოქმედებებთან მიმართებით, როგორიცაა მაგალითად, ღონისძიების ჩატარებაზე ნებართვის გაცემა დამოუკიდებელი ორგანოს მიერ, საზედამხედველო მექანიზმები, შეტყობინების ვალდებულება, მოთხოვნები ფარული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე შუამდგომლობის და სასამართლოს განჩინების მიმართ, მტკიცებულებითი სტანდარტი, გამოყენებული ტექნიკური საშუალებების პოტენციალი უფლებაში ჩარევის კუთხით და სხვ.

ევროპული სასამართლოს პრაქტიკის მიხედვით, ფარული საგამოძიებო მოქმედების თანაზომიერება საქმის კონკრეტული გარემოებების მიხედვით იზომება. შეფასების დროს მხედველობაში მიიღება, მათ შორის, სავარაუდო ღონისძიების ხასიათი, ხანგრძლივობა და ფარგლები, მისი ჩატარების საფუძვლები, მის ჩატარებაზე ნებართვის გამცემი, განმახორციელებელი და ზედამხედველობაზე კომპეტენტური ორგანოები, გასაჩივრების საშუალებები.

3. ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და გამოყენების სფეროში შემუშავებული კონკრეტული საპროცესო-სამართლებრივი გარანტიები

3.1. ფარული მეთვალყურეობის ღონისძიების ჩატარების ფარგლები

ევროპული სასამართლოს პრაქტიკის მიხედვით, ეროვნულმა კანონმდებლობამ უნდა განსაზღვროს ფარული მეთვალყურეობის ღონისძიების გამოყენების ფარგლები, რათა მოქალაქეებს ჰქონდეთ ინფორმაცია სახელმწიფოს მიერ ასეთი ღონისძიების

შესაძლო გამოყენების სამართლებრივი წინაპირობების შესახებ[425]. აღნიშნული მოიცავს ორ ელემენტს – დანაშაულებს, რომელთა შემთხვევაში დასაშვებია ფარული საგამოძიებო მოქმედების განხორციელება და პირებს, რომელთა მიმართაც შესაძლებელია მათი ჩატარება.[426]

3.1.1. დანაშაულები, რომელთა შემთხვევაშიც დასაშვებია ფარული მეთვალყურეობის ღონისძიების გამოყენება

კანონის განჭვრეტადობის პრინციპი სახელმწიფოს არ აკისრებს ვალდებულებას, ეროვნულ კანონმდებლობაში გაითვალისწინოს იმ დანაშაულთა ამომწურავი ჩამონათვალი, რომელთა შემთხვევაშიც გამოიყენებს კომუნიკაციებზე მონიტორინგის ბერკეტს, თუმცა კანონმდებლობამ საკმარისი სიცხადით უნდა განსაზღვროს აღნიშნულ დანაშაულთა კატეგორია.[427]

საერთაშორისო სტანდარტის მიხედვით, ფარული მეთვალყურეობის ღონისძიებების გამოყენება დასაშვებია მხოლოდ „მძიმე დანაშაულთა“ წინააღმდეგ.[428] ამასთან, განჭვრეტადობის პრინციპიდან გამომდინარე, კანონმდებლობა საკმარისად მკაფიოდ უნდა არეგულირებდეს ასეთ დანაშაულთა ცნებებს. ცხადია, სახელმწიფო თვითონ განსაზღვრავს, რომელ დანაშაულებს მოიაზრებს თავის კანონმდებლობაში ამ კატეგორიების ქვეშ, თუმცა თანაზომიერების პრინციპიდან გამომდინარე, ის იზღუდება გარკვეული ფარგლებით კომუნიკაციის მონიტორინგის გამოსაყენებლად შესაძლო დანაშაულთა წრის განსაზღვრის დროს, რაც გულისხმობს იმას, რომ ფარული მეთვალყურეობის ღონისძიებას, როგორც საგამონაკლისო და უკიდურესად მაღალი ინტენსივობით უფლებაშემზღუდველ ქმედებას, მხოლოდ სერიოზული ლეგიტიმური მიზანი გაამართლებს.

აღნიშნულის საილუსტრაციოდ საინტერესო საქმეს წარმოადგენს იორდაჩი მოლდოვის წინააღმდეგ (Iordachi v. Moldova), სადაც ევროპულმა სასამართლომ გააკრიტიკა მოლდოვის სამართლებრივი დებულებები, რომლებიც ფარული

[425] Roman Zakharov v. Russia, [2015] ECtHR, 243.
[426] იქვე.
[427] Kennedy v. United Kingdom, [2010], ECtHR, 149.
[428] Iordachi and others v. Moldova, [2009], ECtHR, 51; Recommendation No R (95) 13 of The Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology, Council of Europe, 11.09.1995, <https://rm.coe.int/native/09000016804f6e76> [20.06.2020].

მეთვალყურეობის ღონისძიების გამოყენების შესაძლებლობას იძლეოდა „მძიმე, ძალზე მძიმე და განსაკუთრებით მძიმე დანაშაულების“ წინააღმდეგ[429]. მართალია, ასეთ დანაშაულთა ცნება ეროვნულ კანონმდებლობაში ამომწურავად იყო განმარტებული, მაგრამ სისხლის სამართლის კოდექსით გათვალისწინებულ დანაშაულთა ნახევარზე მეტი აღნიშნულ კატეგორიაში ექცეოდა.[430] ამდენად, ეროვნულ კანონმდებლობაში “მძიმე დანაშაულის” ცნების იმგვარად ფართოდ განმარტება, რომელიც სისხლის სამართლის კოდექსით გათვალისწინებულ დანაშაულთა უმეტესობას აღნიშნული ცნების ქვეშ განიხილავს, წინააღმდეგობაში მოდის თანაზომიერების პრინციპთან, ვინაიდან მოცემული პრინციპი მოითხოვს ადამიანის პირადი ცხოვრების შეზღუდვას საგამონაკლისო ღონისძიების სახით, მხოლოდ მნიშვნელოვანი საჯარო ინტერესის დაცვის საბაბით.

3.1.2. პირთა კატეგორია, რომელთა მიმართ დასაშვებია ფარული მეთვალყურეობის ღონისძიების გამოყენება

როგორც უკვე აღინიშნა, ეროვნულმა კანონმდებლობამ მკაფიოდ უნდა განსაზღვროს იმ პირთა კატეგორია, რომელთა მიმართაც დაიშვება ფარული მეთვალყურეობის განხორციელება. ევროპული სასამართლოს კრიტიკას, როგორც წესი, იმსახურებს კანონმდებლობაში ზოგადი ჩანაწერები, რომლებიც აღნიშნული პირთა წრის შეუზღუდავი ინტერპრეტაციის საშუალებას იძლევა. მაგალითად, ერთ-ერთ საქმეში ევროპულმა სასამართლომ მოცემული მოთხოვნა დარღვეულად მიიჩნია, როდესაც შიდა კანონმდებლობით ფარული მეთვალყურეობის ღონისძიების ჩატარება დაიშვებოდა ეჭვმიტანილების, ბრალდებულების და „დანაშაულებრივ ქმედებაში ჩაბმული სხვა პირების წინააღმდეგ.“[431] ეს უკანასკნელი ტერმინი საკმარისი სიცხადით ვერ უზრუნველყოფდა იმ პირების განსაზღვრას, რომლებიც სახელმწიფოს მხრიდან ფარული დაკვირვების ობიექტები შეიძლება გამხდარიყვნენ.[432]

ანალოგიური მიდგომა გამოხატა სასამართლომ საქმეში ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia), სადაც რუსეთის კანონმდებლობის მიხედვით,

[429] Iordachi and others v. Moldova, [2009], ECtHR, 43-44.
[430] იქვე.
[431] იქვე, 44.
[432] იქვე.

კომუნიკაციის მონიტორინგი ეჭვმიტანილების და ბრალდებულების გარდა, ასევე დაიშვებოდა იმ პირების წინააღმდეგ, რომლებიც შესაძლოა ფლობდნენ დანაშაულთან დაკავშირებულ მონაცემებს ან სისხლის სამართლის საქმისთვის რელევანტურ სხვა ინფორმაციას[433]. ევროპული სასამართლო ზოგადად არ არის კომუნიკაციის მონიტორინგის ღონისძიებების გამოყენების წინააღმდეგი იმ პირთა მიმართ, რომლებიც არ არიან ბრალდებულები, თუმცა შესაძლოა ფლობდნენ გამოძიებისათვის რელევანტურ ინფორმაციას.[434] თუმცა მოცემულ შემთხვევაში სასამართლოს უკმაყოფილება გამოიწვია რუსეთის კანონმდებლობაში სამართლებრივი დათქმების ან შესაბამისი პრეცედენტული სამართლის არარსებობამ იმასთან დაკავშირებით, თუ როგორ უნდა განმარტებული პრაქტიკაში ცნებები – „პირები, რომლებიც შესაძლოა ფლობდნენ დანაშაულთან დაკავშირებულ ინფორმაციას" ან „სისხლის სამართლის საქმისთვის რელევანტურ სხვა ინფორმაციას."[435]

ევროსასამართლოს პრეცედენტული სამართლის მიხედვით, იმ პირის კომუნიკაციის მონიტორინგი, რომელთან დაკავშირებითაც არ არსებობს დანაშაულის ჩადენის თაობაზე ეჭვი, თუმცა შესაძლოა ფლობდეს ამ დანაშაულის შესახებ ინფორმაციას, შესაძლოა გამართლებულად ჩაითვალოს, იმ პირობით, რომ მის ჩატარებაზე ნებართვის გაცემა და ზედამხედველობა ხორციელდება სასამართლოს მიერ და შემდგომში ღონისძიების ადრესატს ეცნობება მის მიმართ განხორციელებული საგამოძიებო მოქმედების შესახებ.[436]

ზახაროვის საქმისგან განსხვავებით, სხვა შემთხვევაში ევროპულმა სასამართლომ პირადი ცხოვრების უფლების დაცვის მოთხოვნებთან შესაბამისად მიიჩნია ეროვნული საკანონმდებლო რეგულაციები, რომლებიც საკმარისი სიცხადით განმარტავდნენ ფარული მეთვალყურეობას დაქვემდებარებულ პოტენციურ პირთა წრეს – „ბრალდებული ან პირი, რომელთან დაკავშირებითაც ნათელ ფაქტობრივ გარემოებებზე დაყრდნობით საგამოძიებო ორგანომ შესაძლოა დაასკვნას, რომ იღებს

[433] Roman Zakharov v. Russia, [2015] ECtHR, 245.
[434] Greuter v. the Netherlands, [2002], ECtHR.
[435] Roman Zakharov v. Russia, [2015] ECtHR, 249.
[436] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08.2019, 108, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>, [18.06.2020], იხ. ციტირება: Greuter v. the Netherlands, [2002], ECtHR.

ან გადასცემს ბრალდებულისთვის განკუთვნილ კომუნიკაციას ან ბრალდებული იყენებს მის ტელეფონს."[437]

საინტერესოა ასევე ევროპული სასამართლოს პოზიცია „შემთხვევითი" პირების კომუნიკაციის მოსმენის საკითხთან დაკავშირებით. ამ თვალსაზრისით აღსანიშნავია საქმე ამანი შვეიცარიის წინააღმდეგ (Amman v. Switzerland), სადაც ევროპულმა სასამართლომ დაადგინა კანონიერების პრინციპის დარღვევა, ვინაიდან შვეიცარიის კანონმდებლობა არ არეგულირებდა იმ პირების სატელეფონო კომუნიკაციის ფარული მიყურადების საკითხს, რომლებსაც „შემთხვევით" მოუსმინეს, როგორც კანონმდებლობის შესაბამისად მიყურადებული სატელეფონო საუბრის მონაწილეებს[438]. სასამართლომ ყურადღება გაამახვილა იმ ფაქტზე, რომ ეროვნული კანონმდებლობა არ ითვალისწინებდა რაიმე ზომების გათვალისწინების მოთხოვნას ასეთ პირებთან მიმართებით. შესაბამისად, საკმარისი სიცხადით არ იყო განსაზღვრული შესაბამისი ორგანოების დისკრეციის ფარგლები და პირობები ამ საკითხთან დაკავშირებით.[439]

3.2 ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის დაცვა

ადვოკატსა და კლიენტს შორის გაცვლილი ინფორმაციის კონფიდენციალურობის დაცვა კონვენციის მე-6 მუხლით განმტკიცებული სამართლიანი სასამართლოს უფლებიდან იღებს სათავეს და აღნიშნული მუხლით უზრუნველყოფილ ერთ-ერთ ფუნდამენტურ გარანტიას წარმოადგენს.[440] ბრალდებულს აქვს თავის დამცველთან კომუნიკაციის უფლება მესამე პირების მხრიდან მოსმენის გარეშე[441], ისეთ პირობებში, რომელიც იძლევა ინფორმაციის თავისუფლად გაცვლის შესაძლებლობას.[442] ბრალდებულისთვის თავისი ადვოკატისგან კონფიდენციალური ინსტრუქციების მიღების შესაძლებლობის წართმევა პრაქტიკულ ღირებულებას დაუკარგავდა უფლებას სამართლებრივ

[437] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 51.
[438] Amman v. Switzerland, [2000], ECHR 2000-II, 61.
[439] იქვე.
[440] Khodorkovskiy and Lebedev v. Russia, [2013], ECtHR, 627.
[441] იქვე. 629.
[442] Campbell v. United Kingdom, [1992], ECtHR, (Series A no. 233), 46.

დახმარებაზე.[443] ბრალდებულსა და ადვოკატს შორის გაცვლილი ინფორმაციის კონფიდენციალურობა ვრცელდება ნებისმიერი გზით, მათ შორის, ელექტრონული კომუნიკაციის საშუალებებით გაცვლილ ინფორმაციაზე. ბრალდებულსა და ადვოკატს შორის კომუნიკაციის კონფიდენციალურობის უფლებაში ჩარევა ევროპული სასამართლოს პრეცედენტულ სამართალში პირადი ცხოვრების უფლებაში ჩარევად განიხილება, თუმცა ასევე მნიშვნელოვან გავლენას ახდენს კონვენციის მე-6 მუხლით უზრუნველყოფილ სამართლიანი სასამართლოს უფლებაზე.[444]

ევროპული სასამართლოს მიერ დამკვიდრებული პრაქტიკით, ადვოკატსა და კლიენტს შორის კომუნიკაციის კონფიდენციალურობა არ ვრცელდება იმ კომუნიკაციაზე, რომელიც ეხება ადვოკატის დანაშაულებრივ საქმიანობას[445]. მიუხედავად იმისა, რომ ადვოკატსა და ბრალდებულს შორის ურთიერთობის პრივილეგირებული დაცვა ერთ-ერთი ფუნდამენტური გარანტიაა, ის არ მიეკუთვნება აბსოლუტურ უფლებას.[446] აღნიშნული კომუნიკაციის ფარული მიყურადება გამონაკლისის სახით დასაშვებია იმ შემთხვევაში, თუკი ეს ღონისძიება უკავშირდება ადვოკატის მონაწილეობას დანაშაულში. ერთ-ერთ საქმეში ევროპულმა სასამართლომ მისაღებად მიიჩნია ეროვნული რეგულაციები, რომლებიც საგამონაკლისოდ უშვებდა ადვოკატსა და კლიენტს შორის სატელეფონო კომუნიკაციის ფარულ მიყურადებას ადვოკატის დანაშაულებრივ საქმიანობასთან დაკავშირებით. აღნიშნულ საქმეში სასამართლომ ყურადღება გაამახვილა იმ გარემოებაზე, რომ საფრანგეთის კანონმდებლობა ითვალისწინებდა ადვოკატსა და კლიენტს შორის კომუნიკაციის ხელშეუხებლობის გარანტიას და კრძალავდა ასეთი საუბრის ჩაწერას, თუნდაც მოსმენილი ყოფილიყო კანონიერად ჩატარებული ღონისძიების ფარგლებში[447]. ამ ზოგადი წესიდან საგამონაკლისო წესით დაშვებული იყო ადვოკატსა და კლიენტს შორის კომუნიკაციის ჩაწერა, თუკი საუბრის შინაარსიდან გამომდინარე, ივარაუდებოდა ადვოკატის მხრიდან დანაშაულის ჩადენა[448]. ამავდროულად, საფრანგეთის სისხლის სამართლის საპროცესო კოდექსის მიხედვით, არ დაიშვებოდა

[443] S. v. Switzerland, [1991], ECtHR, (Series A no.220), 48; Khodorkovskiy and Lebedev v. Russia, [2013], ECtHR, 627.
[444] Khodorkovskiy and Lebedev v. Russia, [2013], ECtHR, 629.
[445] Versini-Campinchi and Crasnianski v. France, [2016], ECtHR.
[446] იქვე.
[447] იქვე.
[448] იქვე.

იმ საუბრის ჩაწერა, რომელიც დაცვის უფლებას შეეხებოდა[449]. სასამართლომ განსაკუთრებული მნიშვნელობა მიანიჭა იმ გარემოებას, რომ მოცემულ საქმეში არ დარღვეულა ბრალდებულის უფლებები - ბრალდებულსა და მის ადვოკატს შორის საუბრის ჩანაწერი, რომელიც ავლენდა დანაშაულის შესაძლო ფაქტს ადვოკატის მხრიდან, არ ყოფილა გამოყენებული ბრალდებულის წინააღმდეგ[450]. ამასთან, მაგისტრატმა მოსამართლემ საქმიდან ამორიცხა სატელეფონო მიყურადების ის ჩანაწერები, რომლებიც ეხებოდა ადვოკატის მიერ დაცვის ფუნქციის განხორციელებას.[451]

საქმეში კოპი შვეიცარიის წინააღმდეგ (Kopp v. Switzerland), ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის დასაცავად ეროვნულ კანონმდებლობაში ადეკვატური გარანტიების არარსებობის გამო. მიუხედავად შვეიცარიის კანონმდებლობაში განმტკიცებული მოთხოვნისა ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის კონფიდენციალურობასთან დაკავშირებით, აღნიშნული დებულება პრაქტიკაში რეალურად არ სრულდებოდა[452]. სასამართლოს კრიტიკა დაიმსახურა იმ გარემოებამ, რომ კანონმდებლობა არ იძლეოდა ზუსტ განმარტებებს თუ ვის მიერ, რა პირობებში და როგორ უნდა განხორციელებულიყო პრივილეგირებული ინფორმაციის [საუბარია ადვოკატსა და კლიენტს შორის განხორციელებულ ადვოკატის პროფესიულ საიდუმლოებასთან დაკავშირებულ ინფორმაციაზე] გამოცალკავება არაპრივილეგირებულისგან [კომუნიკაციის შესახებ ინფორმაცია, რომელიც არ უკავშირდება ადვოკატის პროფესიულ საქმიანობას]. პიროვნება, რომელიც პრაქტიკაში ამ ორი კატეგორიის ინფორმაციის გამოცალკავებას ახორციელებდა, მუშაობდა საფოსტო დეპარტამენტში იურისტის პოზიციაზე. ევროპული სასამართლოს მიერ უარყოფითად შეფასდა ის გარემოება, რომ ასეთ სენსიტიურ სფეროში ინფორმაციის კონფიდენციალურობის დაცვასთან დაკავშირებული ზომების მიღება სასამართლოს ყოველგვარი ზედამხედველობის

[449] იქვე.
[450] იქვე.
[451] იქვე.
[452] Kopp v. Switzerland, [1998], ECtHR, Reports 1998-II, 73-75.

გარეშე დაევალა საფოსტო დეპარტამენტის იურისტს, რომელიც აღმასრულებელი ხელისუფლების წარმომადგენელი იყო.[453]

სხვა შემთხვევაში ევროპულმა სასამართლომ მოიწონა კანონმდებლობა ადვოკატსა და კლიენტს შორის კომუნიკაციის დაცვასთან დაკავშირებით, რომლებიც განასხვავებდა ადვოკატს როგორც ეჭვმიტანილს და როგორც დამცველს[454]. მართალია, სატელეფონო კომუნიკაციის ფარული მიყურადება დაიშვებოდა, თუ ადვოკატს რაიმე დანაშაულის ჩადენაში ედებოდა ბრალი, მაგრამ მის მიერ დაცვის ფუნქციის განხორციელებასთან დაკავშირებული ინფორმაცია უნდა გამოცალკავებულიყო არაპრივილეგირებული მონაცემებისგან[455]. ადვოკატსა და კლიენტს შორის დაცული კომუნიკაციის ფარგლებში შემდგარი სატელეფონო საუბრის შედეგად მოპოვებული ინფორმაცია უნდა გაეშიფრა პროკურორს. ამასთან, პროკურორის ბრძანებით უნდა განადგურებულიყო მოპოვებული მონაცემები, რომლებიც ხვდებოდა კონფიდენციალურობის დაცვის ქვეშ, ხოლო მოსამართლის ნებართვით საქმის მასალებში შეიტანებოდა მხოლოდ არაპრივილეგირებული კომუნიკაციის შემცველი ინფორმაცია[456]. ამასთან, თუკი ეჭვმიტანილი სარგებლობდა მისი კომუნიკაციის კონფიდენციალურობის პრივილეგიით რაიმე პროფესიული საქმიანობის გამო, ეროვნული კანონმდებლობა ითვალისწინებდა შესაბამისი პროფესიული გაერთიანების (ადვოკატის შემთხვევაში - ადვოკატთა ასოციაციის) წარმომადგენლის ჩართულობას პროკურორის მიერ გადაწყვეტილების მიღების პროცესში. აღნიშნული პირი კონსულტაციას უწევდა პროკურორს იმასთან დაკავშირებით, ხვდებოდა თუ არა ეჭვმიტანილისგან მომდინარე ან მისთვის გადაცემული კომუნიკაცია კონფიდენციალურობის დაცვის ქვეშ. ამ შემთხვევაშიც, საბოლოო სიტყვა სასამართლოს ეკუთვნოდა - მხოლოდ მოსამართლე წყვეტდა, საბოლოო ჯამში, საქმის მასალებში ინფორმაციის შეტანის საკითხს.[457]

ზემოთაღნიშნულ საქმეში ხაზგასმულია კომუნიკაციის მონიტორინგის განხორციელებაზე მუდმივი სასამართლო ზედამხედველობის მნიშვნელობა და აუცილებლობა. ევროპული სასამართლოს განმარტებით, ადვოკატთან

[453] იქვე.
[454] Aalmoes and others v. The Netherlands, [2004], ECtHR.
[455] იქვე.
[456] იქვე.
[457] იქვე.

კონსულტაციით დაინტერესებული ნებისმიერი პირის ინტერესში შედის იურიდიული დახმარების მიღება თავისუფალ პირობებში[458]. სწორედ ამ მიზეზით არის ადვოკატსა და კლიენტს შორის ურთიერთობა პრივილეგირებული[459]. იმის დაშვება, რომ ადვოკატისთვის გადაცემული, ან მისგან მომდინარე ინფორმაცია, რომელიც მიეკუთვნება ადვოკატის პროფესიულ საქმიანობას, შეიძლება დაექვემდებაროს ფარულ მიყურადებას, განსაკუთრებით კი საგამოძიებო ორგანოების მხრიდან, რომლებსაც პირდაპირი დაინტერესება შეიძლება ჰქონდეთ ამ ინფორმაციის მიმართ, არ შეესაბამება კონფიდენციალურობისა და პროფესიული საიდუმლოების დაცვის პრინციპებს, რომლებითაც დაცულია კლიენტისა და ადვოკატის ურთიერთობა[460]. სწორედ აღნიშნული განაპირობებს, რომ ადვოკატებს თავიანთ კლიენტებთან პროფესიული ურთიერთობისას აქვთ თავიანთი პროფესიული საქმიანობის დაცვის გონივრული მოლოდინი.[461] იმისათვის, რათა ეს „გონივრული მოლოდინი“ იყოს დაცული, ტელეკომუნიკაციის მონიტორინგი უნდა მოექცეს ადეკვატური ზედამხედველობის ქვეშ[462]. სასამართლოს განმარტებით, მოცემულ სფეროში, მუდმივად განვითარებადი და დახვეწილი თანამედროვე ტექნოლოგიებისა და შესაბამისი ინდივიდების მხრიდან შეცდომის ან უფლებამოსილების ბოროტად გამოყენების საფრთხის გათვალისწინებით, სასურველია, საზედამხედველო ფუნქცია მოსამართლეს დაეკისროს.[463]

საქმეში იორდაჩი მოლდოვის წინააღმდეგ (Iordachi and others v. Moldova), ევროპულმა სასამართლომ აღნიშნა, რომ მართალია მოლდოვის კანონმდებლობით გათვალისწინებული იყო ადვოკატსა და კლიენტს შორის კომუნიკაციის კონფიდენციალურობის მოთხოვნა, მაგრამ კანონმდებლობა არ განსაზღვრავდა რაიმე პროცედურას, რომელიც პრაქტიკულ მნიშვნელობას შესძენდა ამ პრინციპს. არ იყო დადგენილი ნათელი წესები იმასთან დაკავშირებით, თუ რა უნდა მომხდარიყო მაგალითად, იმ შემთხვევაში, თუკი ადვოკატსა და კლიენტს შორის სატელეფონო ზარი იქნებოდა მიყურადებული.[464]

---

[458] იქვე.
[459] იქვე.
[460] იქვე.
[461] იქვე.
[462] იქვე.
[463] იქვე.
[464] Iordachi and others v. Moldova, [2009], ECtHR, 50.

საბოლოო ჯამში, შეიძლება ითქვას, რომ ევროპული სასამართლოს მიერ დადგენილი სტანდარტის მიხედვით, ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის დაცვისთვის ეროვნულ კანონმდებლობაში მხოლოდ ზოგადი დებულებების გათვალისწინება არ არის საკმარისი, არამედ აუცილებელია ქმედითი მექანიზმების უზრუნველყოფა ამ პრინციპის რეალური იმპლემენტაციის მიზნით, რაც გულისხმობს, შესაბამისი პროცედურის კონკრეტულ საკანონმდებლო რეგლამენტაციას, აღნიშნული ეხება გარემოებებს და პროცედურას, თუ როგორ უნდა მოხდეს პრივილეგირებული ინფორმაციის გამოცალკავება არაპრივილეგირებულისგან. ამასთან, ევროპული სასამართლოს პრაქტიკის შეჯამებით შეიძლება დავასკვნათ, რომ აღნიშნული პროცედურის სათანადო გარანტიების დაცვით წარმართვას ის ეროვნული სასამართლოების აუცილებელ ჩართულობას უკავშირებს. ევროპული სასამართლოს პრაქტიკაში ასევე დადებითად არის შეფასებული შესაბამისი პროფესიული გაერთიანების წარმომადგენლის, მაგალითად, ადვოკატთა ასოციაციის, მონაწილეობა მონაცემების კონფიდენციალურობის დაცვას მიკუთვნებადობის საკითხის გადაწყვეტის დროს, ასეთი დამატებითი მექანიზმი მხოლოდ დადებით გარანტიად შეიძლება შეფასდეს პრივილეგირებული ინფორმაციის დაცვის კუთხით.

ადვოკატსა და კლიენტს შორის კომუნიკაციის კონფიდენციალურობის პრინციპთან დაკავშირებით საყურადღებოა ვენეციის კომისიის მოსაზრებები პოლონეთის კანონმდებლობასთან დაკავშირებულ ანგარიშში. აღსანიშნავია, რომ ადვოკატსა და კლიენტს შორის პრივილეგირებული კომუნიკაციის მონიტორინგის მარეგულირებელმა პოლონეთის კანონმდებლობამ კრიტიკული შეფასება დაიმსახურა ვენეციის კომისიის მხრიდან, კერძოდ, კომისიის განმარტებით, მართალია კანონმდებლობით განსაზღვრულია კონფიდენციალურობის უფლებით დაცული იმ ინფორმაციის ბედი, რომელიც უკვე მოპოვებულია ფარული მეთვალყურეობის შედეგად, მაგრამ კანონმდებლობა დუმს ღონისძიების განხორციელებამდე პრივილეგირებული ინფორმაციის დაცვის საკითხზე - არაფერი უკრძალავს პოლიციას ფარულად მოუსმინოს ადვოკატსა და კლიენტს შორის საუბარს.[465]

[465] European Commission for Democracy Through Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 21-22, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].

კომისიის შეხედულებით, პოლონეთის კანონმდებლობის მოთხოვნები, იმასთან დაკავშირებით, რომ პროფესიული საიდუმლოების ხელშეუხებლობის დარღვევით მოპოვებული ინფორმაციის ბრალდებულის წინააღმდეგ მტკიცებულებად გამოყენება დაუშვებელია და დაუყოვნებლივ განადგურებას ექვემდებარება, არ არის საკმარისი[466]. ადვოკატსა და კლიენტს შორის საუბრის ფარული მიყურადების დროს პოლიციამ შესაძლოა შეიტყოს მნიშვნელოვანი ინფორმაცია, რომელიც თავის მხრივ, სხვა მაინკრიმინირებელი მტკიცებულების მოპოვებას დაედოს საფუძვლად. მიუხედავად იმისა, რომ პოლონეთის კანონმდებლობა კრძალავს იმ ინფორმაციის მტკიცებულებად დაშვებას, რომელიც „აკრძალული ხის ნაყოფს“ წარმოადგენს, ადვოკატსა და კლიენტს შორის კომუნიკაციის მიყურადება საგამოძიებო ორგანოს ანიჭებს ტაქტიკურ უპირატესობას დაცვის მხარესთან შედარებით და ძირს უთხრის დამცველსა და ბრალდებულს შორის ნდობას.[467]

კომისია მიიჩნევს, რომ კანონმდებლობამ უნდა განასხვავოს „გამიზნული“ და „შემთხვევითი“ ჩარევა ადვოკატსა და დაცვის ქვეშ მყოფს შორის პრივილეგირებული კომუნიკაციის დაცვის უფლებაში. „გამიზნული“ ჩარევა, როგორც ზოგადი წესი, აკრძალული უნდა იყოს[468]. ზოგჯერ პოლიციის მხრიდან წინასწარ არის შესაძლებელი ვარაუდი იმის შესახებ, რომ მოპოვებული იქნება პრივილეგირებული ინფორმაცია - მაგალითად, საქმე შეეხება ადვოკატსა და პატიმრობაში ან სასამართლო დარბაზში მყოფ კლიენტს, სატელეფონო კონსულტაციებს და ა.შ. ასეთი კომუნიკაცია, როგორც წესი, დაცული უნდა იქნეს მიყურადებისგან.[469] თუმცა ეს პრეზუმფცია არ არის აბსოლუტური და ვენეციის კომისია ასევე გამონაკლისის სახით მის შეზღუდვას უკავშირებს ადვოკატის მხრიდან დანაშაულის ჩადენის შემთხვევას.[470] კომისია ასევე მიიჩნევს, რომ პრივილეგირებული კომუნიკაციის გამიზნულად მოპოვების თავიდან აცილების პარალელურად, ეროვნული კანონმდებლობით უნდა იქნეს გათვალისწინებული შესაბამისი გარანტიები, როდესაც ასეთი ინფორმაცია შემთხვევით იქნება მოპოვებული.[471] ამავდროულად, კომისია პრივილეგირებული

[466] იქვე. 21
[467] იქვე.
[468] იქვე.
[469] იქვე.
[470] იქვე.
[471] იქვე.

ინფორმაციის დაცვას შესაძლებლად მიიჩნევს მხოლოდ ეფექტიანი ზედამხედველობის მექანიზმების არსებობის პირობებში და აღნიშნავს, რომ პროფესიული კომუნიკაციის დაცვა მხოლოდ „უსიცოცხლო“ გარანტიად დარჩება, თუკი მასზე არ გავრცელდება ზედამხედველობის სათანადო სისტემა.[472]

3.3. ფარული მეთვალყურეობის ღონისძიების ხანგრძლივობა

ფარული მეთვალყურეობის ღონისძიების გარკვეული ვადით შეზღუდვა უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგო მნიშვნელოვან გარანტიას და საერთაშორისო დონეზე განმტკიცებულ ფუნდამენტურ მოთხოვნას წარმოადგენს.[473]

ევროპული სასამართლო ფარული საგამოძიებო მოქმედების ხანგრძლივობის განსაზღვრას იმ ორგანოების კომპეტენციას მიაკუთვნებს, რომლებიც უფლებამოსილნი არიან ღონისძიების ჩატარებისა და გაგრძელების გადაწყვეტილებების მიღებაზე[474]. მიუხედავად აღნიშნულისა, ევროსასამართლოს პრაქტიკის თანახმად, აუცილებელია ეროვნულ კანონმდებლობაში ადეკატური გარანტიების გათვალისწინება თვითნებობისგან დაცვის მიზნით[475]. ასეთი გარანტიები შეეხება კომუნიკაციის მონიტორინგის ღონისძიების ჩატარების თავდაპირველი ხანგძლივობის, მისი გაგრძელებისა და შეწყვეტის საკითხების რეგულირებას.[476]

აღსანიშნავია, რომ ევროპულ სასამართლოს ფარული საგამოძიებო მოქმედებების მაქსიმალური დასაშვები ვადა არ დაუდგენია. აღნიშნული საკითხი წევრი სახელმწიფოების დისკრეციად რჩება, სასამართლო ყოველ კონკრეტულ შემთხვევაში აფასებს, რამდენად შეესაბამება თანაზომიერების პრინციპს ეროვნული კანონმდებლობით გათვალისწინებული ვადები. ერთ შემთხვევაში ასეთი ღონისძიების თავდაპირველი ხანგრძლივობა 2 თვემდე ვადით, მაქსიმუმ 6 თვემდე შემდგომი განახლების პერსპექტივით დასაშვებად იქნა მიიჩნეული[477], ხოლო სხვა

[472] იქვე.
[473] Report of the Special Rapporteur “On the Promotion and Protection of the Right to Freedom of Opinion and Expression”, 17.04.2013, 20 (ბმული იხ. პირველ გვერდზე).
[474] Roman Zakharov v. Russia, [2015] ECtHR, 250.
[475] იქვე.
[476] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 52; Kennedy v. United Kingdom, [2010] ECtHR, 161.
[477] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR.

შემთხვევაში ევროპულმა სასამართლომ გააკრიტიკა ეროვნული რეგულაციები, რომლებიც, მართალია, განსაზღვრავდა ღონისძიების ჩატარების მაქსიმალურ 6 თვიან ვადას, მაგრამ არ შეიცავდა რაიმე აკრძალვას ღონისძიების შემდგომ განახლებასთან დაკავშირებით.[478]

ევროპული სასამართლოს მიდგომის თანახმად, ფარული საგამოძიებო მოქმედებების საერთო ვადა გამოძიების ხაგრძლივობასა და კომპლექსურობაზეა დამოკიდებული. აღნიშნული ვადის განსაზღვრისთვის დანაშაულებრივი ქმედების მასშტაბი და მასში ჩართულ პირთა რაოდენობა უნდა იქნეს მხედველობაში მიღებული.[479] შესაბამისად, ღონისძიების ხანგრძლივობის თანაზომიერების შეფასება ყოველ კონკრეტულ შემთხვევაში უნდა მოხდეს. შიდა სამართლებრივი სისტემით განსაზღვრული ვადა ერთ შემთხვევაში შესაძლოა ლეგიტიმური მიზნის პროპორციულად ჩაითვალოს, ხოლო სხვა შემთხვევაში – მასთან შეუსაბამოდ. ამავდროულად, თანაზომიერების პრინციპიდან გამომდინარე, ღონისძიების ჩატარების მაქსიმალური ვადა არ უნდა იყოს ზედმეტად ხანგრძლივი.

მოცემულ საკითხთან დაკავშირებით საინტერესო საქმეს წარმოადგენს კენედი გაერთიანებული სამეფოს წინააღმდეგ (Kennedy v. United Kingdom), სადაც ბრიტანეთის ეროვნულმა რეგულაციებმა კომუნიკაციის მონიტორინგის ღონისძიების ხანგრძლივობასთან დაკავშირებით ევროპული სასამართლოს მოწონება დაიმსახურა. ამ კონტექსტში განსაკუთრებით აღსანიშნავია ვადის გაგრძელების მექანიზმი, რომლის თანახმადაც, სახელმწიფო მდივნის წინაშე ღონისძიების განახლების შუამდგომლობის წარმდგენ პირს ეკისრებოდა ღონისძიების შემდგომი გაგრძელების აუცილებლობის დასაბუთების ვალდებულება. ხოლო, თავის მხრივ, სახელმწიფო მდივანს ევალებოდა, გაეუქმებინა ღონისძიება, თუ მისი შემდგომი გაგრძელების აუცილებლობაში ვერ დარწმუნდებოდა[480]. აღნიშნული ვალდებულება ფარული თვალთვალის განხორციელებაზე განგრძობადი ზედამხედველობის ბერკეტად იქნა მიჩნეული.[481] აღსანიშნავია, რომ ფარული საგამოძიებო მოქმედების ჩატარების შესახებ სასამართლოს ნებართვის გაცემის შემდგომ აღნიშნული ღონისძიების გაგრძელებაზე

[478] Iordachi and others v. Moldova, [2009], ECtHR, 45.
[479] Kennedy v. United Kingdom, [2010] ECtHR, 161.
[480] იქვე.
[481] იქვე.

განგრძობადი ზედამხედველობა მნიშვნელოვან გარანტიად ითვლება საერთაშორისო დონეზე[482]. გაეროს სპეციალური მომხსენებელი უკმაყოფილებას გამოთქვამს ზოგიერთ სახელმწიფოში აღნიშნული მექანიზმის არარსებობის გამო.[483]

3.4. სამართალდამცავი ორგანოების წვდომა ელექტრონული კომუნიკაციის საშუალებებით გადაცემულ ინფორმაციაზე

სისტემა, რომელიც ელექტრონული კომუნიკაციის საშუალებებით გადაცემულ ინფორმაციაზე წვდომის შესაძლებლობას იძლევა, სხვადასხვა სახელმწიფოში განსხვავებულია. ზოგიერთ შემთხვევაში კომუნიკაციის მონიტორინგს სამართალდამცავი ორგანოები სერვისის პროვაიდერების მეშვეობით ახორციელებენ, სხვა შემთხვევაში კი კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობა გააჩნიათ. ზოგადად ითვლება, რომ სახელმწიფოს მიერ კავშირგაბმულობის არხებთან პირდაპირი წვდომა პირადი ცხოვრების სფეროში თვითნებური ჩარევის მომეტებულ რისკებს შეიცავს.[484]

სწორედ ასეთი სისტემა შეაფასა ევროპულმა სასამართლომ საქმეში ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia). ზოგადად, ზახაროვის საქმე წარმოადგენს ევროპული სასამართლოს ერთ-ერთ ყველაზე მნიშვნელოვან პრეცედენტულ გადაწყვეტილებას ფარული მეთვალყურეობის საკითხთან დაკავშირებით, რომელშიც შეჯამებულია სასამართლოს პრაქტიკა ფარული მეთვალყურეობის მიმართულებით და ამ კონტექსტში დაკონკრეტებულია პირადი ცხოვრების უფლებასთან დაკავშირებული პრინციპები.[485]

როგორც უკვე აღინიშნა, ერთ-ერთი საკითხი, რომელზეც ევროპულმა სასამართლომ ამ საქმეში იმსჯელა, უკავშირდება უშიშროებისა და სამართალდამცავი ორგანოების მიერ კავშირგაბმულობის არხებთან პირდაპირი წვდომის შესაძლებლობას. საქმის გარემოებების მიხედვით, რუსეთის სამართალდამცავ და უშიშროების ორგანოებს გააჩნდათ კომუნიკაციებზე უშუალო წვდომის ტექნიკური

[482] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 14 (ბმული იხ. პირველ გვერდზე).
[483] იქვე.
[484] Roman Zakharov v. Russia, [2015] ECtHR, 268-271.
[485] *Boehm F.,* Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes, European Data Protection Law Review, Vol. 2, No 2, 2016, 181.

შესაძლებლობა[486]. სერვისის მიმწოდებლები სამართალდამცავი ორგანოების მიერ სატელეფონო კომუნიკაციასთან პირდაპირი მიერთების მიზნით უზრუნველყოფდნენ შესაბამისი აპარატურის ინსტალაციას. შედეგად, სამართალდამცავ ორგანოებს არ ეკისრებოდათ სატელეფონო კომუნიკაციების მიყურადების შესახებ სასამართლოს განჩინების სერვისის პროვაიდერებისთვის წარდგენის ვალდებულება[487]. საგამოძიებო ორგანოებს ასევე გააჩნდათ სერვისის მიმწოდებლების მიერ წარმოებულ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზებთან პირდაპირი წვდომის შესაძლებლობაც. ევროპული სასამართლოს განმარტებით, სერვისის მიმწოდებლისთვის სატელეფონო კომუნიკაციის ფარული მიყურადების შესახებ სასამართლოს განჩინების წარდგენა მნიშვნელოვან გარანტიას წარმოადგენს უფლების ბოროტად გამოყენების წინააღმდეგ, ვინაიდან გამორიცხავს სასამართლოს ნებართვის გარეშე სატელეფონო კომუნიკაციის მიყურადების შესაძლებლობას[488]. რუსეთში დამკვიდრებული სისტემა კი სახელმწიფო ხელისუფლების ორგანოებს ანიჭებდა ტექნიკურ შესაძლებლობას, სასამართლოს და სერვის მიმწოდებლების გვერდის ავლით განეხორციელებინათ ფარული მიყურადება[489]. სასამართლოს შეხედულებით, მიუხედავად იმისა, რომ „დაუდევარი, არაკეთილსინდისიერი ან ზედმეტად მოტივირებული მოხელის მხრიდან უკანონო ქმედების განხორციელების რისკი არცერთი სისტემის პირობებში არ არის გამორიცხული, 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“[490]. აღსანიშნავია რომ ამ კონტექსტში ევროპულმა სასამართლომ ხაზი გაუსვა ზედამხედველობის სისტემის ეფექტიანობას. სასამართლოს განმარტებით, ასეთ შემთხვევაში ზედამხედველობის სისტემამ უნდა

[486] Roman Zakharov v. Russia, [2015] ECtHR, 268.
[487] იქვე.
[488] იქვე, 269.
[489] იქვე, 269-270.
[490] იქვე, 270.

უზრუნველყოს კომუნიკაციის მონიტორინგის ღონისძიებების კანონიერად განხორციელება სასამართლოს ნებართვის საფუძველზე.[491]

როგორც ვხედავთ, სასამართლო აპრიორი არ გამორიცხავს ზემოთ აღნიშნული სისტემის მოქმედებას სახელმწიფოში, თუმცა ამგვარი სისტემისთვის დამახასიათებელი თვითნებობის მაღალი რისკის პროპორციულად უფლების ბოროტად გამოყენების საწინააღმდეგო ადეკვატური გარანტიების აუცილებლობაც იზრდება, რაც პირველ რიგში, ფარული მეთვალყურეობის განხორციელების პროცესზე ეფექტიანი და ქმედითი ზედამხედველობის მექანიზმების აუცილებლობაში გამოიხატება.

3.5. კომუნიკაციების მონიტორინგის განხორციელებაზე ნებართვის გაცემის პროცედურა

ფარული მეთვალყურეობის განხორციელებაზე ნებართვის გაცემის პროცედურის შეფასება რამდენიმე ელემენტის გათვალისწინებით ხორციელდება: ორგანო, რომელიც ნებართვას გასცემს, ამ ორგანოს კომპეტენციის ფარგლები გადაწყვეტილების მიღების დროს და ნებართვის შინაარსი.[492]

როგორც წესი, საერთაშორისო სტანდარტი მოითხოვს ფარული საგამოძიებო მოქმედების ჩასატარებლად ნებართვის გაცემას სასამართლოს მიერ,[493] თუმცა სასამართლო ხელისუფლებისათვის აღნიშნული ფუნქციის დაკისრება არ არის იმპერატიული ხასიათის მოთხოვნა - ფარული საგამოძიებო მოქმედების ჩატარებაზე ნებართვის ფუნქციის სხვა ორგანოსათვის მინიჭება შესაძლოა ასევე შესაბამისი იყოს კონვენციასთან, იმ პირობით, რომ ის საკმარისად დამოუკიდებელია აღმასრულებელი ხელისუფლებისგან.[494]

უნდა აღინიშნოს, რომ სასამართლო კონტროლი წარმოადგენს თვითნებობის საწინააღმდეგო მნიშვნელოვან გარანტიას ფარული მეთვალყურეობის ღონისძიების ყველა ეტაპზე, თუკი ასეთი კონტროლი „ეფექტიანია“ როგორც „პრაქტიკაში, ასევე

[491] Roman Zakharov v. Russia, [2015] ECtHR, 270-271.
[492] იქვე. 257.
[493] Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 14 (ბმული იხ. პირველ გვერდზე).
[494] Roman Zakharov v. Russia, [2015] ECtHR, 258.

საკანონმდებლო დონეზე.“[495] წინასწარი სასამართლო კონტროლის მექანიზმს, რომელიც „კარგად მუშაობს“ პრაქტიკაში, შეუძლია “პრევენციული ფუნქციის“ შესრულება - დაუსაბუთებელი შუამდგომლობების გაცხრილვა და საგამოძიებო მოქმედების ვადის შემცირება.[496] გაეროს სპეციალური მომხსენებელი აღნიშნავს, რომ სასამართლოს ჩართულობას, რომელიც აკმაყოფილებს საერთაშორისო სტანდარტებს დამოუკიდებლობის, მიუკერძოებულობის და გამჭვირვალობის კუთხით, შეუძლია ხელი შეუწყოს მთლიანი სამართლებრივი რეჟიმის შესაბამისობას საერთაშორისო სამართლით აღიარებულ მინიმალურ სტანდარტებთან.[497]

მიუხედავად იმისა, რომ სასამართლო კონტროლი თვითნებობის საწინააღმდეგო მნიშვნელოვანი გარანტიაა ფარული მეთვალყურეობის განხორციელების ყველა ეტაპზე[498], სასამართლოს მონაწილეობა არ მიიჩნევა როგორც „უნივერსალური გამოსავალი“[499], მაგალითად, როგორც გაეროს სპეციალური მომხსენებელი ანგარიშში „პირადი ცხოვრების უფლება ციფრულ ეპოქაში“ აღნიშნავს, რომ „ზოგიერთ ქვეყანაში უშიშროების ან დანაშაულის გამოძიების სფეროში სასამართლოს მიერ ფარული მეთვალყურეობის ღონისძიების ჩატარებაზე ნებართვის გაცემა ან შემდგომი გადამოწმება იმდენად ფორმალურ ხასიათს ატარებს, რომ ფაქტობრივად „ბეჭდის დასმის“ ფუნქციამდეა დაყვანილი.“[500] ამიტომაცაა, რომ საერთაშორისო დონეზე თანდათანობით ყურადღებას იპყრობს ზედამხედველობის შერეული მოდელები, როგორიცაა ადმინისტრაციული ორგანოს, სასამართლოს და პარლამენტის ჩართულობა.[501] ასევე სულ უფრო აქტიურად განიხილება სხვადასხვა მექანიზმები სასამართლო კონტროლის ქმედითი და რეალურად ეფექტიანი სისტემის უზრუნველსაყოფად - მაგალითად, ანგარიშში „პირადი ცხოვრების უფლება ციფრულ საუკუნეში“, გაეროს სპეციალური მომხსენებელი აღნიშნავს, რომ განსაკუთრებული

[495] Šantare and Labaznikovs v. Latvia, [2016], ECtHR, 54.

[496] Memorandum on Surveillance and Oversight Mechanisms in The United Kingdom, Commissioner for Human Rights, Council of Europe, 17.05.2016, 5-6, <https://rm.coe.int/16806db72c> [20.06.2020]. აღნიშნული მემორანდუმი ეხება ფარული მეთვალყურეობის სამართლებრივ რეგულირებას უშიშროების სექტორში.

[497] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13 (ბმული იხ. მე-19 გვერდზე).

[498] Šantare and Labaznikovs v. Latvia, [2016], ECtHR, 54.

[499] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13 (ბმული იხ. მე-19 გვერდზე).

[500] იქვე.

[501] იქვე.

ინტერესის ქვეშაა სპეციალური პოზიციის - „საზოგადოებრივი ინტერესების ადვოკატების“ შექმნის იდეა, რომლებიც მონაწილეობას მიიღებენ ნებართვის გაცემის პროცედურაში.[502] იგივე მოსაზრებაა გაჟღერებული ევროპის საბჭოს ადამიანის უფლებების კომისრის მიერ, გაერთიანებულ სამეფოში ფარული მეთვალყურეობისა და ზედამხედველობის მექანიზმების თაობაზე მემორანდუმში“, სადაც კომისარი ხაზს უსვამს შეჯიბრებითი პროცესის მნიშვნელობას და მიიჩნევს, რომ ღონისძიების ადრესატის ინტერესების დაცვის მიზნით „სპეციალური ადვოკატის“ პოზიციის[503] შემოტანას შეუძლია შეამციროს ნებართვის პროცესის შაბლონურ, ფორმალურ პროცედურად გადაქცევის რისკი.[504] ანგარიშში, რომელიც ეხება დემოკრატიულ ზედამხედველობას უშიშროების სექტორში ელექტრონული თვალთვალის განმახორციელებელ ორგანოებზე, ვენეციის კომისია აღნიშნავს, რომ არსებობს ემპირიული მტკიცებულება, რომ როგორც დანაშაულის გამოძიების, ასევე უშიშროების სექტორში ასეთ ადვოკატებს შეუძლიათ გარკვეული მნიშვნელოვანი როლი ითამაშონ, რათა გამოძიება რეალურად შეძლებისდაგვარად შეიზღუდოს.[505] „პირადი ცხოვრების დამცველის“[506] პოზიციის შემოტანის იდეა გაჟღერებულია ასევე ვენეციის კომისიის მიერ ფარული მეთვალყურეობის ღონისძიებების შესახებ პოლონეთის კანონმდებლობასთან დაკავშირებულ ანგარიშში.[507]

საბოლოო ჯამში, შეიძლება ითქვას, რომ სასამართლო კონტროლი წარმოადგენს უმნიშვნელოვანეს და საუკეთესო მექანიზმს ფარული საგამოძიებო მოქმედებების განხორციელების დროს ადამიანის უფლებების დაცვის კუთხით, იმ პირობით, რომ ეს მექანიზმი რეალურად ქმედითი და ეფექტიანია პრაქტიკული თვალსაზრისით. ევროპული სასამართლოს პრაქტიკიდან გამომდინარე, სასამართლო კონტროლი მნიშვნელოვანი გარანტიაა და ამავდროულად - საუკეთესო პრაქტიკაც კი[508], თუმცა მხოლოდ სასამართლოს ზედამხედველობა ვერ ჩაითვლება საკმარის დაცვის

---

[502] იქვე.
[503] “Security-vetted Special Advocates”.
[504] Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, Commissioner for Human Rights, Council of Europe, 17.05.2016, 6, <https://rm.coe.int/16806db72c> [20.06.2020].
[505] European Commission for Democracy through Law (Venice Commission), On the Democratic Oversight of Signal Intelligence Agencies, 15.12.2015, 26, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e> [20.06.2020].
[506] იქვე. 25. დოკუმენტში მოხსენიებულია „Privacy Advocate”.
[507] იქვე.
[508] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 56.

მექანიზმად კონვენციის მე-8 მუხლთან შესაბამისობის კონტექსტში, არამედ მნიშვნელოვანია, რომ მოსამართლეს ჰქონდეს მინიჭებული საკმარისი კომპეტენციის ფარგლები.[509] სწორედ აღნიშნულმა უნდა უზრუნველყოს, რომ მოსამართლის ჩართულობა რეალურად ფორმალურ ხასიათს არ ატარებდეს.

მოსამართლის კომპეტენცია შემდეგი კრიტერიუმებით მოწმდება – უნდა გააჩნდეს ბერკეტი, დაადგინოს: არის თუ არა სახეზე ფარული საგამოძიებო მოქმედების ჩასატარებლად აუცილებელი "გონივრული ეჭვი" ("Reasonable Suspicion") დანაშაულის ჩადენასთან დაკავშირებით, რამდენად პასუხობს მოთხოვნილი ღონისძიება პროპორციულობის პრინციპს, მათ შორის, ხომ არ არსებობს სხვა, უფრო ნაკლებად შემზღუდველი ღონისძიების გამოყენების შესაძლებლობა.[510]

ამ თვალსაზრისით ერთ-ერთ მნიშვნელოვან საქმეს წარმოადგენს ზახაროვი რუსეთის წინააღმდეგ (Zakharov. V. Russia), სადაც ევროპულმა სასამართლომ წარდგენილი ანალიტიკური და სტატისტიკური მასალების საფუძველზე დაადგინა, რომ რუსეთის სასამართლოები არ ადგენდნენ დანაშაულის ჩადენის შესახებ საკმარისი საფუძვლის რეალურ არსებობას საქმეში, არამედ კმაყოფილდებოდნენ სამართალდამცავი ორგანოების მხრიდან გაკეთებული ზოგადი მითითებებით დანაშაულის ჩადენის შესახებ, აღნიშნული დანაშაულის შესაძლო ჩადენის დამადასტურებელი მტკიცებულებების წარდგენის გარეშე.[511]

ზახაროვის საქმეში ევროპულმა სასამართლომ ასევე შეაფასა გადაუდებელი აუცილებლობის საფუძვლით სატელეფონო კომუნიკაციის ფარული მიყურადების ჩატარების პროცედურა. სასამართლოს განმარტებით, რუსეთის კანონმდებლობა ამ თვალსაზრისით ვერ უზრუნველყოფდა საკმარის გარანტიებს იმის უზრუნველსაყოფად, რომ „გადაუდებელი აუცილებლობის" პროცედურა გამოყენებული ყოფილიყო საგამონაკლისო წესით, მხოლოდ სათანადო აუცილებლობის შემთხვევაში[512]. სასამართლოს კრიტიკა გამოიწვია, მათ შორის, სასამართლოს შეზღუდულმა მონაწილეობამ გადაუდებელი აუცილებლობის

[509] Iordachi and others v. Moldova, [2009], ECtHR, 47.
[510] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 51; Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75; Kruslin v. France, [1990], ECtHR, (Ser. A.), 79-80; Roman Zakharov v. Russia, [2015] ECtHR, 260.
[511] Roman Zakharov v. Russia, [2015] ECtHR, 263.
[512] იქვე, 266.

საფუძვლით ჩატარებული ღონისძიების post factum გადამოწმების პროცედურაში - მართალია რუსეთის კანონმდებლობა ითვალისწინებდა სასამართლოს დაუყოვნებლივ ინფორმირებას გადაუდებლად ჩატარებულ ღონისძიებასთან დაკავშირებით, მაგრამ სასამართლოს უფლებამოსილება შეზღუდული იყო მხოლოდ დაწყებული ღონისძიების კანონმდებლობით გათვალისწინებული 48 საათიანი ვადის (გადაუდებელი აუცილებლობის წესით ღონისძიების ჩატარების მაქსიმალური ვადა) მიღმა გაგრძელების საკითხის გადაწყვეტით და არ გააჩნდა კომპეტენცია, შეემოწმებინა რამდენად კანონიერად იქნა გამოყენებული გადაუდებელი აუცილებლობის წესი ან ემსჯელა უკვე მოპოვებული მტკიცებულების შენახვის/განადგურების საკითხზე.[513]

საქმეში იორდაჩი მოლდოვის წინააღმდეგ (Iordachi v. Moldova), ევროპული სასამართლოს კრიტიკა დაიმსახურა მოლდოვის სასამართლოების პრაქტიკამ კომუნიკაციის მონიტორინგთან დაკავშირებით, კერძოდ, სასამართლოს განმარტებით, მოლდოვის მოსამართლეებმა ღონისძიების ჩატარების თაობაზე ნებართვა გასცეს პროკურატურის მიერ წარდგენილ თითქმის ყველა შუამდგომლობასთან დაკავშირებით[514]. შესაბამისი სტატისტიკური მონაცემების მიხედვით, 2005-2007 წლებში დაკმაყოფილდა წარდგენილი შუმდგომლობების დაახლოებით 97-99%, რაც წარმოადგენდა უჩვეულოდ მაღალ რაოდენობას[515]. იმის გათვალისწინებით, რომ სატელეფონო კომუნიკაციის ფარული მიყურადება ადამიანის უფლებებში ძალიან სერიოზული ჩარევაა, მხოლოდ სერიოზულ მიზეზებს შეუძლია გაამართლოს ამ ღონისძიების განხორციელება. ევროპულმა სასამართლომ აღნიშნა, რომ მოლდოვის კანონმდებლობა არ აკონკრეტებდა პირის მიმართ დანაშაულის ჩადენის თაობაზე ეჭვის ხარისხს ნებართვის გაცემის მიზნებისათვის და არ შეიცავდა სათანადო გარანტიებს თვითნებობის საწინააღმდეგოდ[516]. სასამართლოს შეხედულებით, კანონმდებლობის ეს ნაკლოვანებები ჩანდა სასამართლოების პრაქტიკაშიც, ღონისძიების ჩატარების საკითხის გადაწყვეტის დროს მოსამართლეები არ აფასებდნენ, რამდენად არსებობდა მოთხოვნილი საგამოძიებო მოქმედების

[513] იქვე. 266.
[514] Iordachi and others v. Moldova, [2009], ECtHR, 51-53.
[515] იქვე.
[516] იქვე.

განხორციელების „დამაჯერებელი დასაბუთება“[517]. წარდგენილი სტატისტიკური მონაცემები მეტყველებდნენ სწორედ ფარული მეთვალყურეობის სისტემის არაჯეროვან ფუნქციონირებაზე, რაც ნაწილობრივ კანონმდებლობაში შესაბამისი გარანტიების არარსებობით იყო განპირობებული.[518]

მოცემულ კონტექსტში საინტერესო საქმეს წარმოადგენს ასევე დრაგოევიჩი ხორვატიის წინააღმდეგ (Dragojevic v. Croatia), სადაც ევროპულმა სასამართლომ კონვენციის მე-8 მუხლის დარღვევა დაადგინა, კერძოდ, იმის გათვალისწინებით, თუ როგორ იქნა განმცხადებლის საქმეზე ინტერპრეტირებული და გამოყენებული ხორვატიის სისხლის სამართლის საპროცესო კანონმდებლობა, ევროპულმა სასამართლომ მიიჩნია, რომ შესაბამისი სამართლებრივი დებულებები არ შეიცავდა საკმარის განსაზღვრულობას/სიცხადეს ფარული მეთვალყურეობის ღონისძიების ჩატარებაზე ნებართვის გაცემის კონტექსტში შესაბამისი ორგანოებისთვის მინიჭებულ დისკრეციასთან მიმართებით, ასევე ვერ უზრუნველყოფდა შესაძლო თვითნებობის საწინააღმდეგო გარანტიებს პრაქტიკაში[519]. აღნიშნული დასკვნის გამოტანის დროს სასამართლომ ყურადღება გაამახვილა იმ გარემოებაზე, რომ განმცხადებლის საქმეში სატელეფონო კომუნიკაციის ფარული მიყურადების ჩატარებაზე ნებართვის გაცემასთან დაკავშირებული სასამართლო განჩინებები „დაეყრდნო მხოლოდ ბრალდების მხარის განცხადებას ფარული საგამოძიებო მოქმედების ჩატარების მოთხოვნასთან დაკავშირებით და ბრალდების მხარის მიერ გამოყენებულ ფრაზას, რომ გამოძიების სხვა საშუალებებით ჩატარება შეუძლებელი იყო“. სასამართლოს გადაწყვეტილებები არ შეიცავდა შესაბამის „დეტალებს“, რომელიც დაფუძნებული იქნებოდა საქმის კონკრეტულ ფაქტობრივ გარემოებებზე და მიუთითებდა დანაშაულის შესაძლო ჩადენასთან დაკავშირებით „დასაბუთებულ ვარაუდზე“ და იმაზე, რომ „სხვა, ნაკლებად ინტენსიური საგამოძიებო მეთოდების გამოყენება შეუძლებელი ან უკიდურესად რთული იყო.“[520]

---

[517] იქვე.

[518] იქვე.

[519] Dragojevic v. Croatia, [2015], ECtHR, 95-101.

[520] იქვე. იგივე არგუმენტებზე დაყრდნობით, რაც საფუძვლად დაედო პირადი ცხოვრების უფლების დარღვევას საქმეში Dragojevic v. Croatia, კონვენციის მე-8 მუხლის დარღვევა დაადგინა ევროპულმა სასამართლომ ასევე საქმეზე Liblik and others v. Estonia, სადაც ფარული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე ნებართვები არ იყო დასაბუთებული მტკიცებულებით სტანდარტთან (გონივრული ეჭვი) და სხვა ნაკლებად ინტენსიური საშუალებების გამოყენების შეუძლებლობასთან დაკავშირებით. უფრო ვრცლად იხ. Liblik and others v. Estonia, [2019], ECtHR.

ანალოგიური საფუძვლით დაადგინა დარღვევა ევროპულმა სასამართლომ ხორვატიის წინააღმდეგ არსებულ სხვა საქმეშიც, სადაც მოსამართლის განჩინება ასევე ეფუძნებოდა მხოლოდ ბრალდების მხარის მოთხოვნას სატელეფონო კომუნიკაციის ფარული მიყურადების ჩატარებასთან დაკავშირებით და განცხადებას, რომ „გამოძიების წარმართვა სხვა საშუალებებით შეუძლებელი ან უკიდურესად რთული იყო“[521]. სასამართლოს განჩინება არ შეიცავდა შესაბამის მსჯელობას საქმის კონკრეტული გარემოებების გათვალისწინებით და განსაკუთრებით, კონკრეტულ მიზეზებს, თუ რატომ იყო შეუძლებელი გამოძიების ჩასატარებლად სხვა ნაკლებად ინტენსიური მეთოდების გამოყენება.[522]

ამდენად, ევროპული სასამართლოს პრაქტიკაში უკვე არაერთხელ გაჟღერდა პოზიცია იმასთან დაკავშირებით, რომ სასამართლოს განჩინებაში მხოლოდ ზოგადი მითითებები დანაშაულის შესაძლო ჩადენასთან, ასევე სხვა ნაკლებად შემზღუდველი ზომების გამოყენების შეუძლებლობასთან/სირთულესთან მიმართებით არ არის საკმარისი განჩინების დასაბუთების მიზნებისათვის, არამედ ვარაუდი როგორც დანაშაულის ჩადენის თაობაზე, აგრეთვე სხვა ნაკლებად ინტენსიური საგამოძიებო მეთოდების გამოყენების შეუძლებლობასთან/სირთულესთან მიმართებით, დადასტურებული უნდა იყოს საქმის კონკრეტული ფაქტობრივი და ინდივიდუალური გარემოებებით.

კიდევ ერთი საკითხი, რომელიც ნებართვის გაცემის პროცედურებთან დაკავშირებით უნდა შეფასდეს, წარმოადგენს სასამართლოს განჩინების შინაარსი. ზოგადი სტანდარტი, რომელიც დამკვიდრდა ევროპული სასამართლოს პრაქტიკაში, მდგომარეობს ამგვარი განჩინების კონკრეტულობის მოთხოვნაში, კერძოდ, განჩინებაში კონკრეტულად უნდა აღინიშნოს პირი, რომლის კომუნიკაციაც სახელმწიფოს მხრიდან მონიტორინგს დაექვემდებარება და ღონისძიების

[521] Bašić v. Croatia, [2017], ECtHR, 33-34;

[522] იქვე. იხ. ასევე Matanović v. Croatia, [2017], ECtHR, 112-115, სადაც ევროპულმა სასამართლომ მითითება გააკეთა გადაწყვეტილებაზე Dragojevic v. Croatia და ანალოგიური საფუძვლებით დაადგინა კონვენციის მე-8 მუხლის დარღვევა. ანალოგიური პოზიცია დააფიქსირა სასამართლომ საქმეში მუსტაფა სეზგინი ტანრიკულუ თურქეთის წინააღმდეგ (Mustafa Sezgin Tanrikulu v. Turkey), სადაც სასამართლოს განჩინება ასევე არ შეიცავდა შესაბამის „დეტალებს“ საქმის კონკრეტულ ფაქტებსა და ინდივიდუალურ გარემოებებთან დაკავშირებით, რომლებიც „დასაბუთებული ვარაუდის“ ხარისხით მიუთითებდნენ, რომ გამოძიების მიზნების მიღწევა სხვა ნაკლებად ინტენსიური მეთოდების გამოყენებით შეუძლებელი იყო. იხ. Mustafa Sezgin Tanrikulu v. Turkey, [2017], ECtHR, 59.

ხანგრძლივობა.[523] პირის იდენტიფიცირება შესაძლებელია ვინაობის, მისამართის, სატელეფონო ნომრის ან სხვა რელევანტური ინფორმაციის საფუძველზე.[524] განჩინება, რომელშიც მითითებული არ არის კონკრეტული პირი ან სატელეფონო ნომერი და რომელიც კონკრეტულ დანაშაულთან დაკავშირებულ ყველა სატელეფონო კომუნიკაციაზე მეთვალყურეობის შესაძლებლობას იძლევა, სამართალდამცავ ორგანოებს ზედმეტად ფართო დისკრეციას ანიჭებს.[525]

3.6. ელექტრონული კომუნიკაციის საშუალებებით გადაცემული ინფორმაციის შემოწმების, გამოყენების, შენახვის, სხვა პირებისთვის გადაცემისა და განადგურების პროცედურა

ევროპულ სასამართლოს არაერთ საქმეზე გამოუხატავს პრინციპული მოსაზრება იმასთან დაკავშირებით, რომ ეროვნული კანონმდებლობა დეტალურად უნდა არეგულირებდეს ფარული მეთვალყურეობის ღონისძიების შედეგად მოპოვებული ინფორმაციის შემოწმების, გამოყენების, შენახვის, სხვა პირებისთვის გადაცემისა და განადგურების წესებს.[526] ამავდროულად, კანონის „ხელმისაწვდომობისა“ და „განჭვრეტადობის“ კრიტერიუმებიდან გამომდინარე, ეს რეგულირება უნდა იყოს საზოგადოებისათვის ხელმისაწვდომი, ანუ საჯაროდ გამოქვეყნებული და მკაფიო, დეტალური, განჭვრეტადი სამართლებრივი დებულებებით განსაზღვრული. მაგალითად, საქმეში ლიბერთი გაერთიანებული სამეფოს წინააღმდეგ (Liberty and others v. United Kingdom), კანონიერების პრინციპის დარღვევის მიზეზი გახდა ის გარემოება, რომ დიდი ბრიტანეთის კანონმდებლობა, საზოგადოებისათვის ხელმისაწვდომი ფორმით არ არეგულირებდა კომუნიკაციის მონიტორინგის შედეგად მოპოვებული მასალის შერჩევის პროცესში აღნიშნული ინფორმაციის გამოკვლევის, შენახვის და განადგურების პროცედურას. [527]

---

[523] Roman Zakharov v. Russia, [2015] ECtHR, 265.

[524] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.) 51; Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR. 80; Kennedy v. United Kingdom, [2010] ECtHR, 160; Mustafa Sezgin Tanrikulu v. Turkey, [2017], ECtHR 57.

[525] Roman Zakharov v. Russia, [2015] ECtHR, 265.

[526] იქვე. 231; Huvig v. France, [1990], ECtHR, (Ser. A.), 34; Amman v. Switzerland, [2000], ECHR 2000-II, 56-58; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46; Prado Bugallo v. Spain, [2003], ECtHR, 30; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 95.

[527] Liberty and others v. United Kingdom, , [2008], ECtHR, 69.

ევროპულმა სასამართლომ რამდენიმე საქმეში მოიწონა შიდა სამართლებრივი რეგულაციები, რომლებიც განსაზღვრავდნენ ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის შენახვის ვალდებულებას ისეთ პირობებში, რომლებიც გამორიცხავენ მათზე უნაბართვო წვდომას, ასევე, აწესრიგებდნენ სასამართლოში მისი მტკიცებულებად გამოყენების საკითხებს.[528] მნიშვნელოვანია ასევე, რომ კანონი ადგენდეს შეზღუდვას ხანდაზმულობის ზედა ზღვართან ან იმ ვადასთან მიმართებით, რომლის განმავლობაშიც დაიშვება ინფორმაციის შენახვა.[529]

როგორც წესი, ევროპული სასამართლოს უარყოფით შეფასებას იწვევს ისეთი ვითარება, როდესაც ეროვნული კანონმდებლობა არ ითვალისწინებს რაიმე სახის პროცედურას, თუ რა წესით უნდა მოხდეს მოპოვებული ინფორმაციის გადარჩევა ან განადგურება.[530]

ფარული მიყურადების შედეგად მოპოვებული მასალის გამოკვლევისა და განადგურების პროცედურა არაჯეროვნად იქნა მიჩნეული საქმეში იორდაჩი მოლდოვის წინააღმდეგ (Iordachi v. Moldova). ევროპული სასამართლოს უარყოფითი შეფასება დაიმსახურა იმ გარემოებამ, რომ მოლდოვის კანონმდებლობა საკმარისი სიცხადით არ განსაზღვრავდა მოპოვებული ინფორმაციის გადარჩევის, ამ ინფორმაციის მთლიანობის შენარჩუნებისა და კონფიდენციალურობის დაცვის პროცედურას, ისევე როგორც მისი განადგურების წესს.[531] ანალოგიური მოსაზრება დააფიქსირა სასამართლომ ასევე საქმეში ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ (Association for European Integration and Human Rights and Ekimdziev v. Moldova).[532]

ამ კუთხით საინტერესოა ასევე საქმე კენედი გაერთიანებული სამეფოს წინაარმდეგ (Kennedy v. United Kingdom), სადაც ევროპულმა სასამართლომ დადებითად შეაფასა კომუნიკაციის მონიტორინგის ღონისძიებების მარეგულირებელი ბრიტანეთის კანონმდებლობა. მოპოვებული მასალის გამოკვლევის, გამოყენებისა და შენახვის პროცედურასთან დაკავშირებით სასამართლომ აღნიშნა, რომ ბრიტანეთის კანონმდებლობის მიხედვით,

[528] Roman Zakharov v. Russia, [2015] ECtHR, 163, 253.
[529] Rotaru v. Romania, [2000], ECHR 2000-V, 57.
[530] Iordachi and others v. Moldova, [2009], ECtHR, 48; Huvig v. France, [1990], ECtHR, (Ser. A.), 34.
[531] Iordachi and others v. Moldova, [2009], ECtHR, 48.
[532] Association for European Integration and Human Rights and Ekimdzhiev v. Moldova, [2007], ECtHR, 86.

მონიტორინგის განმახორციელებელი ორგანო უფლებამოსილი იყო, მოესმინა მოპოვებული პრაქტიკულად მთელი მოცულობის ჩანაწერისთვის[533]. სასამართლომ ეს შემთხვევა განასხვავა საქმისგან ლიბერთი გაერთიანებული სამეფოს წინააღმდეგ (Liberty v. United Kingdom), რომელიც ეხებოდა ბრიტანეთის ფარგლებს გარეთ განხორციელებული სატელეფონო კომუნიკაციის ფარულ მიყურადებას. ლიბერთის საქმეში სასამართლოს უარყოფითი შეფასება დაიმსახურა იმ გარემოებამ, რომ უფლებამოსილი ორგანოების დისკრეცია ინფორმაციის შერჩევის და შერჩეული ინფორმაციის გამოკვლევის კუთხით იყო შეუზღუდავი. ხოლო კენედის საქმეში სასამართლომ აღნიშნა, რომ ლიბერთის საქმე ეხებოდა ქვეყნის ფარგლებს გარეთ განხორციელებული ზარების მონიტორინგს, ხოლო განსახილველი შემთხვევა - ქვეყნის შიგნით კომუნიკაციის ფარულ მიყურადებას, რომელიც ბრიტანეთის კანონმდებლობის მიხედვით, ხორციელდებოდა არა განუსაზღვრელი პირების, არამედ კონკრეტული ადრესატის მიმართ და შესაბამისად, კომპეტენტური ორგანოების უფლებამოსილების ფარგლები კომუნიკაციის გადაჭერასა და მოსმენასთან დაკავშირებით იყო შეზღუდული. გარდა ამისა, მოპოვებული ინფორმაცია, რომელიც არ იყო საქმისათვის რელევანტური, დაუყოვნებლივ განადგურებას ექვემდებარებოდა.[534]

საბოლოო ჯამში, მოცემულ საკითხთან დაკავშირებით ევროპული სასამართლოს პრაქტიკის შეჯამებით შეიძლება დავასკვნათ, რომ სასამართლოს ერთმნიშვნელოვან მოთხოვნას წარმოადგენს მონაცემთა გამოკვლევის (გადარჩევის) საკითხის საკანონმდებლო რეგულირება განჭვრეტადი და ხელმისაწვდომი ფორმით. ამასთან, სასამართლო უფრო მკაცრ ტესტს იყენებს მონაცემთა გამოკვლევის საკითხთან მიმართებით, როდესაც საქმე ეხება უშიშროების სექტორში მასობრივი მონიტორინგის ღონისძიებებს.[535] ამ უკანასკნელ შემთხვევაში სასამართლო მიიჩნევს, რომ კომუნიკაციის ფარული მიყურადების დისკრეცია არის უფრო ფართო, თუმცა სამაგიეროდ, მონაცემთა გამოკვლევის ეტაპზე უნდა იქნეს გამოყენებული უფრო მკაცრი მოთხოვნები. ხოლო რაც შეეხება სისხლის სამართლის საქმის გამოძიების მიზნებისათვის კონკრეტული ადრესატის მიმართ გამოყენებულ ღონისძიებას,

[533] Kennedy v. United Kingdom, [2010] ECtHR, 162.
[534] იქვე.
[535] "Bulk Interception Rejime".

სასამართლოს შეხედულებით, კომუნიკაციის ის ტიპი, რომლის გადაჭერაც უნდა განხორციელდეს, თავიდანვე უნდა იყოს შეზღუდული, „ვიწროდ განსაზღვრული“, ხოლო როდესაც ღონისძიება განხორციელდება, შესაძლოა მოპოვებული კომუნიკაციის მთლიანი (ან თითქმის მთლიანი) ანალიზი გახდეს საჭირო.[536]

არსებით საკითხს წარმოადგენს აგრეთვე მონაცემთა განადგურების პროცედურის დეტალური მოწესრიგება. ამ კონტექსტში მნიშვნელოვანია, ეროვნული კანონმდებლობა განსაზღვრავდეს იმ ინფორმაციის დაუყოვნებლივ განადგურების მოთხოვნას, რომელსაც პრაქტიკული ღირებულება არ გააჩნია საქმისთვის, ასევე ზედმეტად ფართო დისკრეციას არ ანიჭებდეს მოსამართლეს სისხლის სამართლის საქმის დასრულების შემდეგ მტკიცებულებად გამოყენებულ მონაცემთა შენახვასა და განადგურებასთან მიმართებით – აუცილებელია კანონმდებლობა დეტალურად აწესრიგებდეს მონაცემთა შენახვის წესებს სისხლის სამართლის საქმის დასრულების შემდეგ.[537]

მნიშვნელოვან მოთხოვნას მიეკუთვნება ფარული საგამოძიებო მოქმედების განხორციელების შემდეგ მოპოვებულ მონაცემთა შენახვის აუცილებლობაზე მუდმივი ზედამხედველობა. ევროპულმა სასამართლომ რამდენიმე საქმეში აღნიშნა, რომ ხელისუფლების ორგანოთა მხრიდან მონაცემთა შენახვა, როგორი ხერხითაც არ უნდა იყოს იგი მოპოვებული, პირდაპირ ზემოქმედებას ახდენს ინდივიდის პირადი ცხოვრების ინტერესებზე[538]. საქმეში ვებერი და სარავია გერმანიის წინააღმდეგ (Weber and Saravia v. Germany), ადამიანის უფლებათა ევროპულმა სასამართლომ მოიწონა ეროვნული კანონმდებლობა, რომელიც აღნიშნულ საკითხს დეტალურად არეგულირებდა - უწყებას, რომელიც ინახავდა მონაცემებს, ეკისრებოდა აღნიშნული მონაცემების შემდგომი შენახვის აუცილებლობის გადამოწმება ყოველ ექვს თვეში ერთხელ. იმ შემთხვევაში, თუკი თავდაპირველი ლეგიტიმური მიზნის მისაღწევად მონაცემთა შენახვა დაკარგავდა საჭიროებას, მონაცემები უნდა განადგურებულიყო, წაშლილიყო, ან მინიმუმ, მათზე წვდომა უნდა შეზღუდულიყო. განადგურების

[536] აღნიშნულ საკითხთან დაკავშირებით იხ. ადამიანის უფლებათა ევროპული სასამართლოს პოზიცია საქმეზე Big Brother Watch and Others v. United Kingdom, [2018], ECtHR, 329. აღსანიშნავია, რომ აღნიშნული გადაწყვეტილება ამჟამად ევროპული სასამართლოს დიდი პალატის წინაშეა გასაჩივრებული.

[537] Roman Zakharov v. Russia, [2015], ECtHR, 255-256.

[538] S and Marper v. United Kingdom, [2008], ECtHR, 121.

პროცედურა ფორმდებოდა ოქმის შედგენით და მიმდინარეობდა სასამართლო წარმომადგენლის ზედამხედველობის ქვეშ.[539] აღსანიშნავია, რომ მოპოვებული მასალის შემდგომი შენახვის აუცილებლობის გონივრული პერიოდულობით გადასინჯვის საკანონმდებლო დონეზე უზრუნველყოფის მნიშვნელობასთან დაკავშირებით ევროპულ სასამართლოს სხვა საქმეშიც აქვს ყურადღება გამახვილებული.[540]

ევროპული სასამართლო დიდ ყურადღებას უთმობს ასევე კომუნიკაციის სხვა უფლებამოსილი სახელმწიფო ორგანოებისათვის გადაცემის საფუძვლებისა და წესების რეგულირებას. ამ კუთხით მნიშვნელოვანია, რომ ეროვნულ კანონმდებლობაში გათვალისწინებული იყოს ზომები, რომლებიც უზრუნველყოფენ მონაცემთა სხვა სახელმწიფო ორგანოებისათვის უსაფრთხოდ გადაცემას და ამასთან - მხოლოდ იმ მოცულობით, რაც ინფორმაციის მიმღებ ორგანოს მისთვის კანონმდებლობით დაკისრებული ფუნქციების შესასრულებლად ესაჭიროება.[541] ევროპულმა სასამართლომ საქმეში ვებერი და სარავია გერმანიის წინააღმდეგ (Weber and Saravia v. Germany), მოიწონა გერმანიის კანონმდებლობა, რომელიც საკმაოდ მკაცრად და დეტალურად არეგულირებდა მოცემულ საკითხს, კერძოდ, მონაცემთა სხვა სახელმწიფო ორგანოებისთვის გადაცემა დაიშვებოდა მხოლოდ იმ შემთხვევაში, როდესაც არსებობდა კონკრეტული ფაქტობრივი გარემობებიდან გამომდინარე ეჭვი, რომ ჩადენილი იყო კანონმდებლობით სპეციალურად განსაზღვრული მძიმე დანაშაულები; ასევე მონაცემთა გადაცემის საკითხს წყვეტდა თანამდებობის პირი, რომელიც იყო სასამართლო ხელისუფლების წარმომადგენელი. მონაცემთა გადაცემის კანონიერებაზე ზედამხედველობის ფუნქცია გააჩნდა დამოუკიდებელ კომისიას და მონაცემთა გადაცემის თითოეული ფაქტი წერილობით უნდა გაფორმებულიყო შესაბამისი ოქმის შედგენით.[542]

ამ საქმისგან ევროპულმა სასამართლომ განასხვავა საქმე ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ (The Association for European Integration and Human Rights and Ekimdzhiev

[539] Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 100.
[540] Kennedy v. United Kingdom, [2010] ECtHR, 164.
[541] Roman Zakharov v. Russia, [2015] ECtHR, 253; Kennedy v. United Kingdom, [2010] ECtHR, 163.
[542] Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 123-129.

v. Bulgaria), სადაც შინაგან საქმეთა მინისტრი შეუზღუდავი დისკრეციის პირობებში და დამოუკიდებელი ორგანოს ყოველგვარი ზედამხედველობის გარეშე წყვეტდა იმ ინფორმაციის ბედს, რომელიც თავდაპირველი შუამდგომლობის ფარგლებს მიღმა ღონისძიების შედეგად იქნებოდა მოპოვებული და ხვდებოდა ფარული მეთვალყურეობის ღონისძიებების ჩატარებაზე უფლებამოსილი სხვა ორგანოს კომპეტენციაში.[543]

3.7. ზედამხედველობის მექანიზმები ფარულ საგამოძიებო მოქმედებებზე

ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობის მექანიზმების ეფექტიანობა აღნიშნული ღონისძიებების თანაზომიერების შეფასებისას ერთ-ერთი ყველაზე მნიშვნელოვანი ასპექტი და საერთაშორისო დონეზე განმტკიცებული თვითნებობის საწინააღმდეგო ფუნდამენტური გარანტიაა.[544] უფლების ბოროტად გამოყენების საწინააღმდეგო გარანტიები დამოუკიდებელი ორგანოს კონტროლის გარეშე არაეფექტიანად არის აღიარებული საერთაშორისო დონეზე.[545] მიუხედავად იმისა, რომ ასეთი გარანტიები შესაძლოა მრავალფეროვან წესებში გამოიხატოს, ხელისუფლების ყველა შტოს, მათ შორის, დამოუკიდებელი ორგანოს ჩართულობა ზედამხედველობის პროცესში უფლების დაცვის ფუნდამენტურ გარანტიად ითვლება.[546]

ევროპული სასამართლოს პრაქტიკის მიხედვით, ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობის საკითხი რამდენიმე ეტაპზე დგას დღის წესრიგში – ასეთი ღონისძიების ჩასატარებლად ნებართვის გაცემისას, მისი განხორციელების

---

[543] Association for European Integration and Human Rights and Ekimdzhiev v. Moldova, [2007], ECtHR, 89; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 125-128.

[544] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 12-13, (ბმული იხ. მე-19 გვერდზე). Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 21 (ბმული იხ. პირველ გვერდზე).

[545] *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 46,
<http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf>
[10.06.2020].

[546] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 12-13 (ბმული იხ. მე-19 გვერდზე).

პროცესში და ღონისძიების შეწყვეტისას[547]. პირველ ორ შემთხვევაში თავად ღონისძიების ხასიათი მოითხოვს მის განხორციელებას იმ პირის ინფორმირების გარეშე, რომლის კომუნიკაციის მონიტორინგიც მიმდინარეობს. შესაბამისად, ვინაიდან პირი აღნიშნულ პროცესში ჩართული არ არის, აუცილებელია, რომ მოცემული საგამოძიებო მეთოდის გამოყენების პროცედურა უზრუნველყოფდეს შესაფერის გარანტიებს მისი უფლებების დასაცავად[548]. „სფეროში, სადაც ინდივიდუალურ შემთხვევებში უფლების ბოროტად გამოყენების პოტენციური რისკი ასეთი მაღალია, მისი თანმდევი შედეგები კი - მთლიანად დემოკრატიული ღირებულებებისთვის საზიანო, სასურველია რომ ზედამხედველობის ბერკეტს სასამართლო ფლობდეს."[549] „სასამართლო კონტროლი წარმოადგენს დამოუკიდებლობის, მიუკერძოებულობის და სათანადო პროცედურის უზრუნველყოფის საუკეთესო გარანტიას."[550] თუმცა როგორც უკვე აღინიშნა, ევროპული სასამართლოს პოზიცია ზედამხედველობის ფუნქციის სასამართლოსთვის მინიჭებასთან დაკავშირებით არ არის იმპერატიული. სასამართლო კონვენციასთან შესაბამისად მიიჩნევს ასევე აღნიშნული უფლებამოსილების განხორციელებას სხვა ორგანოს მიერ, იმ პირობით, რომ ის დამოუკიდებელია ფარული საგამოძიებო მოქმედებების განმახორციელებელი უწყებისგან და მინიჭებული აქვს საკმარისი უფლებამოსილება "ეფექტიანი და განგრძობადი კონტროლის" განსახორციელებლად.[551]

ზედამხედველი ორგანოს დამოუკიდებლობა ერთ-ერთი არსებითი მოთხოვნაა. დამოუკიდებლობის მოთხოვნის შეფასებისას ევროპული სასამართლო ყურადღებას ამახვილებს ზედამხედველი ორგანოს (პირის) არჩევის/დანიშვნის წესზე და იურიდიულ სტატუსზე.[552] აღნიშნული უნდა უზრუნველყოფდეს მის ინსტიტუციურ და ფუნქციურ დამოუკიდებლობას.

[547] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 55-56; Roman Zakharov v. Russia, [2015] ECtHR, 233.
[548] იქვე.
[549] იქვე.
[550] Roman Zakharov v. Russia, [2015] ECtHR, 233; Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 55-56.
[551] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 56.
[552] Roman Zakharov v. Russia, [2015] ECtHR, 278.

ზედამხედველობის მექანიზმის შეფასების კონტექსტში ერთ-ერთ ფუნდამენტურ საქმეს წარმოადგენს ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia), სადაც სასამართლომ უარყოფითად შეაფასა რუსეთის კანონმდებლობით გათვალისწინებული კომუნიკაციის მონიტორინგის ღონისძიებებზე ზედამხედველობის მექანიზმები. რუსეთის სამართლებრივი სისტემის მიხედვით, სამართალდამცავ ორგანოებს გააჩნდათ უწყვეტი მიერთების შესაძლებლობა კავშირგაბმულობის არხებთან, რომლის უზრუნველსაყოფად სერვისის პროვაიდერები ახდენდნენ შესაბამისი მოწყობილობის ინსტალაციას. აღნიშნული მოწყობილობა საშუალებას იძლეოდა, არ დაფიქსირებულიყო ფარული მიყურადების განხორციელების ფაქტის შესახებ ინფორმაცია[553]. სასამართლომ მიიჩნია, რომ ჩატარებული ღონისძიებების შესახებ მონაცემების აღრიცხვა განსაკუთრებით მნიშვნელოვანი გარანტიაა ზედამხედველი ორგანოს მიერ ღონისძიებების ჩატარების შესახებ ინფორმაციასთან ეფექტიანი წვდომის მიზნებისათვის. შესაბამისად, აღნიშნული ინფორმაციის დაფიქსირების შეუძლებლობა პრაქტიკულად გამორიცხავდა ზედამხედველი ორგანოს მიერ შესაბამისი ნებართვის გარეშე ღონისძიების ჩატარების ფაქტის დადგენას.[554] აღნიშნული დებულებისა და სამართალდამცავი ორგანოების მიერ ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის გათვალისწინებით, ევროპულმა სასამართლომ მიიჩნია, რომ რუსეთში შემუშავებული ზედამხედველობის მექანიზმი მოკლებული იყო ფარული მიყურადების განხორციელების პროცესში უკანონო ქმედების გამოაშკარავების შესაძლებლობას.[555]

როგორც უკვე აღინიშნა, საზედამხედველო მექანიზმის ეფექტიანობის კონტექსტში ერთ-ერთ გადამწყვეტ კრიტერიუმს ზედამხედველი ორგანოს უფლებამოსილების ფარგლები წარმოადგენს. ამ თვალსაზრისით მნიშვნელოვანია, რომ ეფექტიანი ზედამხედველობა იყოს გათვალისწინებული ღონისძიების აღსრულების მთელ პროცესზე. საქმეში ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria), ევროპულმა

[553] იქვე.
[554] იქვე.
[555] იქვე.

სასამართლომ განასხვავა სატელეფონო კომუნიკაციის ფარული მიყურადების ორი ეტაპი - ნებართვის გაცემის და ღონისძიების უშუალოდ განხორციელების.[556] მეორე ეტაპთან მიმართებით სასამართლოს უარყოფითი შეფასება გამოიწვია გამომძიებელი მოსამართლის შეზღუდულმა კომპეტენციამ. ბულგარეთის კანონმდებლობა არ ითვალისწინებდა ფარული მეთვალყურეობის ღონისძიებების აღსრულებაზე ზედამხედველობას ამ ღონისძიებათა განხორციელებაზე პასუხისმგებელი სუბიექტებისგან დამოუკიდებელი ორგანოს/პირის მხრიდან. კანონმდებლობის მიხედვით, ფარული საგამოძიებო მოქმედებების პრაქტიკულ აღსრულებაზე პასუხისმგებელი პირების გარდა, არავინ აკონტროლებდა, მოქმედებდნენ თუ არა ეს ორგანოები სასამართლოს ნებართვის შესაბამისად და რამდენად კეთილსინდისიერად ასახავდნენ ორიგინალ მონაცემებს წერილობითი სახით. ანალოგიურად, არ არსებობდა კონტროლის მექანიზმი ორიგინალი მონაცემების განადგურების მოთხოვნის შესრულებაზე კანონმდებლობით განსაზღვრულ 10 დღიან ვადაში, თუკი ფარული მეთვალყურეობა უშედეგო აღმოჩნდებოდა[557]. მართალია კანონმდებლობა ითვალისწინებდა სასამართლოს ინფორმირების ვალდებულებას ღონისძიების დამთავრებასთან დაკავშირებით, ასევე სასამართლოს ინფორმირებას ნებართვით გათვალისწინებულ ვადამდე ღონისძიების დასრულების შესახებ, მაგრამ არ განსაზღვრავდა სასამართლოს მიერ ღონისძიების შედეგების გაცნობის შესაძლებლობას და ასევე არ ავალდებულებდა მოსამართლეს, გადაემოწმებინა, რამდენად იქნა დაცული კანონმდებლობის მოთხოვნები ღონისძიების განხორციელებისას.[558]

ამ თვალსაზრისით აღსანიშნავია ასევე საქმე იორდაჩი მოლდოვის წინააღმდეგ (Iordachi and others v. Moldova), სადაც კონტროლის მექანიზმები უარყოფითად იქნა შეფასებული - მოლდოვის სისხლის სამართლის საპროცესო კანონმდებლობის თანახმად, სწორედ მოსამართლე გასცემდა კომუნიკაციის თუ ფარულ თვალთვალთან დაკავშირებულ ბრძანებას. კანონმდებლობა აგრეთვე ითვალისწინებდა, რომ "გამომძიებელ მოსამართლეს" შეეძლო შეენახა კომუნიკაციის კონტროლის შედეგად

[556] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 84; Iordachi and others v. Moldova, [2009], ECtHR, 42.
[557] იქვე. 84-85.
[558] იქვე.

წარმოებული ჩანაწერების დედნები სპეციალურად დალუქულ კონვერტებში, ასევე გაენადგურებინა ის მასალა, რომელიც მნიშვნელოვანი არ იყო სისხლის სამართლის საქმისათვის. მიუხედავად ამისა, კანონმდებლობა არ ითვალისწინებდა მოსამართლის მიერ აღნიშნული ღონისძიების შედეგად მიღწეული შედეგების გაცნობის შესაძლებლობას და ასევე არ მოითხოვდა, რომ მოსამართლეს ზედამხედველობა განეხორციელებინა ფარული თვალთვალის კანონიერებაზე.[559] კრიტიკა იქნა გამოხატული სხვა საქმეშიც, სადაც ეროვნული კანონმდებლობა ასევე არ განსაზღვრავდა რაიმე სახის ვალდებულებას, რომ შესაბამისი ორგანოების მიერ მოხსნილი ინფორმაცია წარედგინათ სასამართლოსთვის ან მოსამართლეს ჰქონოდა შესაძლებლობა, გადაემოწმებინა ფარული მეთვალყურეობის ღონისძიების მართლზომიერება.[560]

ანალოგიური პოზიცია გამოხატა ევროპულმა სასამართლომ საქმეში ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia). სასამართლოს კრიტიკა დაიმსახურა იმ გარემოებამ, რომ კომუნიკაციის მონიტორინგის ღონისძიების ჩატარებაზე ნებართვის გამცემ სასამართლოს არ გააჩნდა მის იმპლემენტაციაზე კონტროლის განხორციელების კომპეტენცია - არ ხდებოდა სასამართლოს ინფორმირება ღონისძიების შედეგების შესახებ და ამავდროულად, მოსამართლე მოკლებული იყო უფლებამოსილებას, განეხორციელებინა მის მიერ გაცემული ნებართვის მოთხოვნების შესრულებაზე კონტროლი[561]. ევროპულმა სასამართლომ მიიჩნია, რომ რუსეთის სასამართლოები მოკლებული იყვნენ ფარული მეთვალყურეობის ღონისძიებების განხორციელების მთელ პროცესზე ზედამხედველობის კომპეტენციას, სასამართლოს როლი შემოიფარგლებოდა მხოლოდ ნებართვის გაცემის ეტაპზე წინასწარი კონტროლის ფუნქციით. შემდგომი ზედამხედველობა კი მინიჭებული ჰქონდა პრეზიდენტს, პარლამენტს, მთავრობას და პროკურატურას. პრეზიდენტის, პარლამენტისა და მთავრობის ზედამხედველობასთან დაკავშირებით ევროპულმა სასამართლომ აღნიშნა, რომ არ არსებობდა საჯაროდ ხელმისაწვდომი

[559] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, 207 <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [25.06.2020], იხ. ციტირება: Iordachi and others v. Moldova, [2009], ECtHR.
[560] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, 207 <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [25.06.2020], იხ. ციტირება: Huvig v. France, [1990], ECtHR, (Ser. A.).
[561] Roman Zakharov v. Russia, [2015] ECtHR, 274.

რეგულაცია/ინსტრუქცია მათი მხრიდან ზედამხედველობის განხორციელების წესსა და პროცედურასთან დაკავშირებით. რაც შეეხება პროკურორების მხრიდან ზედამხედველობას, სასამართლომ მიიჩნია, რომ პროკურორები არ იყვნენ აღჭურვილი ეფექტიანი ზედამხედველობის განსახორციელებლად აუცილებელი დამოუკიდებლობის ხარისხითა და შესაბამისი კომპეტენციით. ამდენად, რუსეთის კანონმდებლობით ორგანიზებული ზედამხედველობის სისტემა ვერ უზრუნველყოფდა თვითნებობის საწინააღმდეგო ადეკვატურ და ეფექტურ გარანტიებს.[562]

როდესაც საუბარია ზედამხედველო ორგანოს კომპეტენციაზე, ერთ-ერთი მნიშვნელოვანი ფაქტორი, რომელსაც ყურადღება ექცევა ზედამხედველობის ეფექტიანობის კონტექსტში, არის მაკონტროლებელი ორგანოს უფლებამოსილება რაიმე დარღვევის აღმოჩენის კუთხით - მაგალითად, ევროპულმა სასამართლომ დადებითად შეაფასა მაკონტროლებელი ორგანოს კომპეტენციის ფარგლები, როდესაც კომუნიკაციის მონიტორინგის განმახორციელებელ ორგანოს ეკისრებოდა ღონისძიების შეწყვეტის ვალდებულება საზედამხედველო კომისიის მიერ მისი „უკანონოდ“ ან „არააუცილებლად“ მიჩნევისას;[563] ასევე, როდესაც მაკონტროლებელი ორგანოს მიერ ჩატარებული ღონისძიების უკანონოდ მიჩნევის შემთხვევაში მოპოვებული ინფორმაცია განადგურებას ექვემდებარებოდა.[564] მაკონტროლებელი ორგანოს მიერ შემოწმების განხორციელების პროცესში უკანონოდ მოპოვებული ინფორმაციის განადგურების მოთხოვნის მნიშვნელობაზე ევროპულ სასამართლოს სხვა საქმეშიც აქვს ყურადღება გამახვილებული.[565] ამასთან, ზედამხედველობის სისტემის ეფექტიანობის მიზნებისათვის აუცილებელია, რომ მაკონტროლებელ ორგანოს გააჩნდეს წვდომა ყველა რელევანტურ დოკუმენტაციაზე, მათ შორის, გასაიდუმლოებულ მასალებზე და სამართალდამცავმა ორგანოებმა ხელი შეუწყონ მისი ამ უფლების პრაქტიკაში რეალიზებას.[566]

კიდევ ერთი ასპექტი, რომელსაც ზედამხედველობის სისტემის ეფექტიანობის კონტექსტში ექცევა ყურადღება, უკავშირდება მაკონტროლებელი ორგანოს

[562] იქვე. 274-285.
[563] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 53.
[564] Kennedy v. United Kingdom, [2010] ECtHR, 168.
[565] Roman Zakharov v. Russia, [2015] ECtHR, 282.
[566] იქვე. 281.

საქმიანობის საჯაროობას, გამჭვირვალობის მექანიზმებს, მაგალითად, მოცემული მოთხოვნა დარღვეულად იქნა მიჩნეული საქმეში ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria), სადაც არც შინაგან საქმეთა მინისტრს და არც სხვა რომელიმე თანამდებობის პირს არ ეკისრებოდა დამოუკიდებელი ორგანოს ან საზოგადოების წინაშე ანგარიშვალდებულება ფარული მეთვალყურეობის სისტემის ზოგად ფუნქციონირებასთან ან ინდივიდუალურ შემთხვევებში გამოყენებულ ღონისძიებებთან დაკავშირებით.[567] ამ კუთხით მნიშვნელოვანია ასევე საქმე ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia). ამ საქმეში ზედამხედველი პირები (პროკურორები) წელიწადში ორჯერ წარადგენდნენ ანგარიშებს განხორციელებულ შემოწმებებსა და აღმოჩენილ დარღვევებთან დაკავშირებით, თუმცა სასამართლომ უარყოფითად შეაფასა ის ფაქტი, რომ ეს ანგარიშები შეეხებოდა ყველა სახის ოპერატიულ-სამძებრო ღონისძიებას მთლიანობაში, ისე რომ სატელეფონო კომუნიკაციის მონიტორინგი არ იყო სხვა ღონისძიებებისგან გამოცალკავებულად განხილული. გარდა ამისა, ეს ანგარიშები შეიცავდა მხოლოდ სტატისტიკურ ინფორმაციას და არაფერი იყო ნათქვამი დარღვევის ხასიათის და მის გამოსასწორებლად მიღებული ზომების თაობაზე. ამასთანავე, ანგარიში წარმოადგენდა კონფიდენციალურ დოკუმენტს და საზოგადოებას ხელი არ მიუწვდებოდა მასზე.[568]

3.8. ღონისძიების ადრესატისთვის შეტყობინების ვალდებულება და ჩატარებული ღონისძიების გასაჩივრება

ფარული საგამოძიებო მოქმედების განხორციელების შესახებ ადრესატისათვის შეტყობინების საკითხი საერთაშორისო დონეზე განმტკიცებულ უფლების ბოროტად გამოყენების საწინააღმდეგო ერთ-ერთ უმნიშვნელოვანეს გარანტიას წარმოადგენს. აღნიშნული პირდაპირ უკავშირდება უფლების დაცვის სამართლებრივი მექანიზმების ეფექტიანობას.[569] მოცემული გარანტიის დანიშნულება

[567] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 88.
[568] Roman Zakharov v. Russia, [2015], ECtHR, 283.
[569] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13-14 (ბმული იხ. მე-19 გვერდზე).

ადრესატისათვის განხორციელებული ღონისძიების კანონიერების შემდგომი გადამოწმების შესაძლებლობის უზრუნველყოფაში მდგომარეობს. აღსანიშნავია, რომ „პოლიციის სექტორში პერსონალურ მონაცემთა დამუშავების თაობაზე" ევროსაბჭოს მინისტრთა კომიტეტის რეკომენდაცია პირდაპირ მიუთითებს მონაცემთა დამუშავების ფაქტის ადრესატისათვის შეტყობინების საკითხზე, კერძოდ, აღნიშნული რეკომენდაციის თანახმად, „როდესაც ხდება პირის შესახებ ინფორმაციის შეგროვება და შენახვა მისი ცოდნის გარეშე და ეს მონაცემები არ არის განადგურებული, საჭიროების შემთხვევაში, პირს უნდა ეცნობოს ამის თაობაზე მას შემდეგ, რაც აღარ იარსებებს პოლიციის საქმიანობისთვის ხელის შეშლის საფრთხე."[570]

არც ევროპული სასამართლოს პრეცედენტული სამართალი და არც სხვა საერთაშორისო სტანდარტები იმპერატიულად არ მოითხოვს ღონისძიების დასრულებისთანავე ადრესატისთვის დაუყოვნებლივ შეტყობინებას. ევროპულ სასამართლოს არაერთხელ აღუნიშნავს, რომ პრაქტიკაში ყოველთვის შესაძლებელი არ არის განხორციელებული ღონისძიების შესახებ ადრესატისათვის შემდგომი შეტყობინება[571]. ქმედება ან საფრთხეები, რომელთან მიმართებაშიც დაიწყო კომუნიკაციის მონიტორინგის ღონისძიებები, შესაძლოა მათი დასრულების შემდეგ წლების და ათწლეულების განმავლობაშიც კი გრძელდებოდეს. მათ შესახებ პირის ინფორმირებამ კი შესაძლოა დააზიანოს ლეგიტიმური მიზანი, რომელიც საფუძვლად დაედო მის ჩატარებას[572]. შესაბამისად, ფარული საგამოძიებო მოქმედების დამთავრებისთანავე ადრესატის არაინფორმირებულობის ფაქტი თავისთავად არ ნიშნავს, რომ პირად ცხოვრებაში ჩარევა არ წარმოადგენს აუცილებლობას დემოკრატიულ საზოგადოებაში, ვინაიდან სწორედ ფარული ხასიათი განაპირობებს ღონისძიების ეფექტიანობას[573]. მიუხედავად აღნიშნულისა, შეტყობინება აუცილებელია მაშინვე, როდესაც საფრთხეს არ უქმნის შეზღუდვის ლეგიტიმური მიზნის განხორციელებას.[574]

---

[570] Recommendation R(87)15 of the Committee of Ministers Regulating the Use of Personal Data in The Police Sector, Council of Europe, 17/09/1987.

[571] Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI· 135; Klass and Others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 58; Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 90-91.

[572] იქვე.

[573] იქვე.

[574] იქვე.

საქმეებში კლასი და სხვები გერმანიის წინააღმდეგ (Klass and others v. Germany) და ვებერი და სარავია გერმანიის წინააღმდეგ (Weber and Saravia v. Germany), ევროპულმა სასამართლომ შეაფასა გერმანიის კანონმდებლობა, რომელიც ითვალისწინებდა ფარული მეთვალყურეობის ღონისძიების დასრულების შემდეგ ადრესატისათვის შეტყობინებას, როგორც კი აღნიშნული საზიანო არ იქნებოდა ლეგიტიმური მიზნისთვის. სასამართლომ მხედველობაში მიიღო ის გარემოება, რომ გადაწყვეტილებას იმის შესახებ, უნდა განხორციელებულიყო თუ არა პირის ინფორმირება ჩატარებული ღონისძიების შესახებ, იღებდა დამოუკიდებელი ორგანო (G10 კომისია). ევროპულმა სასამართლომ გერმანიის კანონმდებლობით განსაზღვრული შეტყობინების მექანიზმი ლეგიტიმური მიზნის მიღწევის პროპორციულ საშუალებად მიიჩნია.[575]

შეტყობინების მოთხოვნა დარღვეულად იქნა მიჩნეული საქმეში ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia), სადაც რუსეთის კანონმდებლობა არ ითვალისწინებდა ადრესატისთვის მის მიმართ ჩატარებული ღონისძიების შესახებ შეტყობინებას პროცესის არცერთ სტადიაზე. როგორც გაირკვა, თუკი ამ პირის მიმართ სისხლისსამართლებრივი პროცედურები არ განხორციელდებოდა და მოპოვებულ ინფორმაციას მტკიცებულებად არ გამოიყენებდა ბრალდების მხარე, ან თუკი ინფორმაცია არ გამოჟონავდა შესაბამისი ორგანოდან, პირი ვერასდროს შეიტყობდა მისი კომუნიკაციის მონიტორინგის შესახებ.[576]

როგორც უკვე აღინიშნა, შეტყობინების საკითხი პირდაპირ უკავშირდება პირის უფლებას, შესაბამის უფლებამოსილ ორგანოსთან გადაამოწმოს ჩატარებული ღონისძიების კანონიერება, დარღვევის აღმოჩენის შემთხვევაში კი მოითხოვოს ზიანის ანაზღაურება. კომუნიკაციის მონიტორინგის ადრესატისთვის უნდა იყოს ხელმისაწვდომი აღნიშნული ღონისძიების კანონიერების „ეფექტიანი შემოწმების“ შესაძლებლობა.[577] ამასთან, ინდივიდისთვის თავისი სატელეფონო კომუნიკაციის მიყურადების გასაჩივრების უფლებაზე უარის თქმა იმ არგუმენტზე დაყრდნობით,

---

[575] Klass and Others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 57; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 135.

[576] Roman Zakharov v. Russia, [2015], ECtHR, 289.

[577] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08.2019, 104, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>, [18.06.2020], იხ. ციტირება: Marchiani v. France, [2008], ECtHR.

რომ ადგილი ჰქონდა მხოლოდ „მესამე პირის სატელეფონო ხაზის“ მოსმენას, არ შეესაბამება კონვენციის მოთხოვნებს.[578] გარდა ამისა, ევროპული სასამართლოს მიდგომის მიხედვით, აუცილებელია ჩატარებული ღონისძიების გასაჩივრების მოთხოვნის უფლება გააჩნდეს არამარტო იმ პირს, ვის მიმართაც დაიწყო სისხლისსამართლებრივი პროცედურები, რომელთან დაკავშირებითაც შეიტყო ღონისძიების ჩატარების ფაქტი, არამედ იმ პირსაც, რომლის მიმართაც ფარული მეთვალყურეობის ღონისძიებების შედეგად ასეთი პროცედურები არ განხორციელებულა.[579]

ფარული საგამოძიებო მოქმედების გასაჩივრების მექანიზმის ეფექტიანობასთან დაკავშირებით ევროპულმა სასამართლომ განმარტა, რომ ზედამხედველ ორგანოს უნდა გააჩნდეს უფლებამოსილება, შეამოწმოს ღონისძიების ჩატარებაზე ნებართვის გაცემის და მისი განხორციელების კანონიერება. ღონისძიების რეტროსპექტიული შემოწმების დროს შესაბამისი პირი, როგორც მინიმუმ, უზრუნველყოფილი უნდა იყოს საკმარისი ინფორმაციით ნებართვის არსებობასთან და იმ გადაწყვეტილებასთან დაკავშირებით, რომლითაც მოხდა ნებართვის გაცემა.[580]

3.9. შეჯამება

განხილული საერთაშორისო სტანდარტების შეჯამების შედეგად გამოიკვეთა ფარული მეთვალყურეობის სფეროში შემუშავებული შემდეგი პროცედურული გარანტიები:

- ფარული მეთვალყურეობის ღონისძიების ჩატარება შესაძლებელია მხოლოდ მძიმე დანაშაულის წინააღმდეგ. ეროვნულმა კანონმდებლობამ “მძიმე” დანაშაულის ცნება არ უნდა განმარტოს იმგვარად ფართოდ, რომ სისხლის სამართლის კოდექსით გათვალისწინებულ დანაშაულთა უმეტესობა ამგვარი ცნების ქვეშ მოიაზრებოდეს.

- ეროვნულმა სამართლებრივმა რეგულაციებმა უნდა განსაზღვრონ კონკრეტულ პირთა კატეგორია, რომელთა მიმართაც დაიშვება კომუნიკაციის მონიტორინგი. თუკი

[578] Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08.2019, 104, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>, [18.06.2020], იხ. ციტირება: Lambert v. France, [1998], Reports of Judgments and Decisions 1998-V, 38-41.

[579] Roman Zakharov v. Russia, [2015] ECtHR, 295.

[580] Šantare and Labaznikovs v. Latvia, [2016], ECtHR, 55.

კანონმდებლობა უშვებს მესამე პირთა მიმართ ასეთი ღონისძიების გამოყენების შესაძლებლობას, აუცილებელია საკმარისი სიცხადით დარეგულირდეს, თუ როდის შეიძლება მესამე პირი დაექვემდებაროს ზედამხედველობას, კერძოდ, უნდა განისაზღვროს თუ რა გზით შეიძლება ფლობდეს ის გამოძიებისათვის რელევანტურ ინფორმაციას (მაგალითად, იყენებს ბრალდებულის ტელეფონს);

კანონმდებლობა საკმარისი სიცხადით უნდა არეგულირებდეს იმ პირებთან მიმართებით ღონისძიების განხორციელების საკითხს, რომლებიც შემთხვევით დაექვემდებარნენ კომუნიკაციის მონიტორინგს და შესაბამისი ორგანოების დისკრეციის ფარგლებს ამ შემთხვევაში.

- ფარული საგამოძიებო მოქმედების საერთო ხანგრძლივობა უნდა იყოს თანხვედრაში თანაზომიერების პრინციპთან. აღნიშნულ ვადაზე განრძობადი ზედამხედველობა უნდა განხორციელდეს და ღონისძიება შეწყდეს მაშინვე, როდესაც მისი გაგრძელება აღარ არის აუცილებელი ლეგიტიმური მიზნის მისაღწევად.

- სისტემა, რომელიც სამართალდამცავ ორგანოებს ანიჭებს ელექტრონულ კომუნიკაციებზე პირდაპირი წვდომის შესაძლებლობას, ნებისმიერ შემთხვევაში მიდრეკილია უფლებამოსილების ბოროტად გამოყენების რისკისკენ, ვინაიდან ასეთ შემთხვევაში ეფექტიანი ზედამხედველობის განხორციელება ძალიან რთულდება. კომუნიკაციებზე წვდომის სისტემამ, საერთო ჯამში, უნდა უზრუნველყოს, რომ ტექნიკურად შეუძლებელი იყოს ფარული საგამოძიებო ღონისძიების ჩატარება სასამართლოს ნებართვის გარეშე და ჩატარებული ღონისძიების ნებისმიერი ფაქტი იყოს აღრიცხული, რათა ზედამხედველმა პირმა შეძლოს ღონისძიების ჩატარების კანონიერების გადამოწმება. ვინაიდან, პირდაპირი მიერთების ტექნიკური შესაძლებლობის პირობებში სამართალდამცავი ორგანოების ტექნიკური შესაძლებლობები ძალიან ძლიერია, ყოველთვის რჩება კითხვის ნიშნები მათი მხრიდან შესაძლო თვითნებობასთან დაკავშირებით, აქედან გამომდინარე, ასეთი სისტემა, ზოგადი თვალსაზრისით, დადებითად არ არის შეფასებული. ქვეყანაში ამგვარი სისტემის არსებობის შემთხვევაში, განსაკუთრებული მნიშვნელობა ზედამხედველობის ეფექტიან და ქმედით მექანიზმებს ენიჭება; სწორედ კონტროლის ასეთმა სისტემამ უნდა დააბალანსოს სახელმწიფოს ხელთ არსებული მძლავრი ტექნიკური შესაძლებლობების თანმდევი საფრთხეები.

- ფარული მეთვალყურეობის ღონისძებებზე სასამართლოს ზედამხედველობა წარმოადგენს ზოგად წესს, თვითნებობისგან დაცვის უმნიშვნელოვანეს მექანიზმს, თუმცა გადამწყვეტი მნიშვნელობა ენიჭება ამ მექანიზმის პრაქტიკაში ეფექტიანობას; ერთ-ერთი არსებითი ფაქტორი, რომლითაც სასამართლო კონტროლის ეფექტიანობა იზომება, წარმოადგენს მოსამართლის კომპეტენციის ფარგლები.

აუცილებელია ნებართვის გამცემ ორგანოს გააჩნდეს რეალური ბერკეტი შეამოწმოს, რამდენად არის საქმეში წარმოდგენილი საკმარისი ფაქტობრივი საფუძველი ღონისძიების ჩასატარებლად და რამდენად არსებობს დანაშაულის ჩადენის თაობაზე საკმარისი საფუძველი (ევროპული სასამართლოს პრაქტიკის მიხედვით - "Reasonable suspicion"). აღნიშნულის უზრუნველსაყოფად სასამართლოს უნდა წარედგინოს ყველა რელევანტური მტკიცებულება. ამასთან, სასამართლომ უნდა შეამოწმოს, რამდენად წარმოადგენს მოთხოვნილი ღონისძიება უფლების ყველაზე ნაკლებად შემზღუდველ საშუალებას და ხომ არ არსებობს სხვა უფრო ნაკლებად ინტენსიური მეთოდის გამოყენების შესაძლებლობა. სასამართლოს გადაწყვეტილება აღნიშნულ საკითხთან დაკავშირებით უნდა იყოს დასაბუთებული საქმის კონკრეტული ფაქტობრივი და ინდივიდუალური გარემოებებით და მხოლოდ „ზოგადი მითითებები" გამოძიების სხვა საშუალებებით წარმართვის „შეუძლებლობაზე ან უკიდურეს სირთულეზე" ვერ ჩაითვლება საკმარისად.

- ეროვნული კანონმდებლობა დეტალურად უნდა არეგულირებდეს ფარული მეთვალყურეობის ღონისძიების შედეგად მოპოვებული ინფორმაციის შემოწმების, გამოყენების, შენახვის, სხვა პირებისთვის გადაცემისა და განადგურების წესებს. ამ თვალსაზრისით ერთ-ერთ არსებით მოთხოვნას წარმოადგენს მონაცემთა გამოკვლევის (გადარჩევის) საკითხის მოწესრიგება განჭვრეტადი და საზოგადოებისათვის ხელმისაწვდომი ფორმით. მნიშვნელოვანია, მონაცემთა შემდგომი შენახვის აუცილებლობის გადამოწმება განხორციელდეს პერიოდულად. სხვა სამართალდამცავი ორგანოებისათვის მონაცემთა გადაცემის შემთხვევაში, უზრუნველყოფილი უნდა იქნეს მონაცემთა უსაფრთხოდ გადაცემა და აგრეთვე მხოლოდ იმ მოცულობით, რაც მიმღებ ორგანოს ესაჭიროება ლეგიტიმური მიზნის მისაღწევად. ამასთან, უზრუნველყოფილი უნდა იყოს აღნიშნულ პროცესზე დამოუკიდებელი ორგანოს მხრიდან ზედამხედველობა.

- ერთ-ერთ ფუნდამენტურ გარანტიას წარმოადგენს ფარულ საგამოძიებო მოქმედებებზე ეფექტიანი ზედამხედველობის განხორციელება. ეფექტიანი ზედამხედველობა უნდა იყოს გათვალისწინებული ღონისძიების აღსრულების მთელ პროცესზე და ზედამხედველი ორგანოს კომპეტენცია არ უნდა იყოს შეზღუდული, მაგალითად, ევროპულმა სასამართლომ არაერთ საქმეში გამოხატა უარყოფითი პოზიცია, როდესაც ეროვნული კანონმდებლობა არ ითვალისწინებდა მოსამართლის მიერ ღონისძიების შედეგების გაცნობისა და ღონისძიების განხორციელების კანონიერებაზე ზედამხედველობის შესაძლებლობას.

- ეროვნული კანონმდებლობით უზრუნველყოფილი უნდა იყოს ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის დაცვის ეფექტიანი და ქმედითი მექანიზმი. აუცილებელია იმ პროცედურის განსაზღვრა, რომლის მიხედვითაც უნდა მოხდეს პრივილეგირებული ინფორმაციის გამოცალკავება არაპრივილეგირებულისგან. ადვოკატსა და კლიენტს შორის ურთიერთობის კონფიდენციალურობა არ ვრცელდება იმ კომუნიკაციაზე, რომელიც ეხება ადვოკატის დანაშაულებრივ საქმიანობას. ამასთან, ადვოკატსა და კლიენტს შორის კომუნიკაციის მიყურადების შედეგად მოპოვებული, ადვოკატის დანაშაულებრივ საქმიანობასთან დაკავშირებული ჩანაწერები არ უნდა იქნეს ბრალდებულის საწინააღმდეგოდ გამოყენებული.

- ფარული მეთვალყურეობის ღონისძიების ადრესატისათვის შეტყობინება ერთ-ერთ არსებით მოთხოვნას განეკუთვნება. ამ უფლების დანიშნულებას ადრესატისათვის ღონისძიების კანონიერების გადამოწმების შესაძლებლობის მიცემა წარმოადგენს. ამ თვალსაზრისით ევროპული სასამართლო უფრო მკაცრ პოზიციას აფიქსირებს, ვიდრე ეს გათვალისწინებულია “პოლიციის სექტორში პერსონალურ მონაცემთა დამუშავების თაობაზე” ევროსაბჭოს მინისტრთა კომიტეტის რეკომენდაციაში, კერძოდ, ევროპული სასამართლოს პრეცედენტული სამართლიდან გამომდინარე, ჩატარებული ღონისძიების შესახებ ადრესატისათვის შეტყობინება აუცილებელია მაშინვე, როგორც კი აღნიშნული ხელს არ შეუშლის გამოძიების ინტერესების განხორციელებას. ამასთან, შეტყობინების მექანიზმის ეფექტიანობა დამოკიდებულია შეტყობინების განმახორციელებელ სუბიექტზე - ევროპულმა სასამართლომ რამოდენიმე საქმეში ყურადღება გაამახვილა იმ გარემოებაზე, რომ აღნიშნული ფუნქცია დაკისრებული ჰქონდა დამოუკიდებელ ორგანოს.

ღონისძიების გასაჩივრების მოთხოვნის უფლება გააჩნია არა მარტო იმ პირს, ვის მიმართაც დაიწყო სისხლისსამართლებრივი პროცედურები, რომელთან დაკავშირებითაც შეიტყო ღონისძიების ჩატარების ფაქტი, არამედ იმ პირსაც, რომლის მიმართაც ასეთი პროცედურები არ განხორციელებულა. ამდენად, შეტყობინება აუცილებელია იმის მიუხედავად, გამოყენებული იქნება თუ არა მოპოვებული ინფორმაცია სასამართლოში პირის საწინააღმდეგო მტკიცებულებად.

4. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის საკითხი

4.1. ზოგადი მიმოხილვა

თანამედროვე კავშირგაბმულობის სამყაროში შინაარსობრივ მონაცემებსა და მეტადატას შორის განსხვავება თანდათანობით უმნიშვნელო ხდება. გადაწყვეტილებაში Tele2 Sverige AB and Watson, ევროკავშირის მართლმსაჯულების სასამართლომ მხარი დაუჭირა ამ იდეას იმით, რომ დაადგინა თანაბარი მიდგომა კომუნიკაციის შინაარსსა და მეტადატასთან მიმართებით და მიიჩნია, რომ მომხმარებლის პირადი „პროფილის“ შედგენა, „პირადი ცხოვრების ხელშეუხებლობის უფლებასთან მიმართებით არ არის ნაკლებად სენსიტიური, ვიდრე თავად კომუნიკაციის შინაარსი.“[581]

როგორც უკვე აღინიშნა, კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გამოყენების შედეგად შესაძლებელია შეიქმნას სანდო და ამომწურავი პორტრეტი ადამიანის პირად ცხოვრებას მიკუთვნებული მრავალი ასპექტის თაობაზე და „სრულყოფილი და ზუსტი სურათიც“ კი მისი პიროვნული იდენტობის შესახებ.[582] ასეთ მონაცემებზე დაკვირვების შედეგად, დაინტერესებულმა პირმა შესაძლებელია დეტალური დასკვნები გამოიტანოს ინდივიდის დასაქმების, გადაადგილების (მგზავრობის) საშუალებების და ქცევის, სამედიცინო, სოციალურ და კომერციულ

[581] *Brkan M.*, The Essence of The Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the Cjeu's Constitutional Reasoning, German Law Journal, Vol. 20, 2019, 873, იხ. ციტირება: *Ojanen T.,* Privacy Is More Than Just a Seven Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance.

[582] Opinion of Advocate General, Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, 12.12.2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293> [20.06.2020].

დაწესებულებებში ვიზიტების, რელიგიური და პოლიტიკური კავშირების და სხვა ასპექტების შესახებ.[583] ევროკავშირის გენერალური ადვოკატის განმარტებით, ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემები შეიძლება გამოყენებულ იქნეს ინდივიდის პირადი პროფილის შესადგენად და ასეთი ინფორმაცია სენსიტიურობის ხარისხით არ ჩამოუვარდება კომუნიკაციის უშუალო შინაარსს[584].

კომუნიკაციის მაიდენტიფიცირებელი მონაცემები (მეტადატა) ექცევა კონვენციის მე-8 მუხლითა და ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7, მე-8 მუხლებით უზრუნველყოფილი კომუნიკაციის ხელშეუხებლობის უფლების დაცვის ქვეშ. საერთაშორისო სტანდარტის მიხედვით, კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შეგროვება და შენახვა თავისთავად წარმოადგენს ჩარევას პირადი ცხოვრების უფლებაში, მიუხედავად იმისა, გამოყენებულ იქნა თუ არა ეს მონაცემები სახელმწიფო ორგანოების მიერ[585].

აღსანიშნავია, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვა აქტიურად განიხილება საერთაშორისო დონეზე. არაერთ საერთაშორისო დოკუმენტში არის გამახვილებული ყურადღება იმ საფრთხეების შესახებ, რასაც სერვისის პროვაიდერების მიერ ამგვარი მონაცემების სავალდებულო შენახვა უქმნის პიროვნების პირადი ცხოვრების ინტერესებს. გაეროს სპეციალური მომხსენებლის ანგარიშის მიხედვით, თანდათანობით უფრო იზრდება სახელმწიფოების მოთხოვნა სერვისის მიმწოდებლების მიერ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა "ყოველი შემთხვევისთვის" შენახვის პრაქტიკაზე[586]. ეროვნული კანონმდებლობები, რომლებიც ავალდებულებს სერვისის მიმწოდებლებს, აღნიშნული ინფორმაცია შეინახონ სამართალდამცავი ორგანოების მიერ შემდგომი გამოყენების მიზნებისთვის,

---

[583] *Forcese C.,* Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives, წიგნში: Law, Privacy and Surveillance in Canada in the Post-Snowden Era, *Geist M. (ed.)*, 2015, 129.

[584] Opinion of Advocate General, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, 19.07.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0203> [20.06.2020].

[585] Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, 13, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf> [15.06.2020].
S and Marper v. United Kingdom, [2008], ECtHR; Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice.

[586] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9 (ბმული იხ. მე-19 გვერდზე).

ვერ აკმაყოფილებს პროპორციულობისა და აუცილებლობის მოთხოვნებს[587] და საფრთხეს უქმნის პირადი ცხოვრების ხელშეუხებლობის უფლებას.[588]

4.2. „მონაცემთა შენახვის შესახებ“ ევროკავშირის პარლამენტისა და საბჭოს დირექტივა

პერსონალურ მონაცემთა დაცვა და პირადი ცხოვრების ხელშეუხებლობის უფლება უკვე დიდი ხანია ევროკავშირის დღის წესრიგში დგას, თუმცა ბოლო წლებში ამ მიმართულებით მუშაობა გაცილებით გააქტიურდა.[589] 2014 წელს ევროკავშირის მართლმსაჯულების სასამართლომ საქმეზე „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“ გამოიტანა ისტორიული გადაწყვეტილება და გააუქმა ევროკავშირის პარლამენტისა და საბჭოს „მონაცემთა შენახვის შესახებ” 2006 წლის 15 მარტის 2006/24/EC დირექტივა, რომელიც საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლებს აკისრებდა ვალდებულებას, შეენახათ ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემები 6 თვიდან 2 წლამდე ვადით სამართალდამცავი ორგანოებისთვის გადაცემის უზრუნველსაყოფად, „მძიმე დანაშაულის“ გამოძიების მიზნებისათვის[590]. მოცემულ საკითხთან დაკავშირებით ევროკავშირის პრინციპულ მოსაზრებას კიდევ უფრო გაესვა ხაზი ევროკავშირის მართლმსაჯულების სასამართლოს 2016 წლის 21 დეკემბრის გადაწყვეტილებით Tele2 Sverige AB and Watson, რომლითაც კიდევ უფრო დაზუსტდა და გაფართოვდა 2014 წლის გადაწყვეტილებით დადგენილი მოთხოვნები.[591]

აღსანიშნავია, რომ „მონაცემთა შენახვის შესახებ” ევროკავშირის პარლამენტისა და საბჭოს დირექტივა მიღებულ იქნა 2006 წელს, როგორც ევროკავშირის ანტიტერორისტული კანონმდებლობის ნაწილი.[592] მონაცემთა შენახვის დირექტივის დანიშნულებას მონაცემთა შენახვასთან დაკავშირებული ეროვნული დებულებების

[587] იქვე.

[588] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 18 (ბმული იხ. მე-80 გვერდზე).

[589] *Stoeva E.,* The Data Retention Directive and the Right to Privacy, ERA (Academy of European Law) Forum, 2014, 15, 575.

[590] Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice.

[591] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice.

[592] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 160.

ჰარმონიზაცია და „მძიმე დანაშაულის“ გამოვლენის, გამოძიების და დევნის მიზნებისათვის კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ხელმისაწვდომობა წარმოადგენდა.[593] დირექტივა ვრცელდებოდა ტრაფიკისა და ადგილმდებარეობის შესახებ მონაცემების და მათთან დაკავშირებული, მომხმარებლის იდენტიფიკაციისათვის საჭირო მონაცემების შენახვაზე (მუხლი 2(2a)). ამასთან, დირექტივა არ ეხებოდა კომუნიკაციის შინაარსობრივ მონაცემებს. უფრო კონკრეტულად კი, დირექტივის მე-5 მუხლი განსაზღვრავდა იმ მონაცემთა ჩამონათვალს, რომლის შენახვაც ევალებოდათ ელექტრონული საკომუნიკაციო სერვისის მიმწოდებლებს:

ა) კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; ბ) კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; გ) კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; დ) კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; ე) მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; ვ) მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები. ამასთან, დირექტივის მე-5 მუხლი ადგენდა იმ მონაცემთა კონკრეტულ ჩამონათვალს, რომელიც შედიოდა მონაცემთა თითოეულ ამ სახეობაში.[594]

ამდენად, დირექტივის მიხედვით, ფიქსირებული და მობილური სატელეფონო სერვისების, ასევე ინტერნეტ სერვისის პროვაიდერებს ეკისრებოდათ ვალდებულება, შეენახათ სერვისის მომხმარებლების მონაცემები, რომლებიც იძლეოდა კომუნიკაციის წყაროს, თარიღის, დროის და ხანგრძლივობის, ასევე კომუნიკაციის ტიპის, გამოყენებული საკომუნიკაციო აღჭურვილობისა და მომხმარებლის ადგილმდებარეობასთან დაკავშირებული მონაცემების იდენტიფიცირების შესაძლებლობას. ასეთი მონაცემები, მათ შორის, მოიცავდა, მომხმარებლის ვინაობას და მისამართს, ზარის ინიციატორის და ადრესატის ტელეფონის ნომრებს და IP

[593] Article 1, Directive 2006/24/EC of the European Parliament and of the Council On the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 15/03/2006 <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024> [20.06.2020].

[594] იქვე, Article 5.

მისამართს ინტერნეტ სერვისების შემთხვევაში[595]. ამასთან, დირექტივა ითვალისწინებდა ამ მონაცემების ტოტალურ შენახვას, რომლის მოცულობაც არ იყო შეზღუდული რაიმე კრიტერიუმით.

აღსანიშნავია, რომ ზოგიერთმა სახელმწიფომ საწინააღმდეგო მოსაზრება გამოხატა დირექტივის ეროვნულ კანონმდებლობაში იმპლემენტაციასთან დაკავშირებით[596]. ეროვნული რეგულაციები „მონაცემთა შენახვის შესახებ“ დირექტივის იმპლემენტაციის თაობაზე დავის საგნად იქცა, მაგალითად, გერმანიაში, ბულგარეთში, რუმინეთში, უნგრეთში, ჩეხეთში, კვიპროსსა და სლოვაკეთში.[597] საბოლოო ჯამში კი, ირლანდიის უმაღლესი სასამართლოსა და ავსტრიის საკონსტიტუციო სასამართლოს მიერ ევროკავშირის მართლმსაჯულების სასამართლოსთვის მიმართვის საფუძველზე, „მონაცემთა შენახვის შესახებ“ დირექტივა მართლმსაჯულების სასამართლოს გადაწყვეტილებით გაუქმებულ იქნა.

4.3. ევროკავშირის მართლმსაჯულების სასამართლოს მიერ დადგენილი სტანდარტები

საქმეზე „სეიტლინგერი და სხვები ირლანდიის წინააღმდეგ” ევროკავშირის მართლმსაჯულების სასამართლომ განიხილა მონაცემთა შენახვის შესახებ დირექტივის შესაბამისობა ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მე-7 მუხლითა და კონვენციის მე-8 მუხლით განმტკიცებულ პირადი ცხოვრების უფლებასა და ქარტიის მე-8 მუხლით უზრუნველყოფილ პერსონალური მონაცემების დაცვის გარანტიასთან. სასამართლომ დაადგინა, რომ დირექტივით გათვალისწინებული ტრაფიკის და ადგილმდებარეობის მონაცემების შენახვა აღნიშნულ უფლებებში ჩარევის არათანაზომიერ საშუალებას წარმოადგენდა.[598]

ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, მიუხედავად იმისა, რომ დირექტივა შინაარსობრივი მონაცემების შენახვის ნებას არ იძლეოდა, ტრაფიკის და ადგილმდებარეობის შესახებ ასეთი დიდი მოცულობის ინფორმაცია,

[595] Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice, 26.
[596] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 160.
[597] *Tzanou M.,* The Fundamental Right to Data Protection, Normative Value in the Context of Counter-Terrorism Surveillance, Oxford, 2017, 75.
[598] S and Marper v. United Kingdom, [2008], ECtHR.

ერთად აღებული, შესაძლებელია გამოყენებულ იქნეს პიროვნების პირადი ცხოვრების არაერთი ასპექტის შესახებ დასკვნების გამოსატანად, როგორიცაა ადამიანის ყოველდღიური ჩვევები, მუდმივი და დროებითი ადგილსამყოფელი, ყოველდღიური და სხვაგვარი გადაადგილება, საქმიანობა, სოციალური კავშირები და სოციალური გარემოცვა. შესაბამისად, ამ მონაცემების შენახვა წარმოადგენს პირად ცხოვრებასა და კომუნიკაციის ხელშეუხებლობის უფლებაში სერიოზულ ჩარევას.[599] სასამართლოს განმარტებით, მონაცემთა სუბიექტის არაინფორმირებულობა მონაცემთა შენახვისა და მისი შემდგომი გამოყენების შესახებ, მოქალაქეებში მათი პირადი ცხოვრების მუდმივი ზედამხედველობის ქვეშ ყოფნის შეგრძნებას იწვევდა. აღნიშნული ჩარევა ჩაითვალა თანაზომიერების პრინციპის საწინააღმდეგოდ, რომლის მიზეზიც, პირველ რიგში, გახდა ის გარემოება, რომ დირექტივა „ნებისმიერი პიროვნების, ნებისმიერი ტრაფიკის მონაცემის შენახვის შესაძლებლობას იძლეოდა ყველა სახის ელექტრონული კომუნიკაციის საშუალების გამოყენებით, ყოველგვარი დიფერენციაციის, შეზღუდვის ან გამონაკლისის გარეშე“, იმისდა მიუხედავად, ჰქონდა თუ არა პირს კავშირი, თუნდაც „არაპირდაპირი“, „მძიმე დანაშაულთან“ და ამასთან, ეხებოდა იმ პირებსაც, რომელთა კომუნიკაციაც მიეკუთვნებოდა პროფესიული საქმიანობიდან გამომდინარე დაცულ ინფორმაციას[600]. აქედან გამომდინარე, მონაცემთა დირექტივა პრაქტიკულად „მთელი ევროპული მოსახლეობის ფუნდამენტური უფლებების შეზღუდვას იწვევდა“[601]. გარდა ამისა, არ ითვალისწინებდა კომპეტენტური ორგანოების მიერ აღნიშნულ კომუნიკაციასთან წვდომის მატერიალურ და პროცედურულ პირობებს და არ შეიცავდა არანაირ „ობიექტურ კრიტერიუმს“, რის საფუძველზეც შესაძლებელი იქნებოდა განსაზღვრა, თუ რომელი დანაშაული წარმოადგენდა საკმარისად „მძიმეს“, რათა გაემართლებინა პირადი ცხოვრების ხელშეუხებლობის უფლებაში ამგვარი ჩარევა[602]. კომპეტენტური ორგანოების მიერ აღნიშნულ ინფორმაციასთან წვდომა არ ექვემდებარებოდა წინასწარ „სასამართლო კონტროლს ან ზედამხედველობას დამოუკიდებელი ორგანოს“ მიერ, რათა მათ მიერ გადაწყვეტილიყო ინფორმაციასთან წვდომისა და გამოყენების

[599] Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice, 27-37.
[600] იქვე. 56-69.
[601] იქვე.
[602] იქვე.

აუცილებლობის საკითხი[603]. და ბოლოს, დირექტივა ითვალისწინებდა მთელი მოცულობის ინფორმაციის შენახვას 6 თვიდან 2 წლამდე ვადით მონაცემების კატეგორიების განსაზღვრის ან მონაცემთა სუბიექტების რაიმე სახით დიფერენციაციის გარეშე. სასამართლომ ასევე მიიჩნია, რომ დირექტივა არ შეიცავდა საკმარის ტექნიკურ და ორგანიზაციულ გარანტიებს მონაცემთა ბოროტად გამოყენების და მასთან უნებართვო წვდომის თავიდან ასარიდებლად.[604]

აღნიშნული გადაწყვეტილება ადამიანის უფლებების დაცვის კუთხით სერიოზულ გამარჯვებად იქნა მიჩნეული.[605] თუმცა გარკვეული კითხვის ნიშნები გაჩნდა იმასთან დაკავშირებით, მონაცემთა შენახვის დირექტივის გაუქმება გამოწვეული იყო დირექტივით გათვალისწინებული მონაცემთა შენახვის რეჟიმით, თუ მხოლოდ აღნიშნულ მონაცემებზე წვდომასთან დაკავშირებული არასაკმარისი გარანტიებით.[606] ანალოგიურად, გაურკვევლობა წარმოიშვა ეროვნული კანონმდებლობებით განსაზღვრულ მონაცემთა შენახვის რეჟიმზე აღნიშნული გადაწყვეტილების სამომავლო გავლენასთან დაკავშირებით. ზოგიერთ წევრმა სახელმწიფომ შეცვალა ან გააუქმა მოცემული სფეროს მარეგულირებელი სამართლებრივი დებულებები, მაშინ როდესაც ზოგიერთმა პასიური პოზიცია დაიკავა[607]. შედეგად, ორმა საჩივარმა, რომელიც სადავოდ ხდიდა დიდ ბრიტანეთსა და შვედეთში ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვის რეჟიმს, ევროკავშირის მართლმსაჯულების სასამართლომდე მიაღწია.[608] 2016 წლის 21 დეკემბერს საქმეზე Tele2 Sverige AB and Watson, ევროკავშირის მართლმსაჯულების სასამართლოში კითხვის ქვეშ დადგა არამარტო მონაცემთა შენახვის არსებული რეჟიმი, არამედ მონაცემთა პრევენციული შენახვის გამოყენების შესაძლებლობა დანაშაულის გამოძიების მიზნებისათვის.[609]

აღნიშნული გადაწყვეტილება ეხება ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების წინასწარი შენახვის მარეგულირებელი ეროვნული დებულებების

---

[603] იქვე.
[604] იქვე.
[605] *Roberts A.,* Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v. Minister for Communications, Modern Law Review, Vol.78, No3, 2015, 536.
[606] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 161.
[607] იქვე.
[608] იქვე.
[609] იქვე.

(შვედეთის და დიდი ბრიტანეთის კანონმდებლობის) შესაბამისობას „ელექტრონული კომუნიკაციის სექტორში პერსონალურ მონაცემთა დამუშავების და პირადი ცხოვრების დაცვის შესახებ" ევროკავშირის პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის N2002/58/EC დირექტივასთან და აღნიშნული დირექტივის შესაბამისი დებულებების ინტერპრეტაციას ძირითად უფლებათა ქარტიით უზრუნველყოფილ პირადი ცხოვრების უფლებასთან.

მითითებული დირექტივის[610] მე-15 (1) მუხლი წევრ სახელმწიფოს ანიჭებს შესაძლებლობას, შემოიღოს მონაცემთა შეზღუდული ვადით შენახვასთან დაკავშირებული სამართლებრივი ნორმები, თუმცა იმ პირობით, რომ ეს დებულებები აკმაყოფილებს მკაცრი აუცილებლობის და თანაზომიერების ტესტს. მონაცემები, რომლებიც აღნიშნული დირექტივის მიხედვით, ექვემდებარება შენახვის რეჟიმს, არ განსხვავდება "მონაცემთა შენახვის შესახებ" დირექტივით გათვალისწინებული მონაცემებისგან. დირექტივაში საუბარია ელექტრონული საკომუნიკაციო სერვისის პროვაიდერების მიერ ტრაფიკის და ადგილმდებარეობასთან დაკავშირებული ინფორმაციის შენახვასთან. ამასთან, „ტრაფიკის მონაცემები" დირექტივაში განმარტებულია როგორც „ინფორმაცია, რომელიც დამუშავებულია ელექტრონულ საკომუნიკაციო ქსელში კომუნიკაციის გადაცემის ან ბილინგის მიზნებისათვის."[611]

---

[610] აღსანიშნავია, რომ ევროკავშირის პარლამენტისა და საბჭოს მიერ 2017 წელს შემუშავებულ იქნა ახალი რეგულაცია ელექტრონული კომუნიკაციის სექტორში, რომელმაც უნდა ჩაანაცვლოს არსებული 2002 წლის 12 ივლისის N2002/58/EC დირექტივა. ახალი რეგულაცია უნდა ამოქმედებულიყო 2018 წლის 25 მაისს, თუმცა ამჟამინდელი მდგომარეობით ისევ არ არის ძალაში შესული. იხ. Proposal for a Regulation of The European Parliament and of The Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10/01/2017,
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> [20.06.2020].

[611] საქმეზე Ministerio Fiscal, ევროკავშირის მართლმსაჯულების სასამართლომ დაადგინა, რომ მოცემული დირექტივით გათვალისწინებული „ტრაფიკის მონაცემების" ცნება მოიცავს „ნებისმიერ მონაცემს, რომლის დამუშავებაც ხდება ელექტრონულ საკომუნიკაციო ქსელში ინფორმაციის გადაცემის ან ბილინგის მიზნებისათვის", რის გამოც სასამართლომ „ტრაფიკის" მონაცემთა კატეგორიას მიაკუთვნა ასევე SIM ბარათის მფლობელის მაიდენტიფიცირებელი მონაცემები (კერძოდ, სახელი, გვარი, საჭიროების შემთხვევაში, მისამართი), თუმცა ამ კონკრეტულ მონაცემებზე სამართალდამცავი ორგანოების დაშვების საკითხთან დაკავშირებით უფრო ნაკლებად მკაცრი სტანდარტები დაადგინა, კერძოდ, სასამართლოს შეხედულებით, ასეთ მონაცემებზე ხელმისაწვდომობის მიზნებისათვის არ არის აუცილებელი „მძიმე დანაშაულის" გამოძიების ინტერესი იყოს სახეზე და ზოგადად, დანაშაულის ინტერესიც საკმარისია. უფრო ვრცლად იხ. Case C-207/16, Ministerio Fiscal, [2018], Court of Justice. აღსანიშნავია, რომ ზოგადად, ზემოაღნიშნული მონაცემები - მომხმარებლის სახელი, გვარი, მისამართი, წარმოადგენს მომხმარებელთან ხელშეკრულების საფუძველზე ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ შენახულ ინფორმაციას და არ არის კავშირში კონკრეტულ კომუნიკაციებთან.

ხოლო "ადგილმდებარეობის შესახებ" ინფორმაციას დირექტივა მიაკუთვნებს ელექტრონულ საკომუნიკაციო ქსელში დამუშავებულ ნებისმიერ ინფორმაციას, რომელიც მიუთითებს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელის მომხმარებლის საკომუნიკაციო აღჭურვილობის გეოგრაფიულ ლოკაციას."[612] ამასთან, დირექტივის რეგულირების ქვეშ არ ხვდება კომუნიკაციის შინაარსთან დაკავშირებული სერვისები (ვებ-სერვისები, მობილური აპლიკაციები).[613]

სასამართლოს გადაწყვეტილებით, მხოლოდ მძიმე დანაშაულის წინააღმდეგ ბრძოლის ლეგიტიმური ინტერესი, როგორი ფუნდამენტურიც არ უნდა იყოს იგი, ვერ ჩაითვლება მონაცემთა ტოტალურად შენახვის თანაზომიერ საშუალებად. სასამართლომ დაიკავა ანალოგიური პოზიცია, რაც საქმეზე „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები" და დაადგინა, რომ ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვის მარეგულირებელი ეროვნული კანონმდებლობა უნდა შეიცავდეს მკაფიო და ნათელ წესებს, მონაცემთა შენახვის მასშტაბთან და გამოყენების ფარგლებთან მიმართებით[614]. კანონმდებლობამ უნდა განსაზღვროს, თუ რა გარემოებებში და პირობებში არის დასაშვები მონაცემთა შენახვის, როგორც პრევენციული ზომის გამოყენება, ისე რომ აღნიშნული განხორციელდეს მხოლოდ მკაცრად აუცილებელ შემთხვევებში.[615] კანონმდებლობა ასევე „მკაფიო და ნათელი სამართლებრივი დებულებებით" უნდა აწესრიგებდეს სამართალდამცავი ორგანოების მიერ აღნიშულ მონაცემებზე წვდომის საკითხს. მონაცემებზე დაშვება უნდა განხორციელდეს იმ ფარგლებით, რაც მკაცრად აუცილებელია გამოძიების ინტერესებისათვის[616]. კანონმდებლობამ უნდა განსაზღვროს დეტალური წესები, თუ რა შემთხვევებში და პირობებში მისცემს სერვისის მიმწოდებელი ხელისუფლების ორგანოებს მის მიერ შეგროვებულ მონაცემებზე დაშვების შესაძლებლობას, ასევე შესაბამისი პროცედურული და მატერიალური პირობები.[617] ქვემოთ უფრო დეტალურად განვიხილავთ, თუ რა

[612] Article 2, Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 12/07/2002 (ბმული იხ. 37-ე გვერდზე).
[613] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 162.
[614] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 103-104.
[615] იქვე.
[616] იქვე, 116.
[617] იქვე. 117-118.

მოთხოვნებს ადგენს სასამართლო მონაცემთა შენახვის/წვდომის მარეგულირებელი ეროვნული კანონმდებლობის მიმართ.

ნიშანდობლივია, რომ ამ საქმეზე დადგენილი მოთხოვნები სასამართლოს მიერ „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“ საქმეზეც იქნა გაჟღერებული, თუმცა, როგორც უკვე აღინიშნა, ამ უკანასკნელმა გაურკვევლად დატოვა, მონაცემთა ზოგადი/პრევენციული შენახვა რამდენად შეიძლება იქნეს გამოყენებული როგორც დანაშაულთან ბრძოლის საშუალება, თუ მისი პროპორციულობა დამოკიდებულია შენახულ მონაცემებზე წვდომასთან დაკავშირებულ პროცედურულ გარანტიებზე.[618] 2016 წლის 21 დეკემბრის გადაწყვეტილებამ კი ერთმნიშვნელოვანი პასუხი გასცა ამ კითხვას – ყველა მომხმარებლის ტრაფიკის და ადგილმდებარეობის შესახებ ყველა მონაცემის ზოგადი, პრევენციული შენახვა, ნებისმიერი საკომუნიკაციო საშუალების გამოყენებით, გამონაკლისის, შეზღუდვის ან დიფერენციაციის გარეშე, დაუშვებელია.[619] თუმცა აღნიშნული არ ნიშნავს, რომ „მძიმე დანაშაულთან“ ბრძოლის მიზნებისათვის მონაცემთა შენახვის, როგორც პრევეციული ზომის გამოყენება არ არის დასაშვები - სასამართლოს კითხვის ნიშნის ქვეშ არ დაუყენებია ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების „მიზანმიმართული“ შენახვის (Targeted retention) ეფექტურობა და შესაფერისობა.[620] არამედ ამ გადაწყვეტილებიდან გამომდინარე, მონაცემთა პრევენციული შენახვა შესანახ მონაცემთა კატეგორიასთან, გამოსაყენებულ საკომუნიკაციო საშუალებებთან, პირებთან, რომელთა მონაცემებიც უნდა იქნეს შეგროვებული და შენახვის ვადასთან მიმართებით უნდა იყოს შეზღუდული მკაცრი აუცილებლობის ტესტით.[621]

---

[618] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 165.

[619] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice; *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 162; *Tracol X.,* The judgment of the Grand Chamber dated 21 December 2016 in the Two Joint *Tele2 Sverige* and *Watson* Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level, Computer Law & Security Review: The International Journal of Technology Law and Practice, 2017, 1, 6-7.

[620] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice; *Tracol X.,* The judgment of the Grand Chamber dated 21 December 2016 in the Two Joint *Tele2 Sverige* and *Watson* Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level, Computer Law & Security Review: The International Journal of Technology Law and Practice, 2017, 6.

[621] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 108.

სასამართლომ მოცემულ გადაწყვეტილებაში ჩამოაყალიბა ეროვნული კანონმდებლობის მიმართ მოთხოვნები, რომლებმაც უნდა უზრუნველყოს, რომ მონაცემთა შენახვა ატარებდეს "მიზანმიმართულ" ხასითს და არ წარმოადგენდეს ტოტალურ, მასობრივ ზომას:

პირის კავშირი „მძიმე დანაშაულთან" - სასამართლოს პოზიცია ცხადი და ერთმნიშვნელოვანია იმასთან დაკავშირებით, რომ ეროვნული კანონმდებლობა უნდა შეიცავდეს „ობიექტურ კრიტერიუმს", რომლის მიხედვითაც დადგინდება პირი, რომლის მონაცემებმაც შეიძლება გამოავლინონ „კავშირი, თუნდაც არაპირდაპირი, მძიმე დანაშაულთან და წვლილი შეიტანონ ასეთ დანაშაულთან ბრძოლის ან საზოგადოების მიმართ არსებული სერიოზული საფრთხის პრევენციის საქმეში"[622]. გარდა აღნიშნულისა, ეროვნული კანონმდებლობა მონაცემთა შენახვასთან დაკავშირებით გამონაკლისის სახით უნდა ითვალისწინებდეს იმ პირთა დაცვას, რომელთა მონაცემებიც მიეკუთვნება პროფესიულ საიდუმლოებას.[623]

სასამართლოს გადაწყვეტილებაში მითითებულია ის კრიტერიუმები, რომლებიც შესაძლებელია გამოყენებულ იქნეს მონაცემთა შენახვის შეზღუდული ხასიათის უზრუნველსაყოფად - შენახვას დაქვემდებარებულ მონაცემებსა და საზოგადოების წინაშე მდგარ საფრთხეს შორის კავშირი შეიძლება განისაზღვროს შემდეგი კრიტერიუმების მხედველობაში მიღებით – „ა) მონაცემები, რომლებიც ეხება კონკრეტულ დროის პერიოდს, გეოგრაფიულ ტერიტორიას ან/და პირთა ჯგუფებს, რომლებიც შესაძლოა მძიმე დანაშაულში იყვნენ ჩაბმული ან ბ) პირი, რომლის შესახებაც შეგროვებულ მონაცემებს, სხვა მიზეზიდან გამომდინარე, შეუძლია წვლილი შეიტანოს დანაშაულთან ბრძოლის საქმეში."[624]

მონაცემთა შენახვის შეზღუდვა გეოგრაფიული კრიტერიუმის გამოყენებით - სასამართლოს განმარტებით, მონაცემთა შენახვა შეიძლება შეიზღუდოს „გეოგრაფიული კრიტერიუმის" გამოყენებით, როდესაც "კომპეტენტური ორგანო ობიექტურ მტკიცებულებაზე დაყრდნობით მიიჩნევს, რომ ერთ ან მეტ გეოგრაფიულ რეგიონში არსებობს მძიმე დანაშაულის მომზადების ან ჩადენის მაღალი რისკი"[625].

[622] იქვე, 111.
[623] იქვე. 105.
[624] იქვე. 106.
[625] იქვე. 111.

აღნიშნული გულისხმობს, რომ გეოგრაფიული კრიტერიუმით შეზღუდული მონაცემთა შენახვა, რომელიც შეეხება კონკრეტულ რეგიონში არსებული ყველა პირის მონაცემებს, არ შეიძლება იყოს ავტომატური და განგრძობადი, არამედ მოითხოვს, რომ 1) შესაბამისმა ორგანომ გამოიტანოს მონაცემთა შენახვის გადაწყვეტილება ზოგად კანონმდებლობაზე დაყრდნობით; 2) ეს გადაწყვეტილება დაფუძნებული იყოს ობიექტურ მტკიცებულებაზე ეროვნული კანონმდებლობით გათვალისწინებული ობიექტური კრიტერიუმის შესაბამისად; 3) ეს მტკიცებულება მიუთითებდეს არა მხოლოდ ზოგად, არამედ მაღალ რისკზე[626]. აღნიშნული ასევე გულისხმობს, რომ როდესაც რისკი აღარ არის მაღალი, მონაცემთა შენახვა უნდა შეწყდეს.[627] გარდა ამისა, სასამართლოს გადაწყვეტილებიდან გამომდინარე, კრიტერიუმი, რომლითაც უნდა შეიზღუდოს მონაცემთა შენახვა, შეიძლება სხვადასხვა სიტუაციაში განსხვავებული იყოს, კერძოდ, სასამართლო შეზღუდვას უქვემდებარებს შემდეგ კრიტერიუმებს: მონაცემები, რომლებიც შეეხება კონკრეტულ დროის მონაკვეთს ან/და გეოგრაფიულ რეგიონს ან/და პირთა ჯგუფს, რომლებიც დაკავშირებული არიან დანაშაულთან. აქედან გამომდინარე, სასამართლო გარკვეული მიხედულობის ფარგლებს უტოვებს წევრ სახელმწიფოებს, აღნიშნული კრიტერიუმებიდან გამოიყენონ შესაბამისი კონკრეტულ პირობებში.[628] მაგალითად, თუკი სახელმწიფო კონკრეტულ სიტუაციაში დგას ტერორისტული დანაშაულის საფრთხის წინაშე, მონაცემთა შენახვა შეიძლება შეიზღუდოს დროის გარკვეული მონაკვეთით (იმ პირობით, რომ ასეთი რისკი აშკარაა) და არ დაექვემდებაროს შეზღუდვას გეოგრაფიული რეგიონის ან პირთა წრის მიხედვით.[629]

მონაცემთა შენახვის ხანგრძლივობა - სასამართლოს გადაწყვეტილება არ შეიცავს რაიმე მინიშნებას შენახვის კონკრეტულ ვადასთან დაკავშირებით. აღსანიშნავია, რომ 2014 წელს გამოტანილ გადაწყვეტილებაშიც, სადაც „მონაცემთა შენახვის შესახებ" დირექტივით განსაზღვრული მინიმუმ 6 თვისა და მაქსიმუმ 2 წლის პერიოდი არათანაზომიერად იქნა მიჩნეული, სასამართლოს რაიმე კონკრეტული მოთხოვნა შენახვის ვადასთან დაკავშირებით არ განუსაზღვრავს.

---

[626] *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 167.

[627] იქვე.

[628] იქვე.

[629] იქვე.

სასამართლოს განმარტებით, ეროვნული კანონმდებლობით განსაზღვრული მონაცემთა შენახვის პერიოდი თანხვედრაში უნდა იყოს თანაზომიერების პრინციპთან[630]. შესაბამისად, შენახვის ვადის დადგენა წევრი სახელმწიფოს დისკრეციას წარმოადგენს, თუმცა აღნიშნული უფლებამოსილების გამოყენება უნდა მოხდეს იმგვარად, რათა უზრუნველყოფილი იქნეს მონაცემთა შენახვა იმ ვადით, რაც მკაცრად აუცილებელია[631]. ამასთან, შენახვის ვადის გასვლის შემდეგ მონაცემები უნდა განადგურდეს.[632]

მონაცემების შენახვა და მათზე წვდომა მხოლოდ „მძიმე დანაშაულთან“ ბრძოლის ინტერესებისათვის – სასამართლოს არაერთხელ აღუნიშნავს, რომ ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვა და სამართალდამცავი ორგანოების მიერ მათზე წვდომა დასაშვებია მხოლოდ „მძიმე დანაშაულთან“ ბრძოლის ინტერესებისათვის[633]. შესაბამისად, სასამართლო განასხვავებს „მძიმე დანაშაულს“ სხვა სახის დანაშაულებისგან, თუმცა არ იძლევა რაიმე მინიშნებას იმასთან დაკავშირებით, თუ როგორ უნდა მოხდეს მათი დიფერენცირება. „მძიმე დანაშაულის” მაგალითად გადაწყვეტილებაში დასახელებულია ორგანიზებული დანაშაული, ტერორიზმი და საზოგადოების უსაფრთხოების მიმართ სერიოზული საფრთხე.[634] მართალია ეს ცნება განსაზღვრული არ არის, მაგრამ ევროკავშირის საბჭომ წევრ ქვეყნებს მოუწოდა „სათანადოდ გაითვალისწინონ“ ევროპული დაპატიმრების შესახებ ბრძანების 2(2) მუხლში მოცემული დანაშაულების ჩამონათვალი ამ საკითხის ეროვნულ კანონდებლობაში რეგულირების დროს.[635] თუმცა იურიდიულ ლიტერატურაში გამოთქმული მოსაზრების თანახმად, აღნიშნული საკმარისად ვერ ჩაითვლება იმ რისკის

---

[630] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 95.
[631] იქვე, 108.
[632] იქვე, 122
[633] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice; Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice.
[634] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 103; *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 168.
[635] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14.02.2014, 14, <https://rm.coe.int/16806af19b> [20.06.2020]. *Tzanou M.,* Data Protection in Eu Law After Lisbon: Challenges, Developments and Limitations, წიგნში: Cyber Law, Privacy and Security: Concepts, Methodologies, Tools and Applications, Hershey PA, 2019, 81.

შესამცირებლად, რომ ზოგიერთ ქვეყანაში ასეთ დანაშაულთა ზედმეტად ვრცელი ჩამონათვალი არ დადგინდეს.[636]

დანაშაულთა კატეგორიის განსაზღვრასთან დაკავშირებით სახელმძღვანელო პრინციპს ეროვნული კანონმდებლისთვის წარმოადგენს ის, რომ უფლებაში ჩარევის ლეგიტიმური მიზანი თანაზომიერი უნდა იყოს პირადი ცხოვრების უფლების მსგავსად სერიოზულ შეზღუდვასთან და მონაცემთა შენახვა, ისევე როგორც მათზე წვდომა, როგორც პირადი ცხოვრების უფლებაში მძიმე ჩარევა, მხოლოდ ღირებულ/მნიშვნელოვან სამართლებრივ ინტერესთან ბრძოლამ შეიძლება გაამართლოს.

სამართალდამცავი ორგანოების წვდომა შენახულ მონაცემებზე – შენახულ მონაცემებზე სამართალდამცავი ორგანოების წვდომასთან მიმართებით სასამართლოს ერთ-ერთ ფუნდამენტურ მოთხოვნას წარმოადგენს ასეთი წვდომის განხორციელება მხოლოდ სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს გადაწყვეტილების საფუძველზე (გარდა გადაუდებელი აუცილებლობისა). გარდა აღნიშნულისა, ისევე როგორც საქმეში „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“, მოცემულ შემთხვევაშიც ხაზგასმითაა აღნიშნული, რომ სასამართლომ ან დამოუკიდებელმა ადმინისტრაციულმა ორგანომ გადაწვეტილება უნდა გამოიტანოს შესაბამისი ორგანოების “დასაბუთებული შუამდგომლობის” საფუძველზე, დანაშაულის პრევენციის, გამოვლენის და დევნისათვის გათვალისწინებული პროცედურების ფარგლებში.[637]

გარდა აღნიშნულისა, შეგროვებულ მონაცემებზე წვდომასთან დაკავშირებით მნიშვნელოვან საკითხს წარმოადგენს იმ პირთა კატეგორიის განსაზღვრა, რომელთა მონაცემებზეც შეიძლება ჰქონდეთ სამართალდამცავ ორგანოებს დაშვება. სასამართლო ხაზგასმით აღნიშნავს, რომ, როგორც წესი, წვდომა შეიძლება განხორციელდეს იმ პირთა მონაცემებზე, რომელთა მიმართებაშიც არსებობს „ეჭვი მძიმე დანაშაულის დაგეგმვის, ჩადენის ან ასეთ დანაშაულში რაიმე გზით მონაწილეობის შესახებ.“[638] თუმცა ეს წარმოადგენს ზოგად წესს და სასამართლო

[636] *Tzanou M.,* Data Protection in Eu Law After Lisbon: Challenges, Developments and Limitations, წიგნში: Cyber Law, Privacy and Security: Concepts, Methodologies, Tools and Applications, Hershey PA, 2019, 81.
[637] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 120.
[638] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 119.

უშვებს მისგან გამონაკლისის დაშვების შესაძლებლობას, კერძოდ, კონკრეტულ სიტუაციაში, როდესაც მაგალითად, სახელმწიფო უშიშროების, თავდაცვის ან საზოგადოების უსაფრთხოების ინტერესებს ემუქრება ტერორისტული დანაშაულიდან მომდინარე საფრთხე, სამართალდამცავი ორგანოების დაშვება შეიძლება განხორციელდეს ასევე სხვა პირის (გარდა იმ პირისა, რომელთან დაკავშირებით არსებობს ეჭვი დანაშაულის ჩადენის ან მასში მონაწილეობის შესახებ) მონაცემებზე, როდესაც არსებობს ობიექტური მტკიცებულება, რომელიც მიუთითებს, რომ ამ მონაცემებს, კონკრეტულ სიტუაციაში შეუძლიათ ეფექტური წვლილი შეიტანონ ასეთ დანაშაულთან ბრძოლის საქმეში.[639] მნიშვნელოვან მოთხოვნას წარმოადგენს ასევე მონაცემთა სუბიექტისთვის განხორციელებული ღონისძიების შესახებ შეტყობინება, როგორც კი აღნიშნული ზიანის მომტანი არ იქნება გამოძიებისათვის.[640]

მონაცემთა უსაფრთხოება - შეგროვებულ მონაცემებზე მესამე პირების მხრიდან არალეგიტიმური წვდომის საფრთხე კიდევ ერთ საყურადღებო საკითხს წარმოადგენს. სასამართლოს განმარტებით, შენახული მონაცემების რაოდენობისა და სენსიტიურობის, ასევე მათზე უნებართვო წვდომის რისკიდან გამომდინარე, აუცილებელია უზრუნველყოფილ იქნეს შეგროვებული მონაცემების დაცვისა და უსაფრთხოების მაღალი დონე.[641]

4.4. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა გერმანიის კანონმდებლობის მიხედვით

საერთაშორისო დონეზე აქტუალურობის პარალელურად, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის საკითხი ევროკავშირის წევრ სახელმწიფოებშიც მნიშვნელოვანი ყურადღების ცენტრში მოექცა. როგორც უკვე აღინიშნა, ჯერ კიდევ საქმეზე „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“ ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილებამდე, არაერთი ევროპული ქვეყნის საკონსტიტუციო სასამართლომ არაკონსტიტუციურად ცნო “მონაცემთა შენახვის შესახებ” დირექტივის

[639] იქვე.
[640] იქვე 121.
[641] იქვე, 122.

იმპლემენტაციის შედეგად მიღებული კანონმდებლობა (მაგ., გერმანია, ბულგარეთი, კვიპროსი, ჩეხეთი, რუმინეთი[642]). კანონმდებლობის არაკონსტიტუციურად ცნობის ძირითად საფუძველს არასაკმარისი ზედამხედველობის და უსაფრთხოების სტანდარტები, კანონიერების, აუცილებლობის და პროპორციულობის პრინციპებთან სამართლებრივი დებულებების შეუსაბამობა წარმოადგენდა.[643]

კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვა დღემდე პრობლემურ საკითხად რჩება გერმანიის კანონმდებლობაში. 2007 წლის დეკემბრიდან მოყოლებული, როდესაც "მონაცემთა შენახვის შესახებ" დირექტივის იმპლემენტაციის მიზნით პირველად იქნა მიღებული მონაცემთა შენახვის მარეგულირებელი ნორმები, ეს საკითხი მუდმივ აქტუალურობას ინარჩუნებს.

კომუნიკაციის მაიდენტიფიცირებელი მონაცემები კონსტიტუციური დაცვის ქვეშ არის მოქცეული გერმანიის კანონმდებლობით, კერძოდ, ძირითადი კანონის მე-10.1. მუხლით უზრუნველყოფილია არამარტო კომუნიკაციის შინაარსის კონფიდენციალურობა, არამედ კომუნიკაციის პროცესთან დაკავშირებული გარემოებებიც.[644]

აღსანიშნავია, რომ გერმანიის ფედერალური საკონსტიტუციო სასამართლოს 2008 წლის გადაწყვეტილებით დირექტივის შესრულების შედეგად მიღებული მონაცემთა შენახვის კანონმდებლობის გარკვეული ნაწილის მოქმედება შეჩერებულ იქნა, ხოლო 2010 წლის 2 მარტის გადაწყვეტილებით არაკონსტიტუციურად იქნა ცნობილი.[645] მოცემული ნორმები სერვისის პროვაიდერებს აკისრებდა ვალდებულებას, 6 თვის ვადით შეენახათ ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემები. გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ დაადგინა, რომ ტრაფიკის მონაცემთა პრევენციული შენახვა 6 თვის ვადით, რომელიც გათვალისწინებული იყო "მონაცემთა შენახვის შესახებ" ევროკავშირის პარლამენტისა და საბჭოს 2006 წლის დირექტივით, ვერ აკმაყოფილებდა კონსტიტუციურ სტანდარტს

---

[642] *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No.2, 2015, 56; *Hert P. D.,* Court, Privacy and Data Protection in Belgium: Fundamental Rights that Might as well Be Struck from the Constitution, წიგნში: Court, Privacy and Data Protection in The Digital Environment, *Brkan M., Psychogiopoulou E. (eds.),* Cheltenham, UK, 2017, 73-75.

[643] იქვე.

[644] BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08.

[645] იქვე. იხ ასევე. *Schwartz P. M.,* Systematic Government Access to Private-sector Data in Germany წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.)*, Oxford, 2017, 70.

შეგროვებულ მონაცემებზე წვდომასთან, მონაცემთა უსაფრთხოებასთან, პროცესის გამჭვირვალობასთან დაკავშირებით, მკაფიოდ განსაზღვრული ნორმების და საკმარისი გარანტიების არარსებობის გამო.[646]

სასამართლომ დაადგინა გარკვეული მოთხოვნები, რომლებსაც უნდა აკმაყოფილებდეს კანონმდებლობა, რათა მონაცემთა შენახვის რეჟიმი თანაზომიერების პრინციპთან არ მოვიდეს წინააღმდეგობაში[647]. სასამართლოს შეფასებით, სამართალდამცავი ორგანოების მიერ მონაცემები შეიძლება გამოყენებულ იქნეს მხოლოდ მძიმე დანაშაულის გამოძიების მიზნებისათვის და შესაბამისი სამართლებრივი საფუძვლები ამომწურავად უნდა განისაზღვროს კანონში; სამართალდამცავი ორგანოების საჭიროებისათვის მონაცემთა ფარულად მოპოვება უნდა განხორციელდეს სასამართლოს ნებართვით ყოველ კონკრეტულ შემთხვევაში (გარდა გადაუდებელი აუცილებლობის შემთხვევებისა, როდესაც საფრთხე ემუქრება ადამიანის სიცოცხლეს ან ჯანმრთელობას). ამასთან, სასამართლოს შეფასებით, იმისათვის, რათა მონაცემთა შენახვის კანონმდებლობამ დააკმაყოფილოს თანაზომიერების პრინციპი, პირველ რიგში, აუცილებელია მონაცემთა შენახვის ფუნქცია მინიჭებული ჰქონდეს არა სახელმწიფოს, არამედ სერვისის პროვაიდერებს, რათა სახელმწიფოს არ მიეცეს მონაცემებზე პირდაპირი წვდომის შესაძლებლობა. აღნიშნული უნდა იყოს უზრუნველყოფილი შესაფერისი სამართლებრივი დებულებებითა და ტექნიკური უსაფრთხოების ზომებით.[648] გარდა აღნიშნულისა, მიღებულ უნდა იქნეს ზომები მონაცემთა უსაფრთხოების უზრუნველსაყოფად, მათ შორის მათ გადაცემასთან, მათზე წვდომასა და განადგურებასთან მიმართებით.[649]

აღნიშნულის შემდგომ, 2015 წლის 16 ოქტომბერს გერმანიის საკანონმდებლო ორგანომ მიიღო ცვლილებები ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემთა შენახვასთან დაკავშირებით, რომლის ძალაში შესვლის ვადად განისაზღვრა 2017 წლის 1 ივლისი. ახალი რეგულაციების მიხედვით, სერვისის პროვაიდერებს დაეკისრათ კომუნიკაციის ტრაფიკთან დაკავშირებული მონაცემების 10 კვირით, ხოლო

[646] BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08.
[647] იქვე.
[648] იქვე. 214, 226-229; 247-251.
[649] იქვე. 221-225, 235-236.

ადგილმდებარეობის შესახებ მონაცემების 4 კვირით შენახვის ვალდებულება.[650] ამასთან, შენახვის ვალდებულებისგან მთლიანად გამოირიცხა ელექტრონული მეილის ტრაფიკთან დაკავშირებული მონაცემები. შენახულ მონაცემებზე წვდომა შეიზღუდა მხოლოდ სისხლის სამართლის საპროცესო კოდექსით კონკრეტულად განსაზღვრული მძიმე დანაშაულის გამოძიების ინტერესებით[651]. გარდა იმისა, რომ დადგენილ იქნა დანაშაულთა წრე, რომელთა შემთხვევაშიც დასაშვებად იქნა მიჩნეული მონაცემების მოპოვება, დამატებით პირობად განისაზღვრა დანაშაულებრივი ქმედების სერიოზულობის სავალდებულო ხასიათი ყოველ კონკრეტულ შემთხვევაში[652]. მონაცემთა მოპოვება დასაშვებად იქნა მიჩნეული მხოლოდ იმ შემთხვევაში, როდესაც ფაქტების გამოძიება ამ მონაცემების გარეშე მნიშვნელოვნად გართულდება და მონაცემების მოპოვება მიზნის მიღწევის ადეკვატური საშუალებაა[653]. ამასთან, კანონმდებლობის მიხედვით, სამართალდამცავი ორგანოების წვდომა შეგროვებულ მონაცემებზე დაუშვებელია, როდესაც ასეთი წვდომა გამოავლენს ინფორმაციას, რომელთან დაკავშირებითაც პირს ექნებოდა ჩვენების მიცემაზე უარის თქმის უფლება[654]. მონაცემები, რომელთა მოპოვება განხორციელდა ამ მოთხოვნის მიუხედავად, დაუყოვნებლივ განადგურებას ექვემდებარება[655]. მონაცემებზე წვდომა დასაშვებია მხოლოდ სასამართლოს ნებართვით, რომელიც გარდა იმისა, რომ უნდა შეიცავდეს სამართალდამცავი ორგანოსათვის კონკრეტულად გადასაცემ ინფორმაციას, ასევე უნდა აფასებდეს მონაცემთა გადაცემის მოთხოვნის პროპორციულობასა და აუცილებლობას.[656]

მიუხედავად საკანონმდებლო კუთხით განხორციელებული მნიშვნელოვანი ნოვაციებისა, რომლითაც დამატებითი გარანტიები იქნა გათვალისწინებული

[650] *Etteldorf C.,* Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law, European Data Protection Law Review, Vol. 3, No 3, 2017, 395.
[651] *Schweda S.,* Parliament Adopts New Data Retention Law, European Data Protection Law Review, Vol. 1, No3, 2015, 223-226.
[652] იქვე.
[653] იქვე.
[654] იქვე.
[655] იქვე.
[656] სასამართლოს ნებართვა არ არის საჭირო, როდესაც საკომუნიკაციო სერვისის პროვაიდერი ახდენს მონაცემების ავტომატურ ანალიზს მომხმარებლისთვის IP მისამართის მინიჭებასთან დაკავშირებით, როდესაც აღნიშნულის მიზანს მხოლოდ მომხმარებლის მაიდენტიფიცირებელი მონაცემის გადაცემის შუამდგომლობაზე რეაგირება წარმოადგენს; იხ. *Schweda S.,* Parliament Adopts New Data Retention Law, European Data Protection Law Review, Vol. 1, No3, 2015, 223-226.

ადამიანის უფლებების დაცვის კუთხით, ძირითადი პრობლემა, რომელიც უკავშირდება ევროკავშირის მართლმსაჯულების სასამართლოს მოთხოვნას მონაცემების ტოტალური, შეუზღუდავი შენახვის აკრძალვასთან დაკავშირებით, კვლავ მნიშვნელოვან გამოწვევად და საზოგადოების კრიტიკის ძირითად ობიექტად დარჩა.[657]

საბოლოოდ, კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის საკითხი ჯერ კიდევ გადასაწყვეტია და აღნიშნულთან დაკავშირებით ახალი დავა წამოიჭრა გერმანიის ადმინისტრაციული სასამართლოების პრაქტიკაში. ამჟამად, საქმის ბედის საბოლოო გადაწყვეტამდე გერმანიის საერთო სარგებლობის ელექტრონული საკომუნიკაციო სერვისის მიმწოდებლებს შეჩერებული აქვთ ტრაფიკის და ადგილმდებარეობის მონაცემების შენახვის ვალდებულება. აღნიშნულ საქმეზე კონკრეტულ სერვისიის მიმწოდებელთან დაკავშირებით მიმდინარე დავის ფარგლებში კიოლნის ადმინისტრაციულმა სასამართლომ გადაწყვიტა, რომ გერმანიის კანონმდებლობით გათვალისწინებული ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვა არ არის შესაბამისობაში ევროკავშირის მართლმსაჯულების სასამართლოს 2016 წლის 21 დეკემბრის გადაწყვეტილებით დადგენილ მოთხოვნებთან, იმ არგუმენტზე დაყრდნობით, რომ ითვალისწინებს ყველა მომხმარებლის ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების ტოტალურ შენახვას და არ ზღუდავს მას მკაცრი აუცილებლობის ტესტით[658]. აღნიშნული გადაწყვეტილება გასაჩივრებულ იქნა გერმანიის ფედერალურ ადმინისტრაციულ სასამართლოში, რომელმაც თავის მხრივ, ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა გერმანიის კანონმდებლობის ევროკავშირის მართლმსაჯულების სასამართლოს 2016 წლის 21 დეკემბრის გადაწყვეტილებასთან შესაბამისობის საკითხის დაზუსტების მიზნით.[659]

ამრიგად, როგორც ვხედავთ, გერმანიაში კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის კანონმდებლობას რთული და წინააღმდეგობრივი ისტორია აქვს და ამ მიმართულებით საბოლოო კონსესუსი ჯერ მიღწეული არ არის. მიუხედავად

[657] იქვე. 226.
[658] *Etteldorf C.,* Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law, European Data Protection Law Review, Vol. 3, No 3, 2017, 394-398.
[659] <https://www.bverwg.de/pm/2019/66> [20.06.2020].

იმისა, რომ გერმანიის ახალმა კანონმდებლობამ გაცილებით მეტი გარანტია გაითვალისწინა ადამიანის უფლებების დაცვის კუთხით, რაც, პირველ რიგში, ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვის საკმაოდ მცირე ვადებში გამოიხატება, ძირითად სირთულედ მონაცემების ტოტალური, შეუზღუდავი შენახვა რჩება და სწორედ ამ საკითხთან დაკავშირებით ევროკავშირის მართლმსაჯულების სასამართლოს მიერ 2016 წლის 21 დეკემბრის გადაწყვეტილებით დადგენილი მოთხოვნებიდან გამომდინარე, გადაწყვიტა გერმანიის ფედერალურმა სასამართლომ ეროვნული კანონმდებლობის ევროკავშირის სტანდარტთან შესაბამისობის შესაფასებლად ევროკავშირის მართლმსაჯულების სასამართლოსთვის მიემართა.

4.5. შეჯამება

ყოველივე აღნიშნულიდან გამომდინარე, აშკარაა, რომ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ტოტალური, შეუზღუდავი შენახვა - ყველა მომხმარებლის ტრაფიკის და ადგილმდებარეობის შესახებ ყველა მონაცემის, ნებისმიერი საკომუნიკაციო საშუალების გამოყენებით, გამონაკლისის, შეზღუდვის ან დიფერენციაციის გარეშე, არ შეესაბამება ევროკავშირის სტანდარტს. ამ საკითხს ევროკავშირის მართლმსაჯულების სასამართლომ საქმეზე Tele2 Sverige AB and Watson ნათელი და თვალსაჩინო პასუხი გასცა. ამავდროულად, სასამართლოს, ზოგადად, კითხვის ნიშნის ქვეშ არ დაუყენებია ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემთა „მიზანმიმართული“ შენახვის დასაშვებობა და დაადგინა მოთხოვნები ეროვნული კანონმდებლობის მიმართ, რათა მონაცემთა შენახვის რეჟიმის ტოტალური, აბსტრაქტული ხასიათი გამოირიცხოს.

სასამართლოს განმარტებით, ეროვნული კანონმდებლობა დამყარებული უნდა იყოს „ობიექტურ კრიტერიუმზე, რომელიც იძლევა შესაძლებლობას, განისაზღვრონ პირები, რომელთა შესახებ მონაცემებს შესაძლოა ჰქონდეთ კავშირი (თუნდაც არაპირდაპირი) მძიმე დანაშაულთან და წვლილი შეიტანონ ასეთ დანაშაულთან ბრძოლის ან საზოგადოების მიმართ სერიოზული საფრთხის აცილების საქმეში“. სასამართლომ ასევე დაადგინა გარკვეული სახელმძღვანელო კრიტერიუმები ამ მიმართულებით.

რაც შეეხება სამართალდამცავი ორგანოების წვდომას ასეთ მონაცემებზე, მხოლოდ მძიმე დანაშაულის გამოძიების ინტერესს შეუძლია ასეთი წვდომის გამართლება, თუმცა მხოლოდ აღნიშნული საკმარისად ვერ ჩაითვლება. ამ მონაცემებზე ხელმისაწვდომობა დასაშვებია მხოლოდ სასამართლოს ან დამოუკიდებელი ადმინისტრაციული ორგანოს გადაწყვეტილებაზე დაყრდნობით (გარდა გადაუდებელი აუცილებლობის შემთხვევებისა), რომელიც "დასაბუთებული შუამდგომლობის" საფუძველზე უნდა იქნეს გამოტანილი.

განხილული იქნა ასევე გერმანიის გამოცდილება ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემთა შენახვის კანონმდებლობასთან დაკავშირებით. გერმანიის ფედერალური საკონსტიტუციო სასამართლოს 2012 წლის გადაწყვეტილების შემდეგ გერმანიის კანონმდებელმა ახლებურად ჩამოაყალიბა კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვასთან დაკავშირებული სამართლებრივი დებულებები და მნიშვნელოვანი გარანტიები გაითვალისწინა მონაცემთა შენახვის და განსაკუთრებით, მათზე წვდომის კუთხით, თუმცა მთავარი პრობლემა, ისევ უკავშირდება მონაცემთა შენახვის მასობრივ, ტოტალურ ხასიათს. გერმანიის გამოცდილებაზე დაყრდნობით შეიძლება ითქვას, რომ ამ საკითხის მოგვარება ევროკავშირის მართლმსაჯულების სასამართლოს მიერ დადგენილი მოთხოვნების შესაბამისად, არ არის მარტივი. სწორედ მონაცემთა ბლანკეტურ, შეუზღუდავ შენახვას უკავშირდება გერმანიის ეროვნულ სასამართლოებში სერვისის მიმწოდებლების ინიციატივით დაწყებული დავები. იქედან გამომდინარე, რომ გერმანიის კანონმდებლობა უფრო მკაცრ სტანდარტებს ითვალისწინებს, ვიდრე ბრიტანეთის ან შვედეთის, რომელიც ევროკავშირის მართლმსაჯულების სასამართლომ საქმეზე Tele2 Sverige AB and Watson ევროკავშირის მოთხოვნებთან შეუსაბამოდ მიიჩნია, გერმანიის ფედერალურმა ადმინისტრაციულმა სასამართლომ მონაცემთა შენახვასთან დაკავშირებული ეროვნული დებულებების ევროკავშირის სტანდარტთან შესაბამისობის თაობაზე გადაწყვეტილების მიღება ევროკავშირის მართლმსაჯულების სასამართლოს მიანდო[660].

[660] <https://eucrim.eu/news/federal-administrative-court-refers-german-data-retention-law-european-court-justice/> [20.06.2020].

VI. ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებები - საქართველოს კანონმდებლობა საერთაშორისო და კონსტიტუციური სტანდარტების ჭრილში

1. სატელეფონო და ინტერნეტკომუნიკაციის რეალურ დროში მოპოვებასთან დაკავშირებული ღონისძიებები სისხლის სამართლის პროცესში

1.1 ზოგადი მიმოხილვა

სსსკ-ის 143[2] მუხლი ფარული საგამოძიებო მოქმედების ჩატარების სავალდებულო მოთხოვნებად განსაზღვრავს კანონიერების, თანაზომიერებისა და ლეგიტიმური მიზნის პრინციპებს. კვლევის წინა თავში დეტალურად იქნა განხილული ფარული საგამოძიებო მოქმედებების ჩატარების პრინციპების კონკრეტული შინაარსი, შემადგენელი კომპონენტები და მათთან დაკავშირებული ცალკეული ასპექტები, მათ შორის, ევროპული სასამართლოს მიერ ჩამოყალიბებული პრაქტიკა და ის კონკრეტული გარანტიები, რომლებსაც მნიშვნელობა ენიჭება ფარული საგამოძიებო მოქმედებების მარეგულირებელი კანონმდებლობის განჭვრეტადობისა და ხელმისაწვდომობის შეფასებისას, ისევე როგორც ამ ღონისძიებათა თანაზომიერების კუთხით. შესაბამისად, ნაშრომის წარმოდგენილ თავში ფარული საგამოძიებო მოქმედებების პრინციპებთან დაკავშირებით შევჩერდებით მხოლოდ ცალკეულ საკითხებზე, უფრო კონკრეტულ კი - თანაზომიერების პრინციპთან დაკავშირებულ ზოგიერთ ასპექტზე.

ამასთან, მოცემულ თავში უკვე კონკრეტულად იქნება განხილული სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული ცალკეული პროცესუალური საკითხები, მათ შორის, შეფასდება კონკრეტული ასპექტები კონსტიტუციურ-სამართლებრივ და საერთაშორისო სტანდარტებთან შესაბამისობის ჭრილში.

როგორც უკვე აღინიშნა, დანაშაულის გამოძიების მიზნებისათვის ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების მარეგულირებელი საგამოძიებო მოქმედებები მოწესრიგებულია სსსკ-ის XVI[1] თავით (ფარული საგამოძიებო მოქმედებები).

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ პუნქტებით გათვალისწინებული სატელეფონო და ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების ღონისძიებები ხორციელდება „კომუნიკაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის“ გამოყენებით, რაც წარმოადგენს „კავშირგაბმულობის ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერას კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული, ნახევრად სტაციონარული ან არასტაციონარული ტექნიკური შესაძლებლობის გამოყენებით“ („ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის „ჰ[56]“ ქვეპუნქტი). ხოლო იმ შემთხვევაში, როდესაც ადგილი აქვს ელექტრონული საკომუნიკაციო სერვისის მიმწოდებელთან შენახული მონაცემების გამოთხოვას, უნდა გავრცელდეს სსსკ-ის XVI თავი - კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებები, კერძოდ, სსსკ-ის 136-ე მუხლი - დოკუმენტის ან ინფორმაციის გამოთხოვა, რომლის პირველი ნაწილი ითვალისწინებს კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაციის ან დოკუმენტის მხარეების მიერ გამოთხოვის შესაძლებლობას სასამართლოს განჩინების საფუძველზე[661], მაგალითად, ამ ნორმის შესაბამისად შესაძლებელია ტელეფონის ნომერზე შემავალი და გამავალი ზარების ამსახველი ინფორმაციის გამოთხოვა, ელექტრონული ფოსტით გადაგზავნილი დოკუმენტების შინაარსის მოპოვება და სხვა.[662]

გარდა აღნიშნულისა, თუკი არსებობს დასაბუთებული ვარაუდი, რომ პირი დანაშაულებრივ ქმედებას ახორციელებს კომპიუტერული სისტემის გამოყენებით, სსსკ-ის 137-ე მუხლის საფუძველზე შესაძლებელია პროკურორმა გამოძიების ადგილის მიხედვით მიმართოს სასამართლოს ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვების შესახებ განჩინების გაცემის მიზნით. ამის მსგავსად, იგივე გარემოების არსებობისას - დასაბუთებული ვარაუდის საფუძველზე, რომ პირი

[661] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის №1/1/650,699 გადაწყვეტილების საფუძველზე ძალადაკარგულად იქნა ცნობილი 136-ე მუხლის პირველი და მე-4 ნაწილების ის ნორმატიული შინაარსი, რომელიც გამორიცხავს დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის შესახებ განჩინების გაცემის შუამდგომლობით სასამართლოსათვის მიმართვას.

[662] *თოლორაია ლ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 424-425.

დანაშაულებრივ ქმედებას ახორციელებს კომპიუტერული სისტემის გამოყენებით, პროკურორის შუამდგომლობის მიმართვის გზით სასამართლოს განჩინების საფუძველზე, შესაძლებელია ასევე შინაარსობრივ მონაცემთა მიმდინარე მოპოვება სსსკ-ის 138-ე მუხლიდან გამომდინარე. ორივე აღნიშნული მუხლი გულისხმობს ამ ღონისძიების განხორციელებას ელექტრონული საკომუნიკაციო სერვისის მიმწოდებლის მიერ, მისი ტექნიკური ინფრასტრუქტურის გამოყენებით, ამ პროცესში არ მონაწილეობს სააგენტო და შესაბამისად, არ გამოიყენება ის ტექნიკური შესაძლებლობები, რაც კანონმდებლობის მიხედვით, დადგენილია კავშირგაბმულობის არხიდან/კომპიუტერული სისტემიდან ინფორმაციის მოხსნა/ფიქსაციის შემთხვევაში (სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი).

აღსანიშნავია ისიც, რომ 136-ე-138-ე მუხლები სსსკ-ში გათვალისწინებულ იქნა 2010 წლის 24 სექტემბრის საკანონმდებლო ცვლილებებით, რაც განპირობებული იყო „კომპიუტერული დანაშაულის შესახებ“ ევროსაბჭოს კონვენციის შესაბამისი დებულებების იმპლემენტაციის აუცილებლობით, კერძოდ, ხსენებული მუხლები წარმოადგენს ამ კონვენციის მე-18 (დოკუმენტის/ინფორმაციის გამოთხოვის ბრძანება), მე-20 (ინტერნეტტრაფიკის მონაცემთა მიმდინარე შეგროვება) და 21-ე (შინაარსობრივ მონაცემთა ხელში ჩაგდება) მუხლებით გათვალისწინებული დებულებების ასახვას ქართულ კანონმდებლობაში.[663] ნიშანდობლივია ისიც, რომ 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებების შედეგად, აღნიშნულ ღონისძიებათა განხორციელებაზე გავრცელდა სსსკ-ის 143[2]-143[10] მუხლების დებულებები, რაც ნიშნავს იმას, რომ ამ ღონისძიებათა ჩატარება დასაშვებად იქნა მიჩნეული ადამიანის უფლებათა დაცვის იმ მექანიზმებისა და გარანტიების პირობებში, რაც კანონმდებელმა გაავრცელა ფარული საგამოძიებო მოქმედებების თავზე.

ნიშანდობლივია ისიც, რომ კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების თავს 2018 წლის 20 ივლისს განხორციელებული ცვლილებების შედეგად, დაემატა 138[1] მუხლი - „კომპიუტერული მონაცემის ან დოკუმენტის მოპოვება უცხო სახელმწიფოდან სამართლებრივი დახმარების აღმოჩენის შესახებ შუამდგომლობის წარდგენის გარეშე“, რაც იძლევა

[663] იხ. კონვენცია კომპიუტერული დანაშაულის შესახებ, ევროპის საბჭო, 23/11/2001.

შესაძლებლობას, უცხო სახელმწიფოს კომპეტენტური ორგანოებიდან პროკურორის შუამდგომლობის საფუძველზე გამოთხოვილ იქნეს სისხლის სამართლის საქმისათვის მნიშვნელოვანი კომპიუტერული მონაცემი ან დოკუმენტი, თუ კომპიუტერული მონაცემის ან/და დოკუმენტის ამ წესით მოპოვება დაშვებულია შესაბამისი საერთაშორისო ხელშეკრულებით, წარმოშობის სახელმწიფოს სამართლით ან/და ამ სახელმწიფოს ნათლად ჩამოყალიბებული პრაქტიკით. ამ წესით ინფორმაციის გამოთხოვისას არ გამოიყენება „სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ“ საქართველოს II თავით დადგენილი წესები (სსსკ-ის 138[1] მუხლის პირველი ნაწილი). ამასთან, ასეთ შემთხვევაში ინფორმაციის მოპოვება ხორციელდება ნებაყოფლობით საწყისებზე უცხოური კომპანიების მხრიდან (სსსკ-ის 138[1] მუხლის მე-2 ნაწილი).[664]

უნდა აღინიშნოს, რომ კომპიუტერულ მონაცემებთან დაკავშირებული საგამოძიებო მოქმედებების თავით გათვალისწინებული საკითხების განხილვა, ისევე როგორც იმ სამართლებრივი ურთიერთობების გააზრება, რაც ამ თავით არის რეგულირებული, სცდება კვლევის თემატიკას. შესაბამისად, წარმოდგენილ ქვეთავში შევეხეთ მხოლოდ ამ საგამოძიებო მოქმედებებთან დაკავშირებულ ზოგად დებულებებს მოცემული თავის რეგულირების სფეროს შესახებ ზოგადი წარმოდგენის შექმნის, შესაბამისად - სისხლის სამართლის პროცესში ელექტრონული კომუნიკაციის მოპოვების შესაძლებლობების უკეთ გააზრების მიზნითა და რაც მთავარია, ზემოაღნიშნული საგამოძიებო მოქმედებების ფარული საგამოძიებო

[664] სსსკ-ის 138[1] მუხლის შინაარსიდან გამომდინარე, საუბარია ისეთ შემთხვევებზე, როდესაც ხდება, მაგალითად, სხვადასხვა ვებსერვისებისა და მობილური აპლიკაციების მწარმოებელი კომპანიებისგან მათთან შენახული ინფორმაციის გამოთხოვა, როგორიცაა, მაგ. Facebook, Gmail, WhatsApp და სხვა. ამასთან, როდესაც შეუძლებელია კომპიუტერული მონაცემების ან დოკუმენტის მოპოვება ამ მუხლის შესაბამისად, აღნიშნული კომპანიებისთვის პირდაპირი მიმართვის გზით, სერვისის მიმწოდებელთან შენახული ინფორმაციის გამოთხოვა შესაძლებელია განხორციელდეს სსსკ-ის 136-ე მუხლის საფუძველზე, უცხო სახელმწიფოსთან საერთაშორისო თანამშრომლობის მეშვეობით. ნიშანდობლივია, რომ სსსკ-ის 138[1] მუხლი საკმაოდ დაბალ სტანდარტებს ადგენს, კერძოდ, იგივე ტიპის ინფორმაციის მოსაპოვებლად, რომლისთვისაც სსსკ-ის 136-ე-138-ე მუხლების მიხედვით სასამართლოს განჩინება არის სავალდებულო, უშვებს მხოლოდ პროკურორის მიერ მათი გამოთხოვის შესაძლებლობას, სასამართლოს ნებართვის გარეშე; გარდა ამისა, მითითებულ ნორმაში არაფერია ნათქვამი შესაბამის მტკიცებულებით სტანდარტზე - „დასაბუთებული ვარაუდზე“; და ბოლოს, სსსკ-ის 136-ე-138-ე მუხლებისგან განსხვავებით, რომლებშიც პირდაპირაა გაწერილი, რომ ამ მუხლებზე ვრცელდება ფარული საგამოძიებო მოქმედებების თავის დებულებები, ასეთ დათქმას 138[1] მუხლი არ შეიცავს და ითვალისწინებს მხოლოდ ზოგად ჩანაწერს იმასთან დაკავშირებით, რომ „ამ მუხლით დადგენილი წესით შესაბამისი კომპიუტერული მონაცემის ან დოკუმენტის მოპოვებისას პროკურორი ვალდებულია დაიცვას სსსკ-ით გათვალისწინებული მოთხოვნები“.

მოქმედებებისგან, კერძოდ, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიებებისგან განსხვავების წარმოჩენის თვალსაზრისით, რომლებიც წარმოადგენს შინაარსობრივად სხვა სახის საგამოძიებო მოქმედებებს და ხორციელდება კომუნიკაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის გამოყენებით, საქართველოს კანონმდებლობით დადგენილი წესით, პროცედურებით, ტექნიკური შესაძლებლობებითა და უფლებამოსილი ორგანოს - სააგენტოს მიერ ტექნიკური აღსრულების გზით.

1.2 ფარული საგამოძიებო მოქმედების ჩატარების საფუძვლები

სსსკ ფარული საგამოძიებო მოქმედების ჩატარების ერთ-ერთ მატერიალურ წინაპირობად განსაზღვრავს სასამართლოს განჩინებას, რომელსაც პროკურორის მოტივირებული შუამდგომლობის საფუძველზე გასცემს რაიონული (საქალაქო) სასამართლოს მოსამართლე გამოძიების ადგილის მიხედვით (სსსკ-ის 143[3] მუხლის პირველი ნაწილი). ამავდროულად, სსსკ-ის 143[3] მუხლის მე-17 ნაწილის შესაბამისად, სახელმწიფო-პოლიტიკური თანამდებობის პირის, მოსამართლის და იმუნიტეტის მქონე პირის მიმართ მოქმედებს განსხვავებული წესი, კერძოდ, ფარული საგამოძიებო მოქმედება შეიძლება ჩატარდეს საქართველოს უზენაესი სასამართლოს მოსამართლის განჩინებით, საქართველოს გენერალური პროკურორის ან მისი მოადგილის მოტივირებული შუამდგომლობის საფუძველზე.

ფარული საგამოძიებო მოქმედების ჩატარების შესაძლებლობას სსსკ ასევე უკავშირებს „დასაბუთებული ვარაუდის“ მტკიცებულებით სტანდარტს, გამოძიების ან/და სისხლისსამართლებრივი დევნის მიმდინარეობას სსსკ-ით სპეციალურად განსაზღვრული დანაშაულების შემთხვევაში და თანაზომიერების პრინციპის, მათ შორის, სუბსიდიარულობის პრინციპის (იგივე აუცილებლობის ტესტის) დაცვას. ეს მოთხოვნები არის კუმულაციური და სსსკ-ის 143[3] მუხლის მე-2-მე-3 ნაწილებიდან გამომდინარე, ფარული საგამოძიებო მოქმედების ჩატარების თითოეული საფუძველი უნდა დასაბუთდეს პროკურორის მიერ მოსამართლისთვის წარდგენილ შუამდგომლობაში.

1.2.1. თანაზომიერების პრინციპი

სსსკ-ის 143[2] მუხლის მე-2 ნაწილის თანახმად, „ფარული საგამოძიებო მოქმედება ტარდება მხოლოდ იმ შემთხვევაში, თუ მისი ჩატარება გათვალისწინებულია ამ კოდექსით და ის აუცილებელია დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად – ეროვნული უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, უწესრიგობის ან დანაშაულის ჩადენის თავიდან ასაცილებლად, ქვეყნის ეკონომიკური კეთილდღეობის ინტერესების ან სხვა პირთა უფლებებისა და თავისუფლებების დასაცავად“.

143[2] მუხლის მე-3 ნაწილი განმარტავს, თუ რას გულისხმობს „დემოკრატიულ საზოგადოებაში აუცილებლობის მოთხოვნა“ - „ფარული საგამოძიებო მოქმედება აუცილებელია დემოკრატიულ საზოგადოებაში, თუ მისი ჩატარება გამოწვეულია გადაუდებელი საზოგადოებრივი საჭიროებით და ის ლეგიტიმური მიზნის მიღწევის შესაფერისი და პროპორციული საშუალებაა“.

თანაზომიერების პრინციპიდან გამომდინარეობს ასევე სსსკ-ის 143[2] მუხლის პირველი ნაწილით გათვალისწინებული დანაწესი, რომელიც ამ მოქმედების ჩატარებას დასაშვებად მიიჩნევს მხოლოდ სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით დადგენილი დანაშაულების გამოძიების მიზნით. ამავდროულად, 143[2] მუხლის მე-5 ნაწილი განსაზღვრავს ფარული საგამოძიებო მოქმედების ფარგლების (ინტენსივობის) მისი ჩატარების ლეგიტიმურ მიზანთან პროპორციულობის მოთხოვნას.

ნიშანდობლივია, რომ თანაზომიერების პრინციპი, როგორც ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასთან დაკავშირებული საგამოძიებო მოქმედებების განხორციელების სავალდებულო მოთხოვნა, სსსკ-ში 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებების შედეგად გაჩნდა. სსსკ-ის 143[2] მუხლში არსებული ზემოთ ხსენებული დათქმები პირდაპირ ეხმიანება თანაზომიერების პრინციპთან დაკავშირებით ევროპული სასამართლოს პრაქტიკასა და სხვა საერთაშორისო სტანდარტების შესაბამისად გაჟღერებულ ზოგად მოთხოვნებს.

როგორც კვლევაში აღინიშნა, სწორედ თანაზომიერების ტესტი უდევს საფუძვლად ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული სხვადასხვა

პროცედურული გარანტიების საკანონმდებლო დონეზე განსაზღვრის აუცილებლობას, ამავდროულად, კონკრეტული ღონისძიების თანაზომიერი ხასიათი ფასდება საქმის ინდივიდუალური გარემოებებიდან გამომდინარე.

სსსკ-ის მიხედვით, ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან გადაუდებელი აუცილებლობის შემთხვევაში მოსამართლის განჩინების გარეშე ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ განჩინებაში მოსამართლემ უნდა დაასაბუთოს სსსკ-ის 143[3] მუხლის მე-2 ნაწილით გათვალისწინებული გარემოებების არსებობა, რაც მათ შორის, გულისხმობს იმის დადასტურებასაც, რომ „ფარული საგამოძიებო მოქმედების ჩატარება გამოწვეულია გადაუდებელი საზოგადოებრივი საჭიროებით და არის დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად აუცილებელი, მისი მიღწევის შესაფერისი და პროპორციული საშუალება;“ ამასთანავე, განჩინებაში ასევე უნდა იქნეს დასაბუთებული, რომ მოთხოვნილი ღონისძიების შედეგად მოპოვებული იქნება გამოძიებისათვის არსებითი მნიშვნელობის მქონე ის ინფორმაცია, რომლის სხვა საშუალებით მოპოვება შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს (სსსკ-ის 143[3] მუხლის მე-10 ნაწილი). ამდენად, სსსკ ითვალისწინებს როგორც პროკურორის, ასევე მოსამართლის მხრიდან იმის არგუმენტირების ვალდებულებას, რომ კონკრეტული ფარული საგამოძიებო მოქმედება წარმოადგენს ლეგიტიმური მიზნის მიღწევის პროპორციულ და თანაზომიერ საშუალებას. ამასთანავე, უნდა გაირკვეს, არსებობს თუ არა საკმარისი და ეფექტიანი გარანტიები ძალაუფლების ბოროტად გამოყენების წინააღმდეგ. აგრეთვე, როდესაც ფარული საგამოძიებო მოქმედებების განხორციელება ეხება „დანაშაულთან პირდაპირ კავშირში მყოფ“ სხვა პირებს (პირთა წრეს), სასამართლომ უნდა იმსჯელოს, ამგვარი შუამდგომლობის დაკმაყოფილება ხომ არ გამოიწვევს „ადამიანთა ძალზე დიდი რაოდენობის“ დატოვებას სამართლებრივი დაცვის საშუალების გარეშე.[665]

კვლევაში განხილული საერთაშორისო სტანდარტების და საქართველოს კანონმდებლობის გათვალისწინებით, თანაზომიერების პრინციპის დარღვევის საკითხი დადგება ისეთ შემთხვევებში, როდესაც, მაგალითად:

[665] *მეზვრიშვილი ნ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 435.

- პროკურორის შუამდგომლობაში/სასამართლოს განჩინებაში არ არის დასაბუთებული სსსკ-ის 143[1] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კონკრეტული დანაშაულის გამოძიების მიზნებისათვის რატომ წარმოადგენს მოთხოვნილი ფარული საგამოძიებო მოქმედება აუცილებელ, პროპორციულ და შესაფერის საშუალებას, არამედ საქმის ინდივიდუალურ გარემოებებზე მსჯელობის გარეშე, შუამდგომლობა/განჩინება ეყრდნობა მხოლოდ ზოგად მითითებას „დანაშაულის სიმძიმეზე“ და „გამოძიების სირთულეზე“.

- გამოძიებისათვის საჭირო ინფორმაციის მოპოვება შესაძლებელია მაგალითად, ჩხრეკა/ამოღების საგამოძიებო მოქმედების საშუალებით, თუმცა ბრალდების მხარე ითხოვს სატელეფონო კომუნიკაციის ფარული მიყურადების შესახებ შუამდგომლობის გამოტანას და სასამართლო აკმაყოფილებს ამ შუამდგომლობას;

- სატელეფონო კომუნიკაციის ფარული მიყურადება ან ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიება ტარდება გამოძიების დაწყებისთანავე, ისე, რომ არ ხდება თავდაპირველ ეტაპზე სხვა ნაკლებად მძიმე საგამოძიებო მოქმედების გამოყენების შესაძლებლობის შეფასება;

- სასამართლოს ნებართვის საფუძველზე ჩატარებული სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ან „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების შედეგად ღონისძიების ვადის (1 თვე) ამოწურვამდე გაცილებით ადრე მოპოვებულია გამოძიებისათვის საჭირო ყველა რელევანტური ინფორმაცია, თუმცა ღონისძიების განხორციელება გრძელდება მხოლოდ იმ მიზეზით, რომ სასამართლოს ნებართვით გათვალისწინებული 1 თვიანი ვადა არ არის ამოწურული;

- დანაშაული რომლისთვისაც მოთხოვნილია ფარული საგამოძიებო მოქმედება, მართალია მიეკუთვნება სსსკ-ის 143[1] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ჩამონათვალს, თუმცა პროკურორის შუამდგომლობაში/სასამართლოს განჩინებაში არ არის დასაბუთებული, კონკრეტულ სიტუაციაში ამ დანაშაულის „სიმძიმე“ და „გამოძიების სირთულე“ რამდენად ამართლებს მოთხოვნილი ფარული საგამოძიებო მოქმედების გამოყენების აუცილებლობას, არამედ აღნიშნულ დანაშაულზე მითითება გაკეთებულია შაბლონურად, მხოლოდ იმ არგუმენტზე დაყრდნობით, რომ ეს დანაშაული ხვდება სსსკ-ის 143[1] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტით განსაზღვრულ ჩამონათვალში;

- გამოძიების მიზნებისათვის საჭიროა მხოლოდ ბრალდებულის კონკრეტულ პირთან/პირებთან კომუნიკაციის შესახებ ინფორმაციის მოპოვება, თუმცა ფარული საგამოძიებო მოქმედების ფარგლებში ხორციელდება ასევე ბრალდებულის კომპიუტერულ სისტემაში შენახული პირადი ხასიათის ინფორმაციის მოპოვება/დამუშავება, მაგალითად, პირადი ხასიათის ფოტოები, ვიდეოები, ფაილები;

- გამოძიების მიზნებისათვის სრულებით საკმარისია მხოლოდ ერთი სახის ფარული საგამოძიებო მოქმედების გამოყენება, თუმცა ტარდება რამდენიმე ფარული საგამოძიებო მოქმედება კომპლექსურად, ისე, რომ ერთზე მეტი ფარული საგამოძიებო მოქმედების ერთდროულად ჩატარების აუცილებლობა არ არის გამოკვეთილი. მაგალითად, სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიების შედეგად დიდი ალბათობით მოპოვებული იქნება გამოძიებისათვის საჭირო ყველა ინფორმაცია, თუმცა ბრალდების მხარე ითხოვს ასევე განხორციელდეს ბრალდებულის ინტერნეტკომუნიკაციების მოპოვებაც (სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი).

1.2.1.1. აუცილებლობის ტესტი

როგორც უკვე აღინიშნა, სამეცნიერო ლიტერატურასა და საერთაშორისო დონეზე არსებულ დოკუმენტებში თანაზომიერების პრინციპის ერთ-ერთ კომპონენტად მოიაზრება აუცილებლობის ტესტი, რაც გულისხმობს, რომ მოთხოვნილი ღონისძიება უნდა წარმოადგენდეს უკანასკნელ ზომას (ultima ratio). ეს ნიშნავს, რომ საგამოძიებო მოქმედებებმა, რომლებიც გამოირჩევა ხელყოფის ნაკლები ხარისხით, ვერ მიაღწიეს სასურველ მიზანს ან საგამოძიებო მოქმედებების განხორციელებასთან დაკავშირებული ხარჯები განუზომლად დიდი იქნება.[666] თუმცა ამ პრინციპის დანერგვა და ნამდვილობა დამოკიდებულია იმაზე, თუ რამდენად მოხდება მისი დაცვის ეფექტურად გაკონტროლება დამოუკიდებელი ორგანოს (სასამართლო) მიერ.[667]

[666] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 37, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].
[667] იქვე.

აღნიშნული მოთხოვნა არის ასახული სსსკ-შიც, კერძოდ, 143[2] მუხლის მე-4 ნაწილიდან გამომდინარე, „ფარული საგამოძიებო მოქმედება შეიძლება ჩატარდეს მხოლოდ მაშინ, როდესაც სხვა საშუალებით გამოძიებისათვის არსებითი მნიშვნელობის მქონე მტკიცებულებების მოპოვება შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს.“

გამოძიება მნიშვნელოვან სირთულეებს უკავშირდება მაშინ, როდესაც სხვა საგამოძიებო მოქმედების ჩატარება „დროში მნიშვნელოვნად გაიწელება და შესაბამისად, შეფერხდება სისხლის სამართლის პროცესი;“[668] ანდა, როდესაც ძირითად უფლებებში მყისიერი ჩარევა, მაგალითად, პირის დაკავება, შედეგად ვერ მოიტანს გამოძიებისათვის საჭირო მნიშვნელოვან მტკიცებულებებს.[669]

მოცემული სტანდარტი ორ ალტერნატიულ კრიტერიუმს აერთიანებს: 1) მოთხოვნილი ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული იქნება გამოძიებისათვის არსებითი მნიშვნელობის მქონე ის ინფორმაცია, რომლის სხვა საშუალებით მოპოვება შეუძლებელია. ამ შემთხვევაში პროკურორი ვალდებულია დაასაბუთოს, გამოძიებისათვის რა არსებითი მნიშვნელობის მქონე ინფორმაცია შეიძლება იქნეს მოპოვებული ფარული საგამოძიებო მოქმედების შედეგად და ასეთი ინფორმაცია უნდა შეესაბამებოდეს ფარული საგამოძიებო მოქმედების ჩატარების მიზნებს, პრინციპებს და მას მნიშვნელობა უნდა ჰქონდეს სისხლის სამართლის საქმის გამოძიებისა და დანაშაულთან დაკავშირებით მტკიცებულების მოპოვების კუთხით[670]; 2) აღნიშნული ინფორმაციის მოპოვება სხვა საშუალებით შეუძლებელია. ამ შემთხვევაში საუბარია იმ (კანონიერ) საშუალებებსა და გამოძიების ინსტრუმენტებზე, რომლებიც მოცემულია სსსკ-ში.[671]

სხვა საშუალებით გამოძიებისათვის არსებითი მნიშვნელობის მქონე ინფორმაციის მოპოვების შეუძლებლობა პროკურორმა შეიძლება დაასაბუთოს,

---

[668] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 106, იხ. ციტირება: Schmitt, in: Meyer-Goßner, StPO, 59. Aufl, 2016, §100a, Rn. 13; Schäfer, in Löwe-Rosenberg, StPO, 25. Aufl., 2003, §§ 100a, 100b, S. 354-355, Rn 43; Rieß, in: Gedschr für Meyer, 367.

[669] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 106, იხ. ციტირება: *Schäfer,* in Löwe-Rosenberg, StPO, 25. Aufl., 2003, §§ 100a, 100b, S. 354-355, Rn 43.

[670] *მეზვრიშვილი ნ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 435-436.

[671] იქვე.

მაგალითად, უკვე ჩატარებული სხვა საგამოძიებო მოქმედების არაეფექტიანობის ჩვენებით - საქმეში უზუნი გერმანიის წინააღმდეგ (Uzun v. Germany) GPS ტექნოლოგიის გამოყენებით პირის ადგილმდებარეობის მონიტორინგის ღონისძიების თანაზომიერების საკითხის შეფასების დროს ევროპულმა სასამართლომ გაითვალისწინა ის გარემოება, რომ ამ ღონისძიების ჩატარება არ მომხდარა თავიდანვე, საწყისი ეტაპის სახით, არამედ მანამდე საგამოძიებო ორგანოების მხრიდან გამოყენებულ იქნა უფრო მსუბუქი საშუალებები, თუმცა განმცხადებელმა და მისმა თანამზრახველმა მოახერხეს ამ მოწყობილობების აღმოჩენა და ასევე მრავალჯერ წარმატებით თავიდან აიცილეს მათ მიმართ გამოყენებული ვიზუალური კონტროლი[672]. ამდენად, სასამართლომ მიიჩნია, რომ მანამდე გამოყენებული სხვა ნაკლებად ინტენსიური მეთოდები იყო არაეფექტიანი.[673]

რაც შეეხება სხვა საშუალებით მტკიცებულების მოპოვების გაუმართლებელ ძალისხმევასთან დაკავშირებულ ასპექტს, პროკურორმა უნდა დაასაბუთოს რომ იმ ინფორმაციის მოპოვება, რომლის გამოც ითხოვს ფარული საგამოძიებო მოქმედების ჩატარებას, თუმცა შესაძლებელია სხვა საშუალებებით, მაგრამ მისი/მათი რეალიზაცია ან გართულებულია საქართველოს ტერიტორიის რაღაც ნაწილში არსებული მდგომარეობის გამო, ან ბრალდებული შესაძლოა იმყოფებოდეს ისეთ ტერიტორიაზე, სადაც ღია ტიპის ძებნას აზრი არ აქვს ან უკუშედეგის მომტანი იქნება, ან გამოიწვევს გამოძიების რესურსების დიდი ნაწილის კონცენტრაციას მხოლოდ ამ მიზნისთვის, ან/და დიდ ფინანსურ ხარჯებს და სხვ[674].

სსსკ-ის მოთხოვნებიდან გამომდინარე, მტკიცების ტვირთი გამოძიებისათვის არსებითი მნიშვნელობის მქონე მტკიცებულების სხვა საშუალებით მოპოვების შეუძლებლობასთან ან გაუმართლებელ ძალისხმევასთან დაკავშირებით აწევს პროკურორს. პროკურორის შუამდგომლობაში უნდა აისახოს ინფორმაცია იმ საგამოძიებო მოქმედების შესახებ (ასეთის არსებობის შემთხვევაში), რომელიც შუამდგომლობის წარდგენამდე ჩატარდა სსსკ-ით დადგენილი წესით და რომლითაც დასახული მიზანი ვერ იქნა მიღწეული (სსსკ-ის 143[3] მუხლი მე-3 ნაწილი). თავის

[672] Uzun v. Germany, [2015], ECtHR. 78.

[673] იქვე.

[674] *მეზვრიშვილი ნ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 436.

მხრივ, მოსამართლის განჩინებაში ასევე უნდა იქნეს დასაბუთებული აღნიშნული გარემოებები. შეფასებას იმასთან დაკავშირებით, შესაძლებელია თუ არა სხვა ნაკლებად ინტენსიური საშუალებით ლეგიტიმური მიზნის მიღწევა, საფუძვლად უნდა დაედოს კონკრეტული საქმის ინდივიდუალური გარემოებები.[675]

ფარული მეთვალყურეობის ღონისძიების უკიდურესი საშუალების სახით გამოყენების პრინციპი ასევე ასახულია აშშ-ის კანონმდებლობაშიც და ითვალისწინებს გარკვეულწილად მსგავს მოთხოვნებს, რასაც სსსკ, კერძოდ, აშშ-ის კანონმდებლობის მიხედვით, ელექტრონული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე პროკურორის შუამდგომლობა უნდა შეიცავდეს „სრულყოფილ და ამომწურავ ინფორმაციას“ იმასთან დაკავშირებით, სხვა უფრო მსუბუქი საგამოძიებო მოქმედებები გამოყენებულ იქნა თუ არა და რამდენად წარმატებული აღმოჩნდა ან რატომ იქნება უშედეგო ან ძალიან სახიფათო, თუკი მომავალში იქნება გამოყენებული[676]. აშშ-ის უზენაესი სასამართლოს განმარტებით, აღნიშნული მოთხოვნის მიზანია, ფარული მეთვალყურეობის ღონისძიება არ იქნას გამოყენებული „რუტინულად“, „გამოძიების საწყისი ეტაპის სახით“ ან „ისეთ ვითარებაში, როდესაც ჩვეულებრივი საგამოძიებო მოქმედებები საკმარისი იქნებოდა.“[677] თუმცა, სამეცნიერო ლიტერატურაში გამოთქმული მოსაზრების თანახმად, პრაქტიკაში ამ სტანდარტს მიეცა უფრო საგამოძიებო საჭიროების, ვიდრე აუცილებლობის მნიშვნელობა.[678] მოცემული პრინციპის პრაქტიკაში დემონსტრირება შესაძლებელია შემდეგი გზებით: 1) იმის ჩვენებით, რომ სხვა საგამოძიებო მოქმედებები წარუმატებელი აღმოჩნდა. ეს მოთხოვნა იმგვარად მკაცრად არ განიმარტება, რომ მოითხოვდეს თითოეული შესაძლო ალტერნატივის მანამდე პრაქტიკაში წარუმატებელ განხორციელებას[679]; 2) სხვა საგამოძიებო მოქმედებების [სამომავლოდ] წარუმატებლობის დადასტურებით, რომელიც, მაგალითად, შეიძლება განხორციელდეს კონკრეტულ დანაშაულებრივ დაჯგუფებაში შეღწევის სირთულის ჩვენებით ან იმის მტკიცებით, რომ სხვა საგამოძიებო მოქმედების (მაგალითად, ჩხრეკა) შედეგად მაინკრიმინებელი

[675] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 9 (ბმული იხ. მე-80 გვერდზე).
[676] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed, 2004, 283.
[677] იქვე.
[678] იქვე.
[679] იქვე. 283-284.

მტკიცებულება სავარაუდოდ ვერ იქნება მოპოვებული[680]; 3) სხვა საგამოძიებო მოქმედებები ძალიან სახიფათოა გამოძიებასთან დაკავშირებით ინფორმაციის გამჟღავნების ან საგამოძიებო ორგანოს თანამშრომლისთვის ან კონფიდენტისთვის ფიზიკური საფრთხის შექმნის თვალსაზრისით.[681]

ნიშანდობლივია, რომ აუცილებლობის ტესტს დიდი ყურადღება დაეთმო ევროპული სასამართლოს ბოლოდროინდელ გადაწყვეტილებებში. კვლევაში განხილული ევროპული სასამართლოს პრეცედენტული სამართლის მოთხოვნებიდან გამომდინარე, სასამართლოს განჩინება სხვა ნაკლებად ინტენსიური საგამოძიებო მეთოდების გამოყენების შეუძლებლობასთან/გაუმართლებელ ძალისხმევასთან დაკავშირებით უნდა დადასტურდეს საქმის კონკრეტული ფაქტობრივი გარემოებებით, რომლებიც „დასაბუთებული ვარაუდით“ მიუთითებენ, რომ გამოძიების მიზნების მიღწევა სხვა ნაკლებად მძიმე საშუალებებით შეუძლებელია[682]. ევროპული სასამართლოს განმარტებით, სასამართლოს განჩინება უნდა შეიცავდეს მსჯელობას და შესაბამის მიზეზებს, თუ რატომ არის სხვა ნაკლებად ინტენსიური მეთოდების გამოყენება შეუძლებელი ან არაეფექტიანი.[683] ამდენად, ევროპული სასამართლოს მიერ დადგენილი სტანდარტებიდან გამომდინარე, პროკურორის დადგენილება და სასამართლოს განჩინება გამოძიებისათვის არსებითი მნიშვნელობის მქონე ინფორმაციის სხვა საშუალებით მოპოვების შეუძლებლობასთან/გაუმართლებელ ძალისხმევასთან დაკავშირებით უნდა იყოს დასაბუთებული საქმის ინდივიდუალური და ფაქტობრივი გარემოებებით.

1.2.2. დანაშაულები, რომელთა შემთხვევაშიც დასაშვებია ფარული საგამოძიებო მოქმედების განხორციელება

სსსკ ფარული საგამოძიებო მოქმედებების ჩატარებას უკავშირებს სპეციალურად განსაზღვრულ დანაშაულთა წრეს, რომელიც ამომწურავია და დადგენილია სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით. დანაშაულთა წრის განსაზღვრასთან დაკავშირებით საყურადღებოა პროფესორი ალბრეხტის პოზიცია დასკვნაში

[680] იქვე.
[681] იქვე.
[682] Mustafa Sezgin Tanrikulu v. Turkey, [2017], ECtHR, 59. Dragojević v. Croatia, [2015], ECtHR, 95.
[683] Dragojević v. Croatia, [2015], ECtHR, 95-101, Bašić v. Croatia, [2017], ECtHR, 33-34; Matanović v. Croatia, [2017], ECtHR, 112-115.

„საქართველოს კანონმდებლობით ევროკავშირის 2006/24 დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე“ (შემდგომში - ფარული საგამოძიებო მოქმედებების შესახებ დასკვნა). „ვინაიდან ფარული საგამოძიებო მოქმედებები, ძირითადად, გამართლებულია ორგანიზებული და მძიმე ტრანსსასაზღვრო დანაშაულის გამოძიების აუცილებლობით“, იმ დანაშაულთა განსაზღვრის მიზნით, რომელთა გამოძიების ინტერესიც შეიძლება საფუძვლად დაედოს აღნიშნულ ღონისძიებათა გამოყენებას, პროფესორი ალბრეხტი განიხილავს ორ მოდელს - „დანაშაულთა სიის დადგენას ან ზოგადი ზღვარის გამოყენებას.“[684] ამასთან, აუცილებელია მოხდეს იმის უზრუნველყოფა, რომ ფარული მეთვალყურეობის უფლებამოსილება არ გავრცელდეს „მსუბუქ დანაშაულებზე“, განსაკუთრებით, „წვრილმან დანაშაულებზე.“[685]

სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტის თანახმად, ფარული საგამოძიებო მოქმედების განხორციელება დასაშვებია, თუკი გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება განზრახი მძიმე ან/და განსაკუთრებით მძიმე დანაშაულის ან საქართველოს სისხლის სამართლის კოდექსის (შემდგომში - სსკ) კონკრეტული მუხლებითა და თავით გათვალისწინებული ზოგიერთი ნაკლებად მძიმე დანაშაულის გამო, რომელთა ჩამონათვალი განსაზღვრულია ამავე ქვეპუნქტში.

აღსანიშნავია, რომ 2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტის (რომლითაც სსსკ-ს დაემატა ფარული საგამოძიებო მოქმედებების თავი) ძალაში შესვლის შემდეგ, სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტში რამდენჯერმე განხორციელდა ცვლილება და აღნიშნულ მუხლით დადგენილ ნაკლებად მძიმე დანაშაულთა სიას დაემატა გარკვეული დანაშაულები, მაგალითად, 254-ე მუხლი, 306[1] მუხლი, 344[2] მუხლი, სამოხელეო დანაშაულის თავი. საყურადღებოა ისიც, რომ 2014 წლის 1 აგვისტოს სსსკ-ში განხორციელებული ცვლილებების განმარტებითი ბარათის მიხედვით, „ფარული საგამოძიებო მოქმედება შესაძლებელია განხორციელდეს მხოლოდ მძიმე, განსაკუთრებით მძიმე და სსსკ-ით განსაზღვრული კონკრეტული

[684] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 37, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].
[685] იქვე.

დანაშაულების გამოძიების პროცესში, რომელიც შეესაბამება ევროკავშირის „დაპატიმრების ორდერის“ ჩარჩო გადაწყვეტილებით გათვალისწინებული დანაშაულების შემადგენლობას.“[686] ამდენად, 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებების შემუშავების პროცესში ფარული საგამოძიებო მოქმედებების საფუძვლად ნაკლებად მძიმე კატეგორიის დანაშაულთა ჩამონათვალის დადგენისას კანონმდებელმა იხელმძღვანელა ევროპის საბჭოს „დაპატიმრების ორდერის“ ჩარჩო გადაწყვეტილებით დადგენილი დანაშაულთა შემადგენლობით. თუმცა აღნიშნულის შემდეგ სსსკ-ში განხორციელებულ ცვლილებებს, რომლებითაც სხვა დანაშაულებიც დაემატა ამ ჩამონათვალს, სხვადასხვა არგუმენტაცია ედებოდა საფუძვლად, მაგალითად, კონკრეტული დანაშაულის გამოძიების სირთულე ფარული საგამოძიებო მოქმედებების ჩატარების შესაძლებლობის გარეშე,[687] კორუფციასთან ეფექტიანი ბრძოლის აუცილებლობა,[688] საკანონმდებლო აქტებში განხორციელებული ცვლილებები, რომლის შედეგადაც სსკ-ით გათვალისწინებულ კონკრეტულ დანაშაულთა თავს დაემატა დანაშაულის ახალი შემადგენლობა[689] და სხვ. აღნიშნულ ფონზე რჩება შთაბეჭდილება, რომ გაუგებარია კრიტერიუმი, რომლითაც კანონმდებელი ხელმძღვანელობს სსსკ-ის 143^3 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით დადგენილი სიის გაფართოებისას.

იმ შემთხვევაში, თუკი სსსკ-ის 143^3 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით დადგენილ ნაკლებად მძიმე დანაშაულთა ჩამონათვალში მომავალშიც გაგრძელდება ახალი შემადგენლობების დამატების ტენდენცია, აუცილებელია გათვალისწინებულ იქნეს საერთაშორისო სტანდარტი, რომელიც ფარული საგამოძიებო მოქმედების გამოყენების შესაძლებლობას მხოლოდ მნიშვნელოვანი სამართლებრივი სიკეთეების

[686] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“; <https://info.parliament.ge/#law-drafting/24> [20.06.2020].

[687] განმარტებითი ბარათი საქართველოს კანონის პროექტზე “ „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/#law-drafting/15289> [20.06.2020].

[688] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/#law-drafting/16624> [20.06.2020].

[689] განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/file/1/BillReviewContent/142892?> [20.06.2020].

დაცვის ინტერესს უკავშირებს[690]. მართალია სახელმწიფოს მინიჭებული აქვს გარკვეული დისკრეცია ასეთ დანაშაულთა წრის დადგენისას, მაგრამ თანაზომიერების პრინციპის გათვალისწინებით, ფარული მეთვალყურეობის ღონისძიება, უფლებაში ჩარევის მაღალი ინტენსივობიდან გამომდინარე, მხოლოდ „სერიოზულ“ დანაშაულთან ბრძოლის ინტერესებმა შეიძლება გაამართლოს. ამ მხრივ მხედველობაშია მისაღები ასევე ევროპული სასამართლოს პრაქტიკაც, რომლის თანახმადაც, კომუნიკაციის მონიტორინგის ღონისძიება „მკაცრად აუცილებელი“ უნდა იყოს ერთი მხრივ, ზოგადად დემოკრატიული საფუძვლების უზრუნველსაყოფად, ხოლო მეორე მხრივ, კონკრეტულ სიტუაციაში სასიცოცხლო მნიშვნელობის ინფორმაციის მოპოვების მიზნით.[691] მეორე მხრივ, ასევე მნიშვნელოვანია, რომ კრიტერიუმი, რომელიც შეიძლება საფუძვლად დაედოს დანაშაულთა სიის გაფართოებას, იყოს თვალსაჩინო და ნათელი, რათა აღნიშნულმა პროცესმა არ მიიღოს რუტინული ხასიათი და არ დაიკარგოს დანაშაულთა შეზღუდული წრის განსაზღვრის დანიშნულება, რომელიც მდგომარეობს ადამიანის კონსტიტუციურ უფლებებში მსგავსად მაღალი ინტენსივობით ჩარევის შესაძლებლობაში მხოლოდ მნიშვნელოვანი სამართლებრივი სიკეთის დაცვის აუცილებლობის საფუძვლით.

როგორც უკვე აღინიშნა, დანაშაულთა კონკრეტული, ლიმიტირებული სიის დადგენას თანაზომიერების პრინციპი უდევს საფუძვლად. ამასთანავე, მეორე მნიშვნელოვან ფაქტორს, რომელსაც ასევე შეუძლია ღონისძიების თანაზომიერებაზე გავლენის მოხდენა, წარმოადგენს შესაბამისი დანაშაულის ხასიათის/სიმძიმის შეფასება ინდივიდუალურ შემთხვევებში. ამ თვალსაზრისით აღსანიშნავია ვენეციის კომისიის ანგარიში ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით პოლონეთის კანონმდებლობაში განხორციელებული ცვლილებების შესახებ, სადაც კომისია აღნიშნავს, რომ ფარული მეთვალყურეობის ღონისძიებების შეზღუდვა დანაშაულთა გარკვეული წრით თანაზომიერების პრინციპის ერთ-ერთ მოთხოვნას წარმოადგენს,

[690] Case NC 293/12 and C 594/12, Digital Rights Ireland Ltd and Seitlinger and others, [2014], Court of Justice; Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.); Iordachi and others v. Moldova, [2009], ECtHR, 51; Recommendation No R (95) 13 of The Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology, Council of Europe, 11.09.1995, <https://rm.coe.int/native/09000016804f6e76> [20.06.2020].

[691] Szabo and Vissy v. Hungary, [2016] ECtHR, 73.

თუმცა თანაზომიერების ტესტი მხოლოდ აღნიშნულით არ შემოიფარგლება.[692] ამის პარალელურად, პროცესის ყველა მონაწილეს - როგორც საგამოძიებო ორგანოს, ასევე სასამართლოს მოეთხოვება ყოველ კონკრეტულ შემთხვევაში შეაფასოს, დანაშაულის სიმძიმე (თუნდაც დანაშაული მიეკუთვნებოდეს იმ ჩამონათვალს, რომლისთვისაც ნებადართულია ფარული მეთვალყურეობა) და გამოძიების სირთულე რამდენად მოითხოვს ფარული მეთვალყურების ღონისძიების განხორციელებას[693]. კომისია აღნიშნავს, რომ მართალია ზოგიერთი განსაკუთრებით სერიოზული დანაშაულის შემთხვევაში შესაძლოა პასუხი იმთავითვე აშკარა იყოს, მაგრამ პოლონეთის კანონმდებლობაში ფარული მეთვალყურეობის საფუძვლად განსაზღვრულ ყველა დანაშაულთან მიმართებით საკითხი ასეთივე თვალსაჩინო ვერ იქნება და დამატებით შეფასებას საჭიროებს.[694] ნიშანდობლივია, რომ ამ საკითხის მიმართ მსგავსი მიდგომა არის გათვალისწინებული გერმანიის სისხლის სამართლის საპროცესო კოდექსშიც, რომელიც გარდა იმისა, რომ სატელეკომუნიკაციო მიყურადებისა და კონტროლის გამოყენებას დასაშვებად მიიჩნევს მხოლოდ 100a (2) პარაგრაფით სპეციალურად დადგენილ დანაშაულებთან დაკავშირებით, ასევე განსაზღვრავს ასეთი დანაშაულის „განსაკუთრებულად მძიმე ხასიათის სავალდებულოობას ინდივიდუალურ შემთხვევაში.“[695]

მიზანშეწონილი იქნება, თუკი სსსკ ასევე გაითვალისწინებს მსგავსი შინაარსის დათქმას და პირდაპირ განსაზღვრავს დანაშაულის სიმძიმის შეფასების მოთხოვნას კონკრეტულ სიტუაციაში საქმის ინდივიდუალური გარემოებებიდან გამომდინარე. როგორც ვენეციის კომისია აღნიშნავს, ფარული მეთვალყურეობის ღონისძიების საფუძვლად დადგენილ დანაშაულთაგან ზოგიერთის შემთხვევაში ამ გარემოებას შესაძლოა დამატებითი შეფასება არც დასჭირდეს, თუმცა გასათვალისწინებელია რომ სსსკ-ის 143^3 მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტში მოცემულ დანაშაულთა წრე მხოლოდ მძიმე და განსაკუთრებით მძიმე დანაშაულებით არ შემოიფარგლება და გათვალისწინებულია ასევე ზოგიერთი ნაკლებად მძიმე დანაშაულის შემთხვევაში

[692] European Commission for Democracy Throgh Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 13, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].
[693] იქვე.
[694] იქვე.
[695] StPO, §100a Abs.1 S.2, 07/04/1987.

ასეთი საგამოძიებო მოქმედების გამოყენების შესაძლებლობაც, მითუმეტეს, რომ ამ კატეგორიიდან გარკვეული დანაშაულები სასჯელის სახით თავისუფლების აღკვეთას საერთოდ არ ითვალისწინებენ[696] ან ითვალისწინებენ მხოლოდ ერთი ან ორი წლის ვადით.[697] მართალია ასეთი შეფასება, ზოგადად, თანაზომიერების პრინციპიდან ისედაც გამომდინარეობს, მაგრამ სსსკ-ში პირდაპირი მოთხოვნის განსაზღვრის შემთხვევაში, უფრო დიდი დატვირთვა მიეცემა. ამასთან, იქედან გამომდინარე, რომ სსსკ ფარული საგამოძიებო მოქმედებების საფუძვლად განსაზღვრავს დანაშაულთა კონკრეტულ სიას, არსებობს რისკი იმისა, რომ კონკრეტული დანაშაულის სიმძიმეს პრაქტიკაში დამატებითი შეფასება აღარც მიეცეს.

აღნიშნულიდან გამომდინარე, მოთხოვნილი/გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული ღონისძიების თანაზომიერების სათანადოდ შეფასების მიზნით, შეიძლება მით უფრო მნიშვნელოვანი იყოს სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით დადგენილი დანაშაულების სერიოზული ხასიათის ყოველ კონკრეტულ შემთხვევაში დამატებით შეფასება.

1.2.3 დასაბუთებული ვარაუდის სტანდარტი

სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტის თანახმად, ფარული საგამოძიებო მოქმედება ტარდება, თუკი არსებობს დასაბუთებული ვარაუდი, რომ პირს, რომლის მიმართაც უნდა ჩატარდეს ფარული საგამოძიებო მოქმედება, ჩადენილი აქვს ამ ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული რომელიმე დანაშაული („დანაშაულთან პირდაპირ კავშირში მყოფი პირი“), ან პირი იღებს ან გადასცემს დანაშაულთან პირდაპირ კავშირში მყოფი პირისათვის განკუთვნილ ან მისგან მომდინარე ინფორმაციას, ან დანაშაულთან პირდაპირ კავშირში მყოფი პირი იყენებს პირის საკომუნიკაციო საშუალებებს. ამდენად, აღნიშნული მუხლი ადგენს ფარული საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელ მტკიცებულებით სტანდარტს „დასაბუთებულ ვარაუდს“ დასახელებულ გარემოებებთან მიმართებით. აღნიშნული სტანდარტი გულისხმობს იმას, რომ ფარული საგამოძიებო მოქმედების განხორციელება აუცილებლად უნდა უკავშირდებოდეს დანაშაულის შესაძლო ჩამდენ

[696] იხ. მაგალითად, სსკ-ის 297-ე მუხლი (მიწის გაუვარგისება), სსკ-ის 298-ე მუხლი (წიაღისეულის გამოყენების ან დაცვის წესის დარღვევა), სსმ, 41(48), 22/07/1999.
[697] იხ. მაგალითად, სსსკ-ის 301-ე მუხლის პირველი ნაწილი (უკანონო ნადირობა), სსმ, 41(48), 22/07/1999.

პირს, მის მოქმედებებს, კომუნიკაციას, ა.შ.[698] „დასაბუთებული ვარაუდის სტანდარტით რაიმე გარემოებების შეფასება, თავისთავად, მოითხოვს მათი (გარემოებების) დადგენისთვის ფაქტების ან ინფორმაციის ერთობლიობის შეფასებას.“[699] სსსკ-ის მე-3 მუხლის მე-11 ნაწილის თანახმად, „დასაბუთებული ვარაუდი“ განიმარტება, როგორც „ფაქტების ან ინფორმაციის ერთობლიობა, რომელიც მოცემული სისხლის სამართლის საქმის გარემოებათა ერთობლიობით დააკმაყოფილებდა ობიექტურ პირს, რათა დაესკვნა პირის მიერ დანაშაულის შესაძლო ჩადენა, სსსკ-ით პირდაპირ გათვალისწინებული საგამოძიებო მოქმედების ჩატარებისთვის ან/და აღკვეთის ღონისძიების გამოყენებისთვის გათვალისწინებული მტკიცებულებითი სტანდარტი.“

დასაბუთებული ვარაუდის სტანდარტის დასაკმაყოფილებლად პროკურორმა შუამდგომლობა უნდა დაასაბუთოს მტკიცებულებებით და არა მასში მოყვანილი გარემოებებით (ფაქტების კონსტატაციით).[700] წარდგენილი მტკიცებულებები უნდა ასაბუთებდეს პირის კავშირს სსსკ-ით განსაზღვრულ კონკრეტულ დანაშაულთან ან დანაშაულთან პირდაპირ კავშირში მყოფ პირთან, რომლის მიმართაც უნდა განხორციელდეს ფარული საგამოძიებო მოქმედება[701].

ზოგადად, ქართული სტანდარტი - დასაბუთებული ვარაუდი, რომელიც 2009 წლის 1 ოქტომბრის სისხლის სამართლის საპროცესო კოდექსმა შემოიტანა საქართველოს კანონმდებლობაში, წარმოადგენს ამერიკული “დასაბუთებული ვარაუდის“ (“Probable cause”) სტანდარტის ანალოგს, რომელიც აუცილებელ მტკიცებულებით სტანდარტს განეკუთვნება ჩხრეკა/ამოღების, ისევე როგორც დაკავების ღონისძიებებთან დაკავშირებით აშშ-ის კონსტიტუციის მე-4 დამატების შესაბამისად.[702] აშშ-ის კანონმდებლობის მიხედვით, „დასაბუთებული ვარაუდის“ ტესტი არის გათვალისწინებული ასევე კომუნიკაციის მონიტორინგის საგამოძიებო

---

[698] *მეზვრიშვილი ნ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 433.

[699] საქართველოს საკონსტიტუციო სასამართლოს 2014 წლის 23 მაისის №3/1/574 გადაწყვეტილება, II - 79.

[700] *მეზვრიშვილი ნ.,* საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, თბ., 2015, 434.

[701] იქვე.

[702] *Lippman M.,* Criminal Procedure, 3rd Edition, Los Angeles, 2017, 51, 122-123; *Signorelli W. P.,* Criminal Law, Procedure, and Evidence, New York, 2011, 31-32.

მოქმედებებთან მიმართებითაც,[703] კერძოდ, კომუნიკაციის მონიტორინგის შესახებ მოსამართლის ბრძანება (Interception order) შეიძლება გაიცეს იმ შემთხვევაში, თუკი მოსამართლე წარდგენილი ფაქტობრივი გარემოებების საფუძველზე დაადგენს, რომ არსებობს „დასაბუთებული ვარაუდი“ იმის თაობაზე, რომ ინდივიდს ჩადენილი აქვს კანონმდებლობით სპეციალურად განსაზღვრული რომელიმე დანაშაული, რომ ამ დანაშაულთან შემხებლობაში მყოფი კონკრეტული კომუნიკაციები იქნება მოპოვებული და მოწყობილობები, რომლებიდანაც უნდა მოხდეს კომუნიკაციის მოპოვება, კავშირშია აღნიშნულ დანაშაულთან;[704] აშშ-ის სამეცნიერო ლიტერატურაში დასმულია საკითხი იმის შესახებ, კომუნიკაციის მონიტორინგის ჩასატარებლად აუცილებელი „დასაბუთებული ვარაუდი“ ხომ არ უნდა იქნეს განმარტებული უფრო მკაცრი ტესტის სახით, ვიდრე ეს უნდა განხორციელდეს ჩხრეკის საგამოძიებო მოქმედებასთან მიმართებით.[705] ამ თვალსაზრისით იურიდიულ ლიტერატურაში განხილულია ფარული თვალთვალის უფლებამოსილებასთან დაკავშირებული ერთ-ერთ ცნობილი საქმე ბერგერი აშშ-ს წინააღმდეგ (Berger v. United States), სადაც მოსამართლემ განსხვავებულ აზრში განსაკუთრებული მნიშვნელობა მიანიჭა სასამართლოს ბრძანების კონკრეტულ ხასიათსა და შესაბამისი მტკიცებულების სანდოობის აუცილებლობას საცხოვრებელ სახლში განხორციელებული ფარული აუდიოჩაწერის ღონისძიებასთან დაკავშირებით[706]. მოსამართლის განმარტებით, განხორციელებული ღონისძიება, რომელიც 60 დღიან პერიოდს მოიცავდა, დაკავშირებული იყო კონსტიტუციით დაცული სფეროს მომეტებულ შეზღუდვასთან.

---

[703] აღსანიშნავია, რომ აშშ-ის კანონმდებლობა ერთმანეთისგან განასხვავებს კომუნიკაციის რეალურ დროში მოპოვების და სერვისის მიმწოდებელთან შენახულ მონაცემებზე წვდომის ღონისძიებებს და ამ ორივე შემთხვევაში განსხვავებულ რეგულაციებსა და სტანდარტებს ადგენს. მიმდინარე რეჟიმში შინაარსობრივი მონაცემების მოპოვების ღონისძიებები რეგულირებულია „მოსმენების შესახებ“ აქტით (“Wiretap Act”), რომელიც არეგულირებს სატელეფონო, ზეპირი (რომლის ჩაწერაც ხდება) და კომპიუტერული კომუნიკაციების მოპოვებას. სერვისის მიმწოდებელთან შენახულ ინფორმაციაზე (შინაარსობრივი და მეტადატა) წვდომის საკითხები დარეგულირებულია „შენახული კომუნიკაციების შესახებ“ აქტით (“Stored Communications Act”). „მოსმენების შესახებ“ აქტის ფარგლებში მიმდინარე რეჟიმში კომუნიკაციების მოპოვებისთვის კანონმდებლობით გათვალისწინებულია გაცილებით მკაცრი მოთხოვნები, მათ შორის, „დასაბუთებული ვარაუდის“ სტანდარტის აუცილებლობა ღონისძიების ჩასატარებლად. იხ. *LaFave W., R., Israel J., H., King N., J., Kerr O., S.,* Principles of Criminal Procedure: Investigation, 2nd Ed., 2009, 230-234.

[704] *Ohm P.,* The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E. (eds),* New York, 2017, 499; *Israel J. H., LaFave W. R.,* Criminal Procedure, Constitutional Limitations in a Nutshell, 8th Ed. 2014,166.

[705] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 268-269.

[706] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., Thomson West, 2004, 268-269, იხ. ციტირება: Berger v. New York, 388 U.S. 41 (1967).

აღნიშნულის გათვალისწინებით, მხოლოდ ყველაზე „კონკრეტული“ და „მკაცრი“ „დასაბუთებული ვარაუდის“ სტანდარტი შეიძლება დასდებოდა საფუძვლად ასეთი ინტენსივობით კონსტიტუციურ უფლებაში ჩარევას.[707] ამდენად, მოცემული შეხედულების მიხედვით, მართალია საქმეში არსებული „მტკიცებულებები შესაძლოა საკმარისი ყოფილიყო ჩვეულებრივი ჩხრეკის ან დაკავების განსახორციელებლად, მაგრამ ვერ აკმაყოფილებდა კონსტიტუციურ მოთხოვნას გამოყენებულ ფარულ საგამოძიებო ღონისძიებასთან მიმართებით, მისი ფარგლებისა და ხანგრძლივობის გათვალისწინებით.[708] აღსანიშნავია, რომ მიუხედავად სასამართლო პრაქტიკაში გამოთქმული ამ მოსაზრებისა, ბრალდებულებმა, რომლებიც მოცემულ არგუმენტზე აპელირებდნენ ქვემდგომი ინსტანციის სასამართლოებში, ვერ მიაღწიეს ამ კუთხით მათთვის სასარგებლო გადაწყვეტილებას.[709]

კვლევის ფარგლებში განხილული ევროპული სასამართლოს გადაწყვეტილებებიდან გამომდინარე, ფარული მეთვალყურეობის ღონისძიების ჩასატარებლად აუცილებელი მტკიცებულებითი სტანდარტი (ქართული კანონმდებლობის შემთხვევაში - დასაბუთებული ვარაუდი) უნდა იქნეს დადასტურებული საქმის კონკრეტული ფაქტობრივი გარემოებებითა და მტკიცებულებებით, პროკურორის შუამდგომლობას თან უნდა ახლდეს შესაბამისი მასალები, რომლებითაც სასამართლოს მიეცემა ფარული საგამოძიებო მოქმედების ჩასატარებლად საჭირო შესაბამისი ფაქტობრივი საფუძვლის რეალურად დადგენის შესაძლებლობა. სასამართლოს განჩინებაში, ისევე როგორც პროკურორის შუამდგომლობაში მხოლოდ ზოგადი მითითებები, სსსკ-ით გათვალისწინებული კონკრეტული დანაშაულის ნიშნების არსებობასთან დაკავშირებით, ვერ ჩაითვლება საკმარისად.[710] ღონისძიების ჩატარება დასაშვებია მხოლოდ „დამაჯერებელი დასაბუთების“ პირობებში,[711] ამავდროულად, სასამართლოს უნდა გააჩნდეს წვდომა ყველა შესაბამის დოკუმენტაციასა და ინფორმაციასთან, მათ შორის, საიდუმლო მასალებთან, რათა მიეცეს შესაძლებლობა, რეალურად შეამოწმოს, რამდენად

[707] იქვე.
[708] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., Thomson West, 2004, 268-269.
[709] იქვე.
[710] Dragojević v. Croatia, [2015], ECtHR, 95-101; Bašić v. Croatia, [2017], ECtHR, 33-34.
[711] Dragojević v. Croatia, [2015], ECtHR, 94.

არსებობს საქმეში ღონისძიების ჩასატარებლად აუცილებელი მტკიცებულებითი სტანდარტი.[712]

1.2.4. შეჯამება

ამდენად, პროკურორის შუამდგომლობაში, ისევე როგორც სასამართლოს განჩინებაში უნდა იქნეს დასაბუთებული მოთხოვნილი ფარული საგამოძიებო მოქმედების თანაზომიერების პრინციპთან შესაბამისობა. კვლევის წინა თავში დეტალურად იქნა განხილული, თუ რა გარემოებებს ენიჭება მნიშვნელობა თანაზომიერების პრინციპის კონტექსტში. სსსკ-ის 143[3] მუხლის მოთხოვნებიდან გამომდინარე, პროკურორის შუამდგომლობასა და სასამართლოს განჩინებაში დასაბუთებას ექვემდებარება ის გარემოებაც, რომ მოთხოვნილი ღონისძიების შედეგად მოპოვებული იქნება გამოძიებისათვის არსებითი მნიშვნელობის ის მტკიცებულება, რომლის სხვა, ნაკლებად მძიმე საშუალებებით მოპოვება შეუძლებელია ან გაუმართლებელ ძალისხმევას საჭიროებს. აღნიშნული უნდა განხორციელდეს საქმის კონკრეტული ფაქტობრივი გარემოებებით და მხოლოდ მითითება სხვა საგამოძიებო მოქმედების განხორციელების შეუძლებლობის ან გაუმართლებელი ძალისხმევის საჭიროების შესახებ ვერ ჩაითვლება საკმარისად.

რაც შეეხება სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით განსაზღვრულ დანაშაულთა ჩამონათვალს, ვინაიდან 2014 წლის 1 აგვისტოდან მოყოლებული შეინიშნება ნაკლებად მძიმე დანაშაულთა სიის გაფართოების ტენდენცია, მიზანშეწონილია, კრიტერიუმი, რომლითაც შეიძლება შეირჩეს დანაშაული, რომელიც ამ ჩამონათვალს დაემატება, იყოს მკაფიო და ნათელი; ასევე მნიშვნელოვანია, აღნიშნულ ჩამონათვალში ახალი დანაშაულის დამატება მხოლოდ საკმარისად წონადი სამართლებრივი სიკეთეების დაცვის მიზნით იყოს ნაკარნახევი.

ნაშრომში ასევე გამოითქვა მოსაზრება იმასთან დაკავშირებით, რომ სასურველი იქნება სსსკ დანაშაულის სიმძიმის შეფასების პირდაპირ მოთხოვნას ითვალისწინებდეს ყოველ კონკრეტულ სიტუაციაში, საქმის ინდივიდუალური გარემოებების მხედველობაში მიღებით. მიგვაჩნია, რომ ასეთი დათქმა ხელს შეუწყობს ღონისძიების თანაზომიერებასთან დაკავშირებული ასპექტების სრულფასოვან

[712] Roman Zakharov v. Russia, [2015] ECtHR, 281.

ანალიზს და განსაკუთრებით მნიშვნელოვანი შეიძლება იყოს ფარული საგამოძიებო მოქმედების საფუძვლად განსაზღვრული ზოგიერთი დანაშაულის შემთხვევაში, მაგალითად, როდესაც ამ დანაშაულისთვის გათვალისწინებული სასჯელი საერთოდ არ ითვალისწინებს თავისუფლების აღკვეთას ან ითვალისწინებს ძალიან მცირე ვადით, რაც შეიძლება მიანიშნებდეს იმაზე, რომ როდესაც საუბარია ადამიანის ფუნდამენტურ უფლებებში ასეთი მძიმე ფორმით ჩარევაზე, შესაძლოა რეკომენდებული იყოს ურთიერთდაპირისპირებული სამართლებრივი სიკეთეების დამატებით აწონ-დაწონვა.

1.3. ფარული საგამოძიებო მოქმედების ჩატარების წესი

1.3.1 ფარული საგამოძიებო მოქმედების ობიექტი

სსსკ-ის მე-3 მუხლის 31-ე ნაწილის თანახმად, ფარული საგამოძიებო მოქმედების ობიექტს წარმოადგენს პირი, რომლის მიმართაც ხორციელდება ფარული საგამოძიებო მოქმედება, ხოლო 143[3] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტის შესაბამისად, ფარული საგამოძიებო მოქმედების განხორციელება დასაშვებია: 1) იმ პირის მიმართ, რომელთან დაკავშირებითაც არსებობს დასაბუთებული ვარაუდი სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული დანაშაულის ჩადენასთან დაკავშირებით (დანაშაულთან პირდაპირ კავშირში მყოფი პირი); 2) იმ პირის მიმართ, რომელთან დაკავშირებითაც დასაბუთებული ვარაუდის სტანდარტით დასტურდება, რომ იღებს ან გადასცემს დანაშაულთან პირდაპირ კავშირში მყოფი პირისათვის განკუთვნილ ან მისგან მომდინარე ინფორმაციას, ან დანაშაულთან პირდაპირ კავშირში მყოფი პირი იყენებს ამ პირის საკომუნიკაციო საშუალებებს; ამდენად, სსსკ უშვებს ფარული საგამოძიებო მოქმედებების ჩატარების შესაძლებლობას როგორც „დანაშაულთან პირდაპირ კავშირში მყოფი პირის“, ასევე იმ პირის მიმართაც, რომელიც დაკავშირებულია ასეთი პირის კომუნიკაციასთან (იღებს/ან გადასცემს მას) ან საკომუნიკაციო საშუალებებთან.

როგორც უკვე აღინიშნა, „მესამე პირების“ მიმართ ღონისძიების ჩატარების შესაძლებლობა ევროპული სასამართლოს მიდგომის თანახმად, დასაშვებად არის მიჩნეული, იმ პირობით, რომ კანონმდებლობა ზუსტად, მკაფიოდ უნდა განსაზღვრავდეს ასეთ პირთა კატეგორიას, მაგალითად, ფორმულირება

„ბრალდებული ან პირი, რომელთან დაკავშირებითაც საქმის ნათელ ფაქტობრივ გარემოებებზე დაყრდნობით საგამოძიებო ორგანომ შესაძლოა დაასკვნას, რომ იღებს ან გადასცემს ბრალდებულისთვის განკუთვნილ კომუნიკაციას ან ბრალდებული იყენებს მის ტელეფონს" საკმარისად იქნა მიჩნეული ევროსასამართლოს მიერ.[713] ამ თვალსაზრისით შეიძლება ითქვას, რომ ქართული კანონმდებლობა აკმაყოფილებს „განჭვრეტადობის კრიტერიუმს" - ნათლად განსაზღვრავს თუ რა გზით შეიძლება იყოს მესამე პირი დანაშაულის შესაძლო ჩამდენ პირთან დაკავშირებული - „იღებდეს ან გადასცემდეს დანაშაულთან პირდაპირ კავშირში მყოფი პირისთვის განკუთვნილ ან მისგან მომდინარე ინფორმაციას, ან დანაშაულთან პირდაპირ კავშირში მყოფი პირი იყენებდეს ამ პირის საკომუნიკაციო საშუალებებს" (სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ბ" ქვეპუნქტი).

1.3.2 სასამართლო კონტროლი და განჩინებასთან დაკავშირებული მოთხოვნები

1.3.2.1 ნებართვის გაცემის პროცედურა

როგორც უკვე აღინიშნა, საქართველოს კანონმდებლობა ფარული საგამოძიებო მოქმედების ჩატარებაზე ნებართვის გამცემ ორგანოდ განსაზღვრავს მოსამართლეს. კერძო კომუნიკაციის ხელშეუხებლობის უფლების შეზღუდვას მხოლოდ სასამართლო კონტროლის პირობებში, კონსტიტუციური რანგი გააჩნია და ადამიანის უფლებების დაცვის უმნიშვნელოვანეს გარანტიას წარმოადგენს.

სსსკ-ის 143[3] მუხლის მე-5 ნაწილით დადგენილია მოსამართლის მიერ გადაწყვეტილების მიღების პროცედურა, კერძოდ, აღნიშნული ნორმის თანახმად, მოსამართლე საქმეს იხილავს პროკურორის შუამდგომლობისა და თანდართული მასალის სასამართლოში წარდგენიდან 24 საათის განმავლობაში ზეპირის მოსმენის გარეშე ან ზეპირი მოსმენით, დახურულ სხდომაზე, რომელშიც მონაწილეობს პროკურორი. სასამართლოს მიერ მიიღება გადაწყვეტილება ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ. განჩინება დგება 4 ეგზემპლარად, რომელთაგან ერთი რჩება სასამართლოში, ორი მიეწოდება შუამდგომლობის წარმდგენ პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს, რომელთაგან

[713] Klass and others v. Germany, [1978], ECtHR, (Ser. A.), 51.

ერთი მიეწოდება შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს (სააგენტოს) და ერთი განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს - სახელმწიფო ინსპექტორის სამსახურს (შემდგომში - ინსპექტორის სამსახური), ხოლო ინსპექტორის სამსახურის მიერ წარმოებულ სისხლის სამართლის საქმეზე - ზედამხედველ მოსამართლეს.

ფარული საგამოძიებო მოქმედება, როგორც წესი, ტარდება მოსამართლის განჩინებით, თუმცა სსსკ ასევე უშვებს მისი განხორციელების შესაძლებლობას გადაუდებელი აუცილებლობის პირობებში. ასეთ გარემოებას სსსკ-ის 143[3] მუხლის მე-6 ნაწილის საფუძველზე, წარმოადგენს ისეთი შემთხვევები, როდესაც დაყოვნებამ შეიძლება გამოიწვიოს საქმისთვის (გამოძიებისთვის) მნიშვნელოვანი ფაქტობრივი მონაცემების განადგურება ან შეუძლებელი გახადოს ამ მონაცემების მოპოვება. გადაუდებელი აუცილებლობის საფუძვლით ფარული საგამოძიებო მოქმედება ტარდება/იწყება პროკურორის მოტივირებული დადგენილებით. სსსკ-ის 143[3] მუხლის მე-6 ნაწილი განსაზღვრავს რეკვიზიტებს, რომლებიც აღინიშნება პროკურორის დადგენილებაში. დადგენილებაში მითითებული ღონისძიების დაწყების დროიდან არაუგვიანეს 24 საათისა პროკურორი მიმართავს რაიონულ სასამართლოს, რომლის სამოქმედო ტერიტორიაზეც ჩატარდა/ტარდება აღნიშნული მოქმედება, ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ. შუამდგომლობაში უნდა დასაბუთდეს როგორც სსსკ-ის 143[3] მუხლის მე-2 ნაწილით გათვალისწინებული ღონისძიების ჩატარების მატერიალური წინაპირობები, რომლებიც ექვემდებარება პროკურორის მიერ დასაბუთებას ღონისძიების სასამართლოს ნებართვის საფუძველზე ჩატარების დროს (დასაბუთებული ვარაუდის სტანდარტი, ფარული საგამოძიებო მოქმედების თანაზომიერება და ა.შ.), ისე იმ გარემოებების არსებობა, რომლებმაც განაპირობა ფარული საგამოძიებო მოქმედების მოსამართლის განჩინების გარეშე, გადაუდებლად ჩატარება/დაწყება (სსსკ-ის 143[3] მუხლის მე-6 ნაწილი). მოსამართლე პროკურორის შუამდგომლობას განიხილავს მისი წარდგენიდან არაუგვიანეს 24 საათისა, იმავე წესით, რაც გათვალისწინებულია ღონისძიების ჩასატარებლად ნებართვის გაცემის თაობაზე შუამდგომლობის განხილვისათვის. მოსამართლე ამოწმებს, შეესაბამება თუ არა ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედება სსსკ-ის 143[3] მუხლის მე-2 ნაწილით გათვალისწინებულ ღონისძიების ჩატარების საფუძვლებს, ასევე

აუცილებელი იყო თუ არა აღნიშნული ფარული საგამოძიებო მოქმედების გადაუდებლად ჩატარება/დაწყება და იღებს ერთ-ერთ შემდეგ გადაწყვეტილებას: ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ; მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის და მისი ჩატარების ვადის არაუმეტეს 48 საათამდე გაგრძელების შესახებ (აღნიშნული ვადა აითვლება პროკურორის დადგენილებაში მითითებული ფარული საგამოძიებო მოქმედების დაწყების დროიდან); ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების უკანონოდ ცნობის, მისი შეწყვეტის, შედეგების გაუქმების და მის შედეგად მოპოვებული მასალის/ინფორმაციის განადგურების შესახებ (სსსკ-ის 143[3] მუხლის მე-6 ნაწილი).

აღნიშნული გადაწყვეტილების მიღების მიზნით სსსკ-ის 143[3] მუხლის 6[1] ნაწილი მოსამართლის ანიჭებს უფლებამოსილებას, სააგენტოდან გამოითხოვოს გამოთხოვის მომენტისთვის მოპოვებული მასალის ელექტრონული ეგზემპლარი, რომელიც ნადგურდება მისი გაცნობის შემდეგ.

1.3.2.2 სასამართლოს განჩინების შინაარსი

სსსკ-ის 143[3] მუხლის მე-10 ნაწილის საფუძველზე, ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან გადაუდებელი აუცილებლობის შემთხვევაში მოსამართლის განჩინების გარეშე ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ განჩინებაში მოსამართლემ უნდა დაასაბუთოს როგორც ფარული საგამოძიებო მოქმედების ჩატარების 143[3] მუხლის მე-2 ნაწილით გათვალისწინებული საფუძვლების არსებობა, ასევე ფარული საგამოძიებო მოქმედების მოსამართლის განჩინების გარეშე, გადაუდებლად ჩატარების/დაწყების აუცილებლობა (გადაუდებელი აუცილებლობის შემთხვევაში). მოსამართლის განჩინება უნდა შეიცავდეს 143[3] მუხლის მე-10 ნაწილით გათვალისწინებულ რეკვიზიტებს.

ნიშანდობლივია, რომ სსსკ-ის 143[3] მუხლის მე-10 ნაწილში 2017 წლის 22 მარტს შევიდა ცვლილებები, რის შედეგადაც განჩინებაში მისათითებელი ზოგიერთი რეკვიზიტი სხვა ფორმით ჩამოყალიბდა, მაგალითად, თუკი მანამდე განჩინებაში აღინიშნებოდა „ვისზე ვრცელდება ფარული საგამოძიებო მოქმედება“, ცვლილებების შემდეგ ამ რეკვიზიტს დაემატა დათქმა „საჭიროების შემთხვევაში“ (143[3] მუხლის მე-10

ნაწილის „თ“ ქვეპუნქტი). აღსანიშნავია, რომ მოცემული რეკვიზიტის დანიშნულებას წარმოადგენს განჩინების ფარგლების შეძლებისდაგვარად დაკონკრეტება იმ პირთა წრის წინასწარ განსაზღვრის სახით, რომლებსაც შეიძლება შეეხოს ეს ღონისძიება. შესაბამისად, თუკი მოცემული ცვლილების განხორციელებამდე აუცილებელი იყო იმ პირების კონკრეტულად მითითება, ვისზეც გავრცელდებოდა ფარული საგამოძიებო მოქმედება, ცვლილების შედეგად ამ პირების მითითება „საჭიროებისამებრ“ ხდება. ამ კუთხით გაუგებარია, თუ რა სახის „საჭიროებაზეა“ საუბარი ამ ნორმაში ან რატომ შეიძლება არ იყოს საჭირო განჩინების ფარგლების მოცემული სახით დაზუსტება.

2017 წლის 22 მარტის კანონით ამ ნორმაში გათვალისწინებულ რეკვიზიტებს დაემატა ასევე შემდეგი მონაცემი: „სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ა“–„გ“ ქვეპუნქტებით გათვალისწინებული რომელიმე ფარული საგამოძიებო მოქმედების ჩატარების შემთხვევაში – ფარული საგამოძიებო მოქმედების ობიექტის/ობიექტების ტექნიკური იდენტიფიკატორის/იდენტიფიკატორების სულ მცირე ერთი შესაბამისი მონაცემი, რომლის/რომელთა კონტროლიც უნდა განხორციელდეს ფარული საგამოძიებო მოქმედების ფარგლებში“. სსსკ-ის მე-3 მუხლის 37-ე ნაწილის შესაბამისად, ფარული საგამოძიებო მოქმედების ობიექტის ტექნიკურ იდენტიფიკატორს წარმოადგენს „ფარული საგამოძიებო მოქმედების ობიექტის სარგებლობაში არსებული საკომუნიკაციო აღჭურვილობის მაიდენტიფიცირებელი მონაცემი (ნებისმიერი მონაცემი, რომელიც იძლევა საკომუნიკაციო აღჭურვილობის ინდივიდუალური იდენტიფიცირების საშუალებას ან ხელს უწყობს მის ინდივიდუალურ იდენტიფიცირებას (მათ შორის, ტელეფონის ნომერი, ინტერნეტპროტოკოლის მისამართი (IP-მისამართი), მობილური აღჭურვილობის საერთაშორისო იდენტიფიკატორი (IMEI), მობილურის მომხმარებლის საერთაშორისო იდენტიფიკატორი (IMSI), MAC-მისამართი და სხვა)) ან მომხმარებლის სახელი.“ აღნიშნული ცვლილება დადებითად შეიძლება შეფასდეს, ვინაიდან ემსახურება იმ საკომუნიკაციო აღჭურვილობის ზუსტად განსაზღვრას, რომელიც უნდა დაექვემდებაროს მონიტორინგს.

სსსკ-ის 143^3 მუხლის მე-11 ნაწილი განსაზღვრავს მოსამართლის მიერ განჩინებაში მისათითებელ ინფორმაციას ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემაზე ან ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობაზე უარის თქმის შემთხვევაში, კერძოდ, ასეთ დროს

განჩინებაში სხვა მონაცემებთან ერთად უნდა აღინიშნოს, რომ წარმოდგენილი შუამდგომლობით არ დასტურდება ამ მუხლის მე-2 ნაწილით გათვალისწინებული გარემოებების არსებობა და ფარული საგამოძიებო მოქმედების მოსამართლის განჩინების გარეშე, გადაუდებლად ჩატარების/დაწყების აუცილებლობა.

აღსანიშნავია, რომ განჩინებაში შესაბამისი რეკვიზიტების მითითების ვალდებულება უმნიშვნელოვანეს გარანტიას წარმოადგენს ღონისძიების ფარგლების ზუსტად განსაზღვრისა და შესაბამისად, პირადი ცხოვრების უფლებაში თანაზომიერი ჩარევის თვალსაზრისით. საგამოძიებო ორგანოს წარმომადგენელმა წინასწარ უნდა იცოდეს, თუ რას ეძებს ფარული მეთვალყურეობის დროს.[714] შესაბამისად, რაც უფრო მკაცრი მოთხოვნებია გათვალისწინებული პროკურორის შუამდგომლობისა და სასამართლოს განჩინების მიმართ, მით ნაკლებია რისკი, რომ იმაზე მეტი ინფორმაციის მოპოვება მოხდება, ვიდრე ეს კონკრეტულ დანაშაულთან და პირთან დაკავშირებით არის აუცილებელი.

მოცემულ საკითხთან დაკავშირებით საინტერესო იქნება აშშ-ის გამოცდილების განხილვა, სადაც კომუნიკაციის მონიტორინგთან დაკავშირებით სასამართლოს ბრძანების „კონკრეტულობის მოთხოვნას"[715] კონსტიტუციური რანგი გააჩნია და საფუძველს იღებს აშშ-ის კონსტიტუციის მე-4 დამატებით გათვალისწინებული დებულებიდან, რომლის მიხედვითაც „სასამართლოს განჩინებამ კონკრეტულად უნდა განსაზღვროს ჩხრეკის ობიექტის ადგილი, პირი და ამოსაღები ნივთები."[716]

კომუნიკაციის მონიტორინგთან დაკავშირებულ სასამართლოს ბრძანებაში ისევე როგორც პროკურორის შუამდგომლობაში, კანონმდებლობით განსაზღვრულ სხვა მოთხოვნებთან ერთად, მიეთითება „კომუნიკაციის ტიპი, რომლის მონიტორინგიც უნდა განხორციელდეს და ინფორმაცია კონკრეტული დანაშაულის შესახებ, რომელსაც ეხება ეს კომუნიკაცია."[717] პროკურორის შუამდგომლობასა და სასამართლოს ბრძანებაში ასევე აღინიშნება ღონისძიების ხანგრძლივობა, რომელიც

---

[714] *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No4, 2011, 1357.

[715] "Particularity Requirement".

[716] აშშ-ის კონსტიტუციის მე-4 დამატებით უზრუნველყოფილი კონსტიტუციური სტანდარტი სასამართლოს განჩინების შინაარსის კონკრეტულობის მოთხოვნასთან დაკავშირებით ვრცელდება ასევე „მოსმენების შესახებ" აქტით (Wiretap Act) განსაზღვრული კომუნიკაციის მონიტორინგის ღონისძიების ჩატარების შესახებ სასამართლოს ბრძანებაზე (Interception order).

[717] *Israel J. H., LaFave W. R.,* Criminal Procedure, Constitutional Limitations in a Nutshell, 8th Ed. 2014, 166-167.

არ უნდა იყოს 30 დღეზე მეტი და ინფორმაცია იმასთან დაკავშირებით, უნდა შეწყდეს თუ არა ავტომატურად ღონისძიება, როდესაც პირველივე ჯერზე მოხდება ბრძანებაში აღწერილი ინფორმაციის მოპოვება.“[718]

როგორც სამეცნიერო ლიტერატურაშია აღნიშნული, კანონმდებლობის მოთხოვნა მოსაპოვებელი „კომუნიკაციის ტიპის“ სასამართლოს ბრძანებაში განსაზღვრასთან დაკავშირებით ერთ-ერთ ფუნდამენტურ დებულებას წარმოადგენს, ვინაიდან „ემსახურება ორ უაღრესად მნიშვნელოვან მიზანს - უთითებს ღონისძიების განმახორციელებელ სახელმწიფო მოხელეს, სად ეძებოს მოთხოვნილი მტკიცებულება და მიანიშნებს, როდის შეწყვიტოს ღონისძიება, როდესაც ბრძანებაში მითითებული მტკიცებულება მოპოვებულია.“[719]

აშშ-ის სასამართლო პრაქტიკაში განხილულ საქმეში Berger v. New York, ფარულ მეთვალყურეობასთან დაკავშირებული ნიუ-იორკის შტატის კანონმდებლობის არაკონსტიტუციურად ცნობის საფუძვლებს შორის ერთ-ერთს სწორედ „კონკრეტულობის“ კონსტიტუციური სტანდარტის დარღვევა წარმოადგენდა.[720] აშშ-ის უზენაესმა სასამართლომ დაადგინა, რომ ნიუ-იორკის შტატის კანონმდებლობა ძალიან მწირ მოთხოვნებს ითვალისწინებდა „მოსაპოვებელი კომუნიკაციის კონკრეტულად განსაზღვრასთან დაკავშირებით, კერძოდ, სასამართლოს ბრძანებაში საკმარისი იყო მხოლოდ იმ პირის განსაზღვრა, რომლის საუბრის მიყურადება და ჩაწერაც უნდა განხორციელებულიყო.“[721] აშშ-ის უზენაესმა სასამართლომ მიიჩნია, რომ ეს დებულება არ იყო საკმარისი, ვინაიდან „კონკრეტულობის მოთხოვნას“ კომუნიკაციის მიყურადებასთან დაკავშირებულ საქმეებში განსაკუთრებული დატვირთვა გააჩნია, რადგან ასეთ ღონისძიებას თან ახლავს პირადი ცხოვრების უფლებაში მომეტებული ხარისხით ჩარევა.“[722]

მიუხედავად აღნიშნულისა, როგორც აღმოჩნდა, შემდგომში სასამართლო პრაქტიკა სხვა მიმართულებით განვითარდა და ბერგერის საქმეში ჩამოყალიბებულ ამ სტანდარტს მიეცა ინტერპრეტაცია, რომ „მოსაპოვებელი კომუნიკაციის ტიპის

---

[718] იქვე.

[719] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 269.

[720] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 268-269, იხ. ციტირება: Berger v. New York, 388 U.S. 41 (1967); *Slobogin C.,* Privacy at Risk, The New Government Surveillance and The Fourth Amendment, Chicago, 2007, 15.

[721] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 268-269.

[722] იქვე.

დაკონკრეტება შესაძლებელია სასამართლოს ბრძანებაში იმ კონკრეტული დანაშაულის შესახებ ინფორმაციის მითითებით, რომელთან დაკავშირებითაც ხორციელდება ღონისძიება, მოსალოდნელ კომუნიკაციასთან დაკავშირებით დამატებითი დეტალების განსაზღვრის გარეშე.“[723] აღნიშნულის გამამართლებლად დასახელდა ის არგუმენტი, რომ რადგან კომუნიკაცია ჯერ არ განხორციელებულა, მასთან დაკავშირებით წინასწარი პროგნოზის გაკეთება შეუძლებელია.[724]

სამეცნიერო ლიტერატურაში გამოთქმული შეხედულების თანახმად, სასამართლოს ბრძანების „კონკრეტულობის“ კრიტერიუმის უზრუნველყოფის საკითხი განსაკუთრებით პრობლემურია, როდესაც საქმე ეხება ინტერნეტკომუნიკაციას.[725] ინტერნეტსერვისების მიმწოდებლები ინახავენ განუსაზღვრელად დიდი რაოდენობის ინფორმაციას, რის შედეგადაც მოსაპოვებელი მონაცემების მოცულობას განსაკუთრებული მნიშვნელობა ენიჭება. აღნიშნულის საილუსტრაციოდ მოყვანილია ერთ-ერთი საქმე აშშ-ის სამართალდამცავი ორგანოების პრაქტიკიდან, სადაც პოლიციის მიერ გამოქვეყნდა დოკუმენტი, რომელიც შეიცავდა Facebook-სგან გამოთხოვილ ინფორმაციას[726]. აღნიშნული ინფორმაცია, მიმოწერების, მეგობრების სიისა და ფოტოების გარდა, ასევე მოიცავდა Facebook-ის სოციალურ ქსელში ბრალდებულის მიერ დაფიქსირებულ ყველა კომენტარს, მის მიერ წაშლილ ყველა ფოტოს, წაშლილი Facebook მეგობრების ჩამონათვალს, აგრეთვე Facebook-ის გამოყენების დროს მის მიერ განხორციელებული თითოეული აქტივობის ჩანაწერს, თითოეულ გვერდზე სტუმრობის ისტორიას, ყოველი ფოტოს ნახვისა და ინტერნეტ რესურსზე წვდომის ამონაწერს.[727] სამეცნიერო ლიტერატურაში გამოხატული პოზიციით, „სასამართლოს ერთი ბრძანება საკმარისი აღმოჩნდა იმისათვის, რომ რუტინული პრაქტიკიდან გამომდინარე, პოლიციას მოეპოვებინა ყველაფერი, კომუნიკაციის კონკრეტულად განსაზღვრის მოთხოვნის მხედველობაში მიღების გარეშე.“[728]

[723] იქვე, 269.
[724] იქვე.
[725] *Kerr O. S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 402.
[726] იქვე. 392-393.
[727] იქვე.
[728] იქვე. 402.

ინტერნეტკომუნიკაციებთან მიმართებით კონკრეტულობის კონსტიტუციური დოქტრინის დაცვის პრობლემატიკა აშშ-ის სასამართლო პრაქტიკაშიც არ დარჩენილა ყურადღების მიღმა. ერთ-ერთ სისხლის სამართლის საქმეზე მაგისტრატმა მოსამართლემ უარი განაცხადა ელექტრონული ფოსტის ანგარიშის გასაჩხრეკად ნებართვის გაცემაზე იმ საფუძვლით, რომ „წარდგენილი შუამდგომლობა არ იყო საკმარისად კონკრეტული.“[729] შუამდგომლობით მოთხოვნილი იყო გარკვეულ ანგარიშთან დაკავშირებული ყველა ჩანაწერისა და ინფორმაციის მოპოვება, მათ შორის, „წაშლილი კომუნიკაციები, ელექტრონული ფოსტის ან ფაქსის ანგარიშის იდენტიფიკაციასთან დაკავშირებული ყველა მონაცემი, მომხმარებლის მიერ შენახული სხვა მონაცემები, მათ შორის, კონტაქტების სია, კალენდრის მონაცემები, ფოტოები, ფაილები“[730]. მაგისტრატმა მოსამართლემ მიიჩნია, რომ წარდგენილი მოთხოვნა იყო „ზედმეტად განუსაზღვრელი და ზოგადი“, რათა დაეკმაყოფილებინა კონსტიტუციის მე-4 დამატებით უზრუნველყოფილი სტანდარტი[731]. სასამართლომ ასევე განმარტა, რომ ელექტრონული ფოსტის ანგარიშთან დაკავშირებული მთელი შინაარსობრივი ინფორმაციის მოპოვებასთან დაკავშირებული სასამართლოს ბრძანება მსგავსია „ფოსტის ოფისისთვის პირის მიერ როდესმე გაგზავნილი და მიღებული წერილების ასლების მოთხოვნის, რომელიც შესაძლებლობას მისცემდა სახელმწიფო ხელისუფლების წარმომადგენელს, გაეხსნა და წაეკითხა პირის მიერ ოდესმე მიღებული/გაგზავნილი ყველა წერილი, რათა დაედგინა მათი შესაძლო კავშირი დანაშაულთან“[732]. იქედან გამომდინარე, რომ კონსტიტუციის მე-4 დამატებით ასეთი ბრძანების გაცემა არ იყო ნებადართული, ასევე ვერ იქნებოდა დაშვებული ელექტრონულ ფოსტასთან მიმართებით ანალოგიურად ზოგადი ნებართვის გაცემის შესაძლებლობაც, მხოლოდ იმიტომ რომ მოთხოვნილი ინფორმაცია მატერიალურის ნაცვლად, ელექტრონული სახით არსებობდა.“[733]

საბოლოო ჯამში, შეიძლება ითქვას, რომ განჩინების შინაარსის მაქსიმალურად დაკონკრეტებას ცენტრალური მნიშვნელობა აქვს მოსაპოვებელი ინფორმაციის შეზღუდვისა და თანაზომიერების პრინციპის დაცვის კუთხით; ღონისძიების

[729] იქვე. 403-404.
[730] იქვე.
[731] იქვე.
[732] იქვე.
[733] იქვე.

ფარგლების ex ante შეზღუდვა შეიძლება ასევე იქცეს არსებით ხელშემწყობ ფაქტორად სსსკ-ის 143[7] მუხლით უზრუნველყოფილი ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნის პრაქტიკაში ეფექტიანად რეალიზების კუთხით. როდესაც საუბარია ინტერნეტკომუნიკაციაზე, ინტერნეტ სივრცეში კერძო პირებთან დაკავშირებით შეუზღუდავი მოცულობის ინფორმაციის არსებობის გამო, მოსაპოვებელი მონაცემების ფარგლების დავიწროება კიდევ უფრო აქტუალური ხდება. სსსკ სასამართლო განჩინების რეკვიზიტებთან დაკავშირებით არ ადგენს იმდენად მკაცრ მოთხოვნებს, რომ განჩინების გაცემის ეტაპზევე მოხდეს ღონისძიების ფარგლების შეძლებისდაგვარად მაქსიმალურად დაკონკრეტება, მაგალითად, განჩინების რეკვიზიტად არ განსაზღვრავს მოსაპოვებელი ინფორმაციის ტიპს; არსებული რეგულაციით აქცენტი უფრო მეტად გაკეთებულია ღონისძიების აღსრულების ეტაპზე მისი ფარგლების შეზღუდვაზე, რაც მინიმუმამდე დაყვანის მოთხოვნის სახით არის გათვალისწინებული (სსსკ-ის 143[7] მუხლი). თუმცა მხედველობაში უნდა იქნეს მიღებული სსსკ-ის 143[2] მუხლის მე-5 ნაწილი, რომლის თანახმადაც „ფარული საგამოძიებო მოქმედების ჩატარების ფარგლები (ინტენსივობა) ფარული საგამოძიებო მოქმედების ლეგიტიმური მიზნის პროპორციული უნდა იყოს.“ ამდენად, ეს ზოგადი მოთხოვნა, რომელიც თავის მხრივ, თანაზომიერების ტესტის ერთ-ერთ გამოხატულებას წარმოადგენს, გათვალისწინებული უნდა იქნეს როგორც შუამდგომლობის/სასამართლოს განჩინების ფარგლების განსაზღვრის, ასევე ღონისძიების აღსრულების პროცესში მისი ინტენსივობის შეზღუდვის თვალსაზრისით. საყურადღებოა ასევე სსსკ-ის 143[3] მუხლის მე-10 ნაწილის „ვ“ ქვეპუნქტი, რომელიც სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ ღონისძიებებთან დაკავშირებით ადგენს სასამართლოს განჩინებაში ობიექტის ტექნიკური იდენტიფიკატორის/იდენტიფიკატორების სულ მცირე ერთი შესაბამისი მონაცემის მითითების მოთხოვნას. ამ მახასიათებლით შესაძლებელია გამოყენებული საკომუნიკაციო აღჭურვილობის ან მომხმარებლის სახელის მიხედვით ღონისძიების ფარგლების დაკონკრეტება (სსსკ-ის მე-3 მუხლის 37-ე ნაწილი). ამდენად, ამ დებულების პრაქტიკაში გამოყენება უნდა მოხდეს იმგვარად, რომ შესაძლებლობის ფარგლებში განჩინებაში მაქსიმალურად დაკონკრეტდეს ობიექტის ტექნიკური იდენტიფიკატორი/იდენტიფიკატორები. ამასთან, ინტერნეტკომუნიკაციებთან

მიმართებით, სასამართლოს განჩინების შინაარსთან დაკავშირებულ ასპექტებზე კვლევის მომდევნო ქვეთავებშიც იქნება ყურადღება გამახვილებული.

1.3.2.3 გარემოებები, რომლებმაც შესაძლოა ხელი შეუშალოს სასამართლო კონტროლის ეფექტიანობას

როგორც უკვე აღინიშნა, სასამართლო კონტროლი თვითნებობის საწინააღმდეგო მნიშვნელოვანი გარანტიაა ფარული მეთვალყურეობის განხორციელების ყველა ეტაპზე[734], თუმცა საერთაშორისო სტანდარტის მიხედვით, სასამართლოს მონაწილეობა არ მიიჩნევა როგორც „უნივერსალური გამოსავალი.“[735] როგორც გაეროს სპეციალური მომხსენებელი აღნიშნავს, „ზოგიერთ ქვეყანაში უშიშროების ან დანაშაულის გამოძიების სფეროში სასამართლოს მიერ ფარული მეთვალყურეობის ღონისძიების ჩატარებაზე ნებართვის გაცემა ან შემდგომი გადამოწმება იმდენად ფორმალურ ხასიათს ატარებს, რომ ფაქტობრივად „ბეჭდის დასმის“ ფუნქციამდეა დაყვანილი.“[736]. ევროპული სასამართლოს შეხედულების თანახმად, მხოლოდ სასამართლოს ზედამხედველობა ვერ ჩაითვლება საკმარის დაცვის მექანიზმად ადამიანის უფლებების დაცვის კუთხით, თუკი მას არ გააჩნია საკმარისი კომპეტენციის ფარგლები ზედამხედველობის პროცესში.[737] ამიტომ ევროპულმა სასამართლომ შეიძლება დაადგინოს „პირადი ცხოვრების პატივისცემის უფლების დარღვევა იმ შემთხვევაშიც, თუ, ფორმალურად, ეროვნული კანონმდებლობა ითვალისწინებს დამოუკიდებელი და მიუკერძოებელი ორგანოს მიერ კომუნიკაციის მონიტორინგის ბრძანების გაცემის მოთხოვნას, მაგრამ პრაქტიკაში ხსენებული ორგანო მხოლოდ ფორმალურ ფუნქციას ასრულებს და, არსებითად, ადეკვატური გარანტიების გათვალისწინებით, არ აფასებს ხელისუფლების აღმასრულებელი ორგანოების მხრიდან უფლებაში ჩარევის მართლზომიერების საკითხს.“[738]

---

[734] Šantare and Labaznikovs v. Latvia, [2016], ECtHR, 54.

[735] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13, (ბმული იხ. მე-19 გვერდზე).

[736] იქვე.

[737] Iordachi and others v. Moldova, [2009], ECtHR, 47.

[738] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, 206, <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [18.06.2020].

საერთაშორისო დონეზე და სამეცნიერო ლიტერატურაში სასამართლო კონტროლის ეფექტიანობის საკითხი დიდი აქტუალურობით სარგებლობს. სამეცნიერო ლიტერატურაში ხშირად გაჟღერებულია კრიტიკული შეხედულებები სასამართლო კონტროლის არაეფექტიანობის შესახებ, მაგალითად, გამოთქმულია მოსაზრება გერმანიის სამოსამართლო პრაქტიკაში სასამართლო კონტროლის არაეფექტურობასთან დაკავშირებით;[739] ამ თვალსაზრისით აღნიშნულია, რომ გერმანიაში, ისევე როგორც აშშ-ში, კომუნიკაციის მონიტორინგის შესახებ შუამდგომლობების გაცემაზე უარის თქმის შესახებ გადაწყვეტილებას მოსამართლეები თითქმის არ იღებენ.[740] იურიდიულ ლიტერატურაში და საერთაშორისო დოკუმენტებში დასახელებულია ასევე ის ძირითადი ფაქტორები, რომლებმაც შესაძლოა ხელი შეუშალოს სასამართლო კონტროლის ეფექტიანობას და გამოთქმულია შესაბამისი რეკომენდაციებიც სასამართლო ზედამხედველობის ქმედითობის გაზრდის მიზნით. ბუნებრივია, საერთაშორისო დონეზე გამოთქმული კრიტიკა და შესაბამისი რეკომენდაციები რელევანტურია ქართული გამოცდილებისთვისაც.

მოსამართლეთა გადატვირთულობა - ვენეციის კომისია პოლონეთთან დაკავშირებულ ანგარიშში, რომელიც ეთმობა ფარული მეთვალყურეობის მარეგულირებელი კანონმდებლობის შეფასებას, გამოყოფს ორ ფაქტორს, რომელსაც შეუძლია სასამართლო კონტროლის მექანიზმის ეფექტიანობისთვის ხელის შეშლა[741]. ასეთ გარემოებად, პირველ რიგში, განხილულია მოსამართლეთა გადატვირთულობა[742]. კომისია განმარტავს, რომ ფარულ საგამოძიებო მოქმედებებზე სასამართლო კონტროლი უნდა იქნეს აღქმული მოსამართლის ძირითადი საქმიანობის ნაწილად და სამოსამართლო სტატისტიკის შემადგენლობაში უნდა

[739] *Schwartz, P.M*, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, Hastings Law Journals, Vol.54, 793; აღნიშნულ საკითხთან დაკავშრებით იხ. ასევე *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 146-150.

[740] *Schwartz, P.M*, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, Hastings Law Journals, Vol.54, 793.

[741] European Commission for Democracy Through Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 24, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].

[742] იქვე.

შევიდეს[743]. ამასთან, მოსამართლეს დახმარება უნდა გაუწიოს შესაბამისმა კვალიფიციურმა პერსონალმა, რომელიც ერკვევა თანამედროვე ტექნოლოგიებსა და ფარულ მეთვალყურეობასთან დაკავშირებულ პრაქტიკულ საკითხებში[744]. სხვა შემთხვევაში, ადგილი ექნება სასამართლოს მხრიდან აღნიშნული საკითხისადმი მინიმალური ძალისხმევის გამოჩენას და მხოლოდ „ფორმალურ განხილვას.“[745]

პროფესორი ალბრეხტის განმარტებით, როგორც სამეცნიერო კვლევებმა ცხადყო, ტელესაკომუნიკაციო საშუალებების მიყურადება-თვალთვალის შუამდგომლობები მხოლოდ გამონაკლის შემთხვევებში არ კმაყოფილდება[746]. ეს ნაწილობრივ აიხსნება მოსამართლეთა გადატვირთულობითა და ბრძანების გაცემის წინაპირობების შემოწმებისათვის საკმარისი დროის უქონლობით[747]. შესაბამისად, ეფექტური სასამართლო კონტროლისთვის მნიშვნელოვანია სასამართლოს შესაბამისი აღჭურვა როგორც პერსონალურად, ისე საგნობრივად.[748]

არასაკმარისი კომპეტენცია კომუნიკაციის მონიტორინგთან დაკავშირებული ტექნიკური საკითხების თაობაზე - მოსამართლეთა მხრიდან ფარული მეთვალყურეობის საქმეებთან დაკავშირებით კომპეტენციის ნაკლებობა სამეცნიერო ლიტერატურაში ასევე განიხილება სასამართლო ზედამხედველობის ეფექტიანობის ხელშემშლელ ერთ-ერთ გარემოებად.[749] იქედან გამომდინარე, რომ კომუნიკაციის მონიტორინგი ტექნიკური თვალსაზრისით თანდათან უფრო კომპლექსური ხდება, მოსამართლეები უფრო და უფრო ნაკლები ცოდნით არიან აღჭურვილი ადეკვატური ზედამხედველობის განსახორციელებლად საჭირო საკითხებთან დაკავშირებით.[750]

---

[743] იქვე.

[744] იქვე.

[745] იქვე. მოსამართლეთა დატვირთულ სამუშაო რეჟიმთან და დროის უქონლობასთან, როგორც სასამართლო კონტროლის ეფექტიანობის ხელშემშლელ ერთ-ერთ გარემოებასთან დაკავშირებით იხ. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 153.

[746] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 38, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[747] იქვე.

[748] იქვე.

[749] *McIntyre TJ,* Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective, წიგნში: Judges as Guardians of Constitutionalism and Human Rights, Ed. by *Scheinin M., Krunke H., Aksenova M. (eds.),* 2016, 139.

[750] იქვე.

მოხსენებაში „პირადი ცხოვრების უფლება ციფრულ ეპოქაში“ გაეროს სპეციალური მომხსენებელი აღნიშნავს, რომ „დამოუკიდებელი კონსულტაციის გამოყენება“ ფარული მეთვალყურეობის ღონისძიებების განხორციელების საკითხის სათანადოდ შეფასების მიზნით, დადებითად არის შეფასებული.[751] როდესაც საქმე ეხება ტექნიკური თვალსაზრისით ისეთ კომპლექსურ და რთულ ღონისძიებას, როგორიცაა კომპიუტერულ სისტემაში ფარული შეღწევა (მაგ. „დავირუსების“ გზით), ასეთი „დამოუკიდებელი კონსულტაციის“ მაგალითის სახით ერთ-ერთი წამყვანი ადამიანის უფლებათა დამცველი ორგანიზაცია ასახელებს ტექნიკურ საკითხებში სპეციალისტს.[752] აღნიშნული ორგანიზაციის შეხედულებით, ვინაიდან მოსამართლეები ნაკლებად ერკვევიან ამ ღონისძიებასთან დაკავშირებულ ტექნიკურ ასპექტებში, შესაბამისი სპეციალისტის დახმარებას არსებითი მნიშვნელობა ენიჭება მოთხოვნილი ღონისძიების თანაზომიერების საკითხის სათანადოდ გადაწყვეტის კუთხით.[753]

მოსამართლის მიერ შუამდგომლობის ზედაპირული დამუშავება - სამეცნიერო ლიტერატურაში სასამართლო კონტროლის ერთ-ერთ ხარვეზად მოსამართლის მიერ შუამდგომლობის ზედაპირული დამუშავება სახელდება.[754] გამოთქმული მოსაზრების თანახმად, საგამოძიებო ორგანოების მხრიდან ცალმხრივად მიღებული ინფორმაციის საფუძველზე, რომელსაც უკვე გადაწყვეტილების ფორმა აქვს მიცემული, მოსამართლე შესაძლოა „მოექცეს ცდუნების ქვეშ“ და ბრძანების გაცემის წინაპირობები ზედაპირულად შეამოწმოს[755]. აღსანიშნავია, რომ ეს საფრთხე კვლევითაც იქნა დადასტურებული, კერძოდ, ბილეფელდის უნივერსიტეტთან არსებული სამუშაო ჯგუფის მიერ ბაკესის და გუზის ხელმძღვანელობით ჩატარებული კვლევით, რომელიც დასრულდა 2003 წელს და რომლის ფარგლებშიც შესწავლილ იქნა ტელეკომუნიკაციის მიყურადების 554 ღონისძიება 1996 წლიდან 1998

---

[751] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13 (ბმული იხ. მე-19 გვერდზე).

[752] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 26-29, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020].

[753] იქვე.

[754] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 156-167.

[755] იქვე.

წლამდე პერიოდის სისხლის სამართლის 173 საქმიდან[756]. ამ კვლევის მიხედვით, რომლის მიხედვითაც სატელეფონო საუბრის ფარული მიყურადების შესახებ პროკურორის შუამდგომლობა თითქმის ყველა შემთხვევაში დაკმაყოფილდა - 307 შუამდგომლობიდან მხოლოდ ერთი მათგანი არ იქნა დაკმაყოფილებული, ამავდროულად, 90%-ზე მეტ შემთხვევებში პროკურატურის შუამდგომლობა სიტყვა-სიტყვით შეესაბამებოდა მოსამართლის ბრძანების ტექსტს.[757]

შეჯიბრებითი პროცესის ელემენტების ნაკლებობა - პოლონეთის კანონმდებლობასთან დაკავშირებულ ზემოთაღნიშნულ ანგარიშში სასამართლო კონტროლის ეფექტიანობისთვის ხელისშემშლელ მეორე ფაქტორად ვენეციის კომისია ფარულ მეთვალყურეობასთან დაკავშირებულ საქმეებში შეჯიბრებითი პროცესის ელემენტების ნაკლებობას მიიჩნევს[758]. კომისიის განმარტებით, როგორც, პოლონეთის კანონმდებლობიდან ჩანს, სასამართლოები ფარულ საგამოძიებო მოქმედებებთან დაკავშირებულ შუამდგომლობებს იხილავენ მხოლოდ ერთი მხარის - საგამოძიებო ორგანოს მონაწილეობით[759]. ასეთი პრაქტიკა გასაგებია, ვინაიდან ფარული საგამოძიებო მოქმედებების თავისებურება და ლოგიკა სწორედ იმაში მდგომარეობს, რომ მონიტორინგის მთელი პროცესი, ისევე როგორც საკითხის განხილვის პროცედურა, მიმდინარეობს მისი ადრესატისგან დაფარულად[760]. თუმცა ნამდვილი შეჯიბრებითი პროცესის არარსებობის პირობებში, მოსამართლეები საგამოძიებო ორგანოს პოზიციის მიმართ ნაკლებად კრიტიკულ დამოკიდებულებას ავლენენ[761]. მეტიც, თუკი მოსამართლე უარს იტყვის შუამდგომლობის დაკმაყოფილებაზე, იარსებობს ამ გადაწყვეტილების გასაჩივრების რისკი, მაშინ როცა აღნიშნულს ადგილი არ ექნება შუამდგომლობის დაკმაყოფილების შემთხვევაში[762]. ასეთ პირობებში ფარულ საგამოძიებო მოქმედებებზე წინასწარი სასამართლო კონტროლი შეიძლება მხოლოდ ფორმალობად იქცეს[763]. მეორე მხრივ, პროკურორის მონაწილეობას

---

[756] იქვე, გვ. 146-148.
[757] იქვე, გვ. 156-157.
[758] European Commission for Democracy Throgh Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 24-25, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].
[759] იქვე.
[760] იქვე.
[761] იქვე.
[762] იქვე.
[763] იქვე.

ნებართვის გაცემის პროცედურაში, რომელიც გათვალისწინებული იყო პოლონეთის კანონმდებლობით, კომისია დადებითად აფასებს, თუმცა პოლონეთის სისტემისთვის დამახასიათებელი პოლიციისა და პროკურატურის ორგანოებს შორის „ახლო ურთიერთობიდან“ გამომდინარე, არ მიიჩნევს საკმარის პროცედურულ გარანტიად.[764] ვენეციის კომისიის განმარტებით, წინასწარი სასამართლო კონტროლის მექანიზმის ეფექტიანობის გაზრდის მიზნით, შესაძლებელია ახალი სუბიექტის - „პირადი ცხოვრების დამცველის“[765] შემოღება, რომელიც იქნება დამოუკიდებელი პირი, იურიდიული პროფესიის წარმომადგენელი, აღჭურვილი საჭირო კვალიფიკაციით ტექნიკურ საკითხებთან დაკავშირებით და საიდუმლო ინფორმაციაზე დაშვების დონით და არ იქნება ინსტიტუციურად დაკავშირებული პოლიციასთან ან პროკურატურასთან[766]. ასეთი „ადვოკატის“ ფუნქცია უნდა იყოს ფარული საგამოძიებო მოქმედების ადრესატის ინტერესების დაცვა.[767]

როგორც ვხედავთ, საერთაშორისო დონეზე აქტიურად არის მხარდაჭერილი ნებართვის გაცემის ეტაპზე სასამართლო კონტროლის ეფექტიანობის გაზრდის საკითხი. ამ თვალსაზრისით ძირითად რეკომენდაციად სახელდება სასამართლოს აღჭურვა შესაბამისი კვალიფიკაციის (ტექნიკურ და სამართლებრივ საკითხებში) პერსონალით, მოსამართლეთა მიერ ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული ფუნქციის ძირითად სამოსამართლო საქმიანობის ნაწილად მიჩნევა, რაც შესაბამის სტატისტიკაში უნდა აისახოს, შეჯიბრებითი პროცესის ელემენტების გაძლიერება. ამ კუთხით მნიშვნელოვან საერთაშორისო დოკუმენტებში, როგორიცაა ვენეციის კომისიის, გაეროს სპეციალური მომხსენებლის თუ ევროპის საბჭოს ადამიანის უფლებების კომისრის ანგარიშები, უკვე არაერთხელ გაჟღერდა „სპეციალური ადვოკატის“ პოზიციის შემოტანის იდეა. მართალია საერთაშორისო დონეზე ეს შეხედულება ჯერჯერობით სათანადოდ არ არის მომწიფებული და ნაკლებად არის ჩამოყალიბებული კონკრეტული საკითხები „სპეციალური ადვოკატის“ პოზიციის ირგვლივ, მაგრამ საერთაშორისო დოკუმენტებში ამ თემის აქტიურად განხილვის ფონზე, რეალურია, რომ სამომავლოდ მას უფრო მეტი

[764] იქვე.
[765] იქვე. 25. ანგარიშში მითითებულია „Privacy Advocate”.
[766] იქვე.
[767] იქვე.

დატვირთვა მიეცეს და აქტიურად იქნეს გათვალისწინებული ევროპული ქვეყნების ეროვნულ სამართალში. აქედან გამომდინარე, იმის გათვალისწინებით, თუ რა განვითარება ექნება ამ ინსტიტუტს საერთაშორისო პრაქტიკაში, სავსებით შესაძლებელია ვისაუბროთ მისი ქართულ კანონმდებლობაში გათვალისწინების პერსპექტივაზეც; ფარული საგამოძიებო მოქმედების განხორციელებაზე ნებართვის განხილვის დახურულ პროცედურაში ისეთი სუბიექტის შემოყვანა, რომელიც გარკვეულწილად დააბალანსებს დაცვის მხარის მონაწილეობის შეუძლებლობასთან დაკავშირებულ გამოწვევებს, მხარეთა თანასწორობის გაუმჯობესების და შეჯიბრებითი პროცესის ელემენტების გაძლიერების თვალსაზრისით დადებით ნოვაციად შეიძლება ჩაითვალოს; მითუმეტეს რომ საერთაშორისო პრაქტიკის ანალიზმაც ცხადყო ფარულ საგამოძიებო მოქმედებებთან დაკავშირებულ საქმეებში სასამართლო კონტროლთან დაკავშირებული მნიშვნელოვანი ხარვეზები; ამ პირობებში სისხლის სამართლის პროცესში ასეთი ახალი სუბიექტის შემოყვანა დაცვის მხარის სასარგებლოდ, ვფიქრობთ, ერთგვარად „გამოაცოცხლებს“ ხშირ შემთხვევაში ფორმალობად ქცეულ ნებართვის განხილვის პროცედურას. თუმცა, როგორც უკვე აღინიშნა, საინტერესო და მნიშვნელოვანი იქნება, თუ როგორ განვითარდება სამომავლოდ საერთაშორისო პრაქტიკაში მიდგომა ამ ინსტიტუტთან დაკავშირებით.

1.3.3 ფარული საგამოძიებო მოქმედების ხანგრძლივობა

სსსკ-ის 143[3] მუხლის მე-12 ნაწილი განსაზღვრავს ფარული საგამოძიებო მოქმედების ხანგრძლივობას, კერძოდ, ფარული საგამოძიებო მოქმედების ჩატარების შესახებ მოსამართლის განჩინება გაიცემა იმ ვადით, რომელიც საჭიროა გამოძიების მიზნის მისაღწევად, მაგრამ არაუმეტეს 1 თვისა. მოცემული ვადა არის მაქსიმალური, რომელსაც სსსკ ღონისძიების თავდაპირველ ეტაპზე ითვალისწინებს, თუმცა, ბუნებრივია, ეს არ ნიშნავს, რომ ყველა შემთხვევაში ღონისძიების თავდაპირველი ვადა 1 თვით უნდა განისაზღვროს - განჩინება უნდა გაიცეს იმ ვადით, რაც საქმის კონკრეტული გარემოებების გათვალისწინებით აუცილებელია გამოძიების მიზნის მისაღწევად (1 თვიანი ვადის ფარგლებში). როგორც უკვე აღინიშნა, ევროპული სასამართლოს პრაქტიკის მიხედვით, ღონისძიების ვადის განსაზღვრა დამოკიდებულია გამოძიების ხანგრძლივობასა და კომპლექსურობაზე. ვადის

შერჩევისას დანაშაულებრივი ქმედების მასშტაბი და მასში მონაწილე პირთა რაოდენობა უნდა იქნეს გათვალისწინებული.[768]

აღსანიშნავია, რომ ღონისძიების ჩატარება შესაძლოა თავდაპირველ ეტაპზე კონკრეტული ვადის თანაზომიერი იყოს, თუმცა შემდგომში მისი გაგრძელება აღარ გახდეს აუცილებელი, რადგან გამოძიების ორგანოებმა უკვე მოიპოვეს საჭირო ინფორმაცია ან ღონისძიების მიმდინარეობა ცხადყოფს, რომ გამოძიებისათვის საინტერესო ინფორმაციის მოპოვება კონკრეტული ღონისძიების შედეგად შეუძლებელია. იმ შემთხვევაში, როდესაც არსებობს სსსკ-ის 143[6] მუხლის მე-2 ნაწილით გათვალისწინებული ღონისძიების შეწყვეტის შესაბამისი საფუძველი, მაგალითად, შესრულდება ფარული საგამოძიებო მოქმედების შესახებ განჩინებით გათვალისწინებული კონკრეტული ამოცანა (სსსკ-ის 143[6] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი), ან „დადგინდება გარემოებები, რომლებიც ადასტურებს, რომ ფარული საგამოძიებო მოქმედების შესახებ განჩინებით გათვალისწინებული კონკრეტული ამოცანის შესრულება ობიექტურად შეუძლებელია/ფარული საგამოძიებო მოქმედების ჩატარებას გამოძიებისთვის არსებითი მნიშვნელობა აღარ აქვს“ (სსსკ-ის 143[6] მუხლის მე-2 ნაწილის „ბ“ ქვეპუნქტი), ღონისძიება უნდა შეწყდეს, მიუხედავად იმისა, გასულია თუ არა სასამართლოს ნებართვით დადგენილი ვადა. ამავდროულად, ვინაიდან აღნიშნული საფუძვლებით ღონისძიების შეწყვეტის უფლებამოსილება გააჩნია პროკურორს, მასვე ეკისრება ვალდებულება, ზედამხედველობა გაუწიოს სსსკ-ის 143[6] მუხლის მე-2 ნაწილით გათვალისწინებული მოთხოვნების დაცვას.

სსსკ-ის 143[3] მუხლის მე-12 ნაწილით დადგენილი ერთთვიანი ვადის გასვლის შემდეგ სსსკ-ის უშვებს მისი გაგრძელების შესაძლებლობას პროკურორის მოტივირებული შუამდგომლობის საფუძველზე, სასამართლოს განჩინებით, XVI[1] თავით დადგენილი წესით, არა უმეტეს 2 თვისა. ასეთ შემთხვევაში პროკურორმა შუამდგომლობაში უნდა აღნიშნოს „დაწყებული ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მონაცემების შესახებ და ასევე მიუთითოს, რის გამო ვერ მოხერხდა გამოძიებისათვის საკმარისი ინფორმაციის მოპოვება“ (სსსკ-ის 143[3] მუხლის მე-12 ნაწილი). ამავდროულად, ვინაიდან ვადის გაგრძელება ხდება XVI[1] თავით დადგენილი წესით, ამ შემთხვევაშიც უნდა მოხდეს ყველა იმ გარემოების დასაბუთება

[768] Kennedy v. United Kingdom, [2010] ECtHR, 161.

პროკურორის შუამდგომლობასა და სასამართლოს განჩინებაში, რომლის დადასტურებაც ხდება ღონისძიების დასაწყებად ნებართვის გაცემის სტადიაზე.

ვადის გაგრძელება შესაძლებელია კიდევ ერთხელ, არაუმეტეს 3 თვისა, საქართველოს გენერალური პროკურორის შუამდგომლობის საფუძველზე. ფარული საგამოძიებო მოქმედების ჩატარების ვადის შემდგომი გაგრძელება დაუშვებელია (143[3] მუხლის მე-12 ნაწილი).

საქართველოს კანონმდებლობით ფარული საგამოძიებო მოქმედების ვადასთან დაკავშირებით იურიდიულ ლიტერატურაში სავსებით სამართლიანად გამოთქმულია მოსაზრება, რომ 143[3] მუხლის მე-12 ნაწილი არაერთგვაროვანი ინტერპრეტაციის საშუალებას იძლევა, კერძოდ, ნორმის ვიწრო განმარტების შედეგად ფარული საგამოძიებო მოქმედების მაქსიმალური ვადა მისი გაგრძელების ვადის ჩათვლით შესაძლოა იყოს 3 თვე, ხოლო ფართო განმარტებით - 6 თვე.[769] აღნიშნული განპირობებულია იმით, რომ სსსკ-ის 143[3] მუხლის მე-12 ნაწილი ვადის გაგრძელების საკითხის რეგულირებისას ითვალისწინებს ფორმულირებებს „შესაძლებელია გაგრძელდეს არაუმეტეს 2 თვისა“ და „არაუმეტეს 3 თვისა“. ბუნებრივია, კანონის განჭვრეტადობის პრინციპიდან გამომდინარე, ამ საკითხის საკანონმდებლო განსაზღვრულობა განსაკუთრებით მნიშვნელოვანია, ამიტომ მიზანშეწონილი იქნება კოდექსმა ზუსტად, ნათლად დაარეგულიროს ეს საკითხი, ამასთან, მიუხედავად იმისა, რომ საერთაშორისო სტანდარტის მიხედვით ღონისძიების ერთმნიშვნელოვანი ვადა დადგენილი არ არის და ევროპულმა სასამართლომ ერთ-ერთ საქმეზე ასეთი ღონისძიების თავდაპირველი ხანგრძლივობა 2 თვემდე ვადით, მაქსიმუმ 6 თვემდე შემდგომი განახლების პერსპექტივით დასაშვებად მიიჩნია,[770] 3 თვიანი ვადა უფრო გამართლებულად უნდა ჩაითვალოს პირად ცხოვრებაში ჩარევის ინტენსივობის გათვალისწინებით; აღსანიშნავია ისიც, რომ როგორც ირკვევა, პრაქტიკაში ფარული საგამოძიებო მოქმედების მაქსიმალურ ვადად სწორედ 3 თვე გამოიყენება.[771]

საყურადღებოა, რომ ისეთ შემთხვევაში, როდესაც ხდება ღონისძიების გახანგრძლივება გენერალური პროკურორის შუამდგომლობის საფუძველზე, 143[3]

---

[769] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 336.

[770] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR.

[771] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 336.

მუხლის მე-12 ნაწილი აღარ აკონკრეტებს იმ გარემოებებს, რაც უნდა დასაბუთდეს შუამდგომლობაში. უნდა ვივარაუდოთ, რომ ასეთ დროს შუამდგომლობა იგივე წესით განიხილება და ანალოგიური მოთხოვნები არის გათვალისწინებული, რაც პროკურორის შუამდგომლობის მიმართ, როდესაც ხორციელდება ღონისძიების გაგრძელება „არაუმეტეს 2 თვისა“. თუმცა მიზანშეწონილია, ეს ნორმა ცალსახად და პირდაპირ განსაზღვრავდეს, რომ გენერალური პროკურორის მიერ შუამდგომლობის წარდგენისას ასევე უნდა მიეთითოს, ინფორმაცია მოპოვებული მონაცემებისა და იმ გარემოებების შესახებ, რომლის გამოც ვერ მოხერხდა გამოძიებისათვის საკმარისი ინფორმაციის შეგროვება.

1.3.4 ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნა

სსსკ-ის 143[7] მუხლი ითვალისწინებს ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნას, რომელიც ფარული საგამოძიებო მოქმედებების მარეგულირებელი კანონმდებლობის ერთ-ერთ უმნიშვნელოვანეს დებულებას და ადამიანის უფლებების დაცვის ერთ-ერთ არსებით გარანტიას წარმოადგენს. მინიმიზაცია ემსახურება ფარული მეთვალყურეობის ღონისძიების ფარგლებისა და ინტენსივობის შეზღუდვას;[772] აღსანიშნავია, რომ მინიმიზაციის მოთხოვნას სწორედ თანაზომიერების პრინციპი უდევს საფუძვლად.[773]

სსსკ-ის 143[7] მუხლიდან გამომდინარე, ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნა რამდენიმე ასპექტს აერთიანებს:

გამოძიებასთან კავშირში არ მყოფ პირთა დაცვა - აღნიშნული გულისხმობს, რომ ფარული საგამოძიებო მოქმედების განმახორციელებელი ორგანო, აგრეთვე საგამოძიებო ორგანო/პირი ვალდებული არიან, თავიანთი უფლებამოსილების ფარგლებში მაქსიმალურად შეზღუდონ იმ კომუნიკაციისა და პირის მონიტორინგი, რომელთაც გამოძიებასთან კავშირი არ აქვთ.

ცალკეული პროფესიის ან საქმიანობის ნიშნით პირთა დაცვა - სასულიერო პირის, ადვოკატის, ექიმის, ჟურნალისტისა და იმუნიტეტის მქონე პირის მიმართ

---

[772] *Ohm P.,* The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause, წიგნში: The Cambridge Handbook of Surveillance Law, edited by *Gray D., Henderson S.E.,* New York, 2017, 499; *Israel J. H., LaFave W. R.,* Criminal Procedure, Constitutional Limitations in a Nutshell, 8th Ed. 2014, 498.

[773] *Dempsey J., X.; Gate F., H.,* Recommendations for Government and Industry, წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.),* Oxford, 2017, 428.

ფარული საგამოძიებო მოქმედების ჩატარება დასაშვებია მხოლოდ იმ შემთხვევაში, როდესაც ეს არ უკავშირდება შესაბამისად მათ მიერ სასულიერო მოღვაწეობის ან პროფესიული საქმიანობის დროს კანონით დაცული ინფორმაციის მოპოვებას.

სსსკ-ის 143[7] მუხლის მე-3 ნაწილი დამატებითი დაცვის მექანიზმს ითვალისწინებს ადვოკატსა და კლიენტს შორის კომუნიკაციასთან მიმართებით და ადგენს, რომ ადვოკატსა და კლიენტს შორის ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაცია ადვოკატის პირადი კომუნიკაციის შესახებ უნდა გაიმიჯნოს ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის შესახებ ინფორმაციისაგან. ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციის შინაარსი, რომელიც ადვოკატის პროფესიულ საქმიანობას უკავშირდება, დაუყოვნებლივ უნდა განადგურდეს.

იქედან გამომდინარე, რომ საქართველოს მაგალითზე არ არის ხელმისაწვდომი ინფორმაცია იმასთან დაკავშირებით, თუ როგორ განიმარტება და გამოიყენება მინიმუმამდე დაყვანის ზოგადი პრინციპი პრაქტიკაში, საინტერესო იქნება ამ საკითხთან დაკავშირებით აშშ-ის გამოცდილების განხილვა, სადაც მინიმიზაციის დოქტრინას განვითარების საკმაოდ დიდი ისტორია აქვს და სასამართლო პრაქტიკაც ჩამოყალიბებულია ამ საკითხის ირგვლივ.

1.3.4.1 ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნა აშშ-ის პრაქტიკის მიხედვით

აშშ-ის კანონმდებლობის მიხედვით, კომუნიკაციის მონიტორინგის შესახებ სასამართლოს ბრძანება უნდა აღსრულდეს იმგვარად, რათა მინიმუმამდე იქნეს დაყვანილი იმ კომუნიკაციის მონიტორინგი, რომელიც არ არის ღონისძიებასთან კავშირში.[774] ამგვარი კომუნიკაცია შეიძლება განმარტებულ იქნეს, როგორც ისეთი ინფორმაცია, რომელიც არ ეხება დანაშაულს, რომლის საფუძველზეც გაიცა სასამართლოს ბრძანება[775]. აღნიშნული ნიშნავს, რომ კომუნიკაცია არის რელევანტური და შესაბამისად, არ ექვემდებარება მინიმიზაციას, როდესაც შეიცავს გამოძიებისათვის

[774] *McArthur E. D.,* The Search and Seizure of Privileged Attorney-Client Communications, The University of Chicago Law Review, Vol. 72, No. 2, 2005, 741.

[775] *LaFave W., R., Israel J., H., King N., J., Kerr O., S.,* Principles of Criminal Procedure: Investigation, 2nd Ed., 2009, 236.

გამოსადეგ ინფორმაციას, მიუხედავად იმისა, პირდაპირ ამხელს თუ არა ეს მონაცემები კომუნიკაციის მონაწილეს დანაშაულებრივ საქმიანობაში.[776] მინიმიზაცია მიუთითებს პროცესზე, რომელიც მიზნად ისახავს წინასწარ იქნეს შეზღუდული იმ კომუნიკაციის მოცულობა, რომელიც ღონისძიების შედეგად იქნება მოპოვებული.[777] მინიმიზაცია შეიძლება განხორციელდეს სატელეფონო ხაზის ფარული მიყურადებისგან თავის შეკავებით, მაშინ, როდესაც მაგალითად, ეჭვმიტანილი ესაუბრება ოჯახის წევრს ჯანმრთელობის მდგომარეობასთან დაკავშირებული პრობლემების შესახებ.[778] იმისათვის, რათა დადგენილ იქნეს, რამდენად იქნა დაცული მინიმიზაციის პრინციპი, საჭიროა შეფასდეს საქმის კონკრეტული გარემოებები.[779]

ამ მოთხოვნასთან დაკავშირებით ერთ-ერთ ყველაზე მნიშვნელოვან საქმეს წარმოადგენს სკოტი აშშ-ს წინააღმდეგ (Scott v. United States), სადაც სამართალდამცავი ორგანოების თანამშრომლებმა პირთა ჯგუფის მიერ ნარკოტიკული საშუალებების შემოტანა/გავრცელების ფაქტთან დაკავშირებით ერთთვიან პერიოდში განახორციელეს კონკრეტული ტელეფონის ნომერზე განხორციელებული პრაქტიკულად ყველა ზარის ფარული მიყურადება და ჩაწერა, მიუხედავად იმისა, რომ ამ ტელეფონზე შემომავალი/გამავალი ზარების მხოლოდ 40% იყო დაკავშირებული ნარკოტიკულ დანაშაულთან[780]. ამ საქმეში სასამართლომ დაადგინა, რომ მინიმუმამდე დაყვანის მოთხოვნა არ დარღვეულა და განსაზღვრა კონკრეტული გარემოებები, რომლებიც მხედველობაში უნდა იქნეს მიღებული ამ საკითხის გადაწყვეტისას[781]. სასამართლოს განმარტებით, საკითხის გადაწყვეტა მხოლოდ გამოძიებისათვის არარელევანტური ინფორმაციის რაოდენობრივი მაჩვენებლის მიხედვით ვერ ჩაითვლება სწორ მიდგომად. ასეთი კრიტერიუმი შესაძლოა, ზოგჯერ იყოს დამხმარე, თუმცა არის შემთხვევები, როგორიცაა სწორედ მოცემული საქმე, როდესაც გამოძიებისათვის ღირებულების არმქონე კომუნიკაციის რაოდენობრივი მაჩვენებელი მაღალია, თუმცა ფარული მიყურადება გონივრულ ფარგლებში განხორციელდა.[782]

---

[776] იქვე.

[777] *Kerr O.S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 380.

[778] იქვე.

[779] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 287.

[780] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 287, იხ. ციტირება: Scott v. United States, 436 U.S. 128 (1978).

[781] იქვე.

[782] იქვე.

ამის მიზეზები შეიძლება განსხვავდებოდეს - არარელევანტური ზარები შესაძლოა იყოს ძალიან მოკლე, ასევე - მხოლოდ ერთჯერადი ხასიათის, გაუგებარი/ბუნდოვანი შინაარსის ან კოდირებული/დაშიფრული ფორმით[783]. ასეთ შემთხვევებში შესაბამისი პირების მხრიდან რთულია ამ ზარის დასრულებამდე იმის განსაზღვრა, რომ ასეთი კომუნიკაცია არ არის კავშირში გამოძიებასთან“[784].

აშშ-ის სასამართლო პრაქტიკაში ჩამოყალიბდა გარემოებები, რომლებიც მხედველობაში მიიღება მინიმიზაციის მოთხოვნასთან დაკავშირებით გადაწყვეტილების მიღების დროს, მაგალითად, როდესაც გამოძიება მიმდინარეობს დიდი დაჯგუფების მიერ დანაშაულებრივი ქმედების ჩადენის ფაქტზე, შესაძლოა დასაშვები იყოს უფრო ფართო მასშტაბის კომუნიკაციის მონიტორინგი[785]. სხვა ფაქტორებს, რომლებიც ასევე მხედველობაში მიიღება, მიეკუთვნება, მაგალითად, დრო, როდესაც განხორციელდა კომუნიკაციის ჩაწერა (სასამართლოს მიერ ბრძანებით განსაზღვრული ვადის ფარგლებში), კერძოდ, ღონისძიების საწყის ეტაპზე უფლებამოსილ პირებს შეიძლება მოუწიოთ ყველა ზარის მიყურადება, რათა განსაზღვრონ არარელევანტური კომუნიკაციების კატეგორია, რომლებიც შემდგომში აღარ იქნება მიყურადებული. იმავე კატეგორიის ზარების ფარული მიყურადება შემდგომ ეტაპზე შესაძლოა უკვე აღარ ჩაითვალოს გამართლებულად, როდესაც გამოძიებისათვის ღირებულების არმქონე კომუნიკაციების კატეგორიები უკვე დადგენილია და აშკარაა, რომ კონკრეტული კომუნიკაცია ასეთ კატეგორიას მიეკუთვნება[786]. სხვა შემთხვევა შესაძლოა ეხებოდეს ისეთ სიტუაციას, როდესაც არარელევანტური კომუნიკაციის ტიპები არ არის გამოკვეთილი. ასეთ ვითარებაში შესაძლოა არ იყოს არამართებული ყველა „მოკლე საუბრის“ მიყურადება, ვინაიდან მათი რელევანტურობის განსაზღვრა მათ დასრულებამდე შეუძლებელია[787].

ზემოთაღნიშნულ საქმეში (Scott v. United States) სასამართლომ მიიჩნია, რომ იმ ზარების უმეტესობა, რომლებიც არ აღმოჩნდა გამოძიებასთან კავშირში, წარმოადგენდნენ „მოკლე კომუნიკაციას“, „ერთჯერადს“ ან/და „ბუნდოვანი

[783] იქვე.
[784] იქვე.
[785] იქვე. 287-288.
[786] იქვე.
[787] იქვე. 288.

ხასიათისას“, რომლებიც მანამდე გამოკვეთილი ზარების კატეგორიებში ვერ ხვდებოდნენ, შესაბამისად, მინიმიზაციის მოთხოვნა არ დარღვეულა.[788]

აღსანიშნავია, რომ მინიმუმამდე დაყვანის დოქტრინასთან დაკავშირებით არაერთ საკითხზე არსებობს აზრთა სხვადასხვაობა პრაქტიკაში, მაგალითად, პრობლემურია, ეს მოთხოვნა როგორ, რა ეტაპზე უნდა განხორციელდეს ინტერნეტკომუნიკაციასთან მიმართებით[789]. ამ საკითხთან დაკავშირებით აშშ-ის სასამართლო პრაქტიკა არ არის იმდენად განვითარებული, როგორც სატელეფონო კომუნიკაციის შემთხვევაში, ვინაიდან ისტორიულად მინიმიზაციის კონცეფცია სწორედ ხმოვან კომუნიკაციებთან დაკავშირებით ჩამოყალიბდა.[790]

სამეცნიერო ლიტერატურაში აღნიშნულია, რომ ციფრული ტექნოლოგიების განვითარებამდე, მინიმიზაცია ფარული მიყურადების პარალელურად ხორციელდებოდა - პოლიციის ოფიცერი დროებით წყვეტდა სატელეფონო ხაზის ფიზიკურად მიყურადებას, როდესაც დადგინდებოდა, რომ ეს სატელეფონო ზარი არ იყო გამოძიებისათვის რელევანტური[791]. ციფრულ ეპოქაში სამართალდამცავი ორგანოები უფრო იხრებიან პოსტფაქტუმ მინიმიზაციის პროცედურისკენ;[792] აღნიშნული გულისხმობს გამოძიებისათვის ღირებულების თვალსაზრისით ინფორმაციის გადარჩევას და ფილტრაციას მისი მოპოვების შემდგომ. ასეთი პროცედურა უფლებამოსილ პირებს საშუალებას აძლევს, შეაგროვონ ყველაფერი, თუმცა მოეთხოვებათ, შემდგომში „ფილტრებისა“ და „საძიებო ფრაზების“ (search queries) გამოყენებით გამოაცალკევონ არარელევანტური ინფორმაცია რელევანტურისგან.[793]

სამეცნიერო ლიტერატურაში მინიმიზაციის მოთხოვნასთან დაკავშირებით გამოთქმულია კრიტიკული მოსაზრება, რომ აღნიშნული პრინციპი სათანადოდ ვერ ასრულებს თავის ფუნქციას, რადგან მოსამართლეები იშვიათად ადგენენ მის

[788] იქვე, 288.
[789] *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No 4, 2011, 1367-1368.
[790] იქვე.
[791] *Ohm P.,* The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E. (eds.),* New York, 2017, 502.
[792] იქვე.
[793] იქვე.

დარღვევას[794]. მიუხედავად აღნიშნულისა, როგორც ირკვევა, აშშ-ის მოსამართლეები მინიმიზაციის კონცეფციას პრაქტიკაში იყენებენ და ამ პრინციპის დარღვევის საფუძველზე ხშირად მტკიცებულების საქმიდან ამორიცხვაც ხდება, მაგალითად, ერთ-ერთ საქმეში სასამართლომ დაუშვებლად ცნო 22 სატელეფონო ზარის ჩანაწერი, რომელიც განხორციელდა ბრალდებულსა და მის ადვოკატს შორის, იმ საფუძვლით, რომ შესაბამის პირებს უნდა შეეწყვიტათ თითოეული ზარის მიყურადება, როგორც კი მხარეების იდენტიფიკაცია მოხდებოდა.[795] სხვა საქმეში სასამართლომ მინიმიზაციის მოთხოვნის დარღვევის გამო საქმიდან ამორიცხა ღონისძიების შედეგად მოპოვებული მთელი მოცულობის ინფორმაცია.[796]

1.3.4.2 ფარული საგამოძიებო მოქმედების მინიმუმამდე დაყვანის მოთხოვნა ქართულ კანონმდებლობაში

აღსანიშნავია, რომ სსსკ-ის 143[3] მუხლი შეიცავს მხოლოდ ზოგად პრინციპებს, რომლებიც მინიმუმამდე დაყვანის მოთხოვნიდან გამომდინარეობს, თუმცა სსსკ ნაკლებად ეხება ამ მოთხოვნის პრაქტიკულ იმპლემენტაციასთან დაკავშირებულ საკითხებს, შედეგად, სრულებით გაურკვეველია მინიმიზაციის პრაქტიკაში რეალიზებასთან დაკავშირებული არაერთი ასპექტი.

როგორც ზემოთ აღინიშნა, ზოგადი ევროპული სტანდარტი მდგომარეობს მონაცემთა შემოწმებისა და განადგურების წესების საკანონმდებლო რეგულირებაში. როგორც წესი, ევროპული სასამართლოს უარყოფით შეფასებას იწვევს ისეთი ვითარება, როდესაც ეროვნული კანონმდებლობა არ ითვალისწინებს რაიმე სახის პროცედურას, თუ რა წესით უნდა მოხდეს მოპოვებული ინფორმაციის გადარჩევა ან განადგურება.[797] ამავდროულად, კანონის „ხელმისაწვდომობისა“ და „განჭვრეტადობის“ კრიტერიუმებიდან გამომდინარე, ეს რეგულირება უნდა იყოს

[794] *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No 4, 2011, 1377.

[795] *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No4, 2011, 1377-1378, იხ. ციტირება: United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987).

[796] *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No 4, 2011, 1378, იხ. ციტირება: United States v. Renzi, 722 F. Supp. 2d 1100, 1128 (D. Ariz. 2010).

[797] Iordachi and others v. Moldova, [2009], ECtHR, 48; Huvig v. France, [1990], ECtHR, (Ser. A.), 34.

საზოგადოებისათვის ხელმისაწვდომი და მკაფიო, განჭვრეტადი სამართლებრივი დებულებებით გაწერილი.

ამ თვალსაზრისით აღსანიშნავია, რომ სსსკ-ის 143[8] მუხლის პირველი ნაწილის თანახმად, ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაცია, პროკურორის გადაწყვეტილებით, დაუყოვნებლივ უნდა განადგურდეს ფარული საგამოძიებო მოქმედების შეწყვეტის ან დასრულების შემდეგ, თუ მას არ აქვს ღირებულება გამოძიებისათვის. ასეთ შემთხვევაში ინფორმაცია ნადგურდება პროკურორის მიერ შესაბამისი მოსამართლის მონაწილეობით. გამოძიებისათვის ღირებულების არმქონე ინფორმაცია შეიძლება იყოს როგორც იმ პირების შესახებ ინფორმაცია, რომელსაც არ აქვს კავშირი გამოძიებასთან, ასევე გადარჩეული ინფორმაცია, რომლის მტკიცებულებად გამოყენებასაც არ მიიჩნევს ბრალდების მხარე საჭიროდ, ასევე სსსკ-ით დაცული ცალკეული პროფესიის პირთა პრივილეგირებული კომუნიკაცია, რომელიც განსაზღვრულია სსსკ-ის 143[7] მუხლის მე-2 ნაწილით, მათ შორის, ადვოკატსა და კლიენტს შორის კომუნიკაციის შინაარსი და სხვა.

პირველ რიგში, აღსანიშნავია, რომ სსსკ არ განსაზღვრავს ინფორმაციის გადარჩევის ძირითად პრინციპებსა და წესებს, არაფერს ამბობს, თუ რა წესით, ვის მიერ, რა ვადაში უნდა მოხდეს კომუნიკაციის მონიტორინგის განხორციელების დროს ინფორმაციის გადარჩევა და დახარისხება, გამოძიებისათვის ღირებულების არმქონე ინფორმაციის გამიჯვნა საქმისთვის რელევანტური ინფორმაციისგან.[798] შესაბამისად, არ არის განსაზღვრული, თუ რამდენად ექვემდებარება ინფორმაციის გადარჩევის საკითხები ოქმში დაფიქსირებას, რათა შემდგომში შესაძლებელი იყოს მინიმუმამდე დაყვანის მოთხოვნის შესრულების გადამოწმება და კონტროლი. ინფორმაციის დამუშავების საკითხთან დაკავშირებით მსგავსი მოსაზრებაა დაფიქსირებული ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის მონაცემთა დაცვის განყოფილების 2014 წლის დასკვნაში, რომელიც ეხება სამართალდამცავი ორგანოებისა და ეროვნული უშიშროების სამსახურის მიერ ფარულ მეთვალყურეობასთან დაკავშირებულ კანონპროექტებს. აღნიშნული დასკვნის მიხედვით, კანონმდებლობა არაფერს ამბობს ისეთ საკითხზე, როგორიცაა,

[798] *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, (რედ.), თბ., 2019, 389.

მაგალითად, მონაცემთა დამუშავება[799]. პროექტით არ არის გაწერილი პროცედურა ინფორმაციის მოპოვებიდან მის განადგურებამდე, არადა ამ საკითხების დეტალური რეგულირება ევროპული სასამართლოს მოთხოვნას წარმოადგენს.[800]

საქართველოს საკონსტიტუციო სასამართლოში მიმდინარე დავის ფარგლებში, 2017 წლის 29 დეკემბრის საოქმო ჩანაწერიდან იკვეთება, რომ „კომუნიკაციის რეალურ დროში მოპოვებისას ინფორმაციის ღირებულების თვალსაზრისით გამიჯვნას ახდენს საგამოძიებო ორგანოს წარმომადგენელი, რომელმაც წარმოადგინა განჩინება/პროკურორის დადგენილება“[801]. გადაწყვეტილების მიხედვით, „თავად ეს პირი არის უფლებამოსილი, დაამუშავოს და მოითხოვოს ის ინფორმაცია, რომელიც ღირებულების თვალსაზრისით არის მნიშვნელოვანი. ხოლო სააგენტო ამ პროცესისგან დისტანცირებულია.“[802]

როგორც ვხედავთ, ინფორმაციის გადარჩევის პროცესის შესახებ გარკვეულ მინიმალურ წარმოდგენას იძლევა 2017 წლის 29 დეკემბრის საოქმო ჩანაწერი, თუმცა მხოლოდ ეს ინფორმაცია, ბუნებრივია, საკმარისი არ არის ინფორმაციის გადარჩევის პროცედურის შესახებ დასკვნების გამოსატანად, ამავდროულად, სასამართლო პროცესზე მხარის მიერ გაკეთებული განცხადება, რა თქმა უნდა, ვერ ჩაანაცვლებს მსგავსად მნიშვნელოვანი საკითხის ნორმატიულად რეგულირების აუცილებლობას.

გარდა ამისა, აღნიშნულ საკითხთან დაკავშირებით, ჩნდება კითხვა, თუ რა ურთიერთმიმართება არსებობს გამომძიებლისა და პროკურორის კომპეტენციებს შორის, კერძოდ, სსსკ-ის 143[8] მუხლის პირველი ნაწილიდან გამომდინარე, ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაცია, რომელსაც არ აქვს ღირებულება გამოძიებისათვის, ღონისძიების დასრულების ან შეწყვეტის შემდეგ ნადგურდება პროკურორის გადაწყვეტილებით. ამ ჩანაწერიდან იკვეთება რომ: 1) პროკურორს უნდა წარედგინოს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული სრული მოცულობის ინფორმაცია; 2) პროკურორი იღებს

[799] იხ. *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 22, https://rm.coe.int/16806af19b [20.06.2020].

[800] იქვე.

[801] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-82.

[802] იქვე.

გადაწყვეტილებას არა მარტო ინფორმაციის განადგურების შესახებ, არამედ ასევე მოპოვებული ინფორმაციის ღირებულების თაობაზეც; ამდენად, იქედან გამომდინარე, რომ საქართველოს საკონსტიტუციო სასამართლოს ზემოთაღნიშნული საოქმო ჩანაწერის მიხედვით, „ინფორმაციის ღირებულების თვალსაზრისით გამიჯვნას ახდენს საგამოძიებო ორგანოს [შესაბამისი] წარმომადგენელი“ და „თავად ეს პირი არის უფლებამოსილი, დაამუშავოს და მოითხოვოს ის ინფორმაცია, რომელიც ღირებულების თვალსაზრისით არის მნიშვნელოვანი“, ბუნდოვანია, ამ პირის უფლებამოსილების ფარგლების მიმართება პროკურორის კომპეტენციასთან, რომელიც სსსკ-ის 143[8] მუხლის პირველი ნაწილიდან გამომდინარე, იღებს ინფორმაციის განადგურების შესახებ გადაწყვეტილებას გამოძიებისათვის ღირებულების არქონის საფუძვლით და რომელსაც ამავე მუხლიდან გამომდინარე, სრული მოცულობით წარედგინება მოპოვებული ინფორმაცია ამ გადაწყვეტილების მისაღებად.

1.3.4.3 ადვოკატსა და კლიენტს შორის განხორციელებული ადვოკატის პროფესიულ საქმიანობასთან დაკავშირებული კომუნიკაციის დაცვა

ზემოთ განვიხილეთ მინიმუმამდე დაყვანის მოთხოვნასთან დაკავშირებული ქართული კანონმდებლობა. ამ საკითხთან მიმართებით გამოთქმული მოსაზრებები, ბუნებრივია, ასევე ეხება ადვოკატსა და კლიენტს შორის კომუნიკაციის დაცვის საკითხსაც, რომელიც მინიმუმამდე დაყვანის მოთხოვნის ერთ-ერთ შემადგენელ ასპექტს წარმოადგენს, თუმცა ამ საკითხზე უფრო დეტალურად შევჩერდებით, გამომდინარე იქედან, რომ ადვოკატსა და კლიენტს შორის კომუნიკაციის დაცვას ევროპული სასამართლოს პრაქტიკაში განსაკუთრებული ადგილი უჭირავს და 143[7] მუხლიც საგანგებო ყურადღებას უთმობს ამ პროცედურულ გარანტიას.

როგორც უკვე აღინიშნა, სსსკ-ის 143[7] მუხლის მე-3 ნაწილი ითვალისწინებს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ადვოკატის პირადი კომუნიკაციის ადვოკატსა და კლიენტს შორის განხორციელებული კომუნიკაციისგან გამიჯვნისა და ადვოკატსა და კლიენტს შორის განხორციელებული ადვოკატის პროფესიულ საქმიანობასთან დაკავშირებული კომუნიკაციის დაუყოვნებლივ განადგურების მოთხოვნებს. კვლევაში განხილულ იქნა ადვოკატსა და კლიენტს

შორის კომუნიკაციის დაცვასთან დაკავშირებით საერთაშორისო დონეზე შემუშავებული ძირითადი გარანტიები და როგორც გამოიკვეთა, ევროპული სასამართლოს პრაქტიკის თანახმად, ამ პრინციპის დაცვის ქმედითი მექანიზმის უზრუნველსაყოფად აუცილებელია კანონმდებლობამ განსაზღვროს პროფესიულ საიდუმლოებას მიკუთვნებული ინფორმაციის არაპრივილეგირებული ინფორმაციისგან გამიჯვნის წესი და პროცედურა. ევროპული სასამართლოს მიერ ასევე დადებითად არის შეფასებული შესაბამისი პროფესიული გაერთიანების წარმომადგენლის, მაგალითად, ადვოკატთა ასოციაციის, მონაწილეობა მონაცემების გადარჩევის პროცესში. ამავდროულად, აუცილებელია ამ პროცესზე უზრუნველყოფილი იყოს ზედამხედველობის ადეკვატური სისტემა, სასამართლოს აუცილებელი ჩართულობით.

მოცემულ საკითხთან დაკავშირებით საყურადღებოა ასევე გერმანიის გამოცდილებაც - გერმანიის სისხლის სამართლის საპროცესო კოდექსი განსაზღვრავს პროფესიული საიდუმლოების მქონე პირთა წრეს, რომელთა ტელეკომუნიკაციის მონიტორინგი, ძირითადად დაუშვებელია.[803] ამ წრეს მიეკუთვნებიან ისეთი პირები, რომლებიც სარგებლობენ ჩვენების მიცემაზე უარის თქმის უფლებით თავიანთი პროფესიული საქმიანობიდან გამომდინარე. ამავდროულად, გერმანიის საპროცესო კოდექსი დაცვის სხვადასხვა ხარისხით უზრუნველყოფს სხვადასხვა პროფესიათა წარმომადგენლებს, კერძოდ, 160a პარაგრაფიდან გამომდინარე, აბსოლუტური დაცვის უფლებით სარგებლობს ადვოკატი, სასულიერო პირი, ფედერალური მიწის პარლამენტარი, ბუნდესთაგისა და ბუნდესრათის დეპუტატები, აგრეთვე ევროპარლამენტის წევრები გერმანიის ფედერალური რესპუბლიკიდან.[804] ასეთ პირთა მიმართ ტელეკომუნიკაციის მონიტორინგის ჩატარება დაუშვებელია, თუკი მოსალოდნელია ისეთი ინფორმაციის მოპოვება, რომელთან დაკავშირებითაც ამ პირებს ექნებოდათ ჩვენების მიცემაზე უარის თქმის უფლება. ამავდროულად, ინფორმაცია, რომლის მოპოვებაც განხორციელდა არ უნდა იქნეს გამოყენებული და

[803] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 184.

[804] StPO, §160a Abs.1, 07/04/1987; *Weigend T., Ghanayim K.,* Human Dignity in Criminal Procedure: A comparative Overview of Israeli and German Law, Israel Law Review, Vol.44, 222.

დაუყოვნებლივ განადგურებას ექვემდებარება. ინფორმაციის მოპოვებისა და განადგურების ფაქტი უნდა დაფიქსირდეს ოქმში.[805]

ჩვენების მიცემაზე უარის თქმის უფლების მქონე სხვა პირები - ნოტარიუსი, საგადასახადო კონსულტანტი, ექიმი, აფთიაქარი, მედდა და გერმანიის საპროცესო კოდექსის 53-ე პარაგრაფის I აბზაცის მე-3 პუნქტში მოცემული სხვა პირები, ასევე 3a, 3b და მე-5 პუნქტით განსაზღვრული სხვა პირები სარგებლობენ თანაზომიერების პრინციპით დადგენილი, ფარული საგამოძიებო მოქმედების გამოყენებისგან დაცვის „შეფარდებითი უფლებით“.[806]

როგორც ვხედავთ, გერმანიის საპროცესო კანონმდებლობა ითვალისწინებს იმ პირთა პროფესიულ საიდუმლოებას მიკუთვნებული ინფორმაციის დაცვას, რომლებსაც, მინიჭებული აქვთ ჩვენებაზე უარის თქმის უფლება. ამ პირთაგან აბსოლუტური დაცვის ქვეშ მოსარგებლე პირთა კატეგორიაში სხვა ზემოთაღნიშნულ პირებთან ერთად ექცევა ადვოკატი. გერმანიის ფედერალური საკონსტიტუციო სასამართლოს გადაწყვეტილების თანახმად, ადვოკატის სატელეფონო ხაზი ძირითადად არ უნდა ისმინებოდეს.[807] ეს წესი ვრცელდება ისეთ შემთხვევაზეც, როდესაც ადვოკატის წინააღმდეგ არსებობს ეჭვი, რომ ხელს უშლის პირის სისხლისსამართლებრივ პასუხისმგებლობაში მიცემის პროცესს, ხოლო მისი დაცვის ქვეშ მყოფი პირი ეჭვმიტანილია გერმანიის სისხლის სამართლის საპროცესო კოდექსის 100ა პარაგრაფით განსაზღვრული დანაშაულის [რომლისთვისაც დასაშვებია სატელეკომუნიკაციო კონტროლის ღონისძიების გამოყენება] ჩადენაში.[808] თუმცა აღნიშნული აკრძალვა არ ეხება ისეთ შემთხვევას, როდესაც ადვოკატი ფაქტობრივი გარემოებების საფუძველზე, თვითონ არის მისი დაცვის ქვეშ მყოფის მიერ ჩადენილი დანაშაულის მონაწილეობაში ეჭვმიტანილი და ეს დანაშაული მიეკუთვნება გერმანიის სისხლის სამართლის საპროცესო კოდექსის 100a პარაგრაფით

[805] StPO, §160a Abs.1, 07/04/1987.

[806] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 187.

[807] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 188, იხ. ციტირება: BVerfG NJW 07, 2749.

[808] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 188, იხ. ციტირება: Roxin/ Schünemann, Strafverfahrensrecht, 2009, § 36, Rn. 8..

დადგენილ დანაშაულთა წრეს.[809] ამასთან, თუკი სატელეფონო საუბრის ფარული მიყურადების დროს აღმოჩნდება, რომ საუბრის ერთ-ერთი მონაწილე ადვოკატია, მიმდინარე ფარული საგამოძიებო ღონისძიება დაუყოვნებლივ უნდა შეწყდეს.[810] ხოლო იმ შემთხვევაში, თუ სატელეფონო საუბრის მიმდინარე მოსმენისა და ჩაწერის შეწყვეტა ტექნიკურად შეუძლებელია, მაშინ მიღებული მასალის გამოყენება უნდა გამოირიცხოს სისხლის სამართლის პროცესში.[811]

რაც შეეხება ქართულ კანონმდებლობას, ადვოკატსა და კლიენტს შორის განხორციელებული ადვოკატის პროფესიულ საქმიანობასთან დაკავშირებული კომუნიკაციის დაცვის მოთხოვნის საკანონმდებლო დონეზე უზრუნველყოფა, რა თქმა უნდა, მისასალმებელია, თუმცა, მიგვაჩნია, არსებული დაცვის მექანიზმი ზოგადი სახით არის ფორმულირებული და სსსკ-ის 143[7] მუხლი, ამ შემთხვევაშიც, ისევე როგორც მინიმუმამდე დაყვანის მოთხოვნით დაცულ სხვა კომუნიკაციებთან მიმართებით, არ შეიცავს სახელმძღვანელო ნორმებს და ნათელ, განჭვრეტად პროცედურას იმასთან დაკავშირებით, თუ როგორ უნდა განხორციელდეს პრივილეგირებული ინფორმაციის გამოცალკავება არაპრივილეგირებულისგან.

ამ თვალსაზრისით აღსანიშნავია, რომ ევროპის საბჭოს ადამიანის უფლებათა და კანონის უზენაესობის გენერალური დირექტორატის 2014 წლის დასკვნაში სსსკ-ში საკანონმდებლო ცვლილებებთან დაკავშირებით გამოთქმულია მოსაზრება, რომ უნდა გადაიდგას პრაქტიკული ნაბიჯები ადვოკატსა და კლიენტს შორის კომუნიკაციის დაცვის მიზნით[812]. დასკვნაში მოყვანილია მაგალითი ნიდერლანდების კანონმდებლობიდან, სადაც ადვოკატთა ასოციაციის წარმომადგენელი და

[809] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 188, იხ. ციტირება: *Schmitt,* in: Meyer-Goßner, StPO, 59. Aufl, 2016, §100a, Rn. 21.

[810] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 188, იხ. ციტირება: Welp, JZ 1972, 428; Schmitt, in: Meyer-Goßner, StPO, 59. Aufl, 2016, §100a, Rn. 21.

[811] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 188, იხ. ციტირება: BGH StraFO 05, 296; Schmitt, in: Meyer-Goßner, StPO, 59. Aufl, 2016, §100a, Rn. 21.

[812] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 19, <https://rm.coe.int/16806af19b> [20.06.2020].

პროკურორი მონაწილეობენ ადვოკატის პროფესიულ საქმიანობას მიკუთვნებული ინფორმაციის არაპრივილეგირებული ინფორმაციისგან გამიჯვნის პროცესში.[813]

გარდა აღნიშნულისა, მნიშვნელოვანია, ოქმში აისახოს ინფორმაცია მოპოვებული კომუნიკაციის შესახებ. აღნიშნული ეხება როგორც ადვოკატსა და კლიენტს შორის პროფესიულ კომუნიკაციას, ასევე ადვოკატის პირად კომუნიკაციას; მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსის 160a პარაგრაფის პირველი აბზაცის მიხედვით, პროფესიული საქმიანობიდან გამომდინარე, აბსოლუტური დაცვით მოსარგებლე პირების, მათ შორის, ადვოკატის პროფესიული კომუნიკაციის მოპოვების, ისევე როგორც განადგურების შესახებ ინფორმაცია უნდა დაფიქსირდეს ოქმში.[814] ამასთან დაკავშირებით აღსანიშნავია, რომ სსსკ-ის 143^{6} მუხლის მე-14 ნაწილი, რომელიც ადგენს ფარული საგამოძიებო მოქმედების შესახებ ოქმის რეკვიზიტებს, არ ითვალისწინებს ოქმში მოპოვებული ინფორმაციის შესახებ მონაცემთა აღრიცხვის მოთხოვნას. გარდა ამისა, 143^{7} მუხლი, ასევე არ მოითხოვს მონაცემთა დახარისხების შესახებ ინფორმაციის რაიმე ფორმით აღრიცხვის ვალდებულებას არც ადვოკატთან და არც ამ მუხლის მე-2 ნაწილით განსაზღვრულ სხვა პირებთან მიმართებით. პროფესიულ საქმიანობას მიკუთვნებული ინფორმაციის ოქმში დაფიქსირების გარეშე, რთული წარმოსადგენია ზედამხედველი პირის მიერ სსსკ-ის 143^{7} მუხლის მოთხოვნათა შესრულებაზე ეფექტიანი კონტროლის განხორციელება. ამდენად, სსსკ-ში მოცემული საკითხის რეგულირება ძალიან მნიშვნელოვანია ამ პროცესზე ზედამხედველობის სათანადო სისტემის უზრუნველსაყოფად.

1.3.5 პირადი ცხოვრების ძირითადი სფერო და ფარული საგამოძიებო მოქმედებები

გერმანიის ფედერალური საკონსტიტუციო სასამართლოს პრაქტიკაში ჩამოყალიბდა ე.წ. „სფეროთა თეორია“, რომელზეც კვლევაში უკვე გვქონდა საუბარი. სწორედ „სფეროთა თეორიიდან“ და უფრო კონკრეტულად, პირადი ცხოვრების ძირითადი სფეროს - ინტიმური სფეროს დაცვის აბსოლუტური უფლებიდან

[813] იქვე.
[814] StPO, §160a Abs.1, 07/04/1987.

გამომდინარე, გერმანიის სისხლის სამართლის საპროცესო კანონმდებლობა სატელეფონო და ინტერნეტკომუნიკაციების მოპოვების საკითხთან დაკავშირებით ითვალისწინებს ადამიანის უფლებების დაცვის მნიშვნელოვან საპროცესო გარანტიებს.

აღსანიშნავია, რომ „სფეროთა თეორია“ დაცვის სხვადასხვა ხარისხს ანიჭებს პირადი ცხოვრების კერძო, სოციალურ და ინტიმურ სფეროებს, აქედან ინტიმური სფერო სარგებლობს აბსოლუტური დაცვის უფლებით; კერძო სფეროში ჩარევა დასაშვებია თანაზომიერების პრინციპის შესაბამისად და თუკი საჯარო ინტერესი გადაწონის კონფიდენციალურობის დაცვის ინდივიდუალურ ინტერესს.[815] ხოლო სოციალურ სფეროში ჩარევა დასაშვებია ნაკლებად მკაცრი მოთხოვნების დაცვით.[816]

გერმანიის ფედერალური საკონსტიტუციო სასამართლოს განმარტებით, სახელმწიფოს მხრიდან ფარული მეთვალყურეობის ღონისძიებების განხორციელების დროს დაცული უნდა იყოს ინტიმური სფეროს უფლება[817]. უპირატესი საჯარო ინტერესიც კი ვერ გაამართლებს ამ სფეროს შეზღუდვას[818]. პიროვნების თავისუფალი განვითარების უფლება პირადი ცხოვრების ძირითად სფეროში მოიცავს შინაგანი გრძნობების, აღქმების, აზრებისა და ღრმად პირადი ხასიათის გამოცდილებების გამოხატვის შესაძლებლობას, სახელმწიფოს მხრიდან დაკვირვების შიშის გარეშე.[819] პირადი ცხოვრების ძირითადი სფერო წარმოადგენს ემოციებისა და გრძნობების სახელმწიფოს ზედამხედველობის გარეშე გამოხატვის შესაძლებლობას[820]. ამ უფლებით დაცულია ამგვარი ემოციებისა და გრძნობების გამოხატვის ფორმები, განსაკუთრებით, ინტიმური დეტალები და ურთიერთობა ძალიან ახლობელ ადამიანებს შორის.[821]

ინტიმური სფეროს დაცვის უფლება მოიცავს კომუნიკაციას ისეთ პირებთან, რომელზედაც პიროვნებას ნდობის მაღალ ხარისხზე დამყარებული ახლო

---

[815] *Lindemann M., Toor D. V.,* Protection of a Suspect's Privacy in Criminal Procedures, Does the Conceptual Approach of the German Federal Constitutional Court Make a Difference? *Ars Aequi,* Issue 5, 2018, 378.

[816] *Bumke C., Vosskuhle H.C.A.,* German Constitutional Law, Introduction, Cases, Principles, 2019, 115.

[817] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07, 271.

[818] იქვე.

[819] იქვე.

[820] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 34, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[821] იქვე.

ურთიერთობა აკავშირებს, როგორიცაა, მაგალითად, ოჯახის წევრები, ადვოკატი, სასულიერო პირები, ექიმი.[822] გერმანიის საკონსტიტუციო სასამართლოს განმარტებით, პირის პირადი ცხოვრების ძირითადი სფერო არის ხელშეუხებელი და არ ექვემდებარება თუნდაც ინტერესების შეწონვის შესახებ მსჯელობას.[823] ამასთან, კომუნიკაცია, რომელიც ეხება წარსულში ჩადენილ, მიმდინარე ან დაგეგმილ დანაშაულებს, არ ექცევა ამ უფლების დაცვის ქვეშ.[824]

გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ განავითარა ინტიმური სფეროს დაცვის ორსაფეხურიანი კონცეფცია - 1) შესაბამისი კანონმდებლობით უზრუნველყოფილი უნდა იყოს ინტიმური სფეროდან ინფორმაციის გამიზნულად მოპოვების დაუშვებლობა; 2) იმ შემთხვევაში, თუკი პრაქტიკული თვალსაზრისით აუცდენელია ასეთი მონაცემების მოპოვება, საკმარისი დაცვის მექანიზმები უნდა იქნეს გათვალისწინებული მონაცემთა გამოკვლევის სტადიაზე, კერძოდ, ასეთი მონაცემები დაუყოვნებლივ უნდა განადგურდეს და მათი გამოყენება დაუშვებელია.[825]

აღსანიშნავია, რომ პირადი ცხოვრების ინტიმური სფეროს უფლებას გერმანიის სისხლის სამართლის საპროცესო კოდექსში 2017 წელს განხორციელებული ცვლილებების შედეგად, ცალკე ნორმა - 100d პარაგრაფი მიეძღვნა. აღნიშნული პარაგრაფის პირველი აბზაცის თანახმად, ტელეკომუნიკაციის ფარული მიყურადებისა და ჩაწერის (100a პარაგრაფი), ონლაინ ჩხრეკისა (100b პარაგრაფი) და საცხოვრებელ სახლში აკუსტიკური მეთვალყურეობის (100c პარაგრაფი) ღონისძიებების განხორციელება დაუშვებელია, თუკი ფაქტობრივ გარემოებებზე

---

[822] *Nohlen N.,* Germany: The Electronic Eavesdropping Case, International Journal of Constitutional Law, Vol. 3, No. 4, 682; *Jacoby N.,* Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States, Georgia Journal of International and Comparative Law, Vol.35, No.3, 2007, 472-473; *ალბრეხტი, ჰ.-ო.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 35, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[823] *Nohlen N.,* Germany: The Electronic Eavesdropping Case, International Journal of Constitutional Law, Vol. 3, No. 4, 682; *ლომთათიძე ე., ხანთაძე ნ., ზედელაშვილი დ.,* პირადი თავისუფლება და ავტონომია, 2018, 88, <http://ewmi-prolog.org/images/files/5844ResearchRighttoPrivacyFINAL.pdf> [25.06.2020].

[824] *Jacoby N.,* Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States, Georgia Journal of International and Comparative Law, Vol. 35, No.3, 2007, 473.

[825] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07, 280-283. *Bumke C., Vosskuhle H.C.A.,* German Constitutional Law, Introduction, Cases, Principles, New York, 2019, 115.

დაყრდნობით ივარაუდება, რომ მოპოვებული იქნება მხოლოდ პიროვნების ინტიმურ სფეროს მიკუთვნებული ინფორმაცია. ამავე პარაგრაფის მე-2 აბზაცის მიხედვით, დაუშვებელია იმ მონაცემთა გამოყენება, რომელთა მოპოვებაც მოხდება ზემოთაღნიშნული საგამოძიებო მოქმედებების შედეგად; მოპოვებული ინფორმაცია დაუყოვნებლივ განადგურებას ექვემდებარება; ამასთან, ასეთ მონაცემთა მოპოვებისა და განადგურების შესახებ ინფორმაცია უნდა დაფიქსირდეს წერილობით.[826] როგორც ვხედავთ, აღნიშნულ ნორმაში გათვალისწინებულია გერმანიის ფედერალური საკონსტიტუციო სასამართლოს მიერ ჩამოყალიბებული ინტიმური სფეროს დაცვის ორსაფეხურიანი მოდელი.

ნიშანდობლივია, რომ პრაქტიკაში ხშირად თითქმის შეუძლებელია წინასწარ განისაზღვროს ჩასატარებელი საგამოძიებო მოქმედების პირადი ცხოვრების ძირითად სფეროსთან შემხებლობა.[827] ამიტომაც ღონისძიების ჩატარებაზე თავიდანვე უარის თქმა იმ რისკის გამო, რომ შესაძლებელია მოხდეს ძირითად სფეროს მიკუთვნებული ინფორმაციის მოპოვება, არ არის სავალდებულო.[828]

გერმანიის საპროცესო კოდექსის 100d პარაგრაფის პირველი აბზაციდან გამომდინარე, წინასწარ უნდა გაკეთდეს პროგნოზი იმასთან დაკავშირებით, ზემოთაღნიშნული ფარული საგამოძიებო მოქმედებების შედეგად ხომ არ იქნება მოპოვებული მხოლოდ ინტიმურ სფეროს მიკუთვნებული ინფორმაცია.[829] ამასთან მიმართებით, იურიდიულ ლიტერატურაში გამოთქმულია კრიტიკა, რომ პრაქტიკაში თითქმის წარმოუდგენელია ღონისძიების განხორციელების შედეგად გამორიცხული იყოს პირადი ცხოვრების ძირითადი სფეროს მიღმა ინფორმაციის მოპოვება[830]. საილუსტრაციო მაგალითად დასახელებულია ერთ-ერთი საქმე გერმანიის სამართალდამცავი ორგანოების პრაქტიკიდან, სადაც განხორციელდა ბრალდებულსა და მის მეუღლეს შორის კომუნიკაციის მიყურადება[831]. ასეთი სახის კომუნიკაცია,

---

[826] StPO, §100d, 07/04/1987.

[827] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 62, იხ. ციტირება: Beschl. v. 12.10.2011, StV 2012, 259.

[828] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 62, იხ. ციტირება: BVerfG, Beschl. v. 12.10.2011*,* StV 2012, 259.

[829] *Lindemann M., Toor D. V.,* Protection of a Suspect's Privacy in Criminal Procedures, Does the Conceptual Approach of the German Federal Constitutional Court Make a Difference? *Ars Aequi,* Issue 5, 2018, 382.

[830] იქვე, 382-383.

[831] იქვე.

როგორც წესი, ექცევა პირადი ცხოვრების ძირითადი სფეროს დაცვის ქვეშ, თუმცა ამ შემთხვევაში საგამოძიებო ორგანოს წარმომადგენლები ვარაუდობდნენ, რომ ბრალდებული ასევე ისაუბრებდა პირადი ცხოვრების ძირითად სფეროს მიღმა არსებულ თემაზეც - მართლმსაჯულებისთვის ხელის შეშლის საკითხზე[832]. აღსანიშნავია, რომ გერმანიის ფედერალურმა მართლმსაჯულების სასამართლომ გაითვალისწინა საგამოძიებო ორგანოს მხრიდან ასეთი ვარაუდი.[833]

სირთულედ სახელდება ასევე ის გარემოება, რომ თანამედროვე ტექნიკის წყალობით ტელეკომუნიკაციის ფარული მიყურადების დროს მონაცემთა მოპოვების ეტაპზე ინფორმაციის ჩაწერა ხორციელდება ავტომატურ რეჟიმში და პერსონალური კონტროლი, „პარალელური მოსმენა," როგორც წესი, წარმოებს მხოლოდ კონკრეტული ნიშნის გათვალისწინებით.[834]

ტელეკომუნიკაციის ფარული მიყურადების ჩატარებისას ინფორმაციის მოპოვების ეტაპზე მსგავსი სახის სირთულეების გადაჭრის გზად მიიჩნევა მონაცემთა მოპოვების შემდგომ მათი გამოყენების აბსოლუტურ აკრძალვასთან დაკავშირებული სამართლებრივი რეგულაცია.[835]

1.3.6 ქვეთავების 1.3.4 და 1.3.5 შეჯამება

ამდენად, როგორც აშშ-ის კანონმდებლობით გათვალისწინებული მინიმიზაციის დოქტრინა, ასევე გერმანიის პრაქტიკაში ჩამოყალიბებული პირადი ცხოვრების ძირითადი სფეროს დაცვის უფლება ემსახურება კომუნიკაციის მონიტორინგის ღონისძიების ფარგლებისა და გარკვეული სახის ინფორმაციების მოპოვების/გამოყენების შეზღუდვას. აშშ-ის სასამართლო პრაქტიკაში ჩამოყალიბებულია ის კრიტერიუმები, რომლებსაც სასამართლოები სახელმძღვანელოდ იყენებენ მინიმუმამდე დაყვანის მოთხოვნის

---

[832] იქვე.

[833] იქვე.

[834] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 65, იხ. ციტირება: BVerfG, Beschl. v. 12.10.2011*,* StV 2012, 259.

[835] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 65, იხ. ციტირება: Schmitt, in: Meyer-Goßner, StPO, 54. Aufl, 2011, §100a Rn. 25; BVerfG, Beschl. v. 12.10.2011*,* StV 2012, 260; *Lindemann M., Toor D. V.,* Protection of a Suspect's Privacy in Criminal Procedures, Does the Conceptual Approach of the German Federal Constitutional Court Make a Difference? *Ars Aequi,* Issue 5, 2018, 383.

განსახორციელებლად, როგორიცაა მაგალითად, გამოძიების მიმდინარეობა პირთა დიდი დაჯგუფების მიერ დანაშაულებრივი ქმედების ჩადენის ფაქტზე, ღონისძიების განხორციელების ეტაპი, რამდენად არის სახეზე „მოკლე“, „ერთჯერადი“ ან/და „ბუნდოვანი ხასიათის“ კომუნიკაცია. ამ კუთხით, აშშ-ის გამოცდილება, გამოსადეგი შეიძლება იყოს საქართველოს სამართალდამცავი ორგანოების პრაქტიკაში მინიმიზაციის მოთხოვნის ეფექტიანი გამოყენებისა და ინტერპრეტირების კუთხით.

ქართულ კანონმდებლობასთან დაკავშირებით გამოიკვეთა, რომ მინიმუმამდე დაყვანის მოთხოვნასთან დაკავშირებული ასპექტები - მოცემული გარანტიით დაცული ინფორმაციის გამოძიებისათვის რელევანტური ინფორმაციისგან გამიჯვნასთან დაკავშირებული ძირითადი წესები საჭიროებს მოწესრიგებას სსსკ-ში მკაფიო და დეტალური სახით. დღევანდელი რეგულაცია ნაკლებად ინფორმაციული ხასიათისაა იმასთან დაკავშირებით, თუ როგორ, რა წესით უნდა განხორციელდეს ეს პრინციპი პრაქტიკაში, ვინ არის პასუხისმგებელი ინფორმაციის დახარისხებაზე, რამდენად აღირიცხება ეს ინფორმაცია დოკუმენტური წესით და ა.შ. ეს მოსაზრება ეხება, მათ შორის, ადვოკატსა და კლიენტს შორის პროფესიული კომუნიკაციის დაცვასაც, რომელიც ძალიან მნიშვნელოვან გარანტიას წარმოადგენს არამარტო პირადი ცხოვრების, არამედ სამართლიანი სასამართლოს უფლების უზრუნველყოფის კონტექსტშიც. ამასთანავე, მინიმუმამდე დაყვანის მოთხოვნაზე ეფექტური ზედამხედველობის განხორციელების მიზნით მნიშვნელოვანია, ფარული საგამოძიებო მოქმედების შესახებ ოქმში აღირიცხოს სსსკ-ის 143[7] მუხლით გათვალისწინებული მინიმუმამდე დაყვანის მოთხოვნის ფარგლებში დაცულ პირებთან დაკავშირებით მონაცემების მოპოვების შესახებ ინფორმაცია, ისევე როგორც მოპოვებული მასალის გადარჩევასთან დაკავშირებული მონაცემები.

რაც შეეხება პირადი ცხოვრების ძირითადი სფეროს დაცვის გერმანულ დოქტრინას, გერმანიის სისხლის სამართლის საპროცესო კოდექსი პირადი ცხოვრების ძირითადი სფეროს აბსოლუტური დაცვის ქვეშ მოქცევის გზით სერიოზულ გარანტიებს ქმნის კომუნიკაციის მონიტორინგის პროცესში განსაკუთრებით სენსიტიური, პირადი ხასიათის ინფორმაციების დაცვის კუთხით. მართალია პრაქტიკული თვალსაზრისით არ არის მარტივი, ინფორმაციის შეგროვება თავიდანვე მიზანმიმართულად გამოირიცხოს და ამდენად, ამ გარანტიის განხორციელება

ინფორმაციის მოპოვების ეტაპზე დაკავშირებულია გარკვეულ სირთულეებთან,[836] მაგრამ ერთი მხრივ, ასეთი გარანტიის არსებობა თავისთავად ნიშნავს ამ ინფორმაციის დაცვის პრიორიტეტულობას და მნიშვნელობას სისხლის სამართლის პროცესში და აკისრებს გარკვეულ მნიშვნელოვან ვალდებულებებს შესაბამის პირებს ღონისძიების განხორციელების ეტაპზე, ხოლო მეორე მხრივ, ამ მოთხოვნის შესრულების შეუძლებლობის შემთხვევაში, კანონმდებლობა ასევე მნიშვნელოვან ბერკეტს შეიცავს ასეთი მონაცემების გამოყენების აკრძალვის სახით და ამით უფრო მყარ გარანტიებს ქმნის საკანონმდებლო დონეზე ინტიმური ხასიათის ინფორმაციის გამოყენების აკრძალვის კუთხით. მართალია რთულია საკანონმდებლო დონეზე განსაზღვრულ იქნეს კრიტერიუმები, რომლებმაც უნდა უზრუნველყოს პირადი ცხოვრების ძირითადი სფეროს დაცვა,[837] თუმცა სამეცნიერო ლიტერატურაში გამოთქმული მოსაზრების თანახმად, ამ თვალსაზრისით უმთავრესად საჭიროა ფარული მიყურადების ობიექტის სწორად განსაზღვრა[838]. მხოლოდ ისეთი აბონენტის მიყურადებაა დასაშვები, რომელსაც უშუალო კავშირი აქვს კომუნიკაციის სათვალთვალო სამიზნე პირთან[839]; წინააღმდეგ შემთხვევაში დაუყოვნებლივ უნდა შეწყდეს მიყურადება.[840] აღსანიშნავია, რომ ისეთ ინტენსიურ და ტექნიკური თვალსაზრისით კომპლექსურ ღონისძიებასთან მიმართებით, როგორიცაა საინფორმაციო-ტექნოლოგიურ სისტემაში ფარული შეღწევა და სისტემაში შენახული ინფორმაციის მოპოვება (100d პარაგრაფი - ონლაინ ჩხრეკა), გერმანიის კანონმდებელი ასეთ კრიტერიუმად ასახელებს ტექნიკურ ზომებს, რომლითაც შესაძლებლობის მიხედვით, თავიდან უნდა იქნეს აცილებული პირადი ცხოვრების ძირითად სფეროს მიკუთვნებული ინფორმაციის მოპოვება.[841]

საბოლოო ჯამში, შეიძლება ითქვას, რომ პირადი ცხოვრების ძირითადი სფეროს დაცვის საკითხთან დაკავშირებით გერმანული გამოცდილება ქართული კანონმდებლობისთვის რელევანტურია იმის გათვალისწინებით, რომ სსსკ-ით არ არის გათვალისწინებული სპეციალური რეგულაცია ამ სფეროს მიკუთვნებული

[836] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 62-65.
[837] იქვე, 410-411.
[838] იქვე.
[839] იქვე.
[840] იქვე.
[841] StPO, §100d Abs. 3, 07/04/1987.

ინფორმაციის მოპოვების/გამოყენების აკრძალვის კუთხით და სსსკ განსაკუთრებულ დაცვას არ უქვემდებარებს პირადი ცხოვრების ინტიმურ სფეროს. მიგვაჩნია, რომ ამ საკითხის სპეციალური რეგულირება მეტად მნიშვნელოვანია და უკეთეს გარანტიებს შექმნიდა ადამიანის უფლებების დაცვის კუთხით,[842] მითუმეტეს, რომ საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებაში ხაზგასმულია პირადი ცხოვრების ინტიმური სფეროს განსაკუთრებული დაცვის იდეა და სასამართლოს ცალსახა პოზიცია, რომ „პირადი ცხოვრების ძირითადი სფერო - ადამიანის ინტიმური, სექსუალური ურთიერთობები, ოჯახური ცხოვრება, მისი ჩვევები, მოძღვრისთვის აღსარებისას მინდობილი ინფორმაცია, სამედიცინო გამოკვლევების შედეგები, ადამიანის ემოციები და გრძნობები, მათი პრივატულ სფეროში გამოხატვის ფორმები უნდა იყოს განსაკუთრებულად დაცული სახელმწიფოსა და ნებისმიერი მესამე პირის ზედამხედველობისგან.“[843]

1.3.7 ფარული საგამოძიებო მოქმედება „შემთხვევით პირებთან“ მიმართებით და „სხვა დანაშაულის“ ნიშნების გამოვლენისას

ფარული საგამოძიებო მოქმედება შეიძლება შეეხოს არა მარტო იმ პირს, ვინც წარმოადგენს ღონისძიების უშუალო ადრესატს, არამედ ასევე „შემთხვევით პირებსაც“.

2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით ქართულ კანონმდებლობაში გათვალისწინებულ ცვლილებებთან დაკავშირებით ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში ექსპერტთა მიერ გამოთქმულია კრიტიკული მოსაზრება, რომ „საქართველოს კანონმდებლობა არაფერს ამბობს იმ პირთა შესახებ ინფორმაციის ბედზე, რომელთა მიმართებითაც არ არსებობს დასაბუთებული ვარაუდი დანაშაულებრივ ქმედებაში

[842] აღნიშნულ საკითხთან დაკავშირებით იხ. ასევე *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 62-65.

[843] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-12.

მონაწილეობის შესახებ, თუმცა შემთხვევით აღმოჩნდნენ ბრალდებულთან კონტაქტში.“[844]

აღსანიშნავია, რომ სსსკ-ის 143[7] მუხლი, რომელიც არეგულირებს იმ პირის კომუნიკაციის მონიტორინგის შეზღუდვას, რომელსაც გამოძიებასთან კავშირი არ აქვს (143[7] მუხლის პირველი ნაწილი), არ განსაზღვრავს მტკიცებულების ბედს იმ შემთხვევაში, როდესაც მიუხედავად მინიმუმამდე დაყვანის მოთხოვნის დაცვისა, „გამოძიებასთან კავშირში არმყოფ პირებთან“ მიმართებით ინფორმაცია იქნება მოპოვებული. თუმცა ამ საკითხს ეხება სსსკ-ის 143[8] მუხლის პირველი ნაწილი, კერძოდ, ამ ნორმის პირველი წინადადება ითვალისწინებს იმ ინფორმაციის განადგურების მოთხოვნას, რომელსაც ღირებულება არ გააჩნია გამოძიებისათვის. მაგრამ სხვა ვითარებაა, როდესაც ინფორმაციას აქვს გარკვეული მტკიცებულებითი ღირებულება. ეს უკანასკნელი შემთხვევა სსსკ-ით არ არის ნათლად მოწესრიგებული. ამ საკითხთან დაკავშირებით საინტერესო იქნება საერთაშორისო გამოცდილების მოკლე მიმოხილვა.

ევროპული სასამართლოს მიერ დადგენილი სტანდარტის მიხედვით, ეროვნული სამართლით ნათლად უნდა იყოს დადგენილი შესაბამისი პროცედურა „შემთხვევითი პირების“ კომუნიკაციის ფარული მიყურადების შემთხვევაში, მაგალითად, ერთ-ერთ საქმეში კანონიერების პრინციპის დარღვევას სწორედ ის გარემოება დაედო საფუძვლად, რომ კანონმდებლობა არ განსაზღვრავდა რაიმე ზომების გათვალისწინების ვალდებულებას იმ პირებთან მიმართებით, რომლებსაც შემთხვევით მოუსმინეს, როგორც მიყურადებული საუბრის მონაწილეებს[845]; ევროპულმა სასამართლომ მიიჩნია, რომ ეროვნული დებულებები საკმარისი სიცხადით არ არეგულირებდა სახელმწიფო ორგანოების დისკრეციული უფლებამოსილების ფარგლებს ასეთ პირებთან მიმართებით.[846]

„შემთხვევითი პირების“ შესახებ ინფორმაციის პროცესუალური მიზნებით გამოყენებასთან დაკავშირებით საყურადღებოა ვენეციის კომისიის შეხედულება ფარული მეთვალყურეობის შესახებ პოლონეთის კანონმდებლობასთან

[844] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 22, <https://rm.coe.int/16806af19b> [20.06.2020].
[845] Amman v. Switzerland, [2000], ECHR 2000-II, 61.
[846] იქვე.

დაკავშირებულ ანგარიშში, სადაც კომისია უარყოფითად აფასებს საკანონმდებლო ცვლილებებს, რომლებმაც პროკურორს მიანიჭა დისკრეციული უფლებამოსილება, გადაწყვიტოს გამოყენებულ იქნეს თუ არა ფარული საგამოძიებო მოქმედების შედეგად „შემთხვევით პირებთან“ დაკავშირებით მოპოვებული ინფორმაცია სისხლის სამართლის პროცესში ამ პირების წინააღმდეგ[847]. ვენეციის კომისია აღნიშნავს, რომ ასეთ პირებთან მიმართებით მოპოვებული ინფორმაციის მტკიცებულებად გამოყენება შესაძლებელია მხოლოდ საგამონაკლისო წესით და მხოლოდ სასამართლოს გადაწყვეტილებით[848]. კომისიის შეხედულებით, „საეჭვოა ასეთი ინფორმაციის გამოყენება დასაშვები იყოს შედარებით უმნიშვნელო დანაშაულების შემთხვევაში“[849]. კომისია ასევე მიიჩნევს, რომ კანონმა საკმარისი სიცხადით უნდა განსაზღვროს, როდის არის დაუშვებელი ასეთი ინფორმაციის გამოყენება - მაგალითად, როდესაც შემთხვევით მოპოვებული ინფორმაცია შეეხება პრივილეგირებულ კომუნიკაციას.[850] კომისია ასევე აღნიშნავს, რომ პოლონეთის შესაბამისი პირების მიერ მიწოდებული განმარტებების თანახმად, ასეთ შემთხვევაში ინფორმაციის პროცესში გამოყენებასთან დაკავშირებით საკითხს წყვეტს სასამართლო მტკიცებულების დასაშვებობის ეტაპზე[851]. თუმცა ვენეციის კომისიის შეხედულებით, თუკი ასეთი პრაქტიკა არსებობს, ამის შესახებ პირდაპირ უნდა იყოს აღნიშნული კანონმდებლობაში და ამავდროულად, უნდა განისაზღვროს გარემოებები, როდესაც საქმიდან უნდა ამოირიცხოს ასეთი ინფორმაცია.[852]

ამდენად, განხილული საერთაშორისო სტანდარტებიდან გამომდინარე: 1) აუცილებელია კანონმდებლობამ მკაფიოდ დაარეგულიროს საგამოძიებო ორგანოების დისკრეციის ფარგლები და შესაბამისი პროცედურა იმ პირთა შესახებ ინფორმაციის მტკიცებულებად გამოყენებასთან დაკავშირებით, რომლებიც „შემთხვევით“ დაექვემდებარნენ კომუნიკაციის მონიტორინგს; 2) ასეთი ინფორმაციის სისხლის სამართლის პროცესში დაშვება, როგორც წესი, უნდა მოხდეს მხოლოდ შეზღუდულ

[847] European Commission for Democracy Through Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 20, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].
[848] იქვე.
[849] იქვე.
[850] იქვე.
[851] იქვე.
[852] იქვე.

შემთხვევებში და მხოლოდ სასამართლოს გადაწყვეტილებით; ამავდროულად, მისი გამოყენება არ არის გამართლებული ნებისმიერ დანაშაულთან ბრძოლის ინტერესებით და იმ შემთხვევაშიც, თუკი საკითხი მტკიცებულების დასაშვებობის ეტაპზე წყდება, აუცილებელია განისაზღვროს გარემოებები, როდესაც ეს ინფორმაცია არ უნდა იქნეს დაშვებული პროცესში, მაგალითად, ვენეციის კომისია ასეთ გარემოებას უკავშირებს შემთხვევას, როდესაც მოპოვებული ინფორმაცია ეხება პრივილეგირებულ კომუნიკაციას ან როდესაც დაკავშირებულია „უმნიშვნელო დანაშაულებთან.“

იგივე საკითხთან დაკავშირებით საყურადღებოა პროფესორი ალბრეხტის შეხედულებაც, რომელიც აღნიშნავს, რომ ფარული საგამოძიებო მოქმედებების მასალებში შეიძლება აღმოჩნდეს ინფორმაცია ან მტკიცებულება მესამე პირთა (რომლებიც არ წარმოადგენენ კონკრეტული გამოძიების მიზანს) მიერ ჩადენილ დანაშაულებთან დაკავშირებით[853]. როგორც წესი, „შემთხვევით“ აღმოჩენილი მტკიცებულებების მიმართ არსებობს მიდგომა, რომ ისინიც უნდა აკმაყოფილებდნენ ფარული საგამოძიებო მოქმედებების ჩატარების შესახებ ნებართვის მიმართ წაყენებულ მოთხოვნებს.[854]

საბოლოო ჯამში, ქართულ კანონმდებლობასთან დაკავშირებით შეიძლება ითქვას, რომ სსსკ-ით მოცემული საკითხი არ არის სათანადოდ რეგულირებული და პრობლემატურია მისი მიმართება კანონის „განჭვრეტადობის“ პრინციპთან, კერძოდ, სსსკ-ით არ არის მკაფიოდ და ნათლად განსაზღვრული იმ ინფორმაციის მტკიცებულებად გამოყენების საკითხი, რომელიც მართალია ეხება განჩინებაში აღნიშნულ დანაშაულს, (რომელთან დაკავშირებითაც მიმდინარეობს ფარული საგამოძიებო მოქმედება), მაგრამ ღონისძიების ობიექტის გარდა, ავლენს ასევე სხვა „შემთხვევითი პირების“ ამ დანაშაულში შესაძლო მონაწილეობის ფაქტს.

ამავდროულად, ამ საკითხის საკანონმდებლო რეგულირების პროცესში მნიშვნელოვანია, მხედველობაში იქნეს მიღებული ის რეკომენდაციები და მიდგომები, რომლებიც საერთაშორისო გამოცდილების გათვალისწინებით არსებობს,

---

[853] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 41, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[854] იქვე.

მაგალითად, ვენეციის კომისიის ზემოთაღნიშნული ანგარიშის თანახმად, ასეთი პირების წინააღმდეგ მოპოვებული მტკიცებულების გამოყენება არ უნდა წარმოადგენდეს ზოგად წესს და ამასთან, ნებისმიერ დანაშაულთან დაკავშირებით ამ ინფორმაციის გამოყენება პრობლემატურია; როგორც პროფესორი ალბრეხტი აღნიშნავს, ზოგადი სტანდარტის მიხედვით, ასეთ შემთხვევაზე უნდა გავრცელდეს იგივე მოთხოვნები, რაც ფარული საგამოძიებო მოქმედების ჩატარების შესახებ ნებართვის განჩინებაზე. აქედან გამომდინარე, ლოგიკური და მართებული იქნება, თუ ვიტყვით, რომ როგორც მინიმუმ, გათვალისწინებული უნდა იქნეს გარკვეული ფარგლებით ასეთი ინფორმაციის სისხლის სამართლის პროცესში დაშვების შეზღუდვა.

კიდევ ერთი წინააღმდეგობრივი საკითხი უკავშირდება ისეთ შემთხვევას, როდესაც ღონისძიების განხორციელების პროცესში იკვეთება სხვა დანაშაულის ნიშნები, რომელიც არ არის სასამართლოს განჩინებაში აღნიშნული. ამ თვალსაზრისით აღსანიშნავია სსსკ-ის 143[3] მუხლის მე-9 ნაწილი, რომლის თანახმად, თუ „ფარული საგამოძიებო მოქმედებით გამოვლინდა სხვა დანაშაულის ნიშნები, რომელზედაც არ მიმდინარეობს გამოძიება, ამ ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაცია არის სხვა სისხლის სამართლის საქმეზე გამოძიების დაწყების საფუძველი, ხოლო ამ ინფორმაციის ახალ საქმეზე დასაშვებ მტკიცებულებად ცნობის საკითხი გადაწყდება სსსკ-ით დადგენილი ზოგადი წესით, ფარული საგამოძიებო მოქმედებისათვის 143[3] მუხლის მე-2 ნაწილით განსაზღვრული გარემოებების გაუთვალისწინებლად.“

ამ კუთხით აღსანიშნავია, რომ მართალია სსსკ-ის 143[3] მუხლის მე-9 ნაწილი განსაზღვრავს „სხვა დანაშაულთან“ დაკავშირებით მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენების წესს, მაგრამ არაფერს ამბობს ასეთი მტკიცებულების გამოვლენის შემდეგ როგორ უნდა გაგრძელდეს დაწყებული ღონისძიება, კერძოდ, როდესაც დადგინდება, რომ რეალურად სხვა დანაშაულის ნიშნებს აქვს ადგილი და არა სასამართლოს ნებართვაში აღნიშნულს, უნდა შეწყდეს თუ არა ფარული საგამოძიებო მოქმედება და მის გასაგრძელებლად სასამართლოს

ახალი განჩინება იქნეს მოპოვებული, თუ გაგრძელდეს სასამართლოს ნებართვით გათვალისწინებული ვადით.[855]

მეორე საკითხია, რამდენად მართებულია, რომ სსსკ-ის 143[3] მუხლის მე-9 ნაწილი საშუალებას იძლევა მოპოვებული მტკიცებულება გამოყენებულ იქნეს იმ დანაშაულებთან დაკავშირებითაც, რომლებიც არ მიეკუთვნება სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტით განსაზღვრულ ჩამონათვალს; სსსკ-ის 143[3] მუხლის მე-9 ნაწილი ითვალისწინებს ასეთ შესაძლებლობას, რაც შეიცავს სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტისათვის გვერდის ავლის საფრთხეს და წარმოადგენს იმ დანაშაულებთან დაკავშირებით ღონისძიების განხორციელების შესაძლებლობას, რომელთან მიმართებით ეს სსსკ-ით დაშვებული არ არის. როგორც კვლევაში გამოიკვეთა, ფარული საგამოძიებო მოქმედების განხორციელების უფლებამოსილება მხოლოდ საამისოდ სპეციალურად დადგენილ „სერიოზულ“ დანაშაულებთან დაკავშირებით წარმოადგენს ერთ-ერთ ფუნდამენტურ მოთხოვნას ამ სფეროს მარეგულირებელი კანონმდებლობის მიმართ და თანაზომიერების პრინციპის უმნიშვნელოვანეს გამოხატულებას. მეორე მხრივ, დასახელებული საკითხი არ არის მარტივი გადასაწყვეტი იმდენად, რამდენადაც თუკი შესაბამისი საგამოძიებო ორგანოსთვის ცნობილი ხდება დანაშაულის შესახებ ინფორმაცია, სსსკ-ის მე-100 მუხლიდან გამომდინარე, მის ვალდებულებას წარმოადგენს დაიწყოს გამოძიება. ამდენად, თუკი ფარული საგამოძიებო მოქმედების განხორციელების დროს შესაბამის სახელმწიფო ორგანოს არ ექნება შესაძლებლობა, სხვა დანაშაულის ნიშნების გამოვლენისას (გარდა იმისა, რომელიც კანონმდებლობით გათვალისწინებულია ფარული საგამოძიებო მოქმედების განხორციელების საფუძვლად) რეაგირება მოახდინოს, მოუწევს „თვალი დახუჭოს“ დანაშაულზე და შესაბამისად, მის ვალდებულებაზეც დანაშაულთან ბრძოლის კუთხით. მიუხედავად ამისა, გათვალისწინებულ უნდა იქნეს იმ ინტერესის მნიშვნელობა, რომლის დაცვასაც ემსახურება სსსკ-ის 143[3] მუხლის მე-2 ნაწილის „ა“ ქვეპუნქტი; ამ შემთხვევაში საქმე ეხება ადამიანის უფლებებში ჩარევის სსსკ-ით გათვალისწინებულ ერთ-ერთ ყველაზე

[855] აღნიშნულ საკითხთან დაკავშირებით იხ. Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime, UN Office on Drugs and Crime, 2009, 23, <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf> [25.06.2020].

მძიმე ფორმას და ფუნდამენტური მნიშვნელობის საპროცესო გარანტიას ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით, რაც ასეთი ღონისძიების მხოლოდ სპეციალურად განსაზღვრული, საკმარისად წონადი სამართლებრივი სიკეთის დაცვის მიზნით გამოყენების შესაძლებლობაში გამოიხატება, იმისდა მიუხედავად, თუ რამდენად გამოსადეგი შეიძლება იყოს ასეთი ღონისძიება სსკ-ით გათვალისწინებულ სხვა დანაშაულებთან მიმართებით; ეს მიდგომა გამომდინარეობს თანაზომიერების პრინციპიდან, რომელიც ფარული საგამოძიებო მოქმედების განხორციელების შესაძლებლობას უშვებს მხოლოდ მაშინ, როდესაც ის მკაცრად აუცილებელია და აკმაყოფილებს თანაზომიერების ტესტის ყველა ელემენტს. სამეცნიერო ლიტერატურაში გამოთქმული მოსაზრების მიხედვით, თანაზომიერების პრინციპი მოიაზრებს, რომ მონაცემთა გამოყენება და გამჟღავნება შეზღუდულია ლეგიტიმური მიზნით, რომელიც საფუძვლად დაედო მათ მოპოვებას, მაგალითად, მოპოვებული ინფორმაციის გამოყენება უნდა შეიზღუდოს, როგორც მინიმუმ, ისეთივე სიმძიმის დანაშაულთა გამოძიების ინტერესებით, რომელთან დაკავშირებითაც იქნა მოპოვებული.[856]

ამასთან, ამ შემთხვევაშიც საყურადღებოა პროფესორი ალბრეხტის ზემოთ აღნიშნული მოსაზრება, რომ, როგორც წესი, „შემთხვევით“ აღმოჩენილი მტკიცებულებების მიმართ არსებობს მიდგომა, რომ ისინიც უნდა აკმაყოფილებდნენ ფარული საგამოძიებო მოქმედებების ჩატარების შესახებ ნებართვის მიმართ წაყენებულ მოთხოვნებს.

საბოლოო ჯამში, მიზანშეწონილი იქნებოდა, მოცემულ საკითხთან დაკავშირებით ასევე გათვალისწინებულ იქნეს მოპოვებული მტკიცებულების შეზღუდულად გამოყენების შესაძლებლობა და როგორც მინიმუმ, გარკვეული ფარგლებით ასეთი ინფორმაციის სისხლის სამართლის პროცესში დაშვების შეზღუდვა; მაგალითისთვის, კონკრეტული საგამოძიებო მოქმედების შედეგად მოპოვებული მტკიცებულების სხვა სისხლის სამართლის საქმეზე გამოყენების

[856] *Dempsey J., X.; Gate F., H.,* Recommendations for Government and Industry, წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.),* Oxford, 2017, 428.

შეზღუდული შესაძლებლობა არის დადგენილი გერმანიის სისხლის სამართლის საპროცესო კოდექსის 479-ე პარაგრაფით.[857]

1.4 მოპოვებული მასალის შენახვისა და განადგურების საკითხი

ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურების წესსა და პროცედურას არეგულირებს სსსკ-ის 143[8] მუხლი. ნაშრომში უკვე განხილულ იქნა მონაცემთა განადგურებასთან დაკავშირებული ცალკეული ასპექტები მინიმუმამდე დაყვანის მოთხოვნასა და მოპოვებული მასალის გადარჩევის პროცედურასთან მიმართებით, რაზეც აქ აღარ შევჩერდებით.

უნდა აღინიშნოს, რომ სსსკ-ის 143[8] მუხლი ითვალისწინებს საკმაოდ დეტალურ დებულებებს ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებული ინფორმაციის განადგურების შესახებ.[858] ეს მუხლი არეგულირებს სხვადასხვა სახის მონაცემთა განადგურების განსხვავებულ პროცედურას, კერძოდ, გათვალისწინებულია მონაცემთა განადგურების შემდეგი წესები მონაცემთა ტიპების მიხედვით:

1) გამოძიებისათვის ღირებულების არმქონე ინფორმაცია - როგორც უკვე აღინიშნა, ასეთი ინფორმაცია ღონისძიების დასრულების ან შეწყვეტის შემდეგ დაუყოვნებლივ ნადგურდება პროკურორის გადაწყვეტილებით (სსსკ-ის 143[8] მუხლის პირველი ნაწილი);

- ინფორმაცია, რომელიც გადაუდებელი აუცილებლობისას მოსამართლის განჩინების გარეშე ჩატარდა და, მიუხედავად სასამართლოს მიერ მისი კანონიერად ცნობისა, ბრალდების მხარემ სსსკ-ის 83-ე მუხლით დადგენილი წესით არ წარუდგინა მტკიცებულებად საქმის არსებითად განმხილველ სასამართლოს (სსსკ-ის 143[8] მუხლის პირველი ნაწილი);

- ოპერატიულ-სამძებრო ღონისძიების შედეგად მოპოვებული მასალა, რომელიც არ ეხება პირის დანაშაულებრივ საქმიანობას, მაგრამ შეიცავს ცნობებს მისი ან სხვა პირის პირადი ცხოვრების შესახებ და ექვემდებარება განადგურებას „ოპერატიულ-

[857] StPO, §479, 07/04/1987.

[858] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 22-23, <https://rm.coe.int/16806af19b> [20.06.2020].

სამშებრო საქმიანობის შესახებ“ საქართველოს კანონის შესაბამისად; ასეთ ინფორმაციასთან მიმართებით ასევე გათვალისწინებულია დაუყოვნებლივ განადგურების მოთხოვნა (სსსკ-ის 143[8] მუხლის პირველი ნაწილი).

სამივე აღნიშნული სახის ინფორმაცია სსსკ-ის 143[8] მუხლის მე-5 ნაწილიდან გამომდინარე, ნადგურდება შესაბამისი საქმის გამოძიებაზე საპროცესო ზედამხედველობის განმახორციელებელი/სახელმწიფო ბრალდების მხარდამჭერი ან მათი ზემდგომი პროკურორის მიერ, იმ მოსამართლის/სასამართლოს მოსამართლის თანდასწრებით, რომელმაც ან რომლის მოსამართლემაც მიიღო გადაწყვეტილება აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ ან გადაუდებელი აუცილებლობისას ჩატარებული ღონისძიების კანონიერად ან უკანონოდ ცნობის შესახებ. ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალის განადგურების შესახებ დგება ოქმი, რომელიც გადაეცემა ინსპექტორის სამსახურს, ხოლო ინსპექტორის სამსახურის წარმოებაში არსებულ სისხლის სამართლის საქმეზე – ზედამხედველ მოსამართლეს და აისახება ფარული საგამოძიებო მოქმედებების სასამართლო რეესტრში (სსსკ-ის 143[8] მუხლის მე-5 ნაწილი);

ამავე მუხლით დადგენილი წესით ნადგურდება ასევე ინფორმაცია, რომელიც მოპოვებულია გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული ღონისძიების შედეგად და მის მტკიცებულებად გამოყენებას ბრალდების მხარე არ მიიჩნევს საჭიროდ. ასეთ შემთხვევაში ბრალდების მხარე ვალდებულია მიმართოს სასამართლოს საგამოძიებო მოქმედების კანონიერად ცნობის შუამდგომლობით მისი დაწყებიდან 24 საათის განმავლობაში, ხოლო მოპოვებული ინფორმაცია დაუყოვნებლივ განადგურებას ექვემდებარება (143[3] მუხლის მე-8 ნაწილი).

2) ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალა, რომელიც დაუშვებლად არის ცნობილი სასამართლოს მიერ - ასეთი ინფორმაცია განადგურდება საბოლოო ინსტანციის სასამართლოს მიერ საქმეზე განაჩენის გამოტანიდან 6 თვის გასვლის შემდეგ, დაუყოვნებლივ. ხოლო განადგურებამდე ინახება სასამართლოს სპეციალურ საცავში. დაუშვებელია აღნიშნული მასალის გაცნობა, ასლის გადაღება და გამოყენება, გარდა მისი მხარეთა მიერ საპროცესო უფლებამოსილების განსახორციელებლად გამოყენებისა (სსსკ-ის 143[8] მუხლის მე-2 ნაწილი);

3) ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალა, რომელიც საქმეს ნივთიერ მტკიცებულებად დაერთვის - სსსკ-ის შესაბამისად, ასეთი

ინფორმაცია შეინახება სასამართლოში ამ სისხლის სამართლის საქმის შენახვის ვადით და ამ ვადის გასვლის შემდეგ დაუყოვნებლივ ნადგურდება (სსსკ-ის 143[8] მუხლის მე-3 ნაწილი);

ზემოაღნიშნულ ორივე შემთხვევაში ინფორმაციას ანადგურებს ის მოსამართლე ან იმ სასამართლოს მოსამართლე, რომელმაც ან რომლის მოსამართლემაც მიიღო გადაწყვეტილება აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების თაობაზე ან გადაუდებელი აუცილებლობისას მოსამართლის განჩინების გარეშე ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად/უკანონოდ ცნობის შესახებ (სსსკ-ის 143[8] მუხლის მე-6 ნაწილი); ხოლო მონაცემთა განადგურებამდე მის სათანადოდ დაცვისათვის პასუხისმგებლობა ეკისრება იმ სასამართლოს ადმინისტრაციას, სადაც ინახებოდა ეს მასალა (სსსკ-ის 143[8] მუხლის მე-4 ნაწილი).

როგორც პროფესორი ალბრეხტი ფარული საგამოძიებო მოქმედებების შესახებ დასკვნაში აღნიშნავს, თანაზომიერების პრინციპის დამკვიდრება ხდება ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურებითაც (წაშლით)[859]. განადგურებისთვის დადგენილი ვადები უნდა იყოს ორიენტირებული იმაზე, თუ რამდენად მართლზომიერად არის ისინი მოპოვებული ან რამდენად არის ისინი შემდგომი საპროცესო მოქმედებებისთვის საჭირო[860]. ამავე დასკვნის მიხედვით, მონაცემთა განადგურების გარემოება უნდა აღირიცხოს და მკაფიოდ დასტურდებოდეს მონაცემთა განადგურების ფაქტი.[861] აღსანიშნავია, რომ სსსკ ითვალისწინებს ამ რეკომენდაციებს;[862] 143[8] მუხლი ადგენს მონაცემთა განადგურების სხვადასხვა ვადას და პროცედურას მონაცემთა ტიპების მიხედვით; ამავდროულად, მონაცემთა განადგურების ფაქტი ფიქსირდება ოქმში, რომელიც კოდექსით გათვალისწინებულ შესაბამის პირებს გადაეცემათ (სსსკ-ის 143[8] მუხლის მე-5 ნაწილი). მნიშვნელოვანია ასევე, რომ მონაცემები, რომელთა განადგურების შესახებ გადაწყვეტილებასაც პროკურორი იღებს, ნადგურდება იმ

---

[859] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 41, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[860] იქვე.

[861] იქვე.

[862] იხ. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 375.

სასამართლოს/მოსამართლის მონაწილეობით, რომელმაც მიიღო გადაწყვეტილება კონკრეტულ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით.

აღსანიშნავია, რომ მონაცემთა განადგურებასთან დაკავშირებული საპროცესო რეგულაციები დადებითად არის შეფასებული ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში[863], თუმცა ამავე დასკვნაში ხაზგასმულია ის საკითხებიც, რომლებიც პრობლემატურია მონაცემთა უსაფრთხოების თუ მონაცემთა დამუშავების კუთხით[864]. კერძოდ, გამოხატული მოსაზრების თანახმად, საპროცესო კოდექსის დებულებებმა შესაძლოა პრაქტიკაში „არც იმუშაოს“ - ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებული ინფორმაცია ძირითადად არის ციფრულ ფორმატში, ეს ეხება როგორც ელექტრონულ კომუნიკაციებს (შინაარსობრივს და მეტადატას), ასევე აუდიო-ვიდეო ჩანაწერებს, ტროიანის და სხვა ჯაშუში პროგრამების მეშვეობით ღონისძიების ადრესატის კომპიუტერიდან და მობილური ტელეფონიდან მოპოვებულ ინფორმაციას.[865]

ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში ექსპერტთა განმარტებით, მნიშვნელოვანია ტექნიკურ დონეზე იქნეს უზრუნველყოფილი, რომ ფარული საგამოძიებო მოქმედების შედეგად მონაცემების მოპოვება და ჩაწერა განხორციელდეს „გადამოწმებადი“ და „გაუყალბებელი“ სახით[866], ასევე მოპოვებული მონაცემების შენახვა მოხდეს იმგვარად, რომ უზრუნველყოფილი იყოს მხოლოდ სამი ავტორიზებული ასლის შექმნა: ერთი - შესაბამისი სახელმწიფო ხელისუფლების წარმომადგენლებისთვის, ერთი - დაცვის მხარისთვის და მესამე თანაბრად დალუქული ასლი - მტკიცებულების გაყალბების ფაქტის გამოსარიცხად და მის ავთენტურობასთან დაკავშირებული დავის გადასაწყვეტად[867]. ამასთანავე, ტექნიკურ დონეზე უნდა იქნეს უზრუნველყოფილი, რომ სხვა არაავტორიზებული ასლი (გარდა ზემოთაღნიშნული სამი ასლისა) არ

[863] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 20-21, <https://rm.coe.int/16806af19b> [20.06.2020].
[864] იქვე.
[865] იქვე.
[866] იქვე, 21.
[867] იქვე.

შეიქმნება და არაავტორიზებული ასლის შექმნის ნებისმიერი მცდელობა, თავის მხრივ, ტექნიკურად იქნება დაფიქსირებული[868]. დასკვნის მიხედვით, შემოთავაზებული საკანონმდებლო რეგულაციების დონეზე უნდა იქნეს გათვალისწინებული მოცემული ტექნიკური ზომების გატარების საკითხი, ხოლო ამ მოთხოვნების დარღვევისათვის გათვალისწინებული უნდა იქნეს მკაცრი პასუხისმგებლობა.[869]

როგორც ზემოთ უკვე აღინიშნა, კიდევ ერთი მნიშვნელოვანი ასპექტი, რომელიც პრობლემატურად იქნა დანახული ზემოთაღნიშნულ დასკვნაში, უკავშირდება მონაცემთა დამუშავებას. ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში ექსპერტები მიიჩნევენ, რომ ქართულ კანონმდებლობაში ჯერ კიდევ ბევრია გასაკეთებელი სახელმწიფო ხელისუფლების ორგანოებს შორის მონაცემთა გადაცემის, მონაცემთა შემოწმების (სქრინინგის), შესაბამისობისა და ერთმანეთთან დაკავშირების, ისევე როგორც შენახვის პერიოდში მათი მთლიანობისა და კონფიდენციალურობის შენარჩუნების მიზნით[870]; ამდენად, აღნიშნული ეხება პროცედურას მონაცემთა მოპოვებასა და განადგურებას შორის. ეს საკითხები უფლებამოსილების ბოროტად გამოყენების კუთხით არანაკლებ რისკის შემცველია, ვიდრე მონაცემთა განადგურების მოთხოვნის შეუსრულებლობა.[871] ექსპერტები აღნიშნავენ, რომ დასახელებულ ასპექტებთან დაკავშირებით საკანონმდებლო ცვლილებები დუმს, მიუხედავად იმისა, რომ ამ საკითხების დეტალურად რეგულირება წარმოადგენს ევროპული სასამართლოს მოთხოვნას.[872]

ასევე უნდა აღინიშნოს მონაცემთა შენახვის აუცილებლობაზე განგრძობად ზედამხედველობასთან დაკავშირებული მოთხოვნის არარსებობა სსსკ-ში. როგორც ზემოთ განვიხილეთ, მონაცემთა შემდგომი შენახვის პერიოდული გადამოწმება ერთ-ერთ იმ ასპექტს განეკუთვნება, რომელზედაც ევროპული სასამართლო ყურადღებას ამახვილებს; მაგალითად, ერთ-ერთ საქმეში ევროპულმა სასამართლომ მოიწონა ეროვნული კანონმდებლობა, რომელიც აღნიშნულ საკითხს დეტალურად

[868] იქვე.
[869] იქვე.
[870] იქვე. 22.
[871] იქვე.
[872] იქვე.

არეგულირებდა - უწყებას, რომელიც ინახავდა მონაცემებს, ეკისრებოდა აღნიშნული მონაცემების შემდგომი შენახვის აუცილებლობის გადამოწმება ყოველ ექვს თვეში ერთხელ. თუკი თავდაპირველი ლეგიტიმური მიზნის მისაღწევად მონაცემთა შენახვა დაკარგავდა საჭიროებას, მონაცემები უნდა განადგურებულიყო, წაშლილიყო, ან მინიმუმ, მათზე წვდომა უნდა შეზღუდულიყო. ამასთან, განადგურების პროცედურა ფორმდებოდა ოქმის შედგენით.[873] საყურადღებოა, რომ მოპოვებული მასალის შემდგომი შენახვის აუცილებლობის გონივრული პერიოდულობით გადასინჯვის საკანონმდებლო დონეზე უზრუნველყოფის მნიშვნელობას სასამართლომ სხვა შემთხვევაშიც გაუსვა ხაზი.[874] რაც შეეხება ქართულ კანონმდებლობას, მართალია სსსკ-ის 143[8] მუხლი განსაზღვრავს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალის განადგურების წესებს ცალკეულ შემთხვევებში, თუმცა აღნიშნული საგამოძიებო მოქმედებების მარეგულირებელი დებულებები არ შეიცავს რაიმე მითითებას მოპოვებული ინფორმაციის შენახვის აუცილებლობის პერიოდულ გადამოწმებასთან დაკავშირებით, რაც იმას ნიშნავს, რომ მოპოვებული ინფორმაციის შემდგომი შენახვის საჭიროების შეფასებაზე განგრძობადი მეთვალყურეობის მოთხოვნა სსსკ-ით განსაზღვრული არ არის.[875]

1.5 მონაცემთა სხვა პირებისათვის გადაცემა

ფარული საგამოძიებო მოქმედებების მომწესრიგებელი ეროვნული კანონმდებლობის მიმართ ევროპული სასამართლოს ერთ-ერთ მნიშვნელოვან მოთხოვნას მოპოვებული მონაცემების სხვა პირებისათვის გადაცემის წესის ზედმიწევნით რეგულირება წარმოადგენს. როგორც უკვე აღინიშნა, ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნის მიხედვით, აღნიშნული მიეკუთვნება ერთ-ერთ იმ ასპექტს, რომელსაც საქართველოს კანონმდებლობა არ აწესრიგებს.[876] მონაცემთა სხვა პირებისათვის

[873] Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI , 100.
[874] Kennedy v. United Kingdom, [2010] ECtHR, 164.
[875] *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, (რედ.), მერიდიანი, თბ., 2019, 390.
[876] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 22, <https://rm.coe.int/16806af19b> [20.06.2020].

გადაცემის შემთხვევაში მნიშვნელოვანია ეროვნულ კანონმდებლობაში გათვალისწინებული იყოს ზომები, რომლებიც უზრუნველყოფენ მონაცემთა სხვა სახელმწიფო ორგანოებისათვის უსაფრთხოდ გადაცემას და ამასთან, მხოლოდ იმ მოცულობით, რაც ინფორმაციის მიმღებ ორგანოს მისთვის კანონმდებლობით დაკისრებული ფუნქციების შესასრულებლად ესაჭიროება.[877]

როგორც უკვე აღინიშნა, მონაცემთა გადაცემის საკითხი სსსკ-ით მოწესრიგებული არ არის, მაგალითად, სსსკ არ განსაზღვრავს ფარული საგამოძიებო მოქმედების ტექნიკურად აღსრულებაზე პასუხისმგებელი ორგანოს - სააგენტოს და შესაბამის საგამოძიებო ორგანოს შორის მოპოვებული ინფორმაციის მიმოცვლის პროცედურას - სააგენტოს მიერ მოპოვებული ინფორმაციის გამოძიების მწარმოებელი შესაბამისი ორგანოსათვის გადაცემის წესს, სააგენტოში აღნიშნული ინფორმაციის შენახვის ვადას და გამოძიების ორგანოსათვის ინფორმაციის გადაცემის შემდეგ სააგენტოში შენახული ეგზემპლარის განადგურებას მოთხოვნას, ასევე მონაცემთა უსაფრთხოდ გადაცემის მიზნით შესაბამის მოთხოვნებს.

რაც შეეხება სხვა საგამოძიებო ორგანოსათვის ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის გადაცემას, აღნიშნული საკითხი სსსკ-ის მიხედვით, ასევე არ არის სპეციალურად რეგულირებული. ნიშანდობლივია, რომ მონაცემთა გადაცემის საკითხი რელევანტურია აგრეთვე სსსკ-ის 143^3 მუხლის მე-9 ნაწილთან მიმართებითაც, რომელიც აწესრიგებს მტკიცებულების გამოყენების საკითხს იმ დანაშაულის ნიშნების გამოვლენისას, რომელზეც არ მიმდინარეობს გამოძიება.

აღსანიშნავია, რომ ზოგადი წესის თანახმად, დაუშვებელია მონაცემთა შემდგომი დამუშავება თავდაპირველი მიზნისგან განსხვავებული მიზნით.[878] გამონაკლისია ევროკავშირის 2016 წლის „საპოლიციო დირექტივით“ და საქართველოს საპროცესო კანონმდებლობით, სამართალწარმოებაში მონაწილე პირების პერსონალური მონაცემების დამუშავება თავდაპირველი მიზნისგან განსხვავებული მიზნით, როდესაც ეს არის აუცილებელი, კანონიერი და პროპორციული ზომა.[879] ისეთ

[877] Roman Zakharov v. Russia, [2015] ECtHR, 253; Kennedy v. United Kingdom, [2010] ECtHR, 163.

[878] *ფაფიაშვილი ლ.,* სისხლის სამართალწარმოებაში პერსონალური მონაცემების დაცვის ევროპეიზაციის ტენდენციები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *(რედ.)*, მერიდიანი, თბ., 2019, 590.

[879] იქვე.

საკითხებთან დაკავშირებით, როგორიცაა მაგალითად, ფარული საგამოძიებო მოქმედებები, ევროკავშირის 2016 წლის „საპოლიციო დირექტივიდან“ გამომდინარე, დასაშვებია „მიზნის შეზღუდვის“ პრინციპის (რომელიც მოითხოვს მონაცემთა დამუშავებას მხოლოდ იმ მიზნის შესაბამისად, რომელთან დაკავშირებითაც იქნა შეგროვებული და ასევე მონაცემთა შეგროვებას მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული მიზნით) მოქნილად გამოყენების შესაძლებლობა.[880] კონკრეტული სისხლის სამართლის საქმეში მოპოვებული ინფორმაცია შესაძლოა მეტად გამოსადეგი აღმოჩნდეს სხვა სამომავლო საქმეებისთვის.[881]

მონაცემთა სხვა ორგანოსთვის გადაცემის თვალსაზრისით საქმეზე ვებერი და სარავია გერმანიის წინააღმდეგ (Weber and Saravia v. Germany), ევროპულმა სასამართლომ რამდენიმე გარემოებაზე გაამახვილა ყურადღება, კერძოდ, გერმანიის კანონმდებლობის მიხედვით, მონაცემთა გადაცემა სხვა ორგანოსათვის დასაშვები იყო მხოლოდ სპეციალურად განსაზღვრული მძიმე დანაშაულების შემთხვევაში; მონაცემთა გადაცემის ფაქტი ფიქსირდებოდა ოქმით; მონაცემთა გადაცემის პროცესზე გათვალისწინებული იყო ეფექტიანი ზედამხედველობა დამოუკიდებელი ორგანოს მხრიდან.[882]

ამდენად, მნიშვნელოვანია, ერთი მხრივ, სსსკ განსაზღვრავდეს მონაცემთა სხვა საგამოძიებო ორგანოსათვის გადაცემის წესსა და პროცედურას, ხოლო მეორე მხრივ, აღნიშნული რეგულაცია პასუხობდეს ამ საკითხთან დაკავშირებით ევროპული სასამართლოს მიერ ჩამოყალიბებულ მიდგომებს.

1.6 ქვეთავების 1.4 და 1.5 შეჯამება

ამდენად, ფარული საგამოძიებო მოქმედებების შედეგად მოპოვებული ინფორმაციის განადგურების საკითხთან დაკავშირებით გამოიკვეთა, რომ სსსკ საკმაოდ დეტალურ რეგულაციებს შეიცავს, თუმცა არსებობს რიგი მნიშვნელოვანი საკითხები, რომლებიც ისევ პრობლემატურია. ევროპის საბჭოს ადამიანის უფლებათა

[880] Handbook on European Data Protection Law, 2018, 283, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> [25.06.2020].
[881] იქვე.
[882] Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 123-129; იხ. ასევე Association for European Integration and Human Rights and Ekimdzhiev v. Moldova, [2007], ECtHR, 89.

დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში ექსპერტების შეფასებით, ერთ-ერთ საკითხს, რომელიც ღიად არის დატოვებული კანონმდებლობით, განეკუთვნება მოპოვებული მასალის არაავტორიზებული ასლის შექმნის პრევენციისა და გაყალბებისგან დაცვასთან დაკავშირებული ზომების ტექნიკურ დონეზე უზრუნველყოფა. ასეთი ზომების გატარების მოთხოვნა საკანონმდებლო დონეზე უნდა იქნეს გათვალისწინებული.

პრინციპულად მნიშვნელოვან საკითხს წარმოადგენს მონაცემთა დამუშავება; როგორც კვლევაში განხილულ იქნა, მონაცემთა გადარჩევის (შემოწმების) წესები საჭიროებს სათანადოდ რეგულირებას სსსკ-ში; ამ საკითხს ეხმიანება ასევე ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაც, რომლის მიხედვითაც, სსსკ ყურადღებას არ ამახვილებს მონაცემთა მოპოვებასა და განადგურებას შორის პროცედურაზე, როგორიცაა სახელმწიფო ხელისუფლების ორგანოებს შორის მონაცემთა გადაცემა, მონაცემთა შემოწმება (სქრინინგი), ისევე როგორც შენახვის პერიოდში მათი მთლიანობისა და კონფიდენციალურობის შენარჩუნება.

ასევე პრობლემატურ ასპექტად გამოიკვეთა მონაცემთა შემდგომი შენახვის აუცილებლობაზე განგრძობადი კონტროლის რეგულირება; ევროპული სასამართლოს პრაქტიკიდან გამომდინარე, ამ საკითხის მოწესრიგება სსსკ-ში მეტად მნიშვნელოვანია.

მნიშვნელოვანია აგრეთვე სსსკ-ში დარეგულირდეს მონაცემთა სხვა სახელმწიფო ორგანოსათვის გადაცემის საკითხი. ამ თვალსაზრისით, მიგვაჩნია, რომ შესაბამის მოწესრიგებას საჭიროებს საგამოძიებო ორგანოსა და სააგენტოს შორის ინფორმაციის გადაცემის წესები, სააგენტოში აღნიშნული ინფორმაციის შენახვის ვადა და გამოძიების ორგანოსათვის ინფორმაციის გადაცემის შემდეგ სააგენტოში შენახული ეგზემპლარის განადგურების ასპექტი, ასევე მონაცემთა უსაფრთხოდ გადაცემის მიზნით შესაბამისი მოთხოვნები. რაც შეეხება სხვა საგამოძიებო ორგანოსათვის მონაცემთა გადაცემას, ევროპული სტანდარტის მიხედვით, ეს საკითხი ასევე ნათლად უნდა იყოს განსაზღვრული. ევროპული სასამართლოს პრაქტიკიდან გამომდინარე, მნიშვნელოვანია მონაცემთა გადაცემის გარკვეულწილად შეზღუდვა დანაშაულთა წრით, გადაცემის პროცედურაზე ეფექტიანი ზედამხედველობის განხორციელება და გადაცემის ფაქტების აღრიცხვა.

1.7 შეტყობინების ვალდებულება

სამართლებრივი დაცვის შესაძლებლობა და კონტროლის მექანიზმები დამოკიდებულია იმაზე, თუ რამდენად არის პირი ინფორმირებული მის წინააღმდეგ ფარული საგამოძიებო მოქმედების განხორციელების შესახებ.[883] შეტყობინების მოთხოვნას უაღრესად მნიშვნელოვანი როლი ეკისრება ფარული საგამოძიებო მოქმედების გამჭვირვალობისა და ანგარიშვალდებულების უზრუნველყოფად, ხოლო უფლების ბოროტად გამოყენების შემთხვევაში, შესაძლოა იქცეს პირის სამართლებრივი დაცვის უპირველეს წინაპირობად.[884] როგორც პროფესორი ალბრეხტი აღნიშნავს, ტელესაკომუნიკაციო მიყურადებისა და თვალთვალის ღონისძიებები შეიძლება შეეხოს ძალიან ბევრ პირს, რაც შეტყობინების კუთხით სხვადასხვა პრობლემებს წარმოშობს[885]. ერთი მხრივ, აღნიშნულმა შეიძლება გაართულოს სამართალწარმოების ეკონომიურობის პრინციპის დაცვა, ხოლო მეორე მხრივ, დაარღვიოს მიყურადების ობიექტის ინტერესები, განსაკუთრებით იმ შემთხვევაში, თუ არ წარმოადგენდა თვალთვალის ძირითად ობიექტს.[886] ყველა ამ ე.წ. „მესამე პირთა" შეტყობინება მრავალ სირთულესთანაა დაკავშირებული.[887] აღნიშნულიდან გამომდინარე, მიზანშეწონილად მიიჩნევა მხოლოდ იმ პირთა ინფორმირება, რომელთაც უშუალოდ ეხებოდათ კონკრეტული ღონისძიება.[888]

შეტყობინებასთან დაკავშირებული საკითხები მოწესრიგებულია სსსკ-ის 143[9] მუხლით. ამავე მუხლის მე-3 ნაწილი შეტყობინების ადრესატად განსაზღვრავს პირს, რომლის მიმართაც ჩატარდა ფარული საგამოძიებო მოქმედება. ამდენად, ქართული კანონმდებლობის მიხედვით, შეტყობინება სავალდებულოა მხოლოდ იმ პირის, რომელიც წარმოადგენდა ფარული საგამოძიებო მოქმედების ობიექტს. აღნიშნულ

---

[883] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 40, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[884] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 19,<https://rm.coe.int/16806af19b> [20.06.2020].

[885] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 40, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

[886] იქვე.

[887] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 345-346.

[888] იქვე. 345-346.

პირს წერილობით უნდა ეცნობოს ღონისძიების ჩატარების შედეგად მოპოვებული მასალის შინაარსისა და აღნიშნული მასალის განადგურების შესახებ, ასევე გადაეცეს მოსამართლის განჩინება ფარული საგამოძიებო მოქმედების ჩატარების შესახებ და ის მასალა, რომლის საფუძველზე მოსამართლემ მიიღო ეს გადაწყვეტილება (სსსკ-ის 143[9] მუხლის მე-3 ნაწილი). შეტყობინების დროს პირს განემარტება აღნიშნული განჩინების სსსკ-ით დადგენილი წესით გასაჩივრების უფლება. გადაწყვეტილებას შეტყობინების შესახებ იღებს პროკურორი, როგორც სამართალწარმოების მიმდინარეობისას, ასევე მისი დასრულების შემდეგ. ამასთან, აღნიშნული გადაწყვეტილების მიღების დროს პროკურორი ხელმძღვანელობს სამართალწარმოების ინტერესებით (სსსკ-ის 143[9] მუხლის მე-3 ნაწილი).

აღსანიშნავია, რომ ფარული საგამოძიებო მოქმედების დასრულებამდე მოპოვებული ინფორმაციის გაცნობის უფლებით სარგებლობენ მხოლოდ გამომძიებელი, პროკურორი და მოსამართლე (თუ აღნიშნული არსებითად უკავშირდება მათ მიერ განსახილველ საკითხს). ხოლო დაცვის მხარეს მოპოვებული ინფორმაცია მიეწოდება სსსკ-ის 83-ე მუხლის მე-6 ნაწილით დადგენილი წესით, წინასასამართლო სხდომის გამართვამდე არა უგვიანეს 5 დღისა ინფორმაციის გაცვლის პროცედურის ფარგლებში; ასევე საპროცესო შეთანხმების დამტკიცებისას (სსსკ-ის 143[9] მუხლის მე-3 ნაწილი).

სსსკ-ის 143[9] მუხლი ითვალისწინებს შეტყობინების გადავადების შესაძლებლობას, რომლის შესახებ გადაწყვეტილებას იღებს პროკურორი, კერძოდ, თუკი პროკურორი გადაწყვეტს, რომ ფარული საგამოძიებო მოქმედების ჩატარებიდან 12 თვის ვადაში არ შეატყობინოს შესაბამის პირს, იგი აღნიშნული ვადის გასვლამდე არაუგვიანეს 72 საათისა შუამდგომლობით მიმართავს სასამართლოს (რომელმაც მიიღო განჩინება ღონისძიების ჩატარების შესახებ) და მოითხოვს ინფორმაციის შესაბამისი პირისათვის მიწოდების გადავადებას არაუმეტეს 12 თვისა (სსსკ-ის 143[9] მუხლის მე-4 ნაწილი). ამავე ნორმა პროკურორს ავალდებულებს, შუამდგომლობაში დაასაბუთოს ის საფრთხე, რომელიც პირისათვის შეტყობინებით შეექმნება „ფარული საგამოძიებო მოქმედების ლეგიტიმური მიზნის მიღწევას, ამოცანის შესრულებას და სამართალწარმოების ინტერესებს.“ სსსკ-ით დადგენილი წესით შუამდგომლობის განხილვის შედეგად სასამართლო იღებს გადაწყვეტილებას შუამდგომლობის დაკმაყოფილების და ფარული საგამოძიებო მოქმედების ჩატარების თაობაზე

შესაბამისი პირისათვის შეტყობინების გადავადების შესახებ ან შუამდგომლობის დაკმაყოფილებასა და ამგვარი ინფორმაციის მიწოდების გადავადებაზე უარის თქმის შესახებ (სსსკ-ის 143[9] მუხლის მე-4 ნაწილი). დადებითი გადაწყვეტილების მიღების შემთხვევაში შეტყობინების გადავადება ხდება არა უმეტეს 12 თვისა.

აღსანიშნავია, რომ ევროპის საბჭოს ადამიანის უფლებათა და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში შეტყობინების მოთხოვნასთან დაკავშირებული ქართული რეგულაცია დადებითად არის შეფასებული, კერძოდ, დასკვნაში აღნიშნულია, რომ ამ თვალსაზრისით საქართველოს კანონმდებლობა „შესაბამისობაშია და აჭარბებს კიდევაც“ „პოლიციის სექტორში პერსონალურ მონაცემთა დამუშავების თაობაზე” ევროსაბჭოს მინისტრთა კომიტეტის რეკომენდაციით განსაზღვრულ მოთხოვნებს[889] (რეკომენდაციით დადგენილი მოთხოვნის შესახებ იხ. წინა თავში).

როგორც უკვე აღინიშნა, შეტყობინების ვალდებულების მოთხოვნასთან მიმართებით ევროპული სასამართლო ყურადღებას ამახვილებს, თუ რამდენად ხორციელდება ამ მოთხოვნის დაცვაზე ზედამხედველობა დამოუკიდებელი ორგანოს მიერ, მაგალითად, საქმეებში კლასი და სხვები გერმანიის წინააღმდეგ (Klass and others v. Germany) და ვებერი და სარავია გერმანიის წინააღმდეგ (Weber and Saravia v. Germany), შეტყობინების მექანიზმის შეფასებისას სასამართლომ მხედველობაში მიიღო ის გარემოება, რომ დამოუკიდებელი ორგანო (G10 კომისია) იღებდა გადაწყვეტილებას ჩატარებული ღონისძიების შესახებ პირის ინფორმირების თაობაზე.[890] ამ თვალსაზრისით მისასალმებელია, რომ სსსკ-ის 143[9] მუხლის მე-4 ნაწილის მიხედვით, გათვალისწინებულია კანონმდებლობით განსაზღვრულ ვადაში შეტყობინების გადავადების შესაძლებლობაზე სასამართლო კონტროლი და ამავე ნორმის თანახმად, საბოლოოდ, სასამართლო იღებს გადაწყვეტილებას შეტყობინების გადავადების თაობაზე.

აღსანიშნავია, რომ პირისთვის ფარული მიყურადების შესახებ შეტყობინების ვალდებულება არ არის დამოკიდებული იმაზე, იქნება თუ არა ფარული საგამოძიებო

---

[889] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 19, <https://rm.coe.int/16806af19b>[20.06.2020].

[890] Klass and Others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 57; Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI· 135, Roman Zakharov v. Russia, [2015], ECtHR, 288.

ღონისძიების შედეგად მოპოვებული მტკიცებულებები პროცესში გამოყენებული. პირი მაშინაც უნდა ჩაითვალოს ფარული მიყურადების ობიექტად, თუკი მიყურადებული საუბარი არ იყო გამოძიებისთვის რაიმე მნიშვნელობის მქონე და, შესაბამისად, მოპოვებული მასალა განადგურდება[891].

1.8 ფარული საგამოძიებო მოქმედების გასაჩივრება

როგორც უკვე აღინიშნა, შეტყობინების ვალდებულების მიზანი პირისთვის ჩატარებული ღონისძიების კანონიერების post factum გადამოწმების შესაძლებლობის მიცემაში მდგომარეობს. სსსკ-ის 143[3] მუხლი უზრუნველყოფს ამ უფლებას და განასხვავებს ორის სახის პროცედურას, კერძოდ, იმ შემთხვევაში როდესაც პირი სამართალწარმოების მიმდინარეობისას შეიტყობს მის მიმართ ფარული საგამოძიებო მოქმედების ჩატარების თაობაზე, სასამართლოს შესაბამისი განჩინება შეუძლია ერთჯერადად გაასაჩივროს სააპელაციო სასამართლოს საგამოძიებო კოლეგიაში, აღნიშნული ინფორმაციის და განჩინების გასაჩივრების უფლების შესახებ განმარტების მიღებიდან 48 საათის განმავლობაში. ამასთან, სააპელაციო სასამართლოს მიერ გასაჩივრებული განჩინების გაუქმება და ჩატარებული ფარული საგამოძიებო მოქმედების უკანონოდ ცნობა ქმნის ამ მოქმედების შედეგად მოპოვებული ინფორმაციის სსსკ-ით დადგენილი წესით დაუშვებელ მტკიცებულებად ცნობის საფუძველს (სსსკ-ის 143[3] მუხლის მე-14 ნაწილი).

ხოლო იმ შემთხვევაში, როდესაც პირი, მის მიმართ ფარული საგამოძიებო მოქმედების ჩატარების შესახებ შეიტყობს სამართალწარმოების დასრულების შემდეგ, განჩინების გასაჩივრება შეუძლია აღნიშნული ინფორმაციის და განჩინების გასაჩივრების უფლების შესახებ განმარტების მიღებიდან 1 თვის განმავლობაში, სააპელაციო სასამართლოს საგამოძიებო კოლეგიაში. ამდენად, ამ შემთხვევაში კანონმდებლობა ითვალისწინებს გასაჩივრების განსხვავებულ, უფრო ხანგრძლივ ვადას. ასეთ დროს სააპელაციო სასამართლოს მიერ ღონისძიების უკანონოდ ცნობა შეიძლება მიჩნეულ იქნეს სსსკ-ის 310-ე მუხლის „თ“ ქვეპუნქტით გათვალისწინებულ ახლად გამოვლენილ გარემოებად განაჩენის გადასინჯვისთვის, თუ ამ ფარული

[891] *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 194-195.

საგამოძიებო მოქმედების შედეგად მოპოვებული მტკიცებულება საფუძვლად დაედო განაჩენს (სსსკ-ის 143[3] მუხლის მე-15 ნაწილი).

ორივე ზემოთაღნიშნულ ვითარებაში, სააპელაციო სასამართლოს მიერ საჩივარზე მიღებული გადაწყვეტილება შეიძლება საფუძვლად დაედოს სსსკ-ის მე-7 მუხლის მე-3 ნაწილით გათვალისწინებულ მოთხოვნას პირისთვის მისი პირადი ცხოვრების შესახებ ცნობების/პერსონალური მონაცემების უკანონოდ მოპოვებით, შენახვით ან გამჟღავნებით მიყენებული ზიანის ანაზღაურების თაობაზე (სსსკ-ის 143[3] მუხლის მე-14 და მე-15 ნაწილები).

ნიშანდობლივია, რომ ევროპული სასამართლოს პრაქტიკის თანახმად, ჩატარებული ღონისძიების გასაჩივრების მოთხოვნის უფლება უნდა გააჩნდეს არამარტო იმ პირს, ვის მიმართაც დაიწყო სისხლისსამართლებრივი პროცედურები, რომელთან დაკავშირებითაც ეცნობა ღონისძიების ჩატარების ფაქტი, არამედ იმ პირსაც, რომლის მიმართაც ფარული მეთვალყურეობის ღონისძიებების შედეგად ასეთი პროცედურები არ განხორციელებულა.[892] ამ თვალსაზრისით აღსანიშნავია, რომ სსსკ-ის 143[9] მუხლიდან გამომდინარე, სავალდებულოა ღონისძიების ადრესატის შეტყობინება იმისდა მიუხედავად, სასამართლოს განაჩენით დასრულდა საქმე თუ შეწყდა გამოძიება ან/და სისხლისსამართლებრივი დევნა სსსკ-ით დადგენილი წესით. ასევე, 143[3] მუხლის შესაბამისად, აღნიშნულ პირს (რომლის მიმართაც ჩატარდა ღონისძიება) გააჩნია ღონისძიების გასაჩივრების უფლება საქმის საბოლოო ბედის მიუხედავად.

1.9 ფარული საგამოძიებო მოქმედებების რეესტრი

ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული 2014 წლის 1 აგვისტოს საკანონმდებლო ცვლილებების ერთ-ერთ ნოვაციას რეესტრის წარმოებასთან დაკავშირებული დანაწესი წარმოადგენდა. სსსკ-ის 143[10] მუხლი ითვალისწინებს საქართველოს უზენაესი სასამართლოს მიერ ფარული საგამოძიებო მოქმედებების რეესტრის შედგენის მოთხოვნას, რომელშიც აისახება შემდეგი სტატისტიკური ინფორმაცია: ფარული საგამოძიებო მოქმედებების ჩატარებასთან დაკავშირებით სასამართლოებში შესული შუამდგომლობების და სასამართლოთა მიერ მათზე

[892] Roman Zakharov v. Russia, [2015] ECtHR, 295.

მიღებული განჩინებების შესახებ ინფორმაცია, აგრეთვე ოპერატიულ-სამძებრო ღონისძიების შედეგად მოპოვებული მასალის განადგურების თაობაზე ინფორმაცია, რომელიც არ ეხებოდა პირის დანაშაულებრივ საქმიანობას, მაგრამ შეიცავდა ცნობებს მისი ან სხვა პირის პირადი ცხოვრების შესახებ და „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-4 პუნქტის თანახმად განადგურდა. ამასთან, ამავე მუხლის მე-2 ნაწილის შესაბამისად, უზენაესი სასამართლო ვალდებულია ყოველი წლის ბოლოს გამოაქვეყნოს ზემოთაღნიშნული სტატისტიკური მონაცემები.

აღსანიშნავია, რომ რეესტრის მონაცემები უზენაესი სასამართლოს მიერ პირველად გამოქვეყნდა 2014 წელს; რეესტრში ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით ინფორმაცია აისახება როგორც ჯამურად, ასევე სასამართლოების მიხედვით ცალ-ცალკე.

მნიშვნელოვანია ისიც, რომ საქართველოს უზენაესი სასამართლო 2014 წლიდან მოყოლებული ცალკე აქვეყნებს სატელეფონო საუბრის ფარულ მიყურადება/ჩაწერასთან დაკავშირებული შუამდგომლობების განხილვის სტატისტიკას. ეს ვალდებულება, თავდაპირველად, IDFI-ისა და სხვა არასამთავრობო ორგანიზაციების მიერ „ღია მმართველობის პარტნიორობის“ 2014-2015 წწ. სამოქმედო გეგმის ფარგლებში შემუშავებულ რეკომენდაციას წარმოადგენდა.[893] ამავდროულად, 2016 წლიდან სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებასთან დაკავშირებით მონაცემები ქვეყნდება საქალაქო/რაიონული სასამართლოებისა და დანაშაულთა კვალიფიკაციის მიხედვითაც.[894]

სატელეფონო საუბრის ფარული მიყურადებისა და ჩაწერის შესახებ სტატისტიკური მონაცემების გამოქვეყნებას მნიშვნელოვანი ფუნქცია ეკისრება სამართალდამცავ ორგანოებსა და სასამართლო სისტემაზე საზოგადოებრივი კონტროლის განხორციელების, ასევე ამ სფეროში არსებული სახელმწიფო

[893] IDFI, სატელეფონო საუბრის ფარული მიყურადებისა და ფარული საგამოძიებო მოქმედებების 2016 წლის სტატისტიკური მონაცემები, 2017, 3, <https://idfi.ge/public/upload/IDFI_FOTOS_2016/surveillance_regulation/surveillance-update-statistics-03.02.2017-2.pdf> [25.06.2020].

[894] <http://www.supremecourt.ge/farulebi> [25.06.2020].

პოლიტიკის მიმართ საზოგადოების ნდობის ამაღლების თვალსაზრისით.[895] როგორც პროფესორი ალბრეხტი აღნიშნავს, ფარული საგამოძიებო მოქმედებების ერთგვარი კომპენსირება შესაძლებელია ასევე ამ ღონისძიებების სიხშირისა და შედეგების შესახებ სისტემატური ანგარიშგებით[896]. მონაცემთა გამოქვეყნების მიზანია, ერთი მხრივ, გამჭვირვალობის უზრუნველყოფა საზოგადოებისათვის, რომელსაც ამ ინფორმაციაზე დაყრდნობით შესაძლებლობა აქვს ფარული საგამოძიებო მოქმედებების მოცულობასა და შედეგებზე გარკვეული სურათი შეექმნას, ხოლო მეორე მხრივ, დამუშავებული ინფორმაცია უნდა იქცეს ფარული საგამოძიებო მოქმედებების შეფასების საფუძვლად, რაც კანონმდებელს საშუალებას აძლევს საკანონმდებლო რეგულაციები შეფასების შედეგებს მიუსადაგოს.[897]

საქართველოს კანონმდებლობით განსაზღვრულ ინფორმაციის გამოქვეყნების ვალდებულებასთან დაკავშირებით მისასალმებელია ის ფაქტი, რომ უზენაესი სასამართლო სატელეფონო კომუნიკაციის ფარული მიყურადების თაობაზე მონაცემებს აქვეყნებს სხვა ფარული საგამოძიებო მოქმედებებისგან დამოუკიდებლადაც; ამ გზით შესაძლებელია საზოგადოების ინფორმირებულობა კონკრეტულად სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიების პრაქტიკაში გამოყენებასთან დაკავშირებით და შესაბამისად, მნიშვნელოვანია ამ პროცესის უფრო მეტი გამჭვირვალობის უზრუნველსაყოფად. იგივე თვალსაზრისით მიზანშეწონილი იქნებოდა, მსგავსი სახის სტატისტიკა სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ღონისძიებასთან დაკავშირებითაც ქვეყნდებოდეს,[898] მითუმეტეს, რომ ეს ფარული საგამოძიებო მოქმედება ადამიანის უფლებებში ჩარევის არანაკლებ და ხშირ შემთხვევაში შესაძლოა გაცილებით მეტად მძიმე ფორმასაც წარმოადგენდეს. შესაბამისად, ამ კუთხით

---

[895] IDFI, სატელეფონო საუბრის ფარული მიყურადებისა და ფარული საგამოძიებო მოქმედებების 2016 წლის სტატისტიკური მონაცემები, 2017, 3, <https://idfi.ge/public/upload/IDFI_FOTOS_2016/surveillance_regulation/surveillance-update-statistics-03.02.2017-2.pdf> [25.06.2020].

[896] *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, 41, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].

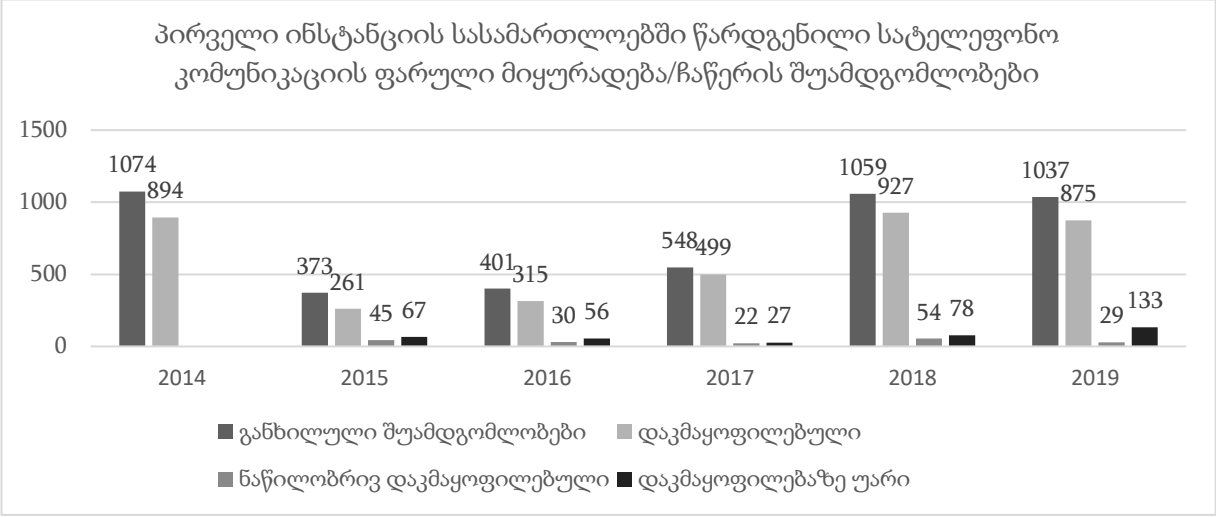
[897] იქვე.

[898] აღნიშნულ საკითხთან დაკავშირებით იხ. ასევე IDFI, სატელეფონო საუბრის ფარული მიყურადებისა და ფარული საგამოძიებო მოქმედებების 2016 წლის სტატისტიკური მონაცემები, 2017, <https://idfi.ge/ge/statistical_data_on_phone_conversation_surveillance> [25.06.2020].

საზოგადოების უფრო მეტ ინფორმირებულობას არსებითი დატვირთვა აქვს. იგივე მოსაზრებიდან გამომდინარე, მიზანშეწონილი იქნება, გამოქვეყნდეს ასევე გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული/მიმდინარე სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების სტატისტიკური მაჩვენებლებიც, რათა საზოგადოებას შეექმნას წარმოდგენა, რამდენად ხშირად გამოიყენება გადაუდებელი აუცილებლობის საფუძველი პრაქტიკაში და როგორია ამ რაოდენობრივი მაჩვენებლის მიმართება ფარული საგამოძიებო მოქმედების ზოგადი წესით - სასამართლოს განჩინების საფუძველზე ჩატარების მონაცემებთან. ამ გზით შესაძლებელი იქნებოდა გარკვეული დასკვნების გამოტანა აღნიშნულ ღონისძიებათა გადაუდებლად ჩატარების უფლებამოსილების საგამონაკლისო წესით, აუცილებლობის მოთხოვნათა დაცვით გამოყენებასთან დაკავშირებით.

1.10 სტატისტიკური მონაცემები

საქართველოს უზენაესი სასამართლოს მიერ 2014-2019 წლებში გამოქვეყნებული მონაცემების თანახმად, სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიებასთან მიმართებით პირველი ინსტანციის სასამართლოებში წარდგენილი შუამდგომლობების დაკმაყოფილების მაჩვენებელი შემდეგნაირად გამოიყურება[899]:



[899] აღნიშნული სტატისტიკური მონაცემები არ მოიცავს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ვადის გაგრძელების თაობაზე განხილულ შუამდგომლობებს. აღნიშნულ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით უფრო დეტალური სტატისტიკური მაჩვენებლები იხ. <http://www.supremecourt.ge/statistics/> [25.06.2020].

როგორც 2015-2018 წლების მონაცემებით ირკვევა, სატელეფონო საუბრის ფარულ მიყურადებასა და ჩაწერაზე სასამართლოებში შესული შუამდგომლობების რაოდენობა ამ წლების განმავლობაში გაზრდილია, მაგალითად, 2018 წელს წინა წელთან შედარებით თითქმის ორჯერ გაიზარდა სასამართლოებში განხილული და დაკმაყოფილებული შუამდგომლობების რიცხვი.[900] ამასთან, 2018 წელს პირველი ინსტანციის სასამართლოებში წარდგენილი სატელეფონო მიყურადების შუამდგომლობები აღემატება წინა ორი წლის მანძილზე წარდგენილი შუამდგომლებების ჯამურ მაჩვენებელს, რაც თითქმის გაუტოლდა 2014 წლის შედეგებს.[901] რაც შეეხება 2019 წლის მონაცემებს, სასამართლოებში შესული შუამდგომლობების რაოდენობა თითქმის უტოლდება (უმნიშვნელოდ დაბალია) წინა წლის იგივე მონაცემს, თუმცა გაზრდილია დაკმაყოფილებაზე უარის თქმის შუამდგომლობების პროცენტული მაჩვენებელი 2018 წლის მონაცემთან შედარებით; სტატისტიკური მონაცემების საფუძველზე იკვეთება, რომ 2017-2018 წლებში გაზრდილია სატელეფონო საუბრის ფარული მიყურადების შუამდგომლობების დაკმაყოფილების წილი. თუ ეს მაჩვენებელი 2014-2016 წლებში 82-86%-ს შორის მერყეობდა, 2017-2018 წლების მანძილზე მოთხოვნათა დაკმაყოფილების ხარისხმა მოიმატა და 93-94% შეადგინა;[902] ხოლო 2019 წელს შეადგინა 87%.[903]

გამოქვეყნებული მონაცემების საფუძველზე იკვეთება, რომ ყველაზე მეტი შუამდგომლობა მოდის თბილისის საქალაქო სასამართლოზე. რაც შეეხება დანაშაულის მიხედვით სტატისტიკას, 2016-2018 წლების პერიოდში განხილული შუამდგომლობების თითქმის ნახევარი მოდის სსკ-ის ექვს მუხლზე - თაღლითობა (სსკ მუხლი 180), გამოძალვა (სსკ მუხლი 181), ქურდული სამყაროს წევრობა, კანონიერი ქურდობა (207 შუამდგომლობა, სსკ მუხლი 223[1]), ქრთამის აღება (სსკ მუხლი 338), ნარკოტიკული საშუალების, მისი ანალოგის, პრეკურსორის ან ახალი ფსიქოაქტიური ნივთიერების უკანონო დამზადება, წარმოება, შეძენა, შენახვა, გადაზიდვა, გადაგზავნა

[900] IDFI, ფარული საგამოძიებო მოქმედებების სტატისტიკა საქართველოში: 2015-2018; 2019, 2, <https://idfi.ge/public/upload/IDFI_2019/General/surveillance_geo_final.pdf> [25.06.2020].

[901] იქვე.

[902] იქვე.

[903] ამ მაჩვენებელში შედის ასევე ნაწილობრივ დაკმაყოფილებული შუამდგომლობების რაოდენობა. ამასთან, არ შედის სატელეფონო საუბრის ფარული მიყურადებისა და ჩაწერის ვადის გაგრძელების თაობაზე რაიონული (საქალაქო) სასამართლოების მიერ დაკმაყოფილებული (ნაწილობრივ დაკმაყოფილებული) შუამდგომლობების რაოდენობა.

ან გასაღება (სსკ მუხლი 260) და ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის დამზადება, გასაღება ან გამოყენება (სსკ მუხლი 210)[904]. რაც შეეხება 2019 წლის მონაცემებს, დანაშაულთა შემადგენლობების მხრივ მცირედი განსხვავება აღენიშნება, კერძოდ, ყველაზე მეტი შუამდგომლობა მოდის შემდეგ ექვს მუხლზე - 223[1] - „ქურდული სამყაროს“ წევრობა, „კანონიერი ქურდობა“ (118 შუამდგომლობა), 180-ე - თაღლითობა (141 შუამდგომლობა), 108-ე - განზრახ მკვლელობა (68 შუამდგომლობა), 260-ე - ნარკოტიკული საშუალების, მისი ანალოგის, პრეკურსორის ან ახალი ფსიქოაქტიური ნივთიერების უკანონო დამზადება, წარმოება, შეძენა, შენახვა, გადაზიდვა, გადაგზავნა ან გასაღება (66 შუამდგომლობა), 338-ე - ქრთამის აღება (56 შუამდგომლობა); 210-ე - ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის დამზადება, გასაღება ან გამოყენება (48 შუამდგომლობა).

ამასთან, 2017 წლის პირველი სექტემბრიდან 2019 წლის 28 თებერვლის ჩათვლით, თბილისის საქალაქო სასამართლომ გადაუდებელი აუცილებლობისას ჩატარებული სატელეფონო საუბრის მიყურადება/ჩაწერიდან 88% ცნო კანონიერად.[905]

რაც შეეხება სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიების სტატისტიკას, 2017 წლის 1 სექტემბრიდან 2019 წლის 28 თებერვლის ჩათვლით თბილისის საქალაქო სასამართლომ აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ 24 შუამდგომლობა განიხილა და ყველა მათგანი იქნა დაკმაყოფილებული. აღნიშნული ღონისძიების დაკანონების შესახებ განხილული იქნა 2 შუამდგომლობა და ორივე მათგანი დაკმაყოფილდა.[906] ამავდროულად, მითითებული ღონისძიების ჩატარების ნებართვის გაცემის, ვადის გაგრძელების, დაკანონების, ნაწილობრივ დაკმაყოფილებისა და უარის თაობაზე სასამართლოებიდან ინსპექტორის სამსახურს მატერიალური სახით წარედგინა 19 განჩინება 2017 წელს, 30 განჩინება 2018 წელს და 9 განჩინება 2019 წელს.[907]

საბოლოო ჯამში, უნდა აღინიშნოს, რომ სატელეფონო საუბრების მიყურადების შესახებ სასამართლოსთვის წარდგენილი შუამდგომლობების რაოდენობა 2014 წელს

[904] IDFI, ფარული საგამოძიებო მოქმედებების სტატისტიკა საქართველოში: 2015-2018; 2019, 7, <https://idfi.ge/public/upload/IDFI_2019/General/surveillance_geo_final.pdf> [25.06.2020].
[905] იქვე, 13.
[906] იქვე. 13.
[907] სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 5 მაისის წერილი (№:SIS 5 20 00006422).

წინა წლებთან შედარებით მნიშვნელოვნად შემცირდა[908], თუმცა 2017-2018 წლებში წინა წლებთან (2014-2016 წწ.) შედარებით ისევ აღინიშნება წარდგენილი შუამდგომლობების, ისევე როგორც მათი დაკმაყოფილების რიცხვის მატება. 2019 წელს შუამდგომლობების რაოდენობის მაღალი მაჩვენებლის ტენდენცია შენარჩუნებულია, თუმცა 2018 წელთან შედარებით შემცირებულია დაკმაყოფილებული შუამდგომლობების პროცენტული მაჩვენებელი. რაც შეეხება სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიების სტატისტიკას, მართალია რაოდენობრივი თვალსაზრისით განხილული შუამდგომლობების რიცხვი მაღალი არ არის, თუმცა საყურადღებოა, რომ სასამართლო (ამ შემთხვევაში თბილისის საქალაქო სასამართლო) ყველა წარდგენილ შუამდგომლობას აკმაყოფილებს.

2. ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების მოპოვება სსსკ-ის 136-ე მუხლის საფუძველზე

როგორც უკვე აღინიშნა, საქართველოს კანონმდებლობით განსაზღვრულია ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვისა და სისხლის სამართლის პროცესში გამოყენების საკითხები. როგორც უკვე აღინიშნა, „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი ითვალისწინებს „ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების“ ცნებას, რომლის ქვეშ მოიაზრება „მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის

[908] მაგალითად, თბილისის საქალაქო სასამართლოში 2011 წელს სატელეფონო საუბრების ფარული მიყურადების შესახებ მხოლოდ თბილისის პროკურატურიდან შესული იყო 7195 შუამდგომლობა, 2012 წელს - 5951 შუამდგომლობა, 2013 წლის პირველ 5 თვეში - 1400 შუამდგომლობა, ხოლო 2014 წლის 9 თვეში ყველა საგამოძიებო ორგანოდან მხოლოდ 952 შუამდგომლობა, <https://idfi.ge/ge/decreased-motions> [25.06.2020]

საჭირო მონაცემები“ (მე-2 მუხლის „ჰ[62]“ ქვეპუნქტი). მოცემული ინფორმაციის ტიპის/შინაარსის განმარტებისას საქართველოს საკონსტიტუციო სასამართლომ აღნიშნა, რომ ამ ნორმიდან გამომდინარე, საქართველოს კანონმდებლობით შესაძლებელია შენახულ იქნეს ინფორმაცია იმასთან დაკავშირებით, „ვინ, ვის, როდის, რა ტექნიკური საშუალებით, რომელი ლოკაციიდან და როგორი ხანგრძლივობით დაუკავშირდა.“[909]

ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების განმარტება და მის შენახვასთან დაკავშირებული რეგულაციები საქართველოს კანონმდებლობაში 2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით იქნა შემოღებული. აღნიშნული ცვლილებები ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნის მიხედვით, „მონაცემთა შენახვის შესახებ“ ევროკავშირის 2006 წლის დირექტივის იმპლემენტაციით იყო ნაკარნახევი; „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის პროექტით გათვალისწინებული დებულებები (რომლებიც მიღებულ იქნა 2014 წლის 1 აგვისტოს) იმეორებდა დირექტივის მე-5 მუხლით განსაზღვრულ მონაცემთა განმარტებას, გარდა ამისა, მონაცემთა შენახვის ვადა ასევე დირექტივის შესაბამისად იყო დადგენილი[910]. მართალია 2014 წლის 30 ნოემბრის კანონით გარკვეული ცვლილებები შევიდა ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა განმარტებაში, კერძოდ, „ელექტრონული კომუნიკაციის შესახებ“ საქართველოს კანონი აღარ ითვალისწინებს მონაცემთა კონკრეტულ, დეტალურ ჩამონათვალს და უფრო ზოგადი სახით განსაზღვრავს მას,[911] მაგრამ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ცნება შინაარსობრივად უცვლელი დარჩა.

საქართველოს კანონმდებლობის მიხედვით, სააგენტოს მინიჭებული აქვს უფლებამოსილება, განახორციელოს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირება და შეინახოს ისინი ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში,

---

[909] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-91.

[910] *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14 February 2014, 13, <https://rm.coe.int/16806af19b>[20.06.2020].

[911] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“, www.matsne.gov.ge, 30/11/2014.

რისთვისაც აქვს წვდომის შესაძლებლობა ელექტრონული კომუნიკაციის კომპანიის შესაბამის მონაცემთა ბაზებზე.[912] მონაცემები სააგენტოს მიერ ინახება 12 თვის ვადით და დასაშვებია ამ ვადის გაგრძელება კანონმდებლობით გათვალისწინებული წინაპირობების არსებობისას.[913] ნაშრომში დეტალურად იქნება განხილული სააგენტოს მიერ კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირების უფლებამოსილებასთან დაკავშირებული კონსტიტუციურ-სამართლებრივი და საერთაშორისო სტანდარტები, ხოლო მოცემული თავი შეეხება ელექტრონული კომუნიკაციის კომპანიასთან/სააგენტოსთან შენახულ კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე სამართალდამცავი ორგანოების დაშვების საკითხებს.

კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გამოთხოვა სისხლის სამართლის პროცესში გამოყენების მიზნით შესაძლებელია როგორც ელექტრონული კომუნიკაციის კომპანიისგან, ასევე ოპერატიულ-ტექნიკური სააგენტოსგან. აღნიშნული ხორციელდება სსსკ-ის 136-ე მუხლის საფუძველზე.

„ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-8 მუხლის მე-4 პუნქტი განსაზღვრავს ელექტრონული კომუნიკაციის კომპანიის ვალდებულებას, საგამოძიებო და ოპერატიულ-სამძებრო საქმიანობის განმახორციელებელ ორგანოს გადასცეს აღნიშნული მონაცემები სსსკ-ის 136-ე მუხლის შესაბამისად. ამასთან, ელექტრონული კომუნიკაციის კომპანიამ უნდა აღრიცხოს ამ მონაცემების სსსკ-ის 112-ე და 136-ე მუხლებით დადგენილი წესებით შესაბამისი სახელმწიფო ორგანოებისათვის გადაცემის ფაქტები და სათანადო ინფორმაცია მიაწოდოს ინსპექტორის სამსახურს. სააგენტოდან ინფორმაციის გამოთხოვის შესაძლებლობას კი ითვალისწინებს „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-15 მუხლის მე-11 პუნქტი.

აღსანიშნავია, რომ სსსკ-ის 136-ე მუხლი ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გამოთხოვის საკითხთან დაკავშირებით ანალოგიურ სტანდარტებს განსაზღვრავს, როგორსაც ფარულ საგამოძიებო მოქმედებებთან მიმართებით, რაც ნიშნავს იმას, რომ ფარულ საგამოძიებო

[912] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი, 8^3 მუხლი, სსმ, 26, 02/06/2005.
[913] „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონი, მე-15 მუხლი, <matsne.gov.ge>, 27/03/2017.

მოქმედებებთან დაკავშირებით ნაშრომში განხილული საკითხები ასევე რელევანტურია კომუნიკაციის მაიდენტიფიცირებელ მონაცემებზე წვდომის საგამოძიებო მოქმედებასთან მიმართებით. მნიშვნელოვან გარანტიათა შორის გათვალისწინებულია მონაცემთა გამოთხოვის შესაძლებლობა მხოლოდ სასამართლოს განჩინების საფუძველზე (გარდა გადაუდებელი აუცილებლობის შემთხვევისა), „დასაბუთებული ვარაუდის“ სტანდარტის არსებობისას და ამასთანავე, 136-ე მუხლზე ვრცელდება ფარული საგამოძიებო მოქმედებების თავის 143^{2}-143^{10} მუხლების დებულებები. ასეთი მიდგომა შეიცავს ადამიანის უფლებების დაცვის მნიშვნელოვან გარანტიებს და ამავდროულად, შეესაბამება ევროკავშირის მართლმსაჯულების სასამართლოს სულისკვეთებას სამართალდამცავი ორგანოების მიერ ტრაფიკისა და ადგილმდებარეობის შესახებ მონაცემთა გამოთხოვის საკითხთან დაკავშირებით. როგორც კვლევაში გამოიკვეთა, საერთაშორისო მიდგომის თანახმად, ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემები სენსიტიურობის ხარისხით არ ჩამოუვარდება კომუნიკაციის შინაარსობრივ მონაცემებს, შესაბამისად, აღნიშნულ მონაცემებზე წვდომასთან მიმართებით ანალოგიური სტანდარტები მოქმედებს, როგორიც შინაარსობრივი ინფორმაციის მოპოვების შემთხვევაში. როგორც უკვე აღინიშნა, ევროკავშირის მართლმსაჯულების სასამართლომ გადაწყვეტილებებში „შპს ირლანდიის ციფრული უფლებები და სეიტლინგერი და სხვები“ და Tele2 Sverige AB and Watson ასეთ მონაცემთა გამოთხოვის შესაძლებლობა დაუკავშირა ეროვნულ კანონმდებლობაში საკმაოდ მკაცრ მოთხოვნებს, „მკაფიო და ნათელი სამართლებრივი დებულებების“ აუცილებლობას, ისევე როგორც თანაზომიერების პრინციპის დაცვას და შესაბამისი მატერიალური და პროცედურული პირობების გათვალისწინებას. მონაცემთა გამოთხოვის საკითხთან მიმართებით ევროკავშირის მართლმსაჯულების სასამართლოს მიერ ძირითად მოთხოვნებად განისაზღვრა „მძიმე დანაშაულთან“ ბრძოლის ინტერესები, სასამართლოს (დამოუკიდებელი ორგანოს) გადაწყვეტილება, რომელიც მიღებულ უნდა იქნეს „დასაბუთებული შუამდგომლობის“ საფუძველზე, „ეჭვი მძიმე დანაშაულის დაგეგმვის, ჩადენის ან ასეთ დანაშაულში რაიმე გზით მონაწილეობის შესახებ“, მონაცემთა სუბიექტისათვის შეტყობინება. აღნიშნულის გათვალისწინებით, დადებითად უნდა შეფასდეს ის გარემოება, რომ მოქმედი კანონმდებლობა ამ მონაცემთა გამოთხოვის შესაძლებლობას ითვალისწინებს იმ დანაშაულებისათვის, რომლისთვისაც დასაშვებია ფარული საგამოძიებო

მოქმედებების განხორციელება, ასევე ადგენს სასამართლოს განჩინების სავალდებულოობის მოთხოვნას და ფარული საგამოძიებო მოქმედების ჩატარების სტანდარტებს ავრცელებს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა გამოთხოვაზე.

რაც შეეხება ზემოთ აღნიშნული სამართლებრივი დებულებების პრაქტიკაში შესრულების საკითხს, როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორის (იმ დროს მოქმედი კანონმდებლობის შესაბამისად) ანგარიშიდან ირკვევა, ადგილი აქვს გარკვეულ სირთულეებს, მაგალითად, 2018 წელს შესწავლილ იქნა ელექტრონული კომუნიკაციის კომპანიების მიერ სამართალდამცავი ორგანოებისთვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კანონდარღვევით გადაცემის და პერსონალურ მონაცემთა დაცვის ინსპექტორის ინფორმირების ვალდებულების ჯეროვნად შეუსრულებლობის 6 ფაქტი[914]. ერთ-ერთ შემთხვევაში ელექტრონული კომუნიკაციის კომპანიამ სასამართლოს განჩინების გარეშე მიაწოდა სამართალდამცავ ორგანოს მოთხოვნილი ინფორმაცია[915]; ასევე გამოვლინდა სამართალდამცავი ორგანოსთვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების მხოლოდ წერილის საფუძველზე, მოსამართლის განჩინებისა და პროკურორის დადგენილების გარეშე გადაცემის ერთი ფაქტი.[916]

აღსანიშნავია, რომ ამ თვალსაზრისით დადებითი ტენდენცია შეინიშნება 2019 წელს, კერძოდ, სახელმწიფო ინსპექტორის სამსახურის 2019 წლის ანგარიშის მიხედვით, 2019 წელს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში მონაცემები დამუშავდა სასამართლოს გაცემული 81 ნებართვის საფუძველზე, რაც 2018 წელთან შედარებით 42%-ით ნაკლებია[917]. საანგარიშო პერიოდში ინსპექტორის სამსახურისთვის წარდგენილი ინფორმაციით/დოკუმენტაციით და შემოწმებებით დგინდება, რომ გაუმჯობესებულია კომპანიების მხრიდან სამართალდამცავი ორგანოებისთვის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების გადაცემის

[914] ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ, 2018, 73, <https://personaldata.ge/ka/press/post/5047> [25.06.2020].
[915] იქვე.
[916] იქვე.
[917] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, 2019, 96-97, <https://personaldata.ge/ka/about-us> [25.06.2020].

შესახებ ინსპექტორის ინფორმირების ვალდებულების შესრულების მაჩვენებელი[918]. ამასთან, 2019 წელს არ გამოვლენილა კომპანიების მიერ ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შესაბამისი სამართლებრივი საფუძვლის გარეშე ან მონაცემთა დამუშავების პრინციპების დარღვევით დამუშავების ფაქტი.[919]

ნიშანდობლივია, რომ საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის №1/1/650,699 გადაწყვეტილებით, არაკონსტიტუციურად იქნა ცნობილი სსსკ-ის 136-ე მუხლის ის ნორმატიული შინაარსი, რომელიც გამორიცხავს დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული დოკუმენტის ან ინფორმაციის გამოთხოვის განჩინების გაცემის შუამდგომლობით სასამართლოსათვის მიმართვის შესაძლებლობას[920]. შესაბამისად, 2017 წლის 27 იანვრიდან დაცვის მხარეს მიენიჭა უფლებამოსილება, დოკუმენტის ან ინფორმაციის გამოთხოვის შუამდგომლობით მიმართოს სასამართლოს.[921] აღნიშნულის გათვალისწინებით, 2019 წელს ინსპექტორმა შეისწავლა ამ საკითხთან დაკავშირებით რამდენად კანონიერად ხდებოდა ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების დამუშავება კომპანიების მიერ[922]. სამი (3) კომპანიის შემოწმების შედეგად მონაცემთა კანონიერი საფუძვლის გარეშე დამუშავებასთან დაკავშირებით დარღვევა არ გამოვლენილა, მაგრამ დადგინდა მონაცემთა უსაფრთხოებასთან დაკავშირებული ხარვეზები[923], კერძოდ, როგორც ანგარიშიდან ირკვევა, ყველა შემთხვევაში არ იყო აღრიცხული დაცვის მხარის შუამდგომლობით დამუშავებული და კომპანიაში დაცული მონაცემების მიმართ განხორციელებული ქმედებები, რაც შეიცავდა ამ მონაცემთა შემთხვევითი ან უკანონო დამუშავების რისკებს, რის გამოც სამივე კომპანიას დაუდგინდა სამართალდარღვევა და დაეკისრა კანონით გათვალისწინებული პასუხისმგებლობის ზომები.[924]

---

[918] იქვე.
[919] იქვე.
[920] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის №1/1/650,699 გადაწყვეტილება.
[921] იქვე.
[922] სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, 2019, 97-98 <https://personaldata.ge/ka/about-us> [25.06.2020].
[923] იქვე.
[924] იქვე.

საბოლოო ჯამში, ზემოთაღნიშნული ანგარიშის მიხედვით, ელექტრონული კომუნიკაციის კომპანიების მისამართით ინსპექტორის რეკომენდაციას მონაცემთა სამართალდამცავი ორგანოებისათვის გადაცემისას „ამ მიზნით გამოყენებულ პროგრამული უზრუნველყოფის საშუალებებში აღრიცხული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა“ წარმოადგენს[925]. ამასთან, ანგარიშის მიხედვით, კომპანიებმა სრულყოფილად უნდა დაარეგისტრირონ მონაცემთა სამართალდამცავი ორგანოებისთვის გადაცემასთან დაკავშირებული ინფორმაცია (რომელი მონაცემი გამჟღავნდა, ვისთვის, როდის და რა სამართლებრივი საფუძვლით).[926]

რაც შეეხება სსსკ-ის 136-ე მუხლის შესაბამისად სააგენტოდან მონაცემთა გამოთხოვის ასპექტებს და ამ თვალსაზრისით კონტროლს, აღნიშნულზე პერსონალურ მონაცემთა დაცვის ინსპექტორის და სახელმწიფო ინსპექტორის ზემოაღნიშნულ ანგარიშებში კონკრეტულად საუბარი არ არის, თუმცა სასურველი იქნებოდა ამ მიმართულებითაც ხდებოდეს საზოგადოების ინფორმირება.

3. გარე კონტროლის მექანიზმები კომუნიკაციის რეალურ დროში მოპოვების ღონისძიებებსა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებზე

3.1 ინსპექტორის სამსახურის უფლებამოსილებები

როგორც უკვე აღინიშნა, სატელეფონო კომუნიკაციის ფარული მიყურადების და ინტერნეტურთიერთობის მონიტორინგის ღონისძიებების განხორციელებაზე გარე კონტროლის ფუნქცია დაკისრებული აქვს ინსპექტორის სამსახურს. ინსპექტორის სამსახური წარმოადგენს დამოუკიდებელ სახელმწიფო ორგანოს, რომელსაც ხელმძღვანელობს ინსპექტორი. ინსპექტორს „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონით დადგენილი წესით ირჩევს საქართველოს პარლამენტი.

ინსპექტორი წარმოადგენს პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლეს, კერძოდ, 2018 წლის 21 ივლისის საკანონმდებლო ცვლილებების

[925] იქვე, 99.
[926] იქვე.

მიხედვით, 2019 წლის 10 მაისიდან გაუქმდა მანამდე არსებული პერსონალურ მონაცემთა დაცვის ინსპექტორის თანამდებობა და სახელმწიფო ინსპექტორი და სახელმწიფო ინსპექტორის სამსახური ჩაითვალა პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლედ.

როგორც უკვე აღინიშნა, ინსპექტორის ერთ-ერთ ძირითად ფუნქცია-მოვალეობას მიეკუთვნება ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლი. „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მიხედვით, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების – სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის (გარდა ინსპექტორის სამსახურის მიერ წარმოებულ სისხლის სამართლის საქმეზე ჩატარებული ფარული საგამოძიებო მოქმედებისა) ჩატარების დროს ინსპექტორის სამსახური აკონტროლებს: ა) კონტროლის ელექტრონული სისტემით – მონაცემთა დამუშავების კანონიერებას; ბ) კონტროლის სპეციალური ელექტრონული სისტემით – მონაცემთა დამუშავების კანონიერებას; გ) მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერებას (ინსპექტირება).

ამასთან, ამავე კანონის მე-18 მუხლის მე-2 პუნქტის თანახმად, სსსკ-ის 136-ე–138-ე მუხლებით გათვალისწინებული საგამოძიებო მოქმედებების ზედამხედველობას ინსპექტორის სამსახური ახორციელებს სასამართლოს, პროკურატურის და ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებლის მიერ მიწოდებული ინფორმაციის შედარებით და მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით (ინსპექტირება). ხოლო 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ზედამხედველობას - მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით (ინსპექტირება) (მე-18 მუხლის მე-3 პუნქტი).

გარდა აღნიშნულისა, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებს ინსპექტორის სამსახური აკონტროლებს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ

მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემითა და მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებით (ინსპექტირება) (მე-18 მუხლის მე-6 პუნქტი).

3.1.1 სსსკ-ით გათვალისწინებული ინსპექტორის საზედამხედველო ფუნქცია

ინსპექტორის სამსახურს სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ფარულ საგამოძიებო მოქმედებაზე კონტროლის შემდეგი სამართლებრივი ბერკეტები გააჩნია:

ა) მიეწოდება სასამართლოს განჩინება მატერიალური სახით:

სსსკ-ის 143[3] მუხლის მე-5 ნაწილის თანახმად, სასამართლოს განჩინება დგება 4 ეგზემპლარად, რომელთაგან ერთი რჩება სასამართლოში, ორი გადაეცემა შუამდგომლობის წარმდგენ პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს, რომელთაგან ერთი მიეწოდება შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს, და ერთი განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სასამართლოს მიერ მიეწოდება ინსპექტორის სამსახურს. მოსამართლის განჩინების ეგზემპლარები სააგენტოს და ინსპექტორის სამსახურს წარედგინება განჩინების გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა, მატერიალური (დოკუმენტური) სახით;

ბ) მიეწოდება განჩინების ელექტრონული ეგზემპლარი სსსკ-ის 143[3] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით განსაზღვრული ღონისძიების შემთხვევაში:

სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ჩატარების ნებართვის გაცემის შესახებ განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სააგენტოს მიერ მისი მიღებისთანავე მიეწოდება ინსპექტორის სამსახურს ელექტრონული ეგზემპლარის სახით, კონტროლის ელექტრონული სისტემის მეშვეობით. მოსამართლის განჩინების ელექტრონული ეგზემპლარის ინსპექტორის სამსახურისათვის პროგრამულად მიწოდების დადასტურებისთანავე სააგენტო იწყებს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას. ამასთან, ელექტრონული ეგზემპლარის მიწოდების მოცემული წესი მოქმედებს

სტაციონარული ტექნიკური შესაძლებლობის გამოყენების შემთხვევაში (143[3] მუხლის 5[1] ნაწილი).

გ) გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული ფარული საგამოძიებო მოქმედების შემთხვევაში მიეწოდება პროკურორის დადგენილება მატერიალური სახით, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ღონისძიების შემთხვევაში ასევე - დადგენილების ელექტრონული ეგზემპლარი;

გადაუდებელი აუცილებლობის შემთხვევაში ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილებას, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არაუგვიანეს 12 საათისა პროკურორი ან პროკურორის დავალებით გამომძიებელი მატერიალური (დოკუმენტური) სახით წარუდგენს ინსპექტორის სამსახურს. სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს, სააგენტოს მიერ მისი მიღებისთანავე მიეწოდება ინსპექტორის სამსახურს ელექტრონული ეგზემპლარის სახით, კონტროლის ელექტრონული სისტემის მეშვეობით. პროკურორის დადგენილების ელექტრონული ეგზემპლარის პროგრამულად მიწოდების დადასტურებისთანავე სააგენტო იწყებს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას. ელექტრონული ეგზემპლარის მიწოდების მოცემული წესი მოქმედებს იმ შემთხვევაში, როდესაც გამოიყენება სტაციონარული ტექნიკური შესაძლებლობა (სსსკ-ის 143[3] მუხლის 6[2] ნაწილი).

გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული ფარული საგამოძიებო მოქმედების შემთხვევაში ინსპექტორს ასევე მიეწოდება აღნიშნული საგამოძიებო მოქმედების კანონიერად/უკანონოდ ცნობის შესახებ მოსამართლის განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს. განჩინება ინსპექტორის სამსახურს წარედგინება მისი გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა, მატერიალური (დოკუმენტური) სახით (სსსკ-ის 143[3] მუხლის მე-7 ნაწილი).

ამდენად, სსსკ-ის მიხედვით, სასამართლოს განჩინების/პროკურორის დადგენილების ელექტრონული ეგზემპლარის (ასევე მატერიალური დოკუმენტის) მიწოდების წესი მოქმედებს სატელეფონო კომუნიკაციის ფარული მიყურადება/ჩაწერის შემთხვევაში; სხვა ფარულ საგამოძიებო მოქმედებებთან, მათ შორის, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ღონისძიებასთან მიმართებით კი მატერიალური სახით ხდება მითითებული საპროცესო დოკუმენტების ინსპექტორისთვის წარდგენა.

დ) სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიების შეჩერების მექანიზმი: 2017 წლის 22 მარტის ცვლილებებით ინსპექტორს მიენიჭა ღონისძიების შეჩერების უფლებამოსილება. ამასთან, აღნიშნული უფლებამოსილება ინსპექტორს გააჩნია მხოლოდ სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიებასთან მიმართებით.

აღსანიშნავია, რომ მანამდე არსებული კანონმდებლობით სხვაგვარი რეგულაცია იყო გათვალისწინებული, კერძოდ, მოქმედებდა ფარული საგამოძიებო მოქმედებების განხორციელების „ორეტაპიანი ელექტრონული სისტემა“, რომელიც გამორიცხავდა პერსონალურ მონაცემთა დაცვის ინსპექტორის[927] ელექტრონული თანხმობის გარეშე სამართალდამცავი ორგანოს მონიტორინგის სისტემის მეშვეობით ობიექტის აქტივაციის შესახებ ბრძანების დამოუკიდებლად განხორციელების შესაძლებლობას.[928] პერსონალურ მონაცემთა დაცვის ინსპექტორის[929] განმარტებით, ორეტაპიანი ელექტრონული სისტემის გაუქმება განპირობებული იყო რამდენიმე გარემოებით - პირველ რიგში, არსებობდა ეჭვი იმისა, რომ ასეთ შემთხვევაში პერსონალურ მონაცემთა დაცვის ინსპექტორი იქცეოდა პროცესის აღმასრულებლად და მაკონტროლებლის ფუნქციების განხორციელებისას არ იქნებოდა ნეიტრალური[930], ამასთან, არსებობდა პოზიციაც იმის თაობაზე, რომ ვინაიდან ფარული საგამოძიებო მოქმედებების განხორციელება ვერ იწყებოდა პერსონალურ მონაცემთა დაცვის

[927] იმ დროს მოქმედი კანონმდებლობის მიხედვით, გათვალისწინებული იყო „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობა.

[928] სსსკ-ის 2017 წლის 21 მარტისათვის არსებული რედაქციის მე-3 მუხლის 31-ე ნაწილი, სსმ, 31, 03/11/2009.

[929] იმ დროინდელი კანონმდებლობით გათვალისწინებული იყო „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობა.

[930] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-92.

ინსპექტორის თანხმობის გარეშე, ამ მხრივ, იგი სასამართლო გადაწყვეტილების აღსრულებას აფერხებდა, რადგან ფარული საგამოძიებო მოქმედებების განხორციელების სამართლებრივი საფუძველი პროკურორის დადგენილებასთან ერთად, სასამართლოს განჩინებაა.[931]

დღეს არსებული კანონმდებლობით, ინსპექტორს შეუძლია კონტროლის ელექტრონული სისტემით შეაჩეროს სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიება თუ:

ა) მისთვის სსსკ-ის 143^3 მუხლის 5^1 ნაწილით დადგენილი წესით მიწოდებული არ არის აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ მოსამართლის განჩინების ელექტრონული ეგზემპლარი, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს;

ბ) მისთვის სსსკ-ის 143^3 მუხლის მე-5 ნაწილით დადგენილი წესით, მატერიალური (დოკუმენტური) სახით წარდგენილი არ არის ნებართვის გაცემის შესახებ განჩინების ეგზემპლარი, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს;

გ) მისთვის სსსკ-ის 143^3 მუხლის 6^2 ნაწილით დადგენილი წესით მიწოდებული არ არის პროკურორის დადგენილების ელექტრონული ეგზემპლარი, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს;

დ) მისთვის სსსკ-ის 143^3 მუხლის 6^2 ნაწილით დადგენილი წესით, მატერიალური (დოკუმენტური) სახით წარდგენილი არ არის გადაუდებელი აუცილებლობის შემთხვევაში აღნიშნული ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარეზოლუციო ნაწილს;

ე) მისთვის ელექტრონული სისტემის მეშვეობით ან მატერიალური (დოკუმენტური) სახით წარდგენილი პროკურორის დადგენილების რეკვიზიტები ან/და სარეზოლუციო ნაწილი ბუნდოვანება-უზუსტობას შეიცავს;

ვ) მისთვის ელექტრონული სისტემის მეშვეობით წარდგენილი პროკურორის დადგენილების ელექტრონული ეგზემპლარის რეკვიზიტებსა და სარეზოლუციო ნაწილში და მატერიალური (დოკუმენტური) სახით წარდგენილი პროკურორის

[931] იქვე.

დადგენილების რეკვიზიტებსა და სარეზოლუციო ნაწილში სსსკ-ის 143[3] მუხლის მე-6 ნაწილით გათვალისწინებული მონაცემი ერთმანეთს არ ემთხვევა.

სსსკ-ის 143[3] მუხლი დეტალურად განსაზღვრავს, თუ რა წესით ხდება თითოეულ ამ შემთხვევაში შეჩერების საფუძვლის აღმოფხვრა და ღონისძიების გაგრძელება.

აღსანიშნავია, რომ საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის საოქმო ჩანაწერის მიხედვით, საკონსტიტუციო დავის ფარგლებში პერსონალურ მონაცემთა დაცვის ინსპექტორმა (იმ დროს მოქმედი კანონმდებლობის მიხედვით) გარკვეული ინფორმაცია მიაწოდა სასამართლოს მისი კონტროლის ფარგლებზე, კერძოდ, მიუთითა რომ „იგი ვერ შეაფასებს მოსამართლის მიერ მიწოდებული განჩინების კანონიერებას, მაგრამ სხვა მოცემულობაა პროკურორის დადგენილებასთან მიმართებით[932]. კერძოდ, იგი შეაჩერებს ფარული საგამოძიებო მოქმედების განხორციელებას მაშინაც, როდესაც პროკურორის დადგენილებით, ფარული საგამოძიებო მოქმედების განხორციელების შესახებ გადაწყვეტილება იქნება მიღებული ისეთ დანაშაულზე, რომელთან მიმართებითაც, კანონით, ფარული საგამოძიებო მოქმედების განხორციელება არ არის ნებადართული.“[933]

ე) *შესაგამისი ოქმების მიწოდების ვალდებულება* - ინსპექტორს მიეწოდება ფარული საგამოძიებო მოქმედების დასრულების ოქმი და ასევე ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალის განადგურების ოქმი (სსსკ-ის 143[6] მუხლის მე-14 ნაწილი; 143[8] მუხლის მე-5 ნაწილი). აღნიშნული წესები ეხება როგორც სატელეფონო კომუნიკაციის ფარული მიყურადების, ასევე ინტერნეტურთიერთობის მონიტორინგის ღონისძიებას. აღსანიშნავია, რომ ფარული საგამოძიებო მოქმედების დასრულების ოქმის ინსპექტორის სამსახურისთვის მიწოდების ვალდებულება განისაზღვრა სსსკ-ში 2017 წლის 22 მარტის ცვლილებებით, ხოლო მანამდე აღნიშნული მოთხოვნა გათვალისწინებული არ იყო.

3.1.2 ინსპექტირების უფლებამოსილება

ინსპექტირების უფლებამოსილება სახელმწიფო ინსპექტორს გააჩნია როგორც სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიებასთან

[932] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-93.
[933] იქვე.

მიმართებით, ასევე ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებითაც, მეტიც - თუკი სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებას აკონტროლებს კონტროლის ელექტრონული სისტემისა და კონტროლის სპეციალური ელექტრონული სისტემის მეშვეობით და კანონმდებლობით გათვალისწინებულ შემთხვევაში შეუძლია შეჩერების მექანიზმის გამოყენება, ინტერნეტკომუნიკაციასთან მიმართებით მას მხოლოდ ინსპექტირების შესაძლებლობა გააჩნია. ინსპექტირების უფლებამოსილებით სარგებლობს ინსპექტორი ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების შემოწმების მიზნით.

ინსპექტირება, გულისხმობს ინსპექტორის ბრძანებით განსაზღვრულ დროსა და ფარგლებში უფლებამოსილი პირების მიერ მონაცემთა დამმუშავებლის ან/და უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებას.[934] საქართველოს საკონსტიტუციო სასამართლოში მიმდინარე დავის ფარგლებში პერსონალურ მონაცემთა დაცვის ინსპექტორმა (იმ დროს მოქმედი კანონმდებლობით) განმარტა, რომ ინსპექტირების განხორციელებისას იყენებს აუდიტის მეთოდოლოგიას, მაგრამ მას არ ეწოდება აუდიტი, ეს არის მონაცემების დამუშავების კანონიერების შემოწმება.[935] თუმცა „პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის დებულების დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის 4 მარტის N1 ბრძანებაში 2018 წლის 28 დეკემბრის ცვლილებით[936] განისაზღვრა, რომ ინსპექტირების პროცესში ინსპექტირების სუბიექტს უფლება აქვს, განახორციელოს მონაცემთა დამუშავებისათვის, მათ შორის, ფარული საგამოძიებო მოქმედებების მიზნებისთვის, გამოყენებული ტექნიკური საშუალებებისა და ინფრასტრუქტურის (მათ შორის – კომპიუტერული სისტემა)

[934] „ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის წესის დამტკიცების შესახებ 2017 წლის 28 დეკემბრის N01/338 ბრძანების არასაიდუმლო N1 დანართი - **„**ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლთან დაკავშირებული ცალკეული ღონისძიებები და პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ინფორმაციული ტექნოლოგიებისა და ინსპეტირების დეპარტამენტის ფუნქციები,“ მუხლი 15, მე-2 პუნქტი.

[935] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-97.

[936] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის 4 მარტის N1 ბრძანება ძალადაკარგულია „სახელმწიფო ინსპექტორის სამსახურის დებულების დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 22 მაისის N1 ბრძანებით.

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონთან შესაბამისობის ტექნიკური აუდიტი (შემოწმება) (მე-18 მუხლის პირველი პუნქტის „გ“ ქვეპუნქტი).[937] ამდენად, ინფრასტრუქტურის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობის დადგენის მიზნით განხორციელებული შემოწმება განისაზღვრა, როგორც ტექნიკური აუდიტი.

აღსანიშნავია, რომ ინსპექტირება ტარდება ინსპექტირების შესახებ ბრძანებით განსაზღვრულ დროსა და ფარგლებში, რომელსაც ადგენს ინსპექტორი (ან მის მიერ ბრძანების გამოცემაზე უფლებამოსილი პირი), შესამოწმებელი საკითხის სირთულის, მოცულობის და სპეციფიკის გათვალისწინებით[938]. „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანების 26-ე მუხლის პირველი პუნქტის თანახმად, ინსპექტირების მიზნების მისაღწევად ინსპექტირების სუბიექტი იყენებს სხვადასხვა მეთოდებს და ტექნიკას. აღსანიშნავია, რომ საქართველოს საკონსტიტუციო სასამართლოში 2017 წელს წარდგენილ საკონსტიტუციო სარჩელში მოსარჩელეები პერსონალურ მონაცემთა დაცვის ინსპექტორის (იმ დროს მოქმედი კანონმდებლობით) მიერ ფარული საგამოძიებო მოქმედებების ჩასატარებლად განკუთვნილი ტექნიკური ინფრასტრუქტურის შემოწმების არსებული მექანიზმის ერთ-ერთი ძირითადი კრიტიკის საფუძვლად სწორედ იმას მიუთითებენ, რომ „ინსპექტორს არ გააჩნია მეთოდოლოგია, თუ რა გზებით ხდება ინსპექტირება, კერძოდ, რა მეთოდოლოგიის გამოყენებით ამოწმებს იგი პროგრამული ინტერფეისების გამართულობას.“[939] ამ თვალსაზრისით აღსანიშნავია, რომ „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანებით ნორმატიულად დადგენილ იქნა ინსპექტირების განხორციელების დროს

[937] დღეს აღნიშნული ჩანაწერი მოცემულია „სახელმწიფო ინსპექტორის სამსახურის დებულების დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 22 მაისის N1 ბრძანების მე-15 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტსა და „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანების მე-13 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტში.

[938] „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანების მე-6 მუხლის მე-2 პუნქტი, www.matsne.gov.ge, 03/07/2019.

[939] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-47.

გამოსაყენებელი მეთოდების ჩამონათვალი და აღწერილობა, როგორიცაა მაგალითად, კითხვარები, შეკითხვები, დოკუმენტების შესწავლა, ზეპირი განხილვა, ინფორმაციისა და დოკუმენტების გამოთხოვა, დოკუმენტების შესწავლა და სხვ. ამავე ბრძანებიდან გამომდინარე, ინსპექტირების პროცესში გამოსაყენებელი მეთოდების ჩამონათვალი ამომწურავი სახით არ არის განსაზღვრული და ინსპექტირების პროცესში შესაძლებელია გამოყენებულ იქნეს ყველა ის მეთოდი და ტექნიკა, რომელიც რელევანტურია და დაეხმარება ინსპექტირების სუბიექტს მტკიცებულების მოპოვებაში და რომელთა გამოყენება არ ეწინააღმდეგება საქართველოს კანონმდებლობას. ამასთან, ინსპექტირების ჩასატარებლად გამოსაყენებელი მეთოდების და ტექნიკის არჩევანი დამოკიდებულია ინსპექტირების მიზანზე, მოცულობაზე და ინსპექტირების ობიექტის მიერ მონაცემთა დამუშავების სპეციფიკაზე (26-ე მუხლის პირველი პუნქტი). ამავდროულად, ამავე ბრძანების 32-ე მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტიდან გამომდინარე, მონაცემთა დამუშავებისათვის გამოყენებული კომპიუტერული ინფრასტრუქტურის, მათ შორის, კომპიუტერული სისტემის, უსაფრთხოების და კანონთან შესაბამისობის ტექნიკური აუდიტის (შემოწმება) ჩატარების მიზნით გამოიყენება ადგილზე შემოწმების მეთოდი. აღნიშნულთან დაკავშირებით ნიშანდობლივია, რომ კომპიუტერული ინფრასტრუქტურის, მათ შორის, კომპიუტერული სისტემების, შემოწმების მიზნით მოცემულ ბრძანებაში ინსპექტირების შესაბამისი მეთოდის (ადგილზე შემოწმება) განსაზღვრის მიუხედავად, 32-ე მუხლის ფორმულირება საკმაოდ ზოგადია და მიზანშეწონილი იქნებოდა მეტი კონკრეტიკის გათვალისწინება კომპიუტერული სისტემების შემოწმების კონტექსტში გამოსაყენებელ მეთოდოლოგიასთან დაკავშირებით.

„სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მე-7 პუნქტი სპეციალურად არეგულირებს ინსპექტორის უფლებამოსილებებს ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით სააგენტოს შემოწმების (ინსპექტირების) განხორციელებისას, კერძოდ, ინსპექტორის სამსახური ასეთ შემთხვევაში უფლებამოსილია: „ა) შევიდეს სააგენტოს შეზღუდული დაშვების არეალში და მიმდინარე რეჟიმში დააკვირდეს უფლებამოსილი ორგანოების მიერ საქმიანობის განხორციელებას; ბ) გაეცნოს სააგენტოს საქმიანობის მარეგულირებელ (მათ შორის, სახელმწიფო საიდუმლოების შემცველ) სამართლებრივ დოკუმენტებს და

ტექნიკურ ინსტრუქციებს; გ) მიიღოს ინფორმაცია ფარული საგამოძიებო მოქმედებების მიზნებისთვის გამოყენებული ტექნიკური ინფრასტრუქტურის შესახებ და შეამოწმოს ეს ინფრასტრუქტურა; დ) სააგენტოს მოსამსახურეებს მოსთხოვოს ახსნა-განმარტებები შემოწმების (ინსპექტირების) განხორციელებისას გამოვლენილ ცალკეულ საკითხებთან დაკავშირებით; ე) განახორციელოს ამ კანონით გათვალისწინებული სხვა უფლებამოსილებები.“[940]

„ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის წესის დამტკიცების შესახებ“ პერსონალურ მონაცემთა დაცვის ინსპექტორის 2017 წლის 28 დეკემბრის N01/338 ბრძანების არასაიდუმლო N1 დანართი - „ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლთან დაკავშირებული ცალკეული ღონისძიებები და პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ინფორმაციული ტექნოლოგიებისა და ინსპექტირების დეპარტამენტის ფუნქციები“[941] ასევე არეგულირებს ინსპექტირების განხორციელების პროცესში შემოწმებაზე უფლებამოსილი პირის უფლებებსა და მოვალეობებს, კერძოდ, აღნიშნული დანართის მე-17 მუხლის თანახმად, შემოწმებაზე უფლებამოსილ პირს უფლება აქვს: ა) ნებისმიერი პირისგან გამოითხოვოს ნებისმიერი ინფორმაცია ან/და დოკუმენტები, მათ შორის, პერსონალური მონაცემების, სახელმწიფო, კომერციული, პროფესიული, საგადასახადო, საბანკო და სხვა საიდუმლოების შემცველი ინფორმაცია ან/და დოკუმენტები (გარდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული გამონაკლისისა); ბ) ინსპექტირების განსახორციელებლად შევიდეს ნებისმიერ საჯარო და კერძო დაწესებულებაში (მათ შორის შეზღუდული დაშვების არეალებში), გაეცნოს ნებისმიერ დოკუმენტს, ინფორმაციას და მასალას (მათ შორის ელექტრონული სახის), მიიღოს ნებისმიერი

[940] ინსპექტირების სუბიექტის უფლება-მოვალეობები ასევე განსაზღვრულია „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანების მე-13 მუხლით, www.matsne.gov.ge, 03/07/2019.

[941] ინსპექტორის სამსახურის 2020 წლის 23 ივნისის წერილის (№ SIS 8 20 00009512) თანახმად, პერსონალურ მონაცემთა დაცვის ინსპექტორის აღნიშნული ბრძანება და მისი N1 არასაიდუმლო დანართი ჯერჯერობით (2020 წლის 23 ივნისის მდგომარეობით) იურიდიული ძალის მქონეა.

დოკუმენტი ან მისი ასლი, ამონაწერი, ამონაბეჭდი, მიმდინარე რეჟიმში დააკვირდეს საქმიანობის პროცესს, მოახდინოს ფოტო და ვიდეო გადაღება, აუდიოჩაწერა, ტესტირება, მიიღოს ინფორმაცია ფარული საგამოძიებო მოქმედებების მიზნებისათვის გამოყენებული ტექნიკური ინფრასტრუქტურის შესახებ და შეამოწმოს ეს ინფრასტრუქტურა; მოითხოვოს ახსნა-განმარტებები ინსპექტირების პროცესში გამოვლენილ ცალკეულ საკითხებთან დაკავშირებით; გ) მოიპოვოს მტკიცებულებები და ამ მიზნით განახორციელოს შესაბამისი მოქმედებები; დ) შეადგინოს შემოწმების ოქმი და ადმინისტრაციული სამართალდარღვევის ოქმი; ე) მოამზადოს შემოწმების დასრულების შესახებ ინსპექტორის გადაწყვეტილების პროექტი და წარუდგინოს ინსპექტორს; ვ) განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებამოსილებები.”

რაც შეეხება დარღვევის აღმოჩენის შემთხვევაში ინსპექტორის სამსახურის კომპეტენციას, „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-16 მუხლი განსაზღვრავს ინსპექტორის სამსახურის ზოგად უფლებამოსილებებს კანონით გათვალისწინებულ ნებისმიერ სფეროში დარღვევასთან მიმართებით. აღნიშნული კანონის პირველი პუნქტის თანახმად, თუ ინსპექტორის სამსახური გამოავლენს ამ კანონის ან მონაცემთა დამუშავების მარეგულირებელი სხვა ნორმატიული აქტის დარღვევას, იგი უფლებამოსილია გამოიყენოს ერთ-ერთი ან ერთდროულად რამდენიმე შემდეგი ღონისძიება: მოითხოვოს დარღვევისა და მონაცემთა დამუშავებასთან დაკავშირებული ნაკლოვანებების მის მიერ მითითებული ფორმით და მითითებულ ვადაში გამოსწორება; მოითხოვოს მონაცემთა დამუშავების დროებით ან სამუდამოდ შეწყვეტა, თუ მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის მიერ მონაცემთა უსაფრთხოების დაცვისთვის მიღებული ზომები და განხორციელებული პროცედურები არ შეესაბამება საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს; მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, მონაცემთა დაბლოკვა, წაშლა, განადგურება ან დეპერსონალიზაცია, თუ მიიჩნევს, რომ მონაცემთა დამუშავება საქართველოს კანონმდებლობის დარღვევით ხორციელდება; მოითხოვოს მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისთვის გადაცემის შეწყვეტა, თუ მონაცემთა გადაცემა საქართველოს კანონმდებლობის დარღვევით ხორციელდება; წერილობით მისცეს რჩევები და გაუწიოს რეკომენდაცია მონაცემთა

დამმუშავებელს ან/და უფლებამოსილ პირს მის მიერ მონაცემთა დამუშავებასთან დაკავშირებული წესების უმნიშვნელოდ დარღვევის შემთხვევაში; დამრღვევს დააკისროს ადმინისტრაციული პასუხისმგებლობა.

საკითხავია, ვრცელდება თუ არა ზემოაღნიშნულ მუხლში მითითებული ყველა უფლებამოსილება ფარულ საგამოძიებო მოქმედებებთან მიმართებით? მაგალითად, აქვს თუ არა ინსპექტორის სამსახურს ღონისძიების შეწყვეტის უფლებამოსილება, თუკი მიიჩნევს, რომ ირღვევა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა დამუშავების რომელიმე პრინციპი? ღონისძიების შეწყვეტასთან დაკავშირებით აღსანიშნავია, რომ ეს უფლება სსსკ-ის 143[6] მუხლის პირველი ნაწილიდან გამომდინარე, მინიჭებული აქვს მხოლოდ პროკურორს, შესაბამისად, ინსპექტორის სამსახური ვერ მოითხოვს ღონისძიების შეწყვეტას, თუნდაც აღმოაჩინოს, რომ მისი მიმდინარეობისას ირღვევა კანონმდებლობის მოთხოვნები. თუკი ინსპექტორის სამსახურს არ გააჩნია ფარული საგამოძიებო მოქმედების შეწყვეტის უფლებამოსილება, მიუხედავად იმისა, რომ მე-16 მუხლი ფარული საგამოძიებო მოქმედებების კონტექსტში ამ უფლებასთან მიმართებით რაიმე საგამონაკლისო დათქმას არ ითვალისწინებს, ხომ არ ნიშნავს ეს იმას, რომ ამ ნორმაში ჩამოთვლილი სხვა უფლებებიც შეიძლება იყოს არარელევანტური ფარულ საგამოძიებო მოქმედებებთან მიმართებით? მითუმეტეს, რომ ზემოთ აღნიშნული N1 დანართი, სადაც გაწერილია შემოწმებაზე პასუხისმგებელი პირის უფლებები, ყურადღებას ამახვილებს მხოლოდ ადმინისტრაციული სამართალდარღვევის ოქმის შედგენაზე და არ აკონკრეტებს დარღვევის აღმოჩენისას ინსპექტორის სამსახურის სხვა მნიშვნელოვან უფლებებს, არამედ ზოგადად, „კანონმდებლობით მინიჭებულ სხვა უფლებამოსილებებზე საუბრობს“. ამ თვალსაზრისით, საკითხავია, აქვს თუ არა მაგალითად, ინსპექტორის სამსახურს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურების მოთხოვნის უფლება, თუკი ამ ინფორმაციის მოპოვება კანონმდებლობის მოთხოვნათა დარღვევით განხორციელდა? ამ კუთხით ნიშანდობლივია, რომ ეს საკითხი კანონმდებლობით არც თუ ისე ცალსახა და ერთმნიშვნელოვანია - ერთი მხრივ, „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-16 მუხლიდან გამომდინარე, ინსპექტორს გააჩნია ეს უფლებამოსილება, თუმცა, მეორე მხრივ, გასათვალისწინებელია სსსკ-ით დადგენილი

წესი და პროცედურა ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურების საკითხთან დაკავშირებით, რომელიც არაფერს ამბობს ინსპექტორის ამ უფლებამოსილებით აღჭურვაზე.

მიუხედავად იმისა, რომ განსახილველ საკითხს კანონმდებლობა არც თუ ისე ნათლად არეგულირებს, მართებული იქნება დავასკვნათ, რომ „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-16 მუხლი ასევე მთელი მოცულობით ვრცელდება ფარულ საგამოძიებო მოქმედებებზე, თუკი ამ მუხლში აღნიშნული რომელიმე უფლების ინსპექტორის სამსახურისთვის მინიჭება წინააღმდეგობაში არ მოდის სხვა საკანონმდებლო აქტის მოთხოვნასთან (მაგალითად, ღონისძიების შეწყვეტის შემთხვევაში). აღნიშნული განპირობებულია იმით, რომ მე-16 მუხლი არის ზოგადი შინაარსის და ამავდროულად, არ აკეთებს საგამონაკლისო დათქმას ფარულ საგამოძიებო მოქმედებებთან მიმართებით. აქედან გამომდინარე, შეიძლება ითქვას, რომ ინსპექტორს ასევე უნდა გააჩნდეს ღონისძიების შედეგად მოპოვებული ინფორმაციის განადგურების მოთხოვნის უფლებაც, თუკი მიიჩნევს, რომ ირღვევა მონაცემთა დამუშავებასთან დაკავშირებული კანონმდებლობის მოთხოვნები.

თუმცა მეტი სამართლებრივი სიცხადისთვის მიზანშეწონილი იქნება, ზემოაღნიშნული N1 დანართის მე-17 მუხლში, რომელიც სპეციალურად არეგულირებს ინსპექტორის სამსახურის შესაბამისი პირის კომპეტენციას ფარული საგამოძიებო მოქმედებების ინსპექტირების პროცესში, უფრო ცხადად და ამომწურავად განისაზღვროს იმ უფლებების ჩამონათვალი, რომლითაც ეს პირი აღჭურვილია ასეთ შემთხვევაში.

საინტერესოა ასევე, რა სახის დარღვევებზე შეიძლება გააჩნდეს ინსპექტორს ინფორმაციის განადგურების მოთხოვნის უფლებამოსილება; შეუძლია თუ არა მაგალითად, კონტროლი სსსკ-ის 143[7] მუხლით გათვალისწინებული მინიმუმამდე დაყვანის პრინციპის დაცვაზე, მაგალითისთვის, შეუძლია თუ არა მოითხოვოს მოპოვებული ინფორმაციის განადგურება, თუკი ჩათვლის, რომ ღონისძიების განხორციელებისას იმაზე მეტი მოცულობის ინფორმაციის მოპოვება ხდება, ვიდრე ეს აუცილებელია. პრაქტიკული თვალსაზრისით ინსპექტორს გაუჭირდება აღნიშნული მოთხოვნის დაცვაზე ზედამხედველობა, ვინაიდან ინფორმაციის გამიჯვნას და

გაფილტვრას ღირებულების თვალსაზრისით ახდენს გამომძიებელი[942] და რთული წარმოსადგენია, ინსპექტორმა მიუთითოს მას, რომელი ინფორმაცია წარმოადგენს ღირებულს გამოძიებისათვის. თუმცა თეორიულად ინსპექტორს აქვს უფლებამოსილება, გავლენა მოახდინოს ამ პროცესზე - მოითხოვოს ღონისძიების ფარგლების მინიმუმამდე დაყვანა, მაგალითად, გამოძიებასთან კავშირში არმყოფი პირების კომუნიკაციის მონიტორინგის შეზღუდვა, რაც საკმაოდ მნიშვნელოვანი ბერკეტი შეიძლება იყოს ეფექტიანი კონტროლის თვალსაზრისით.

როგორც უკვე აღინიშნა, ინსპექტორის სამსახურს მიეწოდება ღონისძიების დასრულების შესახებ ოქმი და მოპოვებული მასალის განადგურების შესახებ ოქმი. მასალის განადგურების შესახებ ოქმით შეუძლია, მაგალითად, შემდეგი სახის კონტროლის განხორციელება - თუკი გამოითხოვს ინფორმაციას ან ინსპექტირების დროს დაადგენს, თუ რა მოცულობის ინფორმაცია მიეწოდა დაცვის მხარეს (სსსკ-ის 83-ე მუხლის მე-6 ნაწილის თანახმად, წინასასამართლო სხდომამდე 5 დღით ადრე დაცვის მხარეს უნდა მიეწოდოს ყველა ის ინფორმაცია, რომლის მტკიცებულებად წარდგენასაც ბრალდების მხარე აპირებს), ან თუკი ინსპექტირების განხორციელების დროს გაარკვევს, თუ რა ოდენობის ინფორმაცია იქნა ღონისძიების შედეგად მოპოვებული, ეს მონაცემები შეუძლია შეადაროს განადგურების ოქმს და გააკეთოს გარკვეული დასკვნები ან/და შესაძლოა გამოავლინოს სამართალდარღვევა. ამასთან დაკავშირებით ნიშანდობლივია, რომ სსსკ-ის 143[6] მუხლის მე-14 ნაწილი, სადაც საუბარია ფარული საგამოძიებო მოქმედების დასრულების შემდეგ ოქმის შედგენის საკითხზე, არ ითვალისწინებს ოქმში მოპოვებული ინფორმაციის შესახებ მონაცემების დაფიქსირების მოთხოვნას. თუკი სსსკ ამგვარ ვალდებულებას გაითვალისწინებს, მიგვაჩნია, რომ ინსპექტორს გაცილებით გაუადვილდება კონტროლი მოპოვებული ინფორმაციის შენახვისა და განადგურების კანონიერებაზე და შესაძლებლობა ექნება, ღონისძიების დასრულებისა და მასალის განადგურების შესახებ ოქმების შედარებით უფრო ეფექტიანად გამოკვეთოს შესაძლო დარღვევა.

[942] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-82.

3.1.3 სტატისტიკური მონაცემები კონკრეტულ პირთა მიმართ ჩატარებული ფარული საგამოძიებო მოქმედებების შესახებ

ინსპექტორის სამსახურისგან გამოთხოვილი საჯარო ინფორმაციის თანახმად, 2017 წლიდან 2019 წლის 1 სექტემბრამდე, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ჩატარებისას მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით ჩატარდა 8 შემოწმება (ინსპექტირება)[943]. აქედან, 3 შემოწმება განხორციელდა მონაცემთა სუბიექტის მიმართვის საფუძველზე, ხოლო 5 შემოწმება - ინსპექტორის ინიციატივით[944]. სამ შემთხვევაში გამოვლინდა ადმინისტრაციული სამართალდარღვევის ფაქტი, ხოლო შემოწმების პროცესში გამოვლენილ ხარვეზებთან მიმართებით „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-16 მუხლის შესაბამისად, მონაცემთა დამმუშავებლებს/უფლებამოსილ პირებს მიეცათ შესაბამისი რეკომენდაციები და დავალებები მონაცემთა დამუშავების პროცესში არსებული ნაკლოვანებების აღმოფხვრის მიზნით.[945]

მოწოდებული ინფორმაციის თანახმად, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების განხორციელების შედეგად მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით ჩატარდა 4 შემოწმება (ინსპექტირება)[946]. აქედან, 2 შემოწმება განხორციელდა მონაცემთა სუბიექტის მომართვის საფუძველზე, ხოლო ორ შემთხვევაში ინსპექტირების პროცესი დაიწყო ინსპექტორის ინიციატივით. აღსანიშნავია, რომ ხსენებული შემოწმებების შედეგად სამართალდარღვევის ფაქტი არ გამოვლენილა[947].

---

[943] სახელმწიფო ინსპექტორის სამსახურის 2019 წლის 18 სექტემბრის წერილი (№SIS 1 19 00003946); სახელმწიფო ინსპექტორის სამსახურს წარედგინა განცხადება შემდეგი საჯარო ინფორმაციის მოთხოვნის თაობაზე: 1) 2017 წლიდან 2019 წლის 1 სექტემბრამდე, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების – სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის - კონტროლის მიზნით განხორციელებული ინსპექტირებების რაოდენობა, რომლის მიზანსაც წარმოადგენდა კონკრეტულ პირთა მიმართ ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერების შესწავლა. ასევე სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედებების რაოდენობა, რომლებსაც შეეხო ეს ინსპექტირებები, ასევე გამოვლენილი დარღვევების რაოდენობა; 2) იგივე ინფორმაცია სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით.

[944] იქვე.

[945] იქვე.

[946] იქვე.

[947] იქვე.

თუმცა, შემოწმების პროცესში გამოვლენილ ხარვეზებთან მიმართებით „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-16 მუხლის შესაბამისად, მონაცემთა დამმუშავებლებს/უფლებამოსილ პირებს მიეცათ შესაბამისი რეკომენდაციები და დავალებები მონაცემთა დამუშავების პროცესში არსებული ნაკლოვანებების აღმოფხვრის მიზნით.[948]

მოწოდებული ინფორმაციის მიხედვით, შემოწმების ფარგლებში შესწავლილი ფარული საგამოძიებო მოქმედებების ობიექტთა რაოდენობასთან დაკავშირებით - სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტთან მიმართებით მონაცემთა სუბიექტის მომართვის საფუძველზე განხორციელებული 3 შემოწმების ფარგლებში შესწავლილ იქნა - 8 ობიექტი, ხოლო კოდექსის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტთან მიმართებით მონაცემთა სუბიექტის მომართვის საფუძველზე განხორციელებული 2 შემოწმების ფარგლებში შესწავლილ იქნა - 8 ობიექტი[949]. მოწოდებული ინფორმაციის თანახმად, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებთან მიმართებით შემოწმების ინსპექტორის ინიციატივის საფუძველზე დაწყების შემთხვევაში მოწმდება, როგორც ფარული საგამოძიებო მოქმედებების ჩატარებისას გამოყენებული ტექნიკური ინფრასტრუქტურა, ასევე შესაბამისი დოკუმენტაცია, მათ შორის, პროკურორის დადგენილებები და სასამართლოს განჩინებები, რომელიც შესაძლოა მიემართებოდეს როგორც ერთ ასევე, რამდენიმე ობიექტს[950]. ამასთან, მოწოდებული ინფორმაციის მიხედვით, ინსპექტორის ინიციატივით ჩატარებული შემოწმებისას არ წარმოებს შესწავლას დაქვემდებარებული ფარული საგამოძიებო მოქმედებების ობიექტთა რაოდენობის აღრიცხვა.[951]

ინსპექტორის სამსახურიდან ასევე გამოთხოვილ იქნა 2019 წლის 1 სექტემბრიდან 2020 წლის 1 მარტამდე პერიოდისათვის ჩატარებული შემოწმებების შესახებ ინფორმაცია, საიდანაც ირკვევა, რომ სსსკ-ის 143[3] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების ჩატარებისას მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით ჩატარდა 3 შემოწმება,

[948] იქვე.
[949] იქვე.
[950] იქვე.
[951] იქვე.

რომლის ფარგლებშიც შესწავლილ იქნა შესაბამისი დოკუმენტაცია, მათ შორის, 2 სასამართლოს განჩინება და 1 პროკურორის დადგენილება; აღნიშნულის შედეგად გამოვლინდა 2 სამართალდარღვევის ფაქტი[952]. რაც შეეხება სსსკ-ის 143^3 მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ღონისძიებას, ჩატარებული 1 შემოწმების ფარგლებში დარღვევა არ გამოვლენილა, თუმცა მონაცემთა დამმუშავებელს მიეცა 3 დავალება და 4 რეკომენდაცია[953]. ამასთან, ინსპექტორის სამსახურის მიერ მოწოდებულ წერილში ასევე ხაზგასმულია, რომ შემოწმების ინსპექტორის ინიციატივით დაწყების შემთხვევაში შემოწმებისას არ წარმოებს შესწავლას დაქვემდებარებული ფარული საგამოძიებო მოქმედებების რაოდენობის, შესწავლილი დოკუმენტაციის, მათ შორის, სასამართლოს განჩინებებისა და პროკურორის დადგენილებების აღრიცხვა.[954]

საბოლოო ჯამში, გამოთხოვილი საჯარო ინფორმაციიდან შეგვიძლია შემდეგი დასკვნების გამოტანა: ა) ინსპექტირების უფლებამოსილება პრაქტიკაში გამოიყენება როგორც სატელეფონო კომუნიკაციის ფარულ მიყურადებასთან, ასევე ინტერნეტურთიერთობის მონიტორინგის ღონისძიებასთან მიმართებით. მოწმდება როგორც ღონისძიების ჩატარებისას გამოყენებული ტექნიკური ინფრასტრუქტურა, ასევე შესაბამისი დოკუმენტაცია, მათ შორის, პროკურორის დადგენილებები და სასამართლოს განჩინებები, რაც ინსპექტირების ეფექტიანობის კუთხით მისასალმებელია; ბ) თუმცა ზუსტი ინფორმაციის გარკვევა, სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული რამდენი ფარული საგამოძიებო მოქმედების შესწავლა ხდება ინსპექტირების ფარგლებში, ასევე შესწავლილი სასამართლოს განჩინებების და პროკურორის დადგენილებების რაოდენობის გარკვევა შეუძლებელია, რადგან ინსპექტორის ინიციატივით განხორციელებული შემოწმებების შემთხვევაში ამ ინფორმაციის აღრიცხვა არ წარმოებს; 2) სასურველი იქნებოდა, ხორციელდებოდეს აღნიშნული მონაცემების შესახებ სტატისტიკის წარმოებაც, რათა უკეთ წარმოჩენილიყო საერთო სურათი, თუ

[952] სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 5 მაისის წერილი (№:SIS 5 20 00006422).
[953] იქვე.
[954] იქვე.

რამდენად მასშტაბურად და ინტენსიურად ხორციელდება ინსპექტირებები და რა მოცულობის დოკუმენტები მოწმდება.

3.2 ზედამხედველი მოსამართლე

აღსანიშნავია, რომ 2018 წლის 21 ივლისს სსსკ-ში განხორციელებული ცვლილებებით შემოღებულ იქნა ფარული საგამოძიებო მოქმედებების კონტროლის ახალი მექანიზმი ზედამხედველი მოსამართლის ინსტიტუტის სახით. აღნიშნული განპირობებულ იქნა კანონმდებლობაში განხორციელებული ცვლილებებით, რომლითაც ინსპექტორის სამსახურს მიენიჭა გარკვეული დანაშაულების გამოძიების უფლებამოსილება, რომელთა ჩამონათვალიც განსაზღვრულია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონით (მუხლი 19). აქედან გამომდინარე, ზედამხედველი მოსამართლის დანიშნულებას წარმოადგენს ინსპექტორის სამსახურის წარმოებაში არსებულ სისხლის სამართლის საქმეებზე სსსკ-ით დადგენილი წესით და ფარგლებში განახორციელოს კონტროლი ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით.

სსსკ-ის მე-3 მუხლის 32^1 ნაწილის თანახმად, ზედამხედველი მოსამართლე არის საქართველოს უზენაესი სასამართლოს თავმჯდომარის მიერ განსაზღვრული საქართველოს უზენაესი სასამართლოს მოსამართლე. ამავე ნაწილის შესაბამისად, ზედამხედველი მოსამართლე აკონტროლებს სსსკ-ის 143^1 მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების სტაციონარული ტექნიკური შესაძლებლობის გამოყენებით ჩატარებას კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით; ხოლო ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებულ აქტივობებს - ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემით.

იქედან გამომდინარე, რომ ზედამხედველი მოსამართლის ფუნქციას წარმოადგენს კონტროლის განხორციელება ინსპექტორის ნაცვლად, ინსპექტორის წარმოებაში არსებულ საქმეებზე, სსსკ აღჭურვავს მას ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული იმ უფლებამოსილებებით, რომლებიც სსსკ-ის ფარგლებში ინსპექტორს აქვს მინიჭებული.

3.3. შეჯამება

ამდენად, კანონმდებლობა განსაზღვრავს ინსპექტორის სამსახურის მხრიდან კონტროლის განსხვავებულ შესაძლებლობებს განსახილველ ღონისძიებებზე. აღსანიშნავია, რომ სატელეფონო კომუნიკაციის ფარულ მიყურადებასთან დაკავშირებით ინსპექტორი აღჭურვილია ზედამხედველობის მრავალმხრივი ბერკეტებით, მაგალითად, კონტროლის ელექტრონული საშუალებებით, მათ შორის, ღონისძიების შეჩერების უფლებამოსილებით.

ინსპექტორის კონტროლის გაძლიერების კუთხით გამოითქვა მოსაზრება, რომ მიზანშეწონილია, ფარული საგამოძიებო მოქმედების დასრულების შესახებ ოქმში აისახოს ინფორმაცია მოპოვებული მონაცემების შესახებ, რადგან ცალკე აღებული განადგურების შესახებ ოქმი, მოპოვებული მონაცემების შესახებ ინფორმაციის გარეშე, შესაძლოა არ იყოს საკმარისად ინფორმაციული მოპოვებული მასალის განადგურებასთან დაკავშირებული მოთხოვნების დაცვის შემოწმების თვალსაზრისით. ასევე გამოითქვა შეხედულება ინსპექტორის ზემოთ ხსენებული ბრძანების N1 დანართში ინსპექტირების პროცესში შემოწმებაზე პასუხისმგებელი პირის ხელთ არსებული უფლებამოსილებების უფრო მკაფიოდ და ამომწურავი სახით რეგულირების თაობაზე, რათა არ დარჩეს კითხვის ნიშნები მის კომპეტენციასთან დაკავშირებით მსგავსად მნიშვნელოვანი ფუნქციის განხორციელების დროს.

ამასთან, ინსპექტირების უფლებამოსილების პრაქტიკაში გამოყენებასთან დაკავშირებით საზოგადოების მეტად ინფორმირების კუთხით სასურველი იქნებოდა ინსპექტორის ინიციატივით ჩატარებული ინსპექტირებების დროს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული შესწავლილი ფარული საგამოძიებო მოქმედებების რაოდენობის და დოკუმენტაციის (სასამართლოს განჩინებები/პროკურორის დადგენილებები) შესახებ სტატისტიკის წარმოება.

ქვემოთ უფრო დეტალურად გვექნება საუბარი ინსპექტორის სამსახურის საზედამხედველო ფუნქციებზე კონსტიტუციურ-სამართლებრივ სტანდარტებთან შესაბამისობის ჭრილში.

4. კონსტიტუციურ-სამართლებრივი სტანდარტები ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების საპროცესო ღონისძიებებთან დაკავშირებით

4.1 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით დადგენილი მოთხოვნები

4.1.1 სახელმწიფო უსაფრთხოების სამსახურის მიერ ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობა და მისი ადმინისტრირების ფუნქცია

საქართველოს საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილს გამოიტანა უაღრესად მნიშვნელოვანი გადაწყვეტილება ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების სფეროში, რომლითაც დადგენილ იქნა კონსტიტუციურ-სამართლებრივი ჩარჩოები ამ სფეროს მარეგულირებელი კანონმდებლობის მიმართ.[955]

ხსენებული გადაწყვეტილებით არაკონსტიტუციურად იქნა ცნობილი „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის 8^3 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი, რომელიც ფარული საგამოძიებო მოქმედებების განსახორციელებლად შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს – სახელმწიფო უსაფრთხოების სამსახურს ანიჭებდა უფლებამოსილებას, ჰქონოდა კავშირგაბმულობის არხებთან პირდაპირი მიერთებისა და გადაცემული ინფორმაციის რეალურ დროში მიღების ტექნიკური შესაძლებლობა[956], კერძოდ, სადავო ნორმა ითვალისწინებდა სახელმწიფო უსაფრთხოების სამსახურის უფლებამოსილებას, „ჰქონოდა კავშირგაბმულობისა და კომუნიკაციის ფიზიკური ხაზებიდან და მათი შემაერთებლებიდან, მეილსერვერებიდან, ბაზებიდან, სასადგურე აპარატურიდან, კავშირგაბმულობის ქსელებიდან და კავშირგაბმულობის სხვა შემაერთებლებიდან ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობა და ამ მიზნით კომუნიკაციის აღნიშნულ საშუალებებთან, საჭიროების შემთხვევაში, უსასყიდლოდ განეთავსებინა მართლზომიერი გადაჭერის მენეჯმენტის სისტემა და სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები.“[957]

---

[955] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება.
[956] იქვე.
[957] იქვე.

სადავო ნორმის თანახმად, ინფორმაციის რეალურ დროში მოპოვების მიზნით, სახელმწიფო უსაფრთხოების სამსახური, კომუნიკაციის აღნიშნულ საშუალებებთან განათავსებდა „მართლზომიერი გადაჭერის მენეჯმენტის სისტემას.“[958] საკონსტიტუციო სასამართლოს განმარტებით, „მართლზომიერი გადაჭერის მენეჯმენტის სისტემა სახელმწიფო უსაფრთხოების სამსახურს უშუალოდ აკავშირებდა კავშირგაბმულობის არხთან.“ იმავდროულად, სადავო ნორმები უფლებამოსილ ორგანოს აღჭურავდა შესაძლებლობით, კომუნიკაციის დასახელებულ საშუალებებთან განეთავსებინა და დაემონტაჟებინა „სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის მოწყობილობები.“[959]

საკონსტიტუციო სასამართლოს გადაწყვეტილებით არაკონსტიტუციურად იქნა ცნობილი არა ზოგადად სახელმწიფოს მიერ ინფორმაციის რეალურ დროში მიღების ტექნიკური შესაძლებლობის ფლობა, არამედ ამ უფლებამოსილებით „პროფესიულად დაინტერესებული“ და „გამოძიებაზე პასუხისმგებელი ორგანოს“ - სახელმწიფო უსაფრთხოების სამსახურის აღჭურვა, კერძოდ, სასამართლოს განმარტებით, „როდესაც სტრუქტურა პასუხისმგებელია წარმატებულ გამოძიებაზე, ბუნებრივია, მის ინტერესებში შედის, მოიპოვოს რაც შეიძლება მეტი ინფორმაცია[960]. შესაბამისად, სახელმწიფო ორგანოების პირდაპირი და მუდმივი წვდომა ელექტრონული კომუნიკაციის მომსახურების მიმწოდებლებთან არსებულ მონაცემებზე და თავად ელექტრონული კომუნიკაციის პროცესზე განუზომლად ზრდიდა ცდუნებას და რისკებს, გამოძიების ინტერესებიდან გამომდინარე, უფლებაში დაუსაბუთებელი და გაუმართლებელი ჩარევისათვის.“[961]

ამასთან, არსებითი მნიშვნელობა მიენიჭა იმ გარემოებას, რომ, სახელმწიფო უსაფრთხოების სამსახური არა მხოლოდ ფლობდა ინფორმაციის რეალურ დროში

---

[958] „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის იმ დროს მოქმედი რედაქციის მე-2 მუხლის „ჰ[59]“ ქვეპუნქტის თანახმად, „მართლზომიერი გადაჭერის მენეჯმენტის სისტემა“ განიმარტებოდა, როგორც „სპეციალური კომპიუტერული სისტემა, რომელიც ინფორმაციის რეალურ დროში მიწოდების ტექნიკური შესაძლებლობის არქიტექტურაში იყო შუამავალი რგოლი სამართალდამცავი ორგანოს მონიტორინგის სისტემასა და მომსახურების მიმწოდებლის ინფრასტრუქტურას შორის და რომელიც უზრუნველყოფდა ობიექტის აქტივაციისა და დეაქტივაციის შესახებ სამართალდამცავი ორგანოს მონიტორინგის სისტემის მიერ ინიცირებულ ბრძანებათა ტექნიკურ აღსრულებას.“

[959] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-50-51.

[960] იქვე, II-55.

[961] იქვე.

ხელმისაწვდომობის ტექნიკურ შესაძლებლობებს, არამედ პასუხისმგებელი იყო ამ სისტემის ადმინისტრირებაზე[962]. ამავდროულად, სასამართლოს განმარტებით, ეს პროცესი გასაიდუმლოებული იყო და გარე კონტროლის განმახორციელებელ ორგანოს - პერსონალურ მონაცემთა დაცვის ინსპექტორს[963] არ გააჩნდა უფლებამოსილება, განეხორციელებინა ინფორმაციის რეალურ დროში მოპოვებისთვის განკუთვნილი „ტექნიკური ინფრასტრუქტურის სრული და ყოვლისმომცველი აუდიტი, რის გამოც, ამ პროცესში არ გამოირიცხებოდა მონაცემთა დამმუშავებლების თვითნებობა, უკანონობა.“[964] სასამართლო აღნიშნავს, რომ „როდესაც პირად ინფორმაციაზე პირდაპირი და უშუალო წვდომის ტექნიკური შესაძლებლობები სახელმწიფო უსაფრთხოების სამსახურის (ან გამოძიების ფუნქციის მქონე სხვა ორგანოს) ხელთაა, ... ობიექტურად ძალიან რთული ხდება, თუ შეუძლებელი არა, გამოძიებაზე უფლებამოსილი ორგანოების ეფექტური კონტროლი.“[965]

აღსანიშნავია, რომ სასამართლომ ცალ-ცალკე შეაფასა გარე კონტროლის მექანიზმები სატელეფონო კომუნიკაციის ფარული მიყურადების და ინტერნეტურთიერთობის მონიტორინგის ღონისძიებებზე.

4.1.2 გარე კონტროლის მექანიზმები სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებაზე

საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით სატელეფონო საუბრების ფარულ მიყურადებაზე პერსონალურ მონაცემთა დაცვის ინსპექტორის (იმ დროს მოქმედი კანონმდებლობის მიხედვით) კონტროლის არსებული ბერკეტები არაეფექტიანად იქნა მიჩნეული. სასამართლოს შეხედულებით, აღნიშნული კონტროლის სისტემა „ვერ გამორიცხავდა ინსპექტორის გვერდის ავლით და შესაბამისად, მოსამართლის გადაწყვეტილების გარეშე სატელეფონო კომუნიკაციის ფარული მიყურადების საფრთხეს.“[966] იმ დროს მოქმედი

[962] იქვე, II-56.
[963] აღნიშნული საკონსტიტუციო დავის მიმდინარეობის დროს კანონმდებლობა ითვალისწინებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობას.
[964] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-56.
[965] იქვე, II-82.
[966] იქვე, II-59.

კანონმდებლობით მონიტორინგის სისტემის აქტივაცია ფარული მიყურადებისას შესაძლებელი იყო მხოლოდ პერსონალურ მონაცემთა დაცვის ინსპექტორის ელექტრონული თანხმობით, ანუ მოქმედებდა „ორეტაპიანი ელექტრონული სისტემა“, რომელიც არ იქნა მიჩნეული კონტროლის „საკმარის“ და „ეფექტურ“ საშუალებად, ვინაიდან აღნიშნული სისტემა მიემართებოდა მხოლოდ „მართლზომიერი გადაჭერის მენეჯმენტის სისტემას - ინსპექტორი ელექტრონულ თანხმობას აძლევდა მხოლოდ მართლზომიერი გადაჭერის მენეჯმენტის სისტემის საშუალებით ინიცირებულ ობიექტის აქტივაციის შესახებ ბრძანებაზე, თუმცა ვინაიდან სადავო ნორმა ასევე ითვალისწინებდა ფარული მიყურადების განხორციელებას „სხვა სათანადო აპარატურითა და პროგრამული უზრუნველყოფის საშუალებებით“, ამ ტექნიკური შესაძლებლობების გამოყენებით ფარული მიყურადება რჩებოდა ინსპექტორის კონტროლის მიღმა.[967] სწორედ „სხვა სათანადო აპარატურისა და პროგრამული უზრუნველყოფის საშუალებების“ განთავსების უფლებამოსილებაში იქნა ამოკითხული ორეტაპიანი ელექტრონული სისტემის გვერდის ავლის შესაძლებლობა[968].

ამასთან, არაეფექტიანად იქნა მიჩნეული ინსპექტირების მექანიზმიც. სასამართლომ განმარტა, რომ „ინსპექტირების მეთოდი შესაძლოა იყოს ეფექტური, მაგრამ მხოლოდ შესაბამის პირობებში - როდესაც უსაფრთხოების სამსახურის ინფორმაციის შედარება შესაძლებელია სხვა წყაროდან მიწოდებულ ინფორმაციასთან, მაგალითად, თუ ინსპექტორი ერთმანეთს შეადარებს დამოუკიდებელი ორგანოს ან კომუნიკაციის კომპანიის მიერ მიწოდებულ ინფორმაციას უსაფრთხოების სამსახურის ინფორმაციასთან[969] - სასამართლოს შეხედულებით, ინსპექტორი სწორედ ორი დამოუკიდებელი წყაროდან ინფორმაციის შედარებას და კონტროლს უნდა ახორციელებდეს.[970]

[967] იქვე. II-59-61.
[968] იქვე.
[969] იქვე. II-65.
[970] იქვე.

4.1.3 გარე კონტროლის მექანიზმები ინტერნეტკომუნიკაციის მონიტორინგზე

ასევე არაეფექტიანად იქნა მიჩნეული გარე კონტროლის მექანიზმები ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებაზე. საკონსტიტუციო სასამართლოში სამართალწარმოების შედეგად დადასტურდა, რომ სახელმწიფოს უფლებამოსილ ორგანოს გააჩნდა შესაძლებლობა, ჰქონოდა „ე.წ. მუდმივი მიერთების სისტემა ინტერნეტპროვაიდერებთანაც“[971]. ასევე დადასტურდა, რომ „დიდ კომპანიებში აქვთ კიდეც განთავსებული ეს აპარატურა“. თუმცა, როგორც გაირკვა, „ეს სისტემა გამოუსადეგარია და მიმართავენ ე.წ. „დავირუსების“ ტექნიკას“[972]. „კერძოდ, მოწმის სიტყვებით: „მიუხედავად იმისა, რომ ჩვენ რიგ დიდ კომპანიებში გვაქვს ეს აპარატურა განთავსებული რეალურ დროში ინფორმაციის მოპოვებისთვის, ეს სისტემა თავისი არსით არ არის ეფექტური, სწორედ ამიტომაც არ მოხდა ინტერნეტთან მიმართებაში რეალურ დროში ამ არქიტექტურის აწყობა...“.[973]

საკონსტიტუციო სასამართლომ მიიჩნია, რომ „სადავო ნორმები არ მიჯნავს ერთმანეთისგან, რომელი ტექნიკური საშუალება რომელი საგამოძიებო მოქმედებისთვის უნდა გამოიყენოს უფლებამოსილმა ორგანომ“[974]. სასამართლოს შეფასებით, აღნიშნული ნორმებიდან რჩება შთაბეჭდილება, რომ ინტერნეტურთიერთობის მონიტორინგისთვის გამოყენებადია, როგორც მართლზომიერი გადაჭერის მენეჯმენტის სისტემა, ასევე „სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“[975]. თუმცა სასამართლო სხდომაზე სახელმწიფო უსაფრთხოების სამსახურის წარმომადგენლის განმარტებით დადგინდა, რომ ინტერნეტთან მიმართებით პრაქტიკაში გამოიყენებოდა მხოლოდ სადავო ნორმებით გათვალისწინებული „სხვა სათანადო აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“[976]. სასამართლოს შეფასებით, ვინაიდან „ინფორმაცია გასაიდუმლოებულია“ და „მინიმალურ დონეზეც კი გამოირიცხება“ იმ „ტექნიკური საშუალებების აუდიტი“, რომელიც გამოიყენება ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნებისათვის, „აბსოლუტურად არაგანჭვრეტადია ინფორმაცია,

[971] იქვე. II-73.
[972] იქვე.
[973] იქვე.
[974] იქვე, II-72.
[975] იქვე.
[976] იქვე, II-75.

თუ როდის, რომელ აპარატურასა და პროგრამული უზრუნველყოფის საშუალებას იყენებს სახელმწიფო[977]. ეს კი გულისხმობს ამ პროცესზე კონტროლის აბსოლუტურ შეუძლებლობას და, შედეგად, უფლების დარღვევის თავისთავად რისკებს.“[978] სასამართლოს განმარტებით, სახელმწიფო არ უნდა იყოს აღჭურვილი „აბსოლუტურად უკონტროლო სივრცით, სადაც არავის არასდროს ეცოდინება, დროის რა პერიოდში, რომელი შემთხვევებისთვის, რა ტიპის/შინაარსის ტექნიკური საშუალებები გამოიყენება და, რაც მთავარია, გამოიყენება თუ არა მხოლოდ კონსტიტუციური მოთხოვნების უპირობო დაცვით.“[979] ასეთ პირობებში აღნიშნული ფარული საგამოძიებო მოქმედების კანონიერებაზე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით[980] გათვალისწინებული კონტროლის ერთადერთი ბერკეტი – ინსპექტირების შესაძლებლობა, არაეფექტიანად იქნა მიჩნეული.[981]

4.1.4 კონსტიტუციურ-სამართლებრივი ჩარჩოები ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირებასთან დაკავშირებით

საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით არაკონსტიტუციურად ცნო „ელექტრონული კომუნიკაციების შესახებ საქართველოს კანონის 8^3 მუხლის პირველი პუნქტის „ბ“ ქვეპუნქტი, რომელიც ითვალისწინებდა სახელმწიფო უსაფრთხოების სამსახურის აღჭურვას როგორც ტექნიკური შესაძლებლობით, ისე უშუალო უფლებამოსილებით, მოეხდინა კავშირგაბმულობის არხში არსებული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირება და 2 წლამდე ვადით შენახვა.

საკონსტიტუციო სასამართლოს განმარტებით, სადავო ნორმა ითვალისწინებდა „კავშირგაბმულობის არხში არსებული აბსოლუტურად ყველას/თითოეული ადამიანის ნებისმიერ ადამიანთან კომუნიკაციისას მაიდენტიფიცირებელი

---

[977] იქვე.
[978] იქვე.
[979] იქვე.
[980] კანონმდებლობაში განხორციელებული ცვლილებების შედეგად, ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით ინსპექტირების უფლებამოსილება დღეს გათვალისწინებულია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონით.
[981] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-76-77.

მონაცემების კოპირების და შენახვის შესაძლებლობას“[982]. სასამართლოს შეხედულებით, აღნიშნულ მონაცემთა ასეთი შენახვა, თავისთავად წარმოადგენს პირადი ცხოვრების უფლებაში ჩარევას, იმისდა მიუხედავად, იქნება თუ არა ეს მონაცემები შემდგომში გამოყენებული ან/და დამუშავებული.[983]

ყურადღება იქნა გამახვილებული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ინფორმაციულ ღირებულებაზე და აღინიშნა, რომ „მეტადატას ანალიზის შედეგად შესაძლებელია დადგინდეს ინდივიდის ქცევა, სოციალური ურთიერთობები, პირადი მახასიათებლები, რაც უშუალოდ კომუნიკაციის შინაარსთან ერთად ამ ინდივიდის შესახებ მნიშვნელოვან ინფორმაციას იძლევა. ასეთ 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“[984]. „მაშასადამე, ეს მონაცემები იძლევა შესაძლებლობას, შეიქმნას პირის პერსონალური და გადაადგილების პროფილი, რაც ცალკეულ ან ხშირ შემთხვევაში საკმარისად ინფორმაციული შეიძლება იყოს პირის პირადი სივრცის შესახებ და ინფორმაციულობის ხარისხით მნიშვნელოვნად არ ჩამოუვარდებოდეს უშუალოდ ტელეკომუნიკაციის შედეგად გაცვლილ ინფორმაციას.“[985]

სადავო ნორმის არაკონსტიტუციურობას რამდენიმე გარემოება დაედო საფუძვლად. უპირველეს ყოვლისა, ყურადღება იქნა გამახვილებული იმაზე, რომ ამ შემთხვევაშიც ინფორმაციის კოპირების და შენახვის ფუნქციით კანონმდებლობამ აღჭურვა სახელმწიფო უსაფრთხოების სამსახური, რომელიც პროფესიულად იყო რაც შეიძლება მეტი ინფორმაციის მოპოვებით დაინტერესებული, რაც ისევ და ისევ, უფლებაში დაუსაბუთებელი ჩარევის მომეტებულ რისკად იქნა შეფასებული.[986]

[982] იქვე, II- 109.
[983] იქვე, II- 93.
[984] იქვე, II- 92.
[985] იქვე.
[986] იქვე, II- 96.

ასევე არაეფექტიანად იქნა მიჩნეული აღნიშნულ პროცესზე პერსონალურ მონაცემთა დაცვის ინსპექტორის[987] კონტროლის ბერკეტებიც: 1) კონტროლი მონაცემთა ბანკების კონტროლის სპეციალური ელექტრონული სისტემის გამოყენებით და 2) ინსპექტირების უფლებამოსილება[988]. სასამართლოს შეფასებით, მართალია, კანონი შენახულ მაიდენტიფიცირებელ მონაცემებზე გამომძიების 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[989]. ამ თვალსაზრისით, გამოიკვეთა, რომ ტექნიკურად შესაძლებელი იყო, მაიდენტიფიცირებელი მონაცემების კოპირების და შენახვის პროცესში შექმნილიყო ე.წ. „ალტერნატიული ბანკი, რომლის არსებობის შესახებ შესაძლოა არავის სცოდნოდა და მასზე დაშვება არც პერსონალურ მონაცემთა დაცვის ინსპექტორს ჰქონოდა”[990]. ხაზი გაესვა იმ გარემოებას, რომ ინსპექტორი ვერ აკონტროლებდა ელექტრონული კომუნიკაციების კომპანიებიდან მონაცემთა ბანკების წამოღების პროცესს. მისი ზედამხედველობა მხოლოდ იმ მონაცემთა ბანკზე ხორციელდებოდა, რომელზეც ინსპექტორის დაშვებას უსაფრთხოების სამსახური ახდენდა.[991] თუმცა ასევე არაეფექტიანად იქნა შეფასებული უკვე კოპირებულ მონაცემებზე კონტროლის მექანიზმებიც - მონაცემთა ბანკების კონტროლის სპეციალური ელექტრონული სისტემის არაეფექტურობას ტექნიკური გაუმართაობა დაედო საფუძვლად[992]. რაც შეეხება ინსპექტირებას, მისი არაეფექტიანობა განაპირობა განხორციელების მეთოდმა - „შემთხვევითი შერჩევის პრინციპმა“[993]. საკონსტიტუციო სასამართლოს განმარტებით, ასეთი მეთოდით უფლების დარღვევის აღმოჩენის ალბათობა შემთხვევითობაზეა დამოკიდებული, ხოლო მეორე მხრივ, დარღვევის აღმოჩენის ალბათობის სათუოობას განუზომლად ზრდის შენახული ინფორმაციის

[987] აღნიშნული საკონსტიტუციო დავის მიმდინარეობის დროს კანონმდებლობა ითვალისწინებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობას.
[988] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-99-104.
[989] იქვე, II-101.
[990] იქვე, II-101, 103.
[991] იქვე, II-101.
[992] იქვე, II-103.
[993] იქვე, II-104.

მოცულობა - აბსოლუტურად ყველა პირის მაიდენტიფიცირებელი მონაცემის 2 წლის ვადით შენახვა.[994]

სადავო ნორმის არაკონსტიტუციურობას ასევე მონაცემთა ხანგრძლივი ვადით - 2 წლით შენახვა დაედო საფუძვლად. სასამართლოს შეფასებით, დამოუკიდებლად იმისა, მონაცემთა შენახვა/კოპირებას მოახდენს თუ არა გამოძიებაზე პასუხისმგებელი ორგანო, 2 წლით ამგვარი ინფორმაციის შენახვა პირად სივრცეში ძალიან მაღალი ინტენსივობით ჩარევას წარმოადგენს, ამიტომ საჭიროებს „მეტად დამაჯერებელ დასაბუთებას ასეთი ინტენსივობით ჩარევის აუცილებლობასა და გარდაუვალობაზე.“[995]

და ბოლოს, სადავო ნორმის არაკონსტიტუციურობა განაპირობა შესანახ მონაცემთა „ძალიან დიდმა მოცულობამ“[996]. ამ საკითხთან დაკავშირებით, საკონსტიტუციო სასამართლოს გადაწყვეტილებაში გაჟღერებულია მსგავსი არგუმენტაცია, რაც ევროკავშირის მართლმსაჯულების სასამართლოს ზემოთხსენებულ 2014 და 2016 წლების გადაწყვეტილებებში, კერძოდ, საკონსტიტუციო სასამართლო აღნიშნავს, რომ სადავო ნორმა ითვალისწინებს კავშირგაბმულობის არხში არსებული „აბსოლუტურად ყველას/თითოეული ადამიანის ნებისმიერ ადამიანთან კომუნიკაციისას მაიდენტიფიცირებელი მონაცემების კოპირების და შენახვის შესაძლებლობას;“[997] მითითებული მონაცემები ინახება „იმისგან დამოუკიდებლად, აქვს თუ არა პირს თუნდაც ჰიპოთეტური კავშირი სავარაუდო (ჩადენილ ან მომავალში დაგეგმილ) დანაშაულთან.“[998] ვინაიდან მონაცემები ინახება „ყოველგვარი ფილტრაციის გარეშე, აბსტრაქტული საფრთხის არარსებობის პირობებშიც კი, შესაძლებელი ხდება ინფორმაციის ავტომატური დამუშავების გამოყენებით სიღრმისეული დასკვნების გამოტანა ადამიანის პირადი ცხოვრების შესახებ“[999]. სასამართლოს შეფასებით, მონაცემთა ასეთი „ტოტალური“, „ბლანკეტური“ შენახვა თავისთავად ზრდის უფლებაში ჩარევის ინტენსივობას, „იმისგან დამოუკიდებლად, ამ ინფორმაციის შემდგომი გამოყენება უკავშირდება თუ

[994] იქვე.
[995] იქვე. II-108.
[996] იქვე, II-109.
[997] იქვე.
[998] იქვე.
[999] იქვე.

არა მხოლოდ კონკრეტული დანაშაულების გახსნას და ინფორმაციის გამოყენება ხდება თუ არა მხოლოდ მოსამართლის განჩინების არსებობისას, ამასთან, ვრცელდება თუ არა ამ პროცესზე ეფექტური გარე კონტროლი.“[1000]

4.2. ქართული კანონმდებლობა საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილების შემდგომ

საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილების შესრულების მიზნით საქართველოს კანონმდებლობაში 2017 წლის 22 მარტის საკანონმდებლო პაკეტით გარკვეული ცვლილებები განხორციელდა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებისა და სისხლის სამართლის პროცესში გამოყენების მიმართულებით. თუმცა დღესდღეობით ინფორმაციის რეალურ დროში მოპოვების მარეგულირებელი ნორმები ისევ საკონსტიტუციო სასამართლოში არის გასაჩივრებული. აღნიშნული დავის ფარგლებში, მოსარჩელეებმა მოითხოვეს ინფორმაციის რეალურ დროში მოპოვების ტექნიკურ შესაძლებლობასთან, ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირებისა და შენახვის უფლებამოსილებასთან დაკავშირებული ნორმების ძალადაკარგულად ცნობა არსებითი განხილვის გარეშე, თუმცა 2017 წლის 29 დეკემბრის საოქმო ჩანაწერით საკონსტიტუციო სასამართლომ მოსარჩელეებს უარი უთხრა სადავო ნორმების არსებითი განხილვის გარეშე ძალადაკარგულად გამოცხადებაზე, ვინაიდან მიიჩნია, რომ ინფორმაციის რეალურ დროში მოპოვების ტექნიკურ შესაძლებლობასთან, ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების კოპირება/შენახვის საკითხებთან დაკავშირებით სადავო ნორმები არ არის საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით ცნობილი ნორმების იდენტური შინაარსის და კანონმდებლობაში განხორციელებული ცვლილებებით არსებითად შეიცვალა მარეგულირებელი კანონმდებლობა[1001]. ამდენად, აღნიშნულ საკითხებთან დაკავშირებით კანონმდებლობის კონსტიტუციურობას

[1000] იქვე.

[1001] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.

საკონსტიტუციო სასამართლო შეაფასებს არსებითი განხილვის ფორმატში.[1002] აღსანიშნავია ისიც, რომ განსახილველ საკითხებთან მიმართებით, საკონსტიტუციო სასამართლოს შემადგენლობაში აზრები ორად გაიყო – სამმა მოსამართლემ განსხვავებული მოსაზრება გამოხატა და მიიჩნია, რომ „კანონმდებლობას არ განუცდია იმგვარი არსებითი ცვლილება, რაც აუცილებელს გახდიდა მასზე დამატებით, არსებითად მსჯელობას.“[1003]

4.2.1 სსიპ ოპერატიულ-ტექნიკური სააგენტო და მისი დამოუკიდებლობის გარანტიები

2017 წლის 22 მარტის საკანონმდებლო ცვლილებების ერთ-ერთ ნოვაციას ახალი ორგანოს - ოპერატიულ-ტექნიკური სააგენტოს შექმნა წარმოადგენს, რომელიც სახელმწიფო უსაფრთხოების სამსახურის მმართველობის ქვეშ მოქმედი საჯარო სამართლის იურიდიული პირის სახით ჩამოყალიბდა და აღიჭურვა ფარული მეთვალყურეობის ღონისძიებების ტექნიკური აღსრულების უფლებამოსილებით.

როგორც უკვე აღინიშნა, საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის საგამოძიებო ორგანოში თავმოყრა დანახულ იქნა უფლებამოსილების ბოროტად გამოყენების მომეტებულ საფრთხედ. აღნიშნულის ფონზე ისეთი სუბიექტის შექმნამ, რომელიც სახელმწიფო უსაფრთხოების სამსახურისგან საკმარისი დამოუკიდებლობის გარანტიებით ისარგებლებდა, განსაკუთრებული დატვირთვა შეიძინა.

ნიშანდობლივია, რომ სააგენტოს წინამორბედი, ოპერატიულ-ტექნიკური დეპარტამენტი, რომელიც მანამდე იყო კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობით აღჭურვილი, წარმოადგენდა სახელმწიფო უსაფრთხოების სამსახურის სტრუქტურულ ქვედანაყოფს და შესაბამისად, მოქმედებდა მის უშუალო დაქვემდებარებაში. საგამოძიებო ფუნქციით აღჭურვილ სახელმწიფო უსაფრთხოების სააგენტოსთან ასეთი მჭიდრო სამართლებრივი

[1002] იქვე.

[1003] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე.

კავშირის და დამოკიდებულების გამო მიჩნეულ იქნა, რომ ოპერატიულ-ტექნიკური დეპარტამენტისათვის ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობის მინიჭება წარმოადგენდა ამ უფლებამოსილების საგამოძიებო ორგანოს ხელში თავმოყრას.[1004]

ამ თვალსაზრისით ნიშანდობლივია, რომ სააგენტო უკვე ცალკე სუბიექტის - საჯარო სამართლის იურიდიული პირის სახით ჩამოყალიბდა და მართალია, წარმოადგენს სახელმწიფო უსაფრთხოების სამსახურის ერთიანი სისტემის შემადგენელ ნაწილს,[1005] მაგრამ კანონმდებლობით აღჭურვილია დამოუკიდებლობის გარკვეული მნიშვნელოვანი გარანტიებით. ამ თვალსაზრისით აღსანიშნავია, „საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-5 მუხლი, რომელიც აწესრიგებს სააგენტოს დამოუკიდებლობის გარანტიებთან დაკავშირებულ საკითხებს. აღნიშნული მუხლის თანახმად, სააგენტო თავისი კომპეტენციის ფარგლებში დამოუკიდებლად ასრულებს მისთვის განსაზღვრულ ამოცანებს. დაუშვებელია სააგენტოს საქმიანობაში სამსახურის სტრუქტურული ქვედანაყოფებისა და თანამდებობის პირების უკანონო ჩარევა. ამასთან, სააგენტოს მოსამსახურე თავის სამსახურებრივ საქმიანობაში დამოუკიდებელია. იგი შეიძლება გათავისუფლდეს სამსახურიდან მხოლოდ კანონით გათვალისწინებულ შემთხვევებში და დადგენილი წესით. ნორმატიულ აქტებს, რომლებიც ეხება სააგენტოს მიერ ფარული საგამოძიებო მოქმედების და ელექტრონული თვალთვალის ღონისძიების განხორციელებას, აგრეთვე ამ მოქმედებისა და ღონისძიების შედეგად მოპოვებული ინფორმაციის გაცნობას, დამუშავებას, შენახვას, გაცემასა და განადგურებას, კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ტექნიკური შესაძლებლობის არქიტექტურისა და შესაბამისი ინტერფეისების განსაზღვრას, კომუნიკაციის რეალურ დროში მოპოვების ნახევრად სტაციონარული ტექნიკური შესაძლებლობის გამოყენებით განხორციელებული კომუნიკაციის შინაარსის და მისი მაიდენტიფიცირებელი მონაცემების მოპოვების წესსა და პროცედურას, გამოსცემს სააგენტოს უფროსი. ამ

[1004] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II-22.

[1005] იქვე. 29. იხ. ასევე „საქართველოს სახელმწიფო უსაფრთხოების სამსახურის დებულების დამტკიცების შესახებ“ საქართველოს მთავრობის 2015 წლის 30 ივლისის N385 დადგენილებით დამტკიცებული დებულების მე-2 მუხლის მე-3 პუნქტი, www.matsne.gov.ge, 30/07/2015.

ნორმატიულ აქტებში ცვლილების შეტანის და მათი გაუქმების უფლება აქვს სააგენტოს უფროსს.

თუმცა არსებობს რიგი მნიშვნელოვანი საკითხები, როდესაც იკვეთება სააგენტოს ინსტიტუციური და ფინანსური დამოკიდებულება სახელმწიფო უსაფრთხოების სამსახურზე; მაგალითად, ერთ-ერთ ასეთ საკითხად შეიძლება განხილულ იქნეს „საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-19 მუხლით გათვალისწინებული სააგენტოს უფროსის შერჩევისა და გათავისუფლების პროცედურა, კერძოდ, მიუხედავად იმისა, რომ სააგენტოს უფროსს თანამდებობაზე ნიშნავს საქართველოს პრემიერ-მინისტრი, კანდიდატურის შერჩევის პროცედურაში აქტიურად მონაწილეობს სახელმწიფო უსაფრთხოების სამსახური უფროსი - სააგენტოს უფროსს შეარჩევს 7 წევრისგან შემდგარი კომისია, რომელსაც თავის მხრივ, უსაფრთხოების სამსახურის უფროსი წარუდგენს 3 კანდიდატურას. აღნიშნულიდან გამომდინარე, ნებისმიერი კანდიდატურა, რომელიც წარდგენილი იქნება სპეციალური კომისიისთვის, ხოლო შემდგომ პრემიერ-მინისტრისთვის, თავდაპირველად სამსახურის უფროსის მიერ არის შერჩეული.[1006] რაც შეეხება სააგენტოს უფროსის გათავისუფლების პროცედურას, ამის თაობაზე გადაწყვეტილებას იღებს საქართველოს პრემიერ-მინისტრი სამსახურის უფროსის წარდგინებით. მართალია კანონის მე-19 მუხლში ამომწურავად არის განსაზღვრული სააგენტოს უფროსის გათავისუფლების საფუძვლები, მაგრამ როგორც საკონსტიტუციო სასამართლოს მოსამართლეები განსხვავებული აზრით აფიქსირებენ, ამ ჩამონათვალს შორის არის „ფართო შინაარსის მქონე საფუძველი, როგორიც არის მისთვის განსაზღვრული უფლებამოსილებების არაჯეროვანი შესრულება“[1007].

აღსანიშნავია, რომ საქართველოს საკონსტიტუციო სასამართლო, 2017 წლის 29 დეკემბრის საოქმო ჩანაწერით, მართალია სააგენტოს მიიჩნევს ოპერატიულ-ტექნიკური დეპარტამენტისგან „თვისობრივად განსხვავებულ“ ორგანოდ, რომელიც სარგებლობს „უფრო მაღალი ავტონომიურობით“, მაგრამ გამოყოფს იმ ფაქტორებსაც,

[1006] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 11.
[1007] იქვე.

რომლებიც განაპირობებენ სახელმწიფო უსაფრთხოების სამსახურის „საკმაოდ მაღალ გავლენას“ სააგენტოზე[1008]. ამ ფაქტორებს შორის სააგენტოს უფროსის დანიშვნა/გათავისუფლების წესის გარდა, სახელდება ის გარემოებაც, რომ სახელმწიფო უსაფრთხოების სამსახურის უფროსი ახორციელებს სააგენტოს სტრუქტურის, საშტატო ნუსხის განსაზღვრას; ასევე წყვეტს სააგენტოს უფროსისთვის სპეციალური დანამატის დაწესებისა და პრემირების საკითხებს და წერილობით ითანხმებს სააგენტოს მოსამსახურეთა სპეციალური დანამატის დაწესებისა და პრემირების საკითხებს[1009]. აღსანიშნავია ასევე, რომ სააგენტოს მოსამსახურეების საქმიანობის შესწავლას ახორციელებს სამსახურის უფროსის წინაშე ანგარიშვალდებული გენერალური ინსპექცია, რაც ასევე „არაპირდაპირ განაპირობებს სამსახურის გავლენას.“[1010]

ამ კუთხით მხედველობაშია მისაღები აგრეთვე „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის 29-ე მუხლის პირველი პუნქტში არსებული ჩანაწერი, რომლის თანახმადაც, „სააგენტოს საქმიანობის სახელმწიფო კონტროლს ახორციელებს სამსახურის უფროსი“. „საჯარო სამართლის იურიდიული პირის შესახებ“ საქართველოს კანონის მე-11 მუხლის პირველი პუნქტიდან გამომდინარე, საჯარო სამართლის იურიდიულ პირზე სახელმწიფო კონტროლი გულისხმობს მის მიერ განხორციელებული საქმიანობის კანონიერების, მიზანშეწონილობის, ეფექტიანობისა და საფინანსო-ეკონომიკური საქმიანობის ზედამხედველობას.“ ამავე მუხლის მე-3 პუნქტის თანახმად, კი „სახელმწიფო კონტროლის განმახორციელებელი ორგანო უფლებამოსილია შეაჩეროს ან გააუქმოს საჯარო სამართლის იურიდიული პირის არამართლზომიერი გადაწყვეტილება.“ სახელმწიფო უსაფრთხოების სამსახურის დებულების მე-4 მუხლის მე-2 პუნქტის „ო“ ქვეპუნქტით განსაზღვრულია, რომ სამსახურის უფროსი ძალადაკარგულად აცხადებს პირველი მოადგილის, მოადგილეების, სამსახურის სისტემაში შემავალი საჯარო სამართლის იურიდიული პირის უფროსისა და სამსახურის სისტემაში სხვა მოსამსახურეთა აქტებსა და მოქმედებებს, რომლებიც არ შეესაბამება საქართველოს კონსტიტუციას, საქართველოს

[1008] იქვე, II- 37-39.
[1009] იქვე, II- 37.
[1010] იქვე, II- 33, 37.

კანონებს, საქართველოს პრეზიდენტის, საქართველოს მთავრობის, საქართველოს პრემიერ-მინისტრისა და სამსახურის უფროსის სამართლებრივ აქტებს, აგრეთვე მათი მიზანშეუწონლობის მოტივით.

ამდენად, კანონმდებლობის მიხედვით, სახელმწიფო უსაფრთხოების სამსახურის უფროსი აღჭურვილია საკმაოდ მნიშვნელოვანი სამართლებრივი ბერკეტით, რაც გამოიხატება სააგენტოს სამართლებრივი აქტების გაუქმების უფლებამოსილებაში, რომელიც ასევე მოიცავს მიზანშეუწონლობის მოტივით აღნიშნული აქტების ძალადაკარგულად ცნობის უფლებას;[1011] მართალია „ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-5 მუხლის მე-6 პუნქტიდან გამომდინარე, ეს უფლებამოსილება არ ვრცელდება იმ ნორმატიულ აქტებზე, რომლებიც შეეხება ინფორმაციის რეალურ დროში მოპოვების საკითხებს, თუმცა, როგორც საკონსტიტუციო სასამართლო 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში აღნიშნავს, ასეთი ტიპის კონტროლის უფლებამოსილება მიუთითებს სახელმწიფო უსაფრთხოების სამსახურის გავლენას სააგენტოზე.[1012]

საბოლოო ჯამში, შეიძლება ითქვას, რომ სააგენტო თავის წინამორბედთან - ოპერატიულ-ტექნიკურ დეპარტამენტთან შედარებით სარგებლობს მეტი ავტონომიურობის ხარისხით, თუმცა არსებობს გარკვეული მნიშვნელოვანი ასპექტები, როდესაც თავს იჩენს სახელმწიფო უსაფრთხოების სამსახურის ზეგავლენა სააგენტოზე; აქედან გამომდინარე, მნიშვნელოვანია, რომ შემცირებულ იქნეს სააგენტოს დაქვემდებარების ხარისხი სახელმწიფო უსაფრთხოების სამსახურზე და კანონმდებლობამ გაითვალისწინოს უფრო ძლიერი და ხელშესახები გარანტიები ხსენებული ახლად შექმნილი ორგანოს დამოუკიდებლობის უზრუნველსაყოფად.

4.2.2 კომუნიკაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობების ახლებური მოწესრიგება

2017 წლის 22 მარტის ცვლილებებით ინფორმაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობების დასახელებები და დეფინიცია ნორმატიულად

[1011] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 17.

[1012] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II-22.

მოწესრიგდა, კერძოდ, ფარული მეთვალყურეობის ღონისძიებებთან დაკავშირებით კანონით განისაზღვრა კომუნიკაციის რეალურ დროში მოპოვების შემდეგი გზები: სტაციონალური, ნახევრად სტაციონალური და არასტაციონალური ტექნიკური შესაძლებლობა. ამასთან, განისაზღვრა, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედება ხორციელდება კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული, ნახევრად სტაციონარული ან არასტაციონარული ტექნიკური შესაძლებლობით.[1013] სატელეფონო კომუნიკაციის ფარული მიყურადება/ჩაწერა ხორციელდება სტაციონალური ტექნიკური შესაძლებლობით, ხოლო კანონმდებლობით გათვალისწინებულ შემთხვევაში შესაძლებელია ასევე ნახევრად სტაციონალური ტექნიკური შესაძლებლობის გამოყენებაც.[1014]

„ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ჰ[57]“ ქვეპუნქტის თანახმად, კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ტექნიკური შესაძლებლობა განსაზღვრულია, როგორც „წინასწარ განსაზღვრული არქიტექტურითა და დადგენილი ინტერფეისებით, კავშირგაბმულობის ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერა უფლებამოსილი ორგანოს მიერ კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე შესაბამისი აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების განთავსებით/მონტაჟით“; ამავე მუხლის „ჰ[58]“ ქვეპუნქტიდან გამომდინარე, კომუნიკაციის რეალურ დროში მიღების არასტაციონალური შესაძლებლობა წარმოადგენს „კავშირგაბმულობის ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერას უფლებამოსილი ორგანოს მიერ კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე მიერთების გარეშე, სპეციალური ტექნიკური ან/და პროგრამული საშუალებების გამოყენებით;“

[1013] საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ საქართველოს კანონის მე-9 მუხლის მე-6 პუნქტი, www.matsne.gov.ge, 27/03/2017.
[1014] საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ საქართველოს კანონის მე-9 მუხლის მე-3 პუნქტი, www.matsne.gov.ge, 27/03/2017.

ხოლო „ჰ[68]“ ქვეპუნქტით განმარტებულია კომუნიკაციის რეალურ დროში მოპოვების ნახევრად სტაციონარული ტექნიკური შესაძლებლობა – „ელექტრონული საკომუნიკაციო ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერა უფლებამოსილი ორგანოს მიერ კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე შესაბამისი აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების დროებითი ან მუდმივი განთავსებით/მონტაჟით.“

4.2.3 ზედამხედველობის მექანიზმები ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებაზე

საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის საოქმო ჩანაწერი გარკვეულ წარმოდგენას იძლევა ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებასთან დაკავშირებული ტექნიკური საკითხების შესახებ, კერძოდ, როგორც საკონსტიტუციო სასამართლოში დადასტურდა, „ინტერნეტკომუნიკაციასთან დაკავშირებული დღეს არსებული ვითარება არის ისეთი, როგორც მაშინ იყო, არ შეცვლილა. ინტერნეტთან მიმართებაში სტაციონალური ტექნიკური შესაძლებლობის გამოყენება არ ხდება მთელი რიგი მიზეზების გამო. პირველ რიგში, ეს არის საკმაოდ ძვირად ღირებული სისტემა. მეორე, ნაკლებად ეფექტურია. ინტერნეტკომუნიკაცია განსხვავებით სატელეფონო ხმოვანი კომუნიკაციისაგან, დღესდღეობით არის დაშიფრულ მდგომარეობაში... სტაციონალური სისტემის აწყობა ინტერნეტთან მიმართებაში ჯერჯერობით ვერ ხერხდება.“[1015]

როგორც უკვე აღინიშნა, 2016 წლის 14 აპრილის გადაწყვეტილებით ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებული ნორმების არაკონსტიტუციურობის ერთ-ერთ ძირითად საფუძვლად საკმარისი გარე კონტროლის მექანიზმების არარსებობა დასახელდა. ამ თვალსაზრისით საკონსტიტუციო სასამართლომ ხაზი გაუსვა პერსონალურ მონაცემთა დაცვის ინსპექტორის (იმ დროს მოქმედი კანონმდებლობით) მიერ ამ ღონისძიების

[1015] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 56.

განსახორციელებლად გამოყენებული ტექნიკური საშუალებების შემოწმების უფლების კანონმდებლობაში რეგლამენტაციის აუცილებლობას. ამ კონტექსტში, 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში საკონსტიტუციო სასამართლომ ინტერნეტთან მიმართებით სადავო ნორმების არსებითად განსახილველად მიღების შესახებ გადაწყვეტილებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში 2017 წლის 22 მარტს განხორციელებული ცვლილებები დაუდო საფუძვლად, კერძოდ, აქცენტი გაკეთდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35^1 მუხლის 4^1 პუნქტზე,[1016] რომელშიც 2017 წლის 22 მარტის ცვლილებებით ხაზგასმით აღინიშნა, რომ „ინსპექტორი უფლებამოსილია შევიდეს სააგენტოს შეზღუდული დაშვების არეალებში და მიმდინარე რეჟიმში დააკვირდეს უფლებამოსილი ორგანოების მიერ საქმიანობის განხორციელებას..., მიიღოს ინფორმაცია ფარული საგამოძიებო მოქმედებების მიზნებისათვის გამოყენებული ტექნიკური ინფრასტრუქტურის შესახებ და შეამოწმოს ეს ინფრასტრუქტურა.“[1017] ნიშანდობლივია, რომ სასამართლო სხდომაზე პერსონალურ მონაცემთა დაცვის ინსპექტორის[1018] მიერ გაკეთებული განმარტებით, მას ისედაც ჰქონდა ეს უფლებამოსილებები, თუმცა გაწერილი იყო მის ბრძანებაში და არა კანონში.[1019]

კვლევის ფარგლებში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატიდან[1020] გამოთხოვილი საჯარო ინფორმაციის თანახმად, „2017-2018 წლებში განხორციელდა სააგენტოს 2 (ორი) არაგეგმური შემოწმება ფარული საგამოძიებო მოქმედების განხორციელების შედეგად მონაცემთა დამუშავების კანონიერების შესწავლის მიზნით.“[1021] ინსპექტორის აპარატის წერილში მითითებულია, რომ

[1016] აღსანიშნავია, რომ კანონმდებლობაში განხორციელებული ცვლილებების თანახმად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 35^1 მუხლი შემდგომში ამოღებულ იქნა და ინსპექტირებასთან დაკავშირებული ამ მუხლში გათვალისწინებული უფლებამოსილებები ანალოგიური შინაარსით აისახა „სახელმწიფოს ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მე-7 პუნქტში, რომელიც ამოქმედდა 2019 წლის 10 მაისიდან.

[1017] საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II- 58, 65-66.

[1018] იმ დროს მოქმედი კანონმდებლობით გათვალისწინებული იყო „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობა.

[1019] იქვე, II-58-59.

[1020] საჯარო ინფორმაციის გამოთხოვის დროს მოქმედი კანონმდებლობით, დღეს არსებული „სახელმწიფო ინსპექტორის სამსახურის“ ნაცვლად ფუნქციონირებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი“.

[1021] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის საჯარო ინფორმაციაზე პასუხისმგებელი პირის 2019 წლის 21 იანვრის წერილი (№: PDP 7 19 00000216).

აღნიშნული ინსპექტირების ფარგლებში, მათ შორის, ჩატარდა იმ ტექნიკური ინფრასტრუქტურის შემოწმება, რომელიც განკუთვნილია სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების განსახორციელებლად[1022]. გარდა ამისა, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით განსაზღვრული საგამოძიებო მოქმედების განხორციელებისათვის განკუთვნილი ტექნიკური ინფრასტრუქტურის შემოწმება ასევე ჩატარდა 2016 წელს საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ოპერატიულ-ტექნიკური დეპარტამენტის ინსპექტირების ფარგლებშიც.[1023]

ყოველივე აღნიშნულიდან გამომდინარე, აშკარაა, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორი (2019 წლის 10 მაისამდე მოქმედი კანონმდებლობის მიხედვით) და მისი უფლებამონაცვლე - სახელმწიფო ინსპექტორის სამსახური, 2016 წლიდან ახორციელებს ინტერნეტურთიერთობის მონიტორინგის ჩასატარებლად გამოყენებული ტექნიკური საშუალებების შემოწმებას. ეს უფლებამოსილება ცხადად იქნა რეგლამენტირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში 2017 წლის მარტის ცვლილებებით (კანონმდებლობაში შემდგომში განხორციელებული ცვლილებებით, რომელიც ამოქმედდა 2019 წლის 10 მაისიდან, დღეს იგივე უფლებამოსილება გათვალისწინებულია „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონის მე-18 მუხლის მე-7 პუნქტში[1024]), თუმცა როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორმა[1025] საკონსტიტუციო სასამართლოში თავადვე დაადასტურა, კანონქვემდებარე აქტით მანამდეც იყო აღჭურვილი ამ შესაძლებლობით. მოცემულ ვითარებაში, შეიძლება ითქვას, რომ საეჭვოა, რეალურად რამდენად განიცადა ინსპექტირების ფუნქციამ ისეთი არსებითი სახეცვლილება, რომლითაც ინსპექტორი მანამდე არარსებული უფლებამოსილებით აღიჭურვა.[1026]

[1022] იქვე.

[1023] იქვე.

[1024] იხ. ასევე „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანების მე-13 მუხლის პირველი პუნქტის „ე“ ქვეპუნქტი.

[1025] აღნიშნული საკონსტიტუციო დავის მიმდინარეობის დროს კანონმდებლობა ითვალისწინებდა „პერსონალურ მონაცემთა დაცვის ინსპექტორის“ თანამდებობას.

[1026] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 126-128. აღნიშნულ საკითხთან დაკავშირებით იხ. ასევე *თუმანიშვილი გ., გეგეშიძე*

საბოლოო ჯამში, უნდა აღინიშნოს, რომ ვინაიდან საკონსტიტუციო სასამართლომ არსებითად განსახილველად მიიღო ინტერნეტკომუნიკაციის რეალურ დროში მოპოვებასთან დაკავშირებული ნორმები, არსებული დავის ფარგლებში გადაწყდება, თუ რამდენად საკმარისია მოქმედი კანონმდებლობით გათვალისწინებული ფარული საგამოძიებო მოქმედებების ჩასატარებლად განკუთვნილი ინფრასტრუქტურის შემოწმებასთან დაკავშირებული უფლებამოსილებები იმისთვის, რათა 2016 წლის 14 აპრილის გადაწყვეტილებაში აღნიშნული „ტექნიკური ინფრასტრუქტურის სრული და ყოვლისმომცველი შემოწმების“ აუცილებლობის მოთხოვნა დაკმაყოფილდეს.[1027]

4.2.4 სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიებასთან დაკავშირებული საკანონმდებლო ცვლილებები

როგორც უკვე აღინიშნა, 2017 წლის 22 მარტის ცვლილებებით ნორმატიულ ენაზე განისაზღვრა კომუნიკაციის რეალურ დროში მოპოვების ტექნიკური შესაძლებლობები. სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიების განხორციელების საშუალებად დადგინდა სტაციონალური ტექნიკური შესაძლებლობა; სატელეფონო კომუნიკაციებთან მიმართებით კანონმდებლობა ასევე ითვალისწინებს ნახევრად სტაციონალური ტექნიკური შესაძლებლობის ორგანიზების საშუალებას, თუმცა განსაზღვრავს შესაბამის რიგითობას, კერძოდ, „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-9 მუხლის მე-3 პუნქტის თანახმად, „თუ ელექტრონული კომუნიკაციის კომპანიის ქსელური ან სასადგურე ინფრასტრუქტურა არ იძლევა კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ტექნიკური შესაძლებლობის ორგანიზების საშუალებას, სააგენტო უფლებამოსილია მიიღოს გადაწყვეტილება კომუნიკაციის რეალურ დროში მოპოვების ნახევრად სტაციონარული ტექნიკური შესაძლებლობის ორგანიზების შესახებ.“ ამასთან, სააგენტო ასეთ შემთხვევაში ვალდებულია კომუნიკაციის რეალურ დროში მოპოვების

თ., მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *(რედ.),* თბ., 2019, 394.

[1027] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 128.

ნახევრად სტაციონარული ტექნიკური შესაძლებლობის ორგანიზების შესახებ დაუყოვნებლივ შეატყობინოს ინსპექტორს ან ზედამხედველ მოსამართლეს.

გარდა აღნიშნულისა, კომუნიკაციის რეალურ დროში მიღების მიზნით გამოსაყენებელი „სხვა [გარდა მართლზომიერი მენეჯმენტის გადაჭერის სისტემისა] აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“, რომლის გამოყენებაც საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით ინსპექტორის გვერდის ავლის შესაძლებლობად იქნა დანახული, ცვლილებების მიხედვით, შინაარსობრივად დაუკავშირდა მართლზომიერი გადაჭერის მენეჯმენტის სისტემას, კერძოდ, „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონში განისაზღვრა, რომ კომუნიკაციის რეალურ დროში მოპოვების სტაციონარული ტექნიკური შესაძლებლობის ქონის მიზნით სააგენტო უფლებამოსილია „საჭიროების შემთხვევაში, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე უსასყიდლოდ განათავსოს/დაამონტაჟოს მართლზომიერი გადაჭერის მენეჯმენტის სისტემა ან/და მასთან დაკავშირებული/მისი ფუნქციონირებისთვის აუცილებელი აპარატურა ან/და პროგრამული უზრუნველყოფის საშუალებები“ (მე-9 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტი). შესაბამისად, აღნიშნული აპარატურა და პროგრამული უზრუნველყოფის საშუალებები უნდა იყოს „მართლზომიერი გადაჭერის მენეჯმენტის სისტემასთან დაკავშირებული ან/და მისი ფუნქციონირებისათვის აუცილებელი“. მოცემული ცვლილება პოზიტიურად შეიძლება შეფასდეს, ვინაიდან აზუსტებს სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში გამოსაყენებელ ტექნიკურ საშუალებებს.[1028]

გარდა ამისა, როგორც უკვე აღინიშნა, ინსპექტორი სსსკ-ის 143^3 მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებას აკონტროლებს კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით. „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-2 მუხლის „ი“

[1028] *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 49,
<http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf>
[10.06.2020].

ქვეპუნქტიდან გამომდინარე, „კონტროლის ელექტრონული სისტემა“ წარმოადგენს „ტექნიკურ და პროგრამულ გადაწყვეტილებათა ერთობლიობას, რომელიც იძლევა ობიექტის ტექნიკური იდენტიფიკატორის აქტივაციის შესახებ უფლებამოსილი ორგანოს მონიტორინგის სისტემის მიერ ინიცირებულ ბრძანებათა ინსპექტორის სამსახურისათვის გაგზავნის შესაძლებლობას; ასევე სსსკ-ით დადგენილი წესით ღონისძიების შეჩერების შესაძლებლობას. რაც შეეხება კონტროლის სპეციალურ ელექტრონულ სისტემას, გულისხმობს „ტექნიკურ და პროგრამულ გადაწყვეტილებათა ერთობლიობას, რომელიც უზრუნველყოფს ობიექტის ტექნიკური იდენტიფიკატორის აქტივაციის შესახებ უფლებამოსილი ორგანოს მონიტორინგის სისტემის მიერ ინიცირებულ ბრძანებათა ლოგირების მონაცემების კრიპტოგრაფიული მეთოდების გამოყენებით დამუშავებას, მართლზომიერი გადაჭერის მენეჯმენტის სისტემის მიერ აღსრულებულ ბრძანებათა ლოგირების მონაცემების ზედამხედველი მოსამართლისთვის ავტომატურად მიწოდებას, ამ მონაცემების კრიპტოგრაფიული მეთოდების გამოყენებით დამუშავებას, მიღებული შედეგების ავტომატურ შედარებას და სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტის საფუძველზე განხორციელებული ქმედების (გარდა სახელმწიფო ინსპექტორის სამსახურის მიერ წარმოებულ სისხლის სამართლის საქმეზე განხორციელებული ფარული საგამოძიებო მოქმედებისა) ლოგირების მონაცემების სახელმწიფო ინსპექტორის სამსახურისათვის გაგზავნას“[1029]. საკონსტიტუციო სასამართლოში მხარეთა და მოწმეთა მიერ გაკეთებული განმარტებების მიხედვით, „აღნიშნული ელექტრონული კონტროლის საშუალებები შესაძლებელს ხდის ინსპექტორს რეალურ დროში მიეწოდებოდეს შესაბამისი ინფორმაცია ფარული მიყურადების განხორციელებასთან, მის მიმდინარეობასთან დაკავშირებით.“[1030]

ამდენად, სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში სატელეფონო კომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიების განხორციელებისას ინსპექტორი ფლობს საკმაოდ მნიშვნელოვან და ეფექტიან კონტროლის ბერკეტებს.

[1029] „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-2 მუხლის „კ“ პუნქტი, matsne.gov.ge, 27/03/2017.

[1030] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 40.

რაც შეეხება ნახევრად სტაციონალურ ტექნიკურ შესაძლებლობას, ასეთ დროს ინსპექტორი კანონმდებლობით არ არის აღჭურვილი კონტროლის იმ საშუალებებით, რომლებსაც ფლობს სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში,[1031] კერძოდ, კანონმდებლობა ასეთ დროს არ ითვალისწინებს ინსპექტორის მიერ სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიების ზედამხედველობას კონტროლის ელექტრონული სისტემითა და კონტროლის სპეციალური ელექტრონული სისტემით, ამდენად, ინსპექტორს ამ შემთხვევაში არც ღონისძიების შეჩერების მექანიზმი გააჩნია. ნახევრად სტაციონალური ტექნიკური შესაძლებლობით სატელეფონო კომუნიკაციის ფარული მიყურადების განხორციელებისას, ისევე როგორც ინტერნეტურთიერთობის მონიტორინგის ღონისძიებასთან მიმართებით, ინსპექტორი აღჭურვილია მხოლოდ ინსპექტირების უფლებამოსილებით.

4.2.5 ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის მარეგულირებელი კანონმდებლობა კონსტიტუციურ-სამართლებრივ და ევროკავშირის სტანდარტებთან შესაბამისობის ჭრილში

2017 წლის 22 მარტის ცვლილებები შეეხო ასევე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის საკითხსაც. მონაცემთა შენახვის ხანგრძლივობასთან დაკავშირებით აღსანიშნავია, რომ 2017 წლის მარტის ცვლილებებით ეს ვადა შემცირდა და „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-15 მუხლის პირველი პუნქტის მიხედვით, განისაზღვრა არა უმეტეს 12 თვის პერიოდით. ამავე მუხლის შესაბამისად, ვადის გაგრძელება დასაშვებია შეზღუდულ პირობებში, კერძოდ, მხოლოდ ერთხელ, 3 თვით, საქართველოს გენერალური პროკურორის, საქართველოს შინაგან საქმეთა მინისტრის, საქართველოს თავდაცვის მინისტრის ან საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის მიმართვის საფუძველზე, საქართველოს უზენაესი სასამართლოს შესაბამისი უფლებამოსილების მქონე მოსამართლის განჩინებით (მე-15 მუხლის მე-2 პუნქტი). მე-15 მუხლი ასევე აწესრიგებს ვადის გაგრძელების საფუძვლებს და შესაბამის პირობებს/წესს.

[1031] იქვე. 45-47.

მონაცემთა შენახვის ვადასთან მიმართებით, ნიშანდობლივია, რომ მართალია ევროკავშირის მართლმსაჯულების სასამართლომ ე.წ. „მონაცემთა შენახვის შესახებ“ დირექტივით გათვალისწინებული ვადა – მინიმუმ 6 თვე და მაქსიმუმ 2 წელი, არათანაზომიერად მიიჩნია, მაგრამ არც 2014 წლის და არც 2016 წლის გადაწყვეტილებაში შენახვის კონკრეტული ვადა არ დაუდგენია. ევროკავშირის მართლმსაჯულების სასამართლოს განმარტებით, ეროვნული კანონმდებლობით განსაზღვრული მონაცემთა შენახვის პერიოდი შესაბამისობაში უნდა იყოს თანაზომიერების პრინციპთან[1032]. აქედან გამომდინარე, შენახვის ვადის განსაზღვრა წევრი სახელმწიფოს დისკრეციას წარმოადგენს, თუმცა აღნიშნული უფლებამოსილების გამოყენება უნდა მოხდეს იმგვარად, რათა უზრუნველყოფილი იქნეს მონაცემთა შენახვა მხოლოდ იმ ვადით, რაც მკაცრად აუცილებელია.[1033]

ამ საკითხთან დაკავშირებით ერთმნიშვნელოვანი საერთაშორისო პრაქტიკის არარსებობის პირობებში, რთული სათქმელია, რამდენად შეესაბამება ევროკავშირის სტანდარტს ქართული კანონმდებლობით შემოთავაზებული ვადა.[1034] როგორც საკონსტიტუციო სასამართლო 2016 წლის 14 აპრილის გადაწყვეტილებაში აღნიშნავს, უფლებაში „ჩარევის ინტენსივობა და ხარისხი ლოგიკურად მზარდია ჩარევის დროის ხანგრძლივობის პროპორციულად.“[1035] გერმანიის კანონმდებელმა, მაგალითად, შენახვის საკმაოდ შემჭიდროებული ვადები აირჩია - ტრაფიკის მონაცემებთან დაკავშირებით 10 კვირა, ხოლო ადგილმდებარეობის შესახებ ინფორმაციასთან მიმართებით - 4 კვირა. მიუხედავად ასეთი მცირე ვადებისა, როგორც კვლევაში გამოიკვეთა, გერმანიაში ისევ მწვავე საკითხად რჩება ტრაფიკის და ადგილმდებარეობის შესახებ მონაცემების შენახვა, რასაც როგორც უკვე აღინიშნა, შენახვას დაქვემდებარებული მონაცემების განუსაზღვრელი, ტოტალური ხასიათი განაპირობებს. ეს საკითხი - მონაცემთა ყოველგვარი ფილტრაციის და დიფერენციაციის გარეშე შენახვა, ქართული კანონმდებლობისთვისაც არ არის უცხო.

[1032] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 95.

[1033] იქვე, 108, 122.

[1034] *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 49, <http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].

[1035] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-108.

აღსანიშნავია, რომ 2016 წლის 14 აპრილის გადაწყვეტილებით კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვის მარეგულირებელი კანონმდებლობის არაკონსტიტუციურობის ერთ-ერთ მიზეზად სწორედ მონაცემთა „ყოველგვარი ფილტრაციის გარეშე“, „ბლანკეტური“, „ტოტალური“ შეგროვება დასახელდა. თუმცა 2017 წლის 22 მარტის საკანონმდებლო პაკეტით ამ მიმართულებით ცვლილებები არ განხორციელებულა და მონაცემები ინახება ისევ იმ მოცულობით, რაც გათვალისწინებული იყო საკონსტიტუციო სასამართლოს მიერ 2016 წლის 14 აპრილის გადაწყვეტილებით არაკონსტიტუციურად ცნობილი ნორმებით.[1036]

ამ საკითხთან მიმართებით კვლევის წინა თავში დეტალურად იქნა განხილული ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკა და სასამართლოს მკაფიო პოზიცია იმასთან დაკავშირებით, რომ მონაცემთა ტოტალური, შეუზღუდავი შენახვა - ყველა მომხმარებლის ტრაფიკის და ადგილმდებარეობის შესახებ ყველა მონაცემის, ნებისმიერი საკომუნიკაციო საშუალების გამოყენებით, გამონაკლისის, შეზღუდვის ან დიფერენციაციის გარეშე, არ შეესაბამება თანაზომიერების პრინციპს[1037]. მონაცემთა შენახვის საკითხთან დაკავშირებით მნიშვნელოვან მოთხოვნას წარმოადგენს ასევე იმ პირთა დაცვა, რომელთა მონაცემებიც მიეკუთვნება პროფესიულ საიდუმლოებას.[1038]

გასათვალისწინებელია, რომ ვინაიდან ამ შემთხვევაში მონაცემთა პრევენციულ შენახვასთან გვაქვს საქმე და ჯერ არ არის გამოკვეთილი დანაშაულები/პირები, რომელთა მიმართებითაც შესაძლოა მომავალში გახდეს საჭირო მონაცემთა გამოთხოვა, არ არის მარტივი იმ კრიტერიუმების დადგენა, რომლითაც წინასწარ შეიზღუდება შესანახ მონაცემთა კატეგორია. ერთ-ერთ მიდგომად შეიძლება განხილულ იქნეს შენახვის ვადის იმგვარად შემცირება, რომ მონაცემთა მოცულობაზე არსებითი გავლენა მოახდინოს, მაგალითად, როგორც გერმანიის კანონმდებლობით არის გათვალისწინებული (ტრაფიკის მონაცემთა შენახვისთვის 10 კვირა, ადგილმდებარეობის შესახებ მონაცემებისთვის 4 კვირა), თუმცა როგორც კვლევაში გამოიკვეთა, ვადის ამგვარი შემცირების მიუხედავად, გერმანიაში მონაცემთა ტოტალური, ბლანკეტური შენახვის პრობლემატიკა ისევ დგას და საბოლოო

[1036] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 73.

[1037] Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice.

[1038] იქვე, 105.

გადაწყვეტილება ამ საკითხზე ევროკავშირის მართლმსაჯულების სასამართლომ უნდა მიიღოს. ნიშანდობლივია, რომ ეს გადაწყვეტილება მნიშვნელოვანი იქნება არამარტო გერმანიის კანონმდებლისთვის, არამედ ზოგადად, ამ საკითხთან დაკავშირებით ევროკავშირის მოთხოვნების უფრო დაზუსტების და ამ სამართლებრივი დილემის უფრო მარტივად გადაჭრის თვალსაზრისით.

მნიშვნელოვანია ისიც, რომ გადაწყვეტილებაში Tele2 Sverige AB and Watson ევროკავშირის მართლმსაჯულების სასამართლომ განსაზღვრა სახელმძღვანელო კრიტერიუმები, რომლებითაც შესაძლოა დადგინდეს კავშირი შენახვას დაქვემდებარებულ მონაცემებსა და საზოგადოების წინაშე მდგარ საფრთხეს, ესენია: „ა) მონაცემები, რომლებიც ეხება კონკრეტულ დროის პერიოდს, გეოგრაფიულ ტერიტორიას ან/და პირთა ჯგუფებს, რომლებიც შესაძლოა დანაშაულში იყვნენ ჩაბმული ან ბ) პირი, რომლის შესახებაც შეგროვებულ მონაცემებს, სხვა მიზეზიდან გამომდინარე, შეუძლია წვლილი შეიტანოს დანაშაულთან ბრძოლის საქმეში.“[1039]

როგორც ვხედავთ, ეს კრიტერიუმები არის ალტერნატიული შინაარსის და ევროკავშირის მართლმსაჯულების სასამართლომ ეროვნულ კანონმდებელს დაუტოვა გარკვეული დისკრეცია, თავად განსაზღვროს, კონკრეტული პირობების მიხედვით მათი გამოყენების საკითხი.[1040]

ყოველივე აქედან გამომდინარე, მოცემულ საკითხთან დაკავშირებით ევროკავშირის სტანდარტების საკანონმდებლო დონეზე გათვალისწინება ძალიან მნიშვნელოვანია, მითუმეტეს, რომ საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება ასევე ეხმიანება ამ მოთხოვნებს და ნორმის არაკონსტიტუციურობის ერთ-ერთ მიზეზად სწორედ მონაცემთა აბსტრაქტული ხასიათის შეგროვებას ასახელებს.

კიდევ ერთი საკითხი, რაც საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებაში ნორმის არაკონსტიტუციურობას დაედო საფუძვლად, უკავშირდება პერსონალურ მონაცემთა დაცვის ინსპექტორის (იმ დროს მოქმედი კანონმდებლობის მიხედვით) არასაკმარისი კონტროლის ბერკეტებს. როგორც საკონსტიტუციო სასამართლომ დაადგინა, კანონმდებლობა არ ითვალისწინებდა

[1039] იქვე, 106.

[1040] იხ. ასევე *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018, 167.

ზედამხედველობის მექანიზმებს მონაცემთა კოპირების პროცესზე. ამ თვალსაზრისით განსაკუთრებული მნიშვნელობა მიენიჭა ე.წ. „ალტერნატიული ბანკის“ შექმნასთან დაკავშირებულ რისკებს.

მიგვაჩნია, რომ 2017 წლის 22 მარტის ცვლილებებს რაიმე ახლებური რეგულირება არ შემოუტანია ინსპექტორის მიერ მონაცემთა კოპირების პროცესის გაკონტროლების თვალსაზრისით[1041]. დადებითი ნოვაცია არის ის, რომ როგორც ირკვევა, არსებული კონტროლის ერთ-ერთი ბერკეტი - ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემა ტექნიკური თვალსაზრისით უკვე გამართულია და მისი საშუალებით ინსპექტორი ახორციელებს კოპირებულ მონაცემთა ბანკში განხორციელებული ქმედებების კონტროლს.[1042] რაც შეეხება ელექტრონული კომუნიკაციის კომპანიებისგან სააგენტოს მიერ მონაცემთა კოპირების პროცესს, აღნიშნულზე ზედამხედველობის ერთადერთ ბერკეტს წარმოადგენს ინსპექტირება. ზედამხედველობის ეს სახე საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით არაეფექტიანად მიიჩნია, მისი განხორციელების მეთოდის გამო, რაც „შემთხვევითი შერჩევის პრინციპში“ მდგომარეობს.

რაც შეეხება მონაცემთა ე.წ. „ალტერნატიული ბანკის“ შექმნასთან დაკავშირებულ საფრთხეს, როგორც საკონსტიტუციო სასამართლოში მოპასუხე სახელმწიფო უსაფრთხოების სამსახურის წარმომადგენელმა თავადვე დაადასტურა, ამ რისკის გამორიცხვა დამოკიდებულია იმ ორგანოს (სააგენტოს) დამოუკიდებლობის ხარისხზე, რომელიც მონაცემთა კოპირებას ახდენს.[1043]

4.3. შეჯამება

ამრიგად, კონსტიტუციურ-სამართლებრივი სტანდარტების განხილვის შედეგად გამოვლინდა, რომ 2017 წლის 22 მარტის საკანონმდებლო ცვლილებებმა გარკვეულ საკითხებთან დაკავშირებით გაითვალისწინა დადებითი ნოვაციები, მაგრამ ძირითად შემთხვევაში არსებული კანონმდებლობის 2016 წლის 14 აპრილის გადაწყვეტილებით

[1041] საპირისპირო მოსაზრებასთან დაკავშირებით იხ. საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II- 84.
[1042] იქვე, II- 96.
[1043] იქვე, I-68.

დადგენილ მოთხოვნებთან შესაბამისობის საკითხი კვლავ პრობლემატურია, რასაც ადასტურებს მიმდინარე საკონსტიტუციო დავაც და განსაკუთრებით, ის ფაქტი, რომ თავად საკონსტიტუციო სასამართლოს შემადგენლობაშიც აზრთა სხვადასხვაობა გამოიწვია მთელი რიგი საკანონმდებლო დებულებების 2016 წლის 14 აპრილის გადაწყვეტილებასთან შესაბამისობის საკითხმა.

პრობლემატურ საკითხებს შორის გამოიკვეთა ინტერნეტურთიერთობის მონიტორინგის ღონისძიებაზე ზედამხედველობის მექანიზმები, ნახევრად სტაციონალური ტექნიკური შესაძლებლობის გამოყენების ფარგლებში კონტროლის ბერკეტები, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემების ბაზების კოპირებასთან დაკავშირებული ასპექტები, როგორიცაა მაგალითად, მონაცემთა შენახვის „ტოტალური“, „მასობრივი“ ხასიათი და ზედამხედველობა მონაცემთა ბაზების კოპირების პროცესზე.

რაც შეეხება ახლად შექმნილი ორგანოს - სააგენტოს დამოუკიდებლობის მექანიზმებს, როგორც გამოვლინდა, მართალია სააგენტო აღჭურვილია ავტონომიურობის მეტი ხარისხით, ვიდრე მისი წინამორბედი ოპერატიულ-ტექნიკური დეპარტამენტი, მაგრამ კვლავ რჩება მნიშვნელოვანი ასპექტები, როდესაც საკმაოდ მაღალია მასზე სახელმწიფო უსაფრთხოების სამსახურის გავლენა.

5. ზედამხედველობის მექანიზმების ეფექტიანობის შეფასება

მოცემული ქვეთავის მიზანია, შეჯამებულ იქნეს კომუნიკაციის რეალურ დროში მოპოვების ღონისძიებებზე და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა კოპირების პროცესზე საქართველოს კანონმდებლობით გათვალისწინებული კონტროლის ბერკეტები. აღნიშნული ეხება როგორც სასამართლოს ზედამხედველობას, ასევე გარე კონტროლის მექანიზმებს.

განხილული საერთაშორისო სტანდარტების შედეგად გამოიკვეთა, რომ სასამართლო კონტროლის ეფექტიანობის განმსაზღვრელ ერთ-ერთ ყველაზე მნიშვნელოვან ფაქტორს სასამართლოს კომპეტენციის ფარგლები წარმოადგენს. საქმეში ევროპული ინტეგრაციისა და ადამიანის უფლებათა ასოციაცია და ეკიმჯიევი ბულგარეთის წინააღმდეგ (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria), ევროპულმა სასამართლომ განასხვავა სატელეფონო კომუნიკაციის ფარული მიყურადების ორი ეტაპი - ნებართვის გაცემის და

ღონისძიების უშუალოდ განხორციელების.[1044] ამ თვალსაზრისით მნიშვნელოვანია, რომ ეფექტიანი ზედამხედველობა იყოს გათვალისწინებული ფარული მეთვალყურეობის ღონისძიების განხორციელების ორივე ამ ეტაპზე. ევროპულმა სასამართლომ არაერთ საქმეში გამოხატა უარყოფითი პოზიცია, როდესაც ეროვნული კანონმდებლობა არ ითვალისწინებდა მოსამართლის მიერ ღონისძიების შედეგების გაცნობისა და ღონისძიების განხორციელების კანონიერებაზე ზედამხედველობის შესაძლებლობას.[1045] მაგალითად, ერთ-ერთ საქმეში კრიტიკა დაიმსახურა იმ გარემოებამ, რომ მართალია კანონმდებლობა ითვალისწინებდა სასამართლოს ინფორმირების ვალდებულებას ღონისძიების დამთავრებასთან დაკავშირებით, ასევე სასამართლოს ინფორმირებას ნებართვით გათვალისწინებულ ვადამდე ღონისძიების დასრულების შესახებ, მაგრამ არ განსაზღვრავდა სასამართლოს მიერ ღონისძიების შედეგების გაცნობის შესაძლებლობას და ასევე არ ავალდებულებდა მოსამართლეს, გადაემოწმებინა, რამდენად იქნა დაცული კანონმდებლობის მოთხოვნები ღონისძიების განხორციელებისას.[1046]

რაც შეეხება ქართულ კანონმდებლობას, როდესაც საუბარია ისეთ სისტემაზე, სადაც სახელმწიფოს აქვს კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობა, ზედამხედველობის ბერკეტების ეფექტიანობა განსაკუთრებით მნიშვნელოვანი და აქტუალურია, ეს მოსაზრება გამომდინარეობს საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან, რომლითაც არაკონსტიტუციურად იქნა ცნობილი კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობით „გამოძიებაზე პასუხისმგებელი“ და „პროფესიულად დაინტერესებული ორგანოს“ სახელმწიფო უსაფრთხოების სამსახურის აღჭურვა. აღნიშნული მოსაზრება გამოხატა ასევე ევროპულმა სასამართლომ საქმეში ზახაროვი რუსეთის წინააღმდეგ (Zakharov v. Russia), სადაც აღნიშნა, რომ სისტემა, რომელიც უსაფრთხოების სამსახურებსა და პოლიციას

[1044] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 84; Iordachi and others v. Moldova, [2009], ECtHR, 42.

[1045] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, 207, <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [18.06.2020], იხ. ციტირება: Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 84-85. იხ. ასევე Iordachi and others v. Moldova, [2009], ECtHR; Huvig v. France, [1990], ECtHR, (Ser. A.).

[1046] Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 85.

შესაძლებლობას აძლევს, სერვისის მიმწოდებლისთვის ან სხვა უფლებამოსილი პირებისათვის შესაბამისი ნებართვის წარდგენის გარეშე, უშუალოდ ჰქონდეთ წვდომა ნებისმიერი მოქალაქის კომუნიკაციის საშუალებებზე, განსაკუთრებით მიდრეკილია უფლების ბოროტად გამოყენებისკენ[1047]. შესაბამისად, საჭიროებს უფლების დაცვის განსაკუთრებით ძლიერი გარანტიების არსებობას, რომლის კონტექსტშიც ზედამხედველობის სისტემის ეფექტიანობა უნდა იქნეს შეფასებული.[1048]

აღნიშნულიდან გამომდინარე, მართალია დღეის მდგომარეობით ფარული საგამოძიებო მოქმედებების ტექნიკურად აღსრულების ფუნქცია ახალ ორგანოს - სააგენტოს აქვს დაკისრებული, მაგრამ კომუნიკაციის რეალურ დროში მოპოვების მარეგულირებელი კანონმდებლობის კონსტიტუციურობა ამჟამად საკონსტიტუციო სასამართლოში ისევ სადაოდ არის გამხდარი, რაც კიდევ ერთხელ უსვამს ხაზს ამ საკითხის აქტუალურობას და სირთულეს. შესაბამისად, ფარული საგამოძიებო მოქმედებების განხორციელებაზე კონტროლის მექანიზმების ეფექტიანობას განსაკუთრებული დატვირთვა აქვს ქართულ რეალობაში.

მიგვაჩნია, რომ ზედამხედველობის მექანიზმებთან დაკავშირებით, ქართულ კანონმდებლობაში ღონისძიების ჩატარებაზე ნებართვის გაცემის ეტაპზე უფრო ქმედითი მექანიზმები არსებობს და გათვალისწინებულია როგორც სასამართლოს კონტროლი, ასევე ინსპექტორის სამსახურის ზედამხედველობა კონტროლის ელექტრონული საშუალებებით სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებასთან მიმართებით, მაგრამ ფარული საგამოძიებო მოქმედების იმპლემენტაციის ეტაპზე კონტროლის მექანიზმების ეფექტიანობა პრობლემურია, კერძოდ, ნებართვის გაცემის შემდეგ ღონისძიების განხორციელების მთლიანი პროცესი ნაკლებად ექცევა მეთვალყურეობის ქვეშ.[1049] ამ თვალსაზრისით საყურადღებოა ღონისძიების დასრულების შემდეგ ოქმის შედგენასთან დაკავშირებით 2017 წლის 22 მარტს შეტანილი ცვლილება სსსკ-ში, კერძოდ, სსსკ-ის

[1047] Roman Zakharov v. Russia, [2015] ECtHR, 270-271.

[1048] იქვე.

[1049] *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, (რედ.), თბ., 2019, 393-394; *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 49, <http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].

143[6] მუხლის მე-14 ნაწილის მიხედვით, შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანო ფარული საგამოძიებო მოქმედების დასრულებისთანავე ადგენს ოქმს. ოქმში აღინიშნება საგამოძიებო მოქმედების ჩატარების სამართლებრივი საფუძველი, მისი დაწყებისა და დასრულების დრო, ოქმის შედგენის ადგილი, ჩატარებული ფარული საგამოძიებო მოქმედების სახე და მისი ჩატარებისას გამოყენებული ტექნიკური საშუალებები, ფარული საგამოძიებო მოქმედების ჩატარების ადგილი, ფარული საგამოძიებო მოქმედების ობიექტი და ობიექტის ტექნიკური იდენტიფიკატორი. მართალია ოქმის შედგენის ვალდებულება საგამოძიებო ორგანოს გააჩნდა 2017 წლის 22 მარტის ცვლილებებამდეც, თუმცა სიახლეს წარმოადგენს ის გარემოება, რომ ოქმი გადაეცემა ინსპექტორის სამსახურს და ფარული საგამოძიებო მოქმედებების სასამართლო რეესტრს, ხოლო ინსპექტორის სამსახურის წარმოებაში არსებული სისხლის სამართლის საქმეების შემთხვევაში - ზედამხედველ მოსამართლეს. თუმცა აღსანიშნავია, რომ ცვლილების მიუხედავად, სსსკ-ის ეს ნორმა არ ითვალისწინებს ოქმის მიწოდების ვალდებულებას იმ სასამართლოსთვის ან იმ მოსამართლისთვის, რომელმაც გასცა ნებართვა აღნიშნული ფარული საგამოძიებო მოქმედების ჩასატარებლად ან რომელმაც დააკანონა იგი. მართალია სსსკ-ით გათვალისწინებულია ოქმის წარდგენის მოთხოვნა სასამართლო რეესტრში, მაგრამ მიგვაჩნია, რომ მხოლოდ აღნიშნული ვერ ჩაითვლება საკმარის გარანტიად, ვინაიდან ინფორმაციის წარდგენა ფარული საგამოძიებო მოქმედებების რეესტრში, რომელსაც აწარმოებს საქართველოს უზენაესი სასამართლო, ემსახურება სსსკ-ის 143[10] მუხლის შესაბამისად, ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით ამ მუხლით გათვალისწინებული სტატისტიკური ინფორმაციის აღრიცხვისა და გამოქვეყნების მიზანს და აქედან გამომდინარე, კავშირში არ არის სასამართლოს მაკონტროლებელი ფუნქციის გაზრდასთან. ამ საკითხთან დაკავშირებით ასევე აღსანიშნავია სსსკ-ში (143[6] მუხლში) 2017 წლის 22 მარტის კანონით შესული სხვა ცვლილებაც, რომლის თანახმადაც, ფარული საგამოძიებო მოქმედების მიმდინარეობისას, პროკურორის/მოსამართლის მოთხოვნის შემთხვევაში, ფარული საგამოძიებო მოქმედების განმახორციელებელი ორგანო ვალდებულია გასცეს შუალედური ოქმი. ამ კუთხით მხედველობაშია მისაღები, რომ სსსკ-ის 143[6] მუხლის მე-15 ნაწილში, სადაც საუბარია შუალედური ოქმის შედგენაზე, საერთოდ არ არის აღნიშნული, რა ინფორმაციას უნდა შეიცავდეს ეს ოქმი და

შესაბამისად, გაურკვეველია თუ რა სახის კომპეტენცია და კონტროლის ფუნქცია გააჩნია სასამართლოს/პროკურორს ამ თვალსაზრისით. მეორე მნიშვნელოვანი და არსებითი საკითხი არის ამ ნორმის ბუნდოვანი ხასიათი, კერძოდ, სსსკ-ის 143[6] მუხლის მე-15 ნაწილიდან გამომდინარე, თითქოს ეს უფლებამოსილება მოსამართლეს (ასევე პროკურორს) ნებისმიერ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით უნდა გააჩნდეს, როგორც მის მიერ ნებადართული, ასევე post factum დაკანონებული, თუმცა, როგორც ირკვევა, ამ ნორმის ინტერპრეტაცია პრაქტიკაში სხვაგვარად ხდება და რეალურად ამ უფლებამოსილებას სასამართლო იყენებს მხოლოდ გადაუდებელი აუცილებლობის საფუძვლით დაწყებული ფარული საგამოძიებო მოქმედების გაგრძელების შესახებ გადაწყვეტილების მისაღებად.[1050]

უნდა აღინიშნოს, რომ საერთაშორისო სტანდარტის მიხედვით, აუცილებელი არ არის განგრძობადი კონტროლი მოსამართლემ განახორციელოს, მაგრამ ასეთ შემთხვევაში კანონმდებლის მიერ არჩეული სხვა ზედამხედველი ორგანოს კომპეტენცია უნდა უზრუნველყოფდეს ადეკვატურ გარანტიებს უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგოდ. ამ კონტექსტში მნიშვნელოვანია, რომ სსსკ-ით გათვალისწინებული ფარული საგამოძიებო მოქმედებების მაკონტროლებელი ორგანოს - ინსპექტორის მიერ ღონისძიების შეჩერების უფლებამოსილებაც, რომელიც საკმაოდ ეფექტიანი მექანიზმია სსსკ-ის 143[6] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებასთან დაკავშირებით, ძირითადად ემსახურება ღონისძიების დასაწყებად შესაბამისი კანონიერი საფუძვლის არსებობის შემოწმებას.[1051]

[1050] ამის თქმის საფუძველს, ასევე იძლევა თბილისის საქალაქო სასამართლოს 2019 წლის 14 აგვისტოს N2058-19 წერილი, კერძოდ, 2019 წლის 9 აგვისტოს თბილისის საქალაქო სასამართლოს გაეგზავნა მოთხოვნა მოსამართლეთა მიერ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედებების შუალედური ოქმის მოთხოვნის სტატისტიკის მოწოდებასთან დაკავშირებით, რის პასუხადაც თბილისის საქალაქო სასამართლოს მიერ მოწოდებულ იქნა სტატისტიკური მონაცემები მხოლოდ გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული ფარული საგამოძიებო მოქმედებების შესახებ და წერილით დამატებით განმარტებულ იქნა, რომ სხვა სახის სტატისტიკური ინფორმაცია თბილისის საქალაქო სასამართლოში არ მუშავდება.

[1051] *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, (რედ.), თბ., 2019, 393. *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 49, <http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].

ზოგადად, ქართული კანონმდებლობით გათვალისწინებული ინსპექტორის სამსახურის ზედამხედველობის მოდელი, ერთ-ერთ უმნიშვნელოვანეს გარანტიად შეიძლება ჩაითვალოს ფარული საგამოძიებო მოქმედებების განხორციელების პროცესში ადამიანის უფლებების დაცვის კუთხით. აღსანიშნავია ისიც, რომ ზედამხედველობის შერეული მოდელები (სასამართლოს ზედამხედველობა, ადმინისტრაციული ორგანოს მხრიდან კონტროლი) დადებითად არის შეფასებული საერთაშორისო დონეზე, რაზეც ხაზგასმით მიუთითებს გაეროს სპეციალური მომხსენებელი ანგარიშში „პირადი ცხოვრების უფლება ციფრულ ეპოქაში“[1052], უფრო მეტიც, ასეთი ზედამხედველობა სასამართლო სისტემის ნაკლოვანებების დამაბალანსებელ ფაქტორადაც კი მიიჩნევა;[1053] აქედან გამომდინარე, საქართველოს კანონმდებლობაში კონტროლის ასეთი სისტემის არსებობა თავისთავად უმნიშვნელოვანეს ბერკეტად შეიძლება შეფასდეს, თუმცა არსებობს რიგი პრობლემატური ასპექტები, რომლებიც საკონსტიტუციო სასამართლოში მიმდინარე დავების ფარგლებში წარმოჩინდა, მაგალითად, ზედამხედველობა ინტერნეტურთიერთობის მონიტორინგის ღონისძიებაზე, ასევე ნახევრად სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში სატელეფონო კომუნიკაციის ფარული მიყურადების კონტროლი, ელექტრონული კომუნიკაციების კომპანიებიდან მონაცემთა ბაზების კოპირების პროცესზე ზედამხედველობა. დღესდღეობით ეს საკითხები ჯერ კიდევ გადასაწყვეტია საკონსტიტუციო სასამართლოში ამჟამად მიმდინარე დავის ფარგლებში.

როგორც ზემოთ აღინიშნა, ინსპექტორის კონტროლთან დაკავშირებით მიზანშეწონილი იქნება, ღონისძიების დასრულების ოქმში, რომელიც სსსკ-ით გათვალისწინებულ სხვა პირებთან ერთად ასევე მიეწოდება ინსპექტორს, სხვა მონაცემებთან ერთად აღინიშნოს აგრეთვე ინფორმაცია ღონისძიების შედეგად მოპოვებული მონაცემების შესახებ. აღსანიშნავია, რომ ინსპექტორს ასევე მიეწოდება ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული მასალის განადგურების ოქმი. შესაბამისად, თუკი მას ეცოდინება რა მოცულობის ინფორმაცია იქნა

[1052] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 13 (ბმული იხ. მე-19 გვერდზე).
[1053] იქვე.

მოპოვებული და რა მოცულობის განადგურდა, შესაძლებლობა მიეცემა, შეადაროს ეს ინფორმაციები ერთმანეთს; მართალია ცალკე აღებულმა ასეთმა შედარებამ შესაძლოა ყოველთვის ზუსტი სურათი არ შექმნას მოპოვებული და განადგურებული ინფორმაციის მოცულობის შესახებ და საჭირო გახდეს სხვა ინფორმაციებთან ერთობლიობაში მათი შეფასება, მაგრამ ამ მონაცემების ცოდნა ინსპექტორს, როგორც მინიმუმ, დაეხმარება შესაძლო დარღვევის უფრო მარტივად გამოვლენაში. დღევანდელი რეგულაციის პირობებში ამ ინფორმაციების შედარება ინსპექტორს შეუძლია მხოლოდ იმ შემთხვევაში, თუკი ჩაატარებს ინსპექტირებას.

როგორც უკვე აღინიშნა, საზედამხედველო ორგანოს კომპეტენციის შეფასებისას ერთ-ერთ მნიშვნელოვან ფაქტორს წარმოადგენს ამ ორგანოს უფლებამოსილება რაიმე დარღვევის აღმოჩენის შემთხვევაში - მაკონტროლებელი ორგანოსთვის მინიჭებული კომპეტენციის ფარგლები დადებითად იქნა შეფასებული ევროპული სასამართლოს მიერ, მაგალითად, როდესაც კომუნიკაციის მონიტორინგის განმახორციელებელ ორგანოს ეკისრებოდა ღონისძიების შეწყვეტის ვალდებულება საზედამხედველო კომისიის მიერ მისი „უკანონოდ“ ან „არააუცილებლად“ მიჩნევისას;[1054] ასევე, როდესაც მაკონტროლებელი ორგანოს მიერ ჩატარებული ღონისძიების უკანონოდ მიჩნევის შემთხვევაში მოპოვებული ინფორმაცია განადგურებას ექვემდებარებოდა.[1055]

ამ თვალსაზრისით მხედველობაშია მისაღები ინსპექტორის კომპეტენცია დარღვევის გამოვლენის კუთხით. როგორც კვლევაში გამოიკვეთა, ეს საკითხი საჭიროებს უფრო მეტ სიცხადეს და კონკრეტიკას, რათა თვალსაჩინო იყოს, რამდენად შეუძლია ინსპექტორს, მოითხოვოს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურება.

როგორც უკვე აღინიშნა, სსსკ-ში 2017 წლის 22 მარტს განხორციელებული ცვლილებების შედეგად სისხლის სამართლის პროცესში შემოტანილ იქნა ზედამხედველი მოსამართლის ინსტიტუტი. აღნიშნული ცვლილება ზედამხედველობის კონტექსტში სასამართლოს უფლებამოსილების გაზრდის სასარგებლოდ იქნა შეფასებული.[1056] თავისთავად ახალი საზედამხედველო

[1054] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 53.
[1055] Kennedy v. United Kingdom, [2010] ECtHR, 168.
[1056] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის N3/4/885-1231 საოქმო ჩანაწერი.

ინსტიტუტის შემოტანა დადებით ნოვაციად შეიძლება შეფასდეს, მითუმეტეს რომ მაკონტროლებელი ფუნქციით ამ შემთხვევაში სასამართლოს ხელისუფლების წარმომადგენელი არის აღჭურვილი, თუმცა ამის მიუხედავად, ზედამხედველი მოსამართლის მაკონტროლებელი ფუნქცია ნაკარნახევია ცალკეულ შემთხვევებში (ინსპექტორის წარმოებაში არსებულ სისხლის სამართლის საქმეებზე) ინსპექტორის სამსახურის მაკონტროლებელი როლის ჩანაცვლებით, რაც განპირობებულია ინსპექტორის სამსახურისთვის საგამოძიებო უფლებამოსილების მინიჭებით. აქედან გამომდინარე, ზედამხედველი მოსამართლე ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით აღჭურვილია იმ კომპეტენციით, რაც სსსკ-ის ფარგლებში ინსპექტორს აქვს მინიჭებული; ამდენად, ნაკლებად სავარაუდოა, ეს ინსტიტუტი ფარულ საგამოძიებო მოქმედებებზე მოსამართლის როლის გაძლიერების კუთხით იყოს გამოსადეგი, არამედ უნდა შეფასდეს როგორც არსებული მოდელის - ინსპექტორის სამსახურის საზედამხედველო მექანიზმის ალტერნატიული საშუალება რიგ შემთხვევებში, როდესაც ინსპექტორის სამსახური ზემოაღნიშნული გარემოებიდან გამომდინარე, კონტროლს თავად ვერ ახორციელებს. ხოლო როდესაც ვსაუბრობთ მოსამართლის საზედამხედველო ფუნქციის გაძლიერებაზე, მიგვაჩნია, რომ უნდა მოიაზრებოდეს მოსამართლე, რომელმაც გასცა ნებართვა ღონისძიების განხორციელებაზე. სწორედ ასეთი მოსამართლე არის მოწოდებული, გაუწიოს ზედამხედველობა მის მიერ განხილულ/ნებადართულ ღონისძიებას.

საბოლოო ჯამში, ზედამხედველობის მექანიზმებთან დაკავშირებით, მიგვაჩნია, რომ სასამართლო რგოლის მეტი ჩართულობა და მისი როლის გაზრდა უფრო გააძლიერებს კომუნიკაციის მონიტორინგის ღონისძიებებზე არსებული კონტროლის მექანიზმებს.[1057] სასამართლოს ზედამხედველობა, ზოგადად, განიხილება საუკეთესო გარანტიად, ვინაიდან როგორც წესი, სასამართლო მიჩნეულია მიუკერძოებელ,

[1057] *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, (რედ.), თბ., 2019, 393-394; *გეგეშიძე თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება - ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №:2, 2017, 49, <http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].

დამოუკიდებელ უწყებად.[1058] ასევე ითვლება, რომ მოსამართლეს ყველაზე უკეთ შეუძლია შეაფასოს ისეთი სამართლებრივი საკითხები, როგორიცაა ღონისძიების აუცილებლობა და პროპორციულობა, რაც ბუნებრივია, არსებით მოთხოვნას წარმოადგენს, როდესაც ღონისძიებას მნიშვნელოვანი გავლენის მოხდენა შეუძლია ადამიანის უფლებებზე.[1059] ამასთანავე, ამგვარი ზედამხედველობა საშუალებას მისცემს მოსამართლეს, უკეთ გაიაზროს ღონისძიების ინტენსივობა, გამოსადეგობა და აუცილებლობა. მაგალითად, ფარული მეთვალყურეობის შესახებ პოლონეთის კანონმდებლობასთან დაკავშირებულ ანგარიშში ვენეციის კომისია ამ ღონისძიებების განხორციელებაზე ეფექტიანი ზედამხედველობის ერთ-ერთ სასურველ მექანიზმად განიხილავს სასამართლოს (რომელიც გასცემს ნებართვას ფარული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე) მიერ მოპოვებული მასალების რეგულარულად გადამოწმების შესაძლებლობას განგრძობადი ზედამხედველობის განხორციელების მიზნით[1060]. კომისიის მოსაზრებით, სასამართლოსთვის ღონისძიების განხორციელებაზე განგრძობადი კონტროლის უფლებამოსილების მინიჭება, საშუალებას მისცემს მოსამართლეს, ერთი მხრივ, შეაფასოს რამდენად მოქმედებდა პოლიცია ნებართვით მინიჭებული მანდატის ფარგლებში, ხოლო, მეორე მხრივ, უკეთ გაიაზროს ღონისძიების გამოსადეგობა და უფლებაშემზღუდველი ხასიათი.[1061] აღსანიშნავია, რომ სასამართლოს განგრძობადი ზედამხედველობის მაგალითები სხვა ქვეყნის კანონმდებლობაშიც გვხვდება, მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსის მიხედვით, უფლებამოსილ მოსამართლეს უნდა ეცნობოს ტელეკომუნიკაციის ფარული მიყურადებისა და ჩაწერის ღონისძიების შედეგები ამ ღონისძიების დასრულების შემდეგ (პარაგრაფი 100 e (5)), ხოლო ონლაინ ჩხრეკის საგამოძიებო მოქმედებასთან მიმართებით (პარაგრაფი 100b) კიდევ უფრო მკაცრი

[1058] *Malgieri, G., Hert, P. D.,* European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges, The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 528.

[1059] *Malgieri, G., Hert, P. D.,* European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges, The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017, 528, იხ. ციტირება: The Council of Europe Commissioner for Human Rights, *supra* note 76, at 55.

[1060] European Commission for Democracy Through Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, 26, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].

[1061] იქვე.

მიდგომა არსებობს და გათვალისწინებულია სასამართლოს ინფორმირების ვალდებულება აგრეთვე ღონისძიების მიმდინარეობის შესახებ.[1062] ამის მსგავსად, მოსამართლის გადაწყვეტილებით, დასახულ მიზანთან მიმართებით ღონისძიების პროგრესისა და მისი შემდგომი გაგრძელების მიზანშეწონილობის შესახებ სასამართლოს პერიოდული ინფორმირების შესაძლებლობა არის გათვალისწინებული აშშ-ის კანონმდებლობითაც.[1063]

თუმცა როდესაც სასამართლო კონტროლზე ვსაუბრობთ, მხედველობაში არის მისაღები, რომ ფარული საგამოძიებო მოქმედებების სპეციფიკურობიდან და თანამედროვე ტექნოლოგიების ტექნიკური მახასიათებლების მუდმივი განვითარებიდან გამომდინარე, სასამართლოს მხოლოდ ჩართულობა, თუნდაც უფრო აქტიური, შეიძლება არასაკმარისი იყოს. ამიტომაცაა, რომ საერთაშორისო დონეზე სულ უფრო აქტიურად განიხილება სხვადასხვა მექანიზმები სასამართლო კონტროლის ქმედითი და რეალურად ეფექტიანი სისტემის უზრუნველსაყოფად. ნაშრომის წინა ქვეთავებში განხილულ იქნა სასამართლო კონტროლის ეფექტიანობის ხელშემშლელი ფაქტორები, როგორიცა მაგალითად, მოსამართლეთა გადატვირთულობა, მოსამართლის მიერ შუამდგომლობის ზედაპირული დამუშავება, შეჯიბრებითი პროცესის ელემენტების ნაკლებობა, მოსამართლეთა კომპეტენციის ნაკლებობა კომუნიკაციის მონიტორინგის ღონისძიებებთან დაკავშირებულ ტექნიკურ და პრაქტიკულ ასპექტებთან დაკავშირებით; შესაბამისად, მნიშვნელოვანია, გათვალისწინებული იქნეს ის რეკომენდაციები, რომლებიც გაჟღერებულია საერთაშორისო დონეზე სასამართლო კონტროლის ეფექტიანობის უზრუნველყოფასთან დაკავშირებით.

აქვე უნდა განვიხილოთ საკითხი, სასამართლოს როლის რაიმე კუთხით გაზრდა წინააღმდეგობაში ხომ არ მოვა სსსკ-ით უზრუნველყოფილ შეჯიბრებითობის პრინციპთან;[1064] მიგვაჩნია, რომ სასამართლოს ინფორმირებულობა ღონისძიების შედეგების შესახებ, რაც უნდა ისახოს ღონისძიების დასრულების ოქმში, სრულებით არ წამოჭრის შეჯიბრებითობის პრინციპთან რაიმე კუთხით შეუსაბამობის საკითხს;

[1062] StPO, §100e Abs.5, 07/04/1987.

[1063] *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed., 2004, 286.

[1064] აღნიშნულ საკითხთან დაკავშირებით იხ. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 418.

მითუმეტეს რომ, დღეს ეს ოქმი მიეწოდება ამ პროცესში ჩართულ ყველა სუბიექტს, ნებართვის გამცემი სასამართლოს გარდა. აქ, ბუნებრივია, საუბარი ვერ იქნება სასამართლოს მხრიდან მოპოვებული მტკიცებულების ბედის გადაწყვეტაზე, რაც შეჯიბრებითობის პრინციპიდან გამომდინარე, მხარეთა შუამდგომლობების საფუძველზე მტკიცებულების დასაშვებობის ეტაპზე წყდება.

გასათვალისწინებელია ის გარემოებაც, რომ ღონისძიების განხორციელების მთელ პროცესზე ეფექტური კონტროლის უზრუნველყოფა ერთ-ერთ მნიშვნელოვან მოთხოვნას წარმოადგენს საერთაშორისო დონეზე. მიგვაჩნია, რომ ღონისძიების დასრულების ოქმში ინფორმაციის ასახვა მიღწეული შედეგების (მოპოვებული მონაცემების შესახებ) თაობაზე და მოსამართლისთვის ამ ოქმის წარდგენა, არათუ წინააღმდეგობაში მოვა შეჯიბრებითობის პრინციპთან, არამედ მხარეთა საპროცესო თანასწორობას შეუწყობს ხელს, იქედან გამომდინარე, რომ გაძლიერდება ნეიტრალური მსაჯულის - მოსამართლის როლი, რომელიც მოწოდებულია დაიცვას ადამიანის უფლებები, განსაკუთრებით ისეთ სფეროში, სადაც დაცვის მხარე პროცესის სპეციფიკის (საიდუმლო რეჟიმში მიმდინარეობა) მიზეზით თვითონ ვერ ახერხებს თავისი საპროცესო უფლებების რეალიზებას. ამიტომ, მიგვაჩნია, რომ ამ კუთხით მოსამართლის მეტი ინფორმირებულობა გაზრდის საგამოძიებო ორგანოების მხრიდან ანგარიშვალდებულებას, მათ დისციპლინირებას და შეამცირებს უფლების ბოროტად გამოყენების რისკებს. ამასთან, როგორც ზემოთ აღინიშნა, ოქმში მოპოვებული მასალის შესახებ ინფორმაციის ასახვა ასევე გაამარტივებს ინსპექტორის სამსახურის მიერ ამ ღონისძიებებზე კონტროლის პროცესს.

შეჯიბრებითობის პრინციპთან ურთიერთმიმართების თვალსაზრისით აღსანიშნავია ისიც, რომ სსსკ მოსამართლეს ისედაც ანიჭებს გარკვეული ინიციატივის უფლებას ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით, მაგალითად, სსსკ-ის 143[3] მუხლის 6[1] პუნქტის თანახმად, გადაუდებელი აუცილებლობის საფუძვლით ჩატარებულ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით გადაწყვეტილების მიღების მიზნით მოსამართლეს შეუძლია უფლებამოსილი ორგანოდან წერილობით გამოითხოვოს გამოთხოვის მომენტისთვის მოპოვებული მასალის ელექტრონული ეგზემპლარი.

6. ცალკეული პრობლემატური ასპექტები ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებასთან მიმართებით

6.1. სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი და მასთან დაკავშირებული ზოგიერთი პრობლემური საკითხი

საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში საუბარია იმაზე, რომ ინტერნეტთან მიმართებით სტაციონარული ტექნიკური შესაძლებლობით კომუნიკაციის რეალურ დროში მოპოვება არ ხდება, ვინაიდან ამისათვის აუცილებელია მძირადღირებული სისტემა და ამასთან, ნაკლებად ეფექტურია[1065]. სისტემის არაეფექტიანობა განპირობებულია ინტერნეტსივრცეში ინფორმაციის დაშიფრული სახით გადაცემის გარემოებით.[1066] ამავდროულად, როგორც უკვე აღინიშნა, საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან იკვეთება, რომ ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნით „მიმართავენ ე.წ. „დავირუსების ტექნიკას“. სამართლებრივ ენაზე, მოქმედი კანონმდებლობის მიხედვით, „დავირუსების ტექნიკა“, სავარაუდოდ, უნდა მოვიაზროთ კომუნიკაციის რეალურ დროში მოპოვების „არასტაციონალური ტექნიკური შესაძლებლობის“ ქვეშ, ვინაიდან „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-2 მუხლის „ზ“ ქვეპუნქტის თანახმად, არასტაციონალური ტექნიკური შესაძლებლობა განმარტებულია სწორედ, როგორც „ელექტრონული საკომუნიკაციო ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერა კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურე ინფრასტრუქტურაზე მიერთების გარეშე, სპეციალური ტექნიკური ან/და პროგრამული საშუალებების გამოყენებით.“ რაც შეეხება ნახევრად სტაციონალურ

[1065] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II-83.

[1066] საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე, 131.

ტექნიკურ შესაძლებლობას, აღნიშნული საშუალების ეფექტიანობასა და პრაქტიკაში გამოყენებასთან დაკავშირებით ინფორმაცია ხელმისაწვდომი არ არის.[1067]

ნიშანდობლივია, რომ საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან არ ჩანს, თუ რა იგულისხმება „დავირუსების ტექნიკის“ ქვეშ, გადაწყვეტილებაში არ არის განვითარებული მსჯელობა იმასთან დაკავშირებით, თუ რა ტექნიკურ შესაძლებლობაზე არის ამ შემთხვევაში საუბარი.[1068] როგორც ზემოთ აღინიშნა, საერთაშორისო დონეზე არსებულ დოკუმენტებში, უფლებადამცველი ორგანიზაციების ანგარიშებსა თუ უცხოურ სამეცნიერო ლიტერატურაში აქტიურად განიხილება და მნიშვნელოვანი ყურადღების ქვეშაა მოქცეული კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება (რომელიც მოიცავს, მათ შორის, „დავირუსებას“[1069]) და მასთან დაკავშირებული ტექნიკური შესაძლებლობები, რასაც განაპირობებს, ზოგადი თვალსაზრისით, ამ მეთოდის უაღრესად ინტენსიური ხასიათი და ინფორმაციის ფართო რესურსზე წვდომის შეუზღუდავი პოტენციალი. როგორც ცნობილია, კომპიუტერულ სისტემაში ფარულად შეღწევის შემდგომ შესაძლებელია სხვადასხვა ტიპის ინფორმაციის მოპოვება, ამრიგად, გამოყოფენ ამ მეთოდის სხვადასხვა ფუნქციურ შესაძლებლობებს.[1070] აღნიშნულის გათვალისწინებით, გაუგებარია, თუ რა შინაარსის ღონისძიებას მოიაზრებს გადაწყვეტილებაში არსებული ჩანაწერი „ე.წ. დავირუსების ტექნიკასთან“ დაკავშირებით.[1071]

ზოგადი თვალსაზრისით, კომპიუტერულ სისტემაში ფარული შეღწევის მეთოდთან მიმართებით უნდა აღინიშნოს, რომ ინტერნეტსივრცეში ინფორმაციის დაშიფრულ ფორმატში მიმოცვლის პირობებში ეს ღონისძიება შესაძლოა ერთ-ერთი

[1067] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 128.

[1068] იქვე.

[1069] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07, 5.

[1070] *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 58-59, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> [17.06.2020]; იხ. ასევე *Sagers G.,* The Role of Security in Wireless Privacy, წიგნში: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, *Lind N.S., Rankin E. (eds.),* Vol.2, California, 2015, 508; Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf> [17.06.2020].

[1071] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 129.

ყველაზე ეფექტიანი და ზოგიერთ შემთხვევაში უალტერნატივო საშუალებაც კი იყოს დანაშაულის გამოძიების მიზნებისათვის, მეორე მხრივ, გასათვალისწინებელია მისი უაღრესად ინტენსიური ხასიათი. ზოგიერთი ევროპული სახელმწიფო პირდაპირ არეგულირებს ამ მეთოდის გამოყენების შესაძლებლობას კანონმდებლობაში, თუმცა, როგორც წესი, ასეთ შემთხვევაში გაცილებით მკაცრი მიდგომა და უფლების დაცვის მნიშვნელოვანი გარანტიებია გათვალისწინებული.[1072] კომპიუტერულ სისტემაში ფარულ შეღწევასთან დაკავშირებით კრიტიკის ერთ-ერთ მთავარ ობიექტს სწორედ სპეციალური საკანონმდებლო რეგულაციების არარსებობის პირობებში მისი გამოყენება წარმოადგენს.[1073] ამ ღონისძიების განხორციელება დასაშვები შეიძლება იყოს მხოლოდ მკაცრად აუცილებელ შემთხვევებში, „კონკრეტული სამართლებრივი რეგლამენტაციისა“ და ადეკვატური გარანტიების პირობებში.[1074] „კონკრეტული ნორმატიული მოწესრიგების მოთხოვნა“ ასევე გულისხმობს, რომ ეს მეთოდი დარეგულირდეს დებულებებით, რომლებიც „მორგებული იქნება მისთვის დამახასიათებელ სპეციფიკას.”[1075] ნორმები, რომლებიც განკუთვნილია ფარული მეთვალყურეობის ტრადიციული ფორმებისთვის, მაგალითად, სატელეფონო კომუნიკაციის ფარული მიყურადებისთვის, არ არის საკმარისი ამ ღონისძიებასთან მიმართებით ადეკვატური გარანტიების უზრუნველსაყოფად[1076]. ანალოგიურად, კომპიუტერულ სისტემაში ფარული შეღწევის მეთოდის მარეგულირებელი კანონმდებლობა, რომელიც იმეორებს ფარული მეთვალყურეობის სხვა

[1072] *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51-54, 58-61, 79-80, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> [17.06.2020]; *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 92, 94-95, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020]. იხ. ასევე BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07.

[1073] *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 67, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> [17.06.2020].

[1074] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 18, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>[17.06.2020].

[1075] იქვე.

[1076] იქვე.

ღონისძიებების მარეგულირებელ წესებს, მოკლებულია დაცვის სათანადო მექანიზმებს.[1077]

როგორც უკვე აღინიშნა, „კანონის განჭვრეტადობის“ კონტექსტში აუცილებელია ფარული მეთვალყურეობის ღონისძიებები დარეგულირდეს ნათელი, მკაფიო სამართლებრივი დებულებებით. მკაფიო და დეტალური ნორმები აუცილებელია ფარული საგამოძიებო მოქმედებების კონტექსტში კანონიერებისა და თანაზომიერების უზრუნველსაყოფად.[1078] ამ საგამოძიებო მოქმედებების ფარული ხასიათიდან და უფლებაში ჩარევის ინტენსივობიდან გამომდინარე, კანონის განსაზღვრულობა ამ შემთხვევაში განსაკუთრებით მნიშვნელოვანია.

აღნიშნულ საკითხთან დაკავშირებით ხაზი უნდა გაესვას იმ გარემოებას, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტი, რომელიც არეგულირებს ინტერნეტთან მიმართებით ინფორმაციის მოპოვების საგამოძიებო მოქმედებას, იმდენად ზოგადი სახით არის ჩამოყალიბებული, რომ პრაქტიკულად მოიაზრებს ინფორმაციის მოპოვებას ნებისმიერი საშუალების გამოყენებით[1079]. აღნიშნული ნორმა ჯერ კიდევ „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონში იყო განსაზღვრული ფარული საგამოძიებო მოქმედების სახით სსსკ-ში გათვალისწინებამდე და 2014 წელს განხორციელებული ცვლილებების შედეგად უცვლელი სახით იქნა გადმოტანილი სსსკ-ში[1080]. თანამედროვე ტექნიკური პროგრესის პირობებში განსაკუთრებით მნიშვნელოვანია კანონმდებლობამ ფეხი აუწყოს ინფორმაციული ტექნოლოგიების მოდერნიზების ტემპს[1081]. ინფორმაციულ რესურსზე წვდომის დღეს არსებული მრავალმხრივი და ფუნქციურად განსხვავებული შესაძლებლობების ფონზე აშკარაა, რომ აღნიშნული ნორმა ვეღარ პასუხობს სამართლებრივი სიცხადის მოთხოვნას.[1082] საკონსტიტუციო სასამართლო 2016 წლის 14 აპრილის გადაწყვეტილებაში მიუთითებს, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიება მოიაზრებს

[1077] იქვე.

[1078] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 14-15 (ბმული იხ. მე-80 გვერდზე).

[1079] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 130.

[1080] იქვე.

[1081] იქვე.

[1082] იქვე.

„სახელმწიფოს მიერ ნებისმიერი ინფორმაციის მოხსნას და ფიქსაციას ყველა კავშირგაბმულობის საშუალებებიდან, კომპიუტერული ქსელებიდან, კომპიუტერული სისტემიდან, რაც ფაქტობრივად გულისხმობს როგორც ინტერნეტურთიერთობის მონიტორინგს, ისე კომპიუტერულ სისტემებში არსებულ, შექმნილ/შენახულ ინფორმაციაზე ხელმისაწვდომობის უზრუნველყოფას.“[1083] სასამართლოს მიერ გამოყოფილი ეს ორი შესაძლებლობა თავისი შინაარსით აბსოლუტურად განსხვავებულ ღონისძიებებს წარმოადგენს.[1084]

საერთაშორისო დონეზე არსებული სხვადასხვა წყაროებისა თუ ევროპული ქვეყნების გამოცდილების გათვალისწინებით, ინტერნეტკომუნიკაციის მოპოვების ღონისძიების მკაფიოდ რეგლამენტაციის საკითხის მნიშვნელობა ასევე ხაზგასმულია „დავირუსების“ ღონისძიებასთან მიმართებითაც[1085], კერძოდ, იმ შემთხვევაში, როდესაც დღის წესრიგში დგას კომპიუტერულ სისტემაში ფარულად შეღწევის ღონისძიების განსხვავებული ფუნქციური შესაძლებლობების გამოყენების საკითხი, რეკომენდებულია, რომ ტექნიკური თვალსაზრისით ძირითადი შესაძლებლობები საკანონმდებლო დონეზე გაიმიჯნოს და მათი ჩატარება ცალ-ცალკე ნებართვის პროცედურას დაექვემდებაროს,[1086] რაც განპირობებულია იმით, რომ პირადი ცხოვრების უფლებაზე გავლენა და ჩარევის ხარისხი განსხვავდება „კომპიუტერულ სისტემაში ფარული შეღწევის“ ღონისძიების სხვადასხვა ტიპების შემთხვევაში, რაც მოითხოვს „თანაზომიერების“ პრინციპთან შესაბამისობის განსხვავებულ შეფასებას.[1087] აღნიშნული ასევე აუცილებელია ამ ღონისძიების მრავალმხრივი ტექნიკური პოტენციალის გადამეტებულად ან თვითნებურად გამოყენების

[1083] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-38.

[1084] იქვე.

[1085] *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51, 89, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [17.06.2020].

[1086] იქვე.

[1087] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020]. დოკუმენტში საუბარია კომპიუტერულ სისტემაში შენახული ინფორმაციის მოპოვებისა და მიმდინარე რეჟიმში თვალთვალის შესაძლებლობების დამოუკიდებელი ნებართვის პროცედურის გზით დიფერენცირებაზე.

პრევენციის მიზნებისათვის.[1088] კომპიუტერული სისტემიდან ინფორმაციის მოპოვების ღონისძიებების ამგვარ საკანონმდებლო დიფერენციაციას ითვალისწინებს, მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსი, რომელშიც დამოუკიდებელი ღონისძიებების სახით არის ჩამოყალიბებული ე.წ. „ონლაინ ჩხრეკა“ და „ტელეკომუნიკაციის მონიტორინგი“ (ე.წ. Source-TKÜ). „ონლაინ ჩხრეკა“ გულისხმობს ღონისძიების ადრესატის ინფორმირების გარეშე ტექნიკური საშუალებებით საინფორმაციო-ტექნოლოგიურ სისტემაში შეღწევას და ამ სისტემიდან ინფორმაციის მოპოვებას (StPO ((Strafprozessordnung), §100b), ხოლო ,,ტელეკომუნიკაციების მონიტორინგის“ ქვეშ მოიაზრება ღონისძიების ადრესატის ინფორმირების გარეშე ტექნიკური საშუალებებით საინფორმაციო-ტექნოლოგიურ სისტემაში შეღწევის გზით ტელეკომუნიკაციის მონიტორინგი და ჩაწერა (StPO, §100a Abs.1 S.3).[1089] ეს ღონისძიება შესაძლებელს ხდის კომუნიკაციის წაკითხვას მის დაშიფვრამდე ან განშიფვრის შემდგომ.[1090] „ტელეკომუნიკაციის მონიტორინგის“ ღონისძიების ფარგლების დაკონკრეტებისა და „ონლაინ ჩხრეკის“ საგამოძიებო მოქმედებისგან გამიჯვნის თვალსაზრისით, მნიშვნელოვანია 100a პარაგრაფის მე-5 აბზაცის მოთხოვნა, რომლის მიხედვითაც, „ტელეკომუნიკაციის მონიტორინგის“ ღონისძიების გამოყენების შემთხვევაში, ტექნიკურ დონეზე უნდა იქნეს

[1088] *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 12, 58, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf> [17.06.2020].

[1089] კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიების ძირითადი ფუნქციონალური შესაძლებლობების დიფერენცირების მოთხოვნა გაჟღერებულია ასევე იტალიის საკასაციო სასამართლოს 2016 წლის 1 ივლისის გადაწყვეტილებაში. იტალიის უზენაესმა სასამართლომ ერთმანეთისგან განასხვავა, კომპიუტერულ სისტემაში ფარული შეღწევის ისეთი ფუნქციონალური შესაძლებლობები, როგორიცაა „კომუნიკაციის მონიტორინგი“ (online surveillance) და ონლაინ ჩხრეკა (online search). აღნიშნულ საკითხთან დაკავშირებით იხ. *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 85, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [17.06.2020].

[1090] <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html> [25.06.2020].

უზრუნველყოფილი, რომ მხოლოდ „მიმდინარე ტელეკომუნიკაცია“ იქნეს მოპოვებული.[1091]

მოცემული საგამოძიებო მოქმედებების საკანონმდებლო მოთხოვნათა შესაბამისად წარმართვის უზრუნველსაყოფად, მათ განსახორციელებლად განკუთვნილი კომპიუტერული პროგრამის გამოყენება შესაძლებელია მხოლოდ შესაბამისი ტესტირების გავლისა და სპეციალურად დადგენილ მინიმალურ სტანდარტებთან შესაბამისობის დადგენის შემდეგ.[1092] ეს მექანიზმი მოცემული საგამოძიებო მოქმედებებისთვის დამახასიათებელი ფართო ტექნიკური

[1091] StPO. §100a Abs. 5, 07/04/1987. აღსანიშნავია, რომ გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ 2008 წლის 27 თებერვლის გადაწყვეტილებით დაადგინა, რომ კომუნიკაციის კონფიდენციალურობის უფლება (გერმანიის ძირითადი კანონის 10.1 პარაგრაფი) არ ვრცელდება ისეთ შემთხვევაზე, როდესაც საინფორმაციო ტექნოლოგიურ სისტემაში შეღწევის გზით შესაბამისი სახელმწიფო ორგანო ახორციელებს ამ სისტემის გამოყენების კონტროლს ან ახორციელებს ამ სისტემის მეხსიერებაში შენახული მონაცემების ჩხრეკას. ასეთი ქმედებებისგან ინდივიდის დაცვის მიზნით სასამართლომ ჩამოაყალიბა „საინფორმაციო-ტექნოლოგიური სისტემების კონფიდენციალურობისა და მთლიანობის უფლება“, რომელიც პიროვნულობის ზოგადი უფლების განუყოფელი ნაწილია. ახალი კონსტიტუციური უფლება იცავს პირს საინფორმაციო ტექნოლოგიურ სისტემაში სახელმწიფოს მხრიდან ფარული შეღწევისგან. ეს უფლება ვრცელდება როგორც საინფორმაციო-ტექნოლოგიური სისტემის მუშა მეხსიერებაში შენახულ, ასევე კომპიუტერული სისტემის ინფორმაციის შემნახველ საშუალებებზე დროებით ან მუდმივად შენახულ მონაცემებზე. იხ. BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07; იხ. ასევე *Abel W., Schafer B.,* The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822, SCRIPTed, Vol. 6, No 1, 2009, 118-121. ამავდროულად, საინფორმაციო-ტექნოლოგიურ სისტემაში ფარული შეღწევა, რომლის მიზანსაც წარმოადგენს მხოლოდ კომუნიკაციებზე [იგულისხმება მიმდინარე კომუნიკაციები] წვდომა, თუკი ეს ტექნიკურად და სამართლებრივად შეზღუდულია ამ მიზნით, არ ექცევა ამ უფლების დაცვის ქვეშ, არამედ მასზე ვრცელდება გერმანიის ძირითადი კანონის მე-10 მუხლით განმტკიცებული კომუნიკაციის კონფიდენციალურობის უფლება. იხ. *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 77, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [17.06.2020].

ამასთანავე, 2008 წლის 27 თებერვლის გადაწყვეტილებით გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ საინფორმაციო-ტექნოლოგიური სისტემების კონფიდენციალურობისა და მთლიანობის უფლებაში ჩარევა დასაშვებად მიიჩნია მხოლოდ მკაცრი გამონაკლისების არსებობისას, მათ შორის - თუკი ფაქტობრივი გარემოებები მიუთითებენ, რომ განსაკუთრებით მნიშვნელოვან სამართლებრივ სიკეთეს ემუქრება კონკრეტული საფრთხე. ასეთ სამართლებრივ სიკეთედ მიჩნეულ იქნა ჯანმრთელობა, სიცოცხლე, თავისუფლება ან ისეთი საჯარო ინტერესები, რომელთა მიმართ საფრთხე გავლენას ახდენს სახელმწიფოს ან კაცობრიობის არსებობის საფუძვლებზე. აღნიშნულიდან გამომდინარე, გერმანიის სისხლის სამართლის საპროცესო კოდექსის 100b პარაგრაფი, რომლითაც გათვალისწინებულია ონლაინ ჩხრეკის საგამოძიებო მოქმედება, ამ ღონისძიების ჩატარების შესაძლებლობას უშვებს დანაშაულთა კიდევ უფრო შეზღუდული წრის (განსაკუთრებით მძიმე დანაშაულები, რომელთა ჩამონათვალი განსაზღვრულია 100b პარაგრაფის მე-2 აბზაცით) შემთხვევაში, ვიდრე ეს დაშვებულია 100a პარაგრაფით განსაზღვრული ტელეკომუნიკაციის ფარული მიყურადება/ჩაწერის დროს.

[1092]<https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html> [25.06.2020].

შესაძლებლობების გადამეტებულად, უკანონოდ გამოყენების საწინააღმდეგო მნიშვნელოვან გარანტიას წარმოადგენს[1093].

ყოველივე აღნიშნულის გათვალისწინებით, მიზანშეწონილია სამართლებრივად დაკონკრეტდეს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული მეთვალყურეობის ტიპები, რათა ერთმანეთისგან გაიმიჯნოს კომუნიკაციის რეალურ დროში მოპოვებისა და კომპიუტერულ სისტემაში შენახულ ინფორმაციაზე წვდომის უფლებამოსილებები.[1094]

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიების მეტი სამართლებრივი სიცხადით რეგულირების პარალელურად, მნიშვნელოვანია, რომ მოცემული ფარული საგამოძიებო მოქმედების ჩატარების ყოველ კონკრეტულ შემთხვევაში მოსამართლე ინფორმირებული იყოს მოთხოვნილი კონკრეტული ღონისძიების განსახორციელებლად გამოსაყენებელი ტექნიკური საშუალებების შესახებ.[1095] როგორც უკვე აღინიშნა, ფარული მეთვალყურეობის ღონისძიების თანაზომიერების შეფასებისას ერთ-ერთ მნიშვნელოვან საზომს წარმოადგენს გამოყენებული ტექნიკური საშუალებების პოტენციალი უფლებაში ჩარევის ინტენსივობის თვალსაზრისით. ფარული თვალთვალის განსახორციელებლად გამოყენებულ ტექნიკურ საშუალებებს შეუძლიათ გავლენა მოახდინონ მოპოვებული ინფორმაციის მოცულობასა და პირად ცხოვრებაში ჩარევის ხარისხზე[1096]. პროპორციულობა ღონისძიებისა, რომელიც ზღუდავს პირადი ცხოვრების უფლებას და კონკრეტული ტექნიკური საშუალების გამოყენებით ფარული მეთვალყურეობის შესაძლებლობას ითვალისწინებს, დამოკიდებულია იმაზე, თუ რა ცოდნა აქვთ შესაბამის ორგანოებს ღონისძიების მასშტაბსა და გამოსაყენებელ ტექნიკურ შესაძლებლობებზე[1097]. აღნიშნული გულისხმობს, რომ ფარული საგამოძიებო მოქმედების გამოყენებამდე წინასწარ უნდა შეფასდეს კონკრეტული ღონისძიების თანმდევი პირადი ცხოვრების სფეროში ჩარევის

[1093] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 131.
[1094] იქვე.
[1095] იქვე. 132.
[1096] *Milaj., J.,* Invalidation Data Retention Directive – Extending the Proportionality Test, Computer Law & Security Review, 31, 2015, 612.
[1097] *Milaj J.,* Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol.30, No 3, 2016, 115.

ინტენსივობა.[1098] ამ კონტექსტში, მხედველობაშია მისაღები ის გარემოება, რომ სსსკ-ის მიხედვით, არც პროკურორის შუამდგომლობის და არც ფარული საგამოძიებო მოქმედების ჩატარებაზე ნებართვის გაცემის თაობაზე სასამართლოს განჩინების სავალდებულო რეკვიზიტად არ არის განსაზღვრული იმ ტექნიკური საშუალებების შესახებ ინფორმაცია, რომელთა გამოყენებითაც უნდა განხორციელდეს სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კონკრეტული ღონისძიება (სსსკ-ის 143[3] მუხლის მე-10 ნაწილი).[1099] გამოყენებული ტექნიკური საშუალებების თაობაზე ინფორმაციის აღნიშვნა სავალდებულოა მხოლოდ ფარული საგამოძიებო მოქმედების ოქმში, რომელიც ღონისძიების დასრულების შემდეგ დგება (სსსკ-ის 143[6] მუხლის მე-14 ნაწილი). რაც შეეხება სასამართლოს განჩინებას და პროკურორის შუამდგომლობას, სსსკ-ით ამ დოკუმენტების სავალდებულო რეკვიზიტებად განსაზღვრული მონაცემები საკმარისი არ არის იმისთვის, რათა მოსამართლეს შეექმნას მკაფიო წარმოდგენა იმის შესახებ, თუ როგორ უნდა განხორციელდეს კონკრეტული საგამოძიებო მოქმედება პრაქტიკული თვალსაზრისით[1100]. შესაბამისად, რთული წარმოსადგენია სათანადოდ შეფასდეს, რამდენად წარმოადგენს კონკრეტული ფარული საგამოძიებო მოქმედება პირად ცხოვრებაში ჩარევის პროპორციულ, ყველაზე ნაკლებად შემზღუდველ, თანაზომიერ საშუალებას.[1101] გამოსაყენებელი ტექნიკური საშუალებების შესახებ ინფორმაციის სასამართლოს განჩინებაში ასახვა ასევე მნიშვნელოვანია ღონისძიების ფარგლების მკაფიოდ განსაზღვრისა და დაკონკრეტების თვალსაზრისით.

6.2 ზოგიერთი პროცესუალური გარანტია „კომპიუტერულ სისტემაში ფარული შეღწევის“ გზით ინტერნეტკომუნიკაციის მონიტორინგთან დაკავშირებით

ევროპული ქვეყნების გამოცდილებისა და ადამიანის უფლებათა დამცველი ორგანიზაციების რეკომენდაციების გათვალისწინებით, შეიძლება გამოიყოს ცალკეული მინიმალური გარანტიები, რომლებსაც ცენტრალური მნიშვნელობა ენიჭება „კომპიუტერულ სისტემაში ფარული შეღწევის“ გზით

[1098] იქვე.
[1099] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 131.
[1100] იქვე.
[1101] იქვე.

ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების ღონისძიების საკანონმდებლო რეგლამენტაციის კუთხით. ერთ-ერთ არსებით რეკომენდაციას წარმოადგენს კომპიუტერულ სისტემაში ფარული შეღწევის გამოყენება მხოლოდ მძიმე დანაშაულის გამოძიების მიზნებისათვის[1102]. ამ მეთოდისთვის დამახასიათებელი უფლების შეზღუდვის მაღალი ინტენსივობიდან გამომდინარე, ასეთ შემთხვევაში „მძიმე დანაშაულთა“ კატეგორია განსაკუთრებით ვიწროდ უნდა განიმარტოს.[1103]

ასევე მნიშვნელოვანია, რომ შესაბამისმა ორგანოებმა სასამართლოსთვის წარდგენილ შუამდგომლობაში მიუთითონ ინფორმაცია „მოთხოვნილი ღონისძიების განხორციელების მეთოდისა და ფარგლების შესახებ.“[1104] ნიშანდობლივია, რომ „კომპიუტერულ სისტემაში ფარული შეღწევის“ ღონისძიება მოიაზრებს მუდმივად განვითარებად საშუალებებს, რომელთა უმრავლესობა ტექნიკური თვალსაზრისით კომპლექსურობით ხასიათდება[1105]. იმისათვის, რომ სასამართლომ განსაზღვროს მოთხოვნილი საგამოძიებო მოქმედების პროპორციულობა და აუცილებლობა, უნდა ჰქონდეს შესაძლებლობა, შეაფასოს, რამდენად შეესაბამება კონკრეტული ღონისძიების ჩატარების ამოცანას ის საქმიანობა, რასაც ამ ამოცანის შესასრულებლად ტექნიკურ დონეზე განახორციელებს შესაბამისი ორგანო[1106]. ამ თვალსაზრისით ღონისძიებასთან დაკავშირებულ ტექნიკურ დეტალებს გადამწყვეტი მნიშვნელობა ენიჭება თანაზომიერების საკითხის შესაფასებლად.[1107] ბუნებრივია, ასეთი შეფასების გაკეთება სასამართლოს გაუჭირდება ტექნიკურ საკითხებში სპეციალისტის

[1102] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020].

[1103] იქვე.

[1104] იქვე. 26. მაგალითისთვის, ესპანეთის კანონმდებლობით გათვალისწინებული რეგულაცია კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიებასთან (ამ კონკრეტულ შემთხვევაში, ონლაინ ჩხრეკის საგამოძიებო მოქმედებასთან) მიმართებით ითვალისწინებს განჩინებაში ღონისძიების ფარგლების და იმ მეთოდის/ხერხის მითითების მოთხოვნას, რომლითაც უნდა მოხდეს გამოძიებისათვის რელევანტური ინფორმაციის მოპოვება. იხ. *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 95, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020].

[1105] Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 26, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020].

[1106] იქვე.

[1107] იქვე.

მონაწილეობის გარეშე; ამ თვალსაზრისით აღსანიშნავია, რომ საერთაშორისო დონეზე გამოთქმულია მოსაზრება სასამართლოს მიერ ასეთი ღონისძიების ჩატარების ნებართვის პროცედურაში ტექნიკურ საკითხებში სპეციალისტის მონაწილეობის მიზანშეწონილობის თაობაზე[1108]. როგორც ზემოთ აღინიშნა, ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების ღონისძიების ჩატარების საკითხის განხილვისას, მიზანშეწონილია, მოსამართლეს მიეწოდოს ინფორმაცია მოთხოვნილი ღონისძიების განსახორციელებლად გამოსაყენებელი ტექნიკური საშუალებების შესახებ. როგორც ვხედავთ, ასეთი კონკრეტიკა კომპიუტერულ სისტემაში ფარული შეღწევის გზით ინტერნეტკომუნიკაციის მონიტორინგის განსახორციელებლად განსაკუთრებით მნიშვნელოვანია და ეხმიანება საერთაშორისო გამოცდილებას სასამართლოს განჩინების შინაარსთან დაკავშირებით.

საგამოძიებო მოქმედების ფარგლების შეზღუდვის მიზნით მნიშვნელოვანია შესაბამისი კომპიუტერული სისტემის/მისი ნაწილის კონკრეტულად აღწერის მოთხოვნა სასამართლოს განჩინებაში. ასეთი მიდგომა არის გათვალისწინებული მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსში, კერძოდ, „ტელეკომუნიკაციის მონიტორინგის“ (ე.წ. Source-TKÜ) ღონისძიებასთან დაკავშირებულ სასამართლოს განჩინებაში სავალდებულოა იმ საინფორმაციო-ტექნოლოგიური სისტემის მაქსიმალურად შესაძლო სიზუსტით აღწერა, რომელში შეღწევაც უნდა განხორციელდეს.[1109]

მნიშვნელოვან გარანტიად უნდა ჩაითვალოს ასევე ჩატარებული ღონისძიების შესახებ დეტალური ინფორმაციის აღრიცხვა მისი დასრულების შემდეგ. ასეთ მოთხოვნას ითვალისწინებს მაგალითად, გერმანიის სისხლის სამართლის საპროცესო კოდექსის 100a პარაგრაფის მე-6 აბზაცი, კერძოდ, „ტელეკომუნიკაციის მონიტორინგის“ (ე.წ. Source-TKÜ) ღონისძიებასთან მიმართებით წერილობით აღრიცხვას ექვემდებარება შემდეგი მონაცემები: გამოყენებული ტექნიკური საშუალებების შესახებ ინფორმაცია და გამოყენების დრო; შესაბამისი საინფორმაციო-ტექნოლოგიური სისტემის საიდენტიფიკაციო მონაცემები და მასში განხორციელებული ცვლილებები; მონაცემები, რომელიც მოპოვებული ინფორმაციის

[1108] იქვე, 28-29.

[1109] StPO, §100e Abs. 3, S.5, 07/04/1987. იგივე მოთხოვნა არის გათვალისწინებული „ონლაინ ჩხრეკის“ საგამოძიებო მოქმედებასთან დაკავშირებითაც (StPO, §100e Abs. 3, S.6).

განსაზღვრის შესაძლებლობას იძლევა და დანაყოფი, რომელიც ახორციელებს ღონისძიებას. ასევე უნდა აღინიშნოს 100a პარაგრაფის მე-5 აბზაცის მე-2 წინადადებით გათვალისწინებული დათქმა, რომლის თანახმადაც, საინფორმაციო-ტექნოლოგიურ სისტემაში შეიძლება განხორციელდეს მხოლოდ ისეთი ცვლილებები, რომლებიც აუცილებელია ინფორმაციის მოსაპოვებლად.

საბოლოო ჯამში, შეიძლება ითქვას, რომ კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება ექვემდებარება უფრო მკაცრ სტანდარტებს, ვიდრე ტრადიციული კომუნიკაციის ფარული მიყურადების ღონისძიებები; ძირითად გარანტიათა შორის შეიძლება გამოიყოს ამ ღონისძიების განხორციელების შესაძლებლობა მხოლოდ „მძიმე დანაშაულთა“ წინააღმდეგ, ღონისძიების ჩატარების მეთოდისა და ფარგლების შესახებ სასამართლოს ინფორმირება, რაც შეიძლება განხორციელდეს, მაგალითად, იმ ტექნიკური საშუალებების აღნიშვნით, რომლითაც უნდა ჩატარდეს ეს საგამოძიებო მოქმედება, ნებართვის გაცემის პროცედურის ფარგლებში ტექნიკურ საკითხებში სპეციალისტის მონაწილეობა, ასევე ღონისძიების ფარგლების შეზღუდვა შესაბამისი კომპიუტერული სისტემის წინასწარ მაქსიმალურად დაზუსტებით, ისევე როგორც ღონისძიების დასრულების შემდეგ მასთან დაკავშირებული ინფორმაციის მაქსიმალურად დეტალურად დაფიქსირება, რაც მოიცავს, მათ შორის, კომპიუტერულ სისტემაში განხორციელებული ცვლილებებისა და მოპოვებული ინფორმაციის შესახებ მონაცემების აღრიცხვასაც.

6.3 შეჯამება

ამდენად, როგორც გამოიკვეთა, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტის ზოგადი ფორმულირება იწვევს ამ ნორმის ქვეშ ინტერნეტკომუნიკაციის რეალურ დროში მოპოვებისა და კომპიუტერულ სისტემაში შენახულ ინფორმაციაზე წვდომის შინაარსობრივად განსხვავებული უფლებამოსილებების თავმოყრას, რაც სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების განხორციელებისას შესაბამის ორგანოს ფაქტობრივად შეუზღუდავი შესაძლებლობებით აღჭურავს ინფორმაციულ რესურსზე წვდომის თვალსაზრისით. აქედან გამომდინარე, მიზანშეწონილია ეს უფლებამოსილებები ერთმანეთისგან გაიმიჯნოს და სხვადასხვა ფარული საგამოძიებო მოქმედებების სახით ჩამოყალიბდეს. ეს საკითხი აქტუალურია ასევე

„დავირუსების“ ღონისძიებასთან მიმართებითაც, კერძოდ, როგორც საერთაშორისო გამოცდილების განხილვის შედეგად გამოიკვეთა, იმ შემთხვევაში, როდესაც საჭიროა პრაქტიკაში გამოყენებულ იქნეს კომპიუტერულ სისტემაში ფარულად შეღწევის ღონისძიების განსხვავებული ფუნქციური შესაძლებლობები, რეკომენდებულია, ტექნიკური თვალსაზრისით ძირითადი შესაძლებლობები საკანონმდებლო დონეზე გაიმიჯნოს და მათი ჩატარება ცალ-ცალკე ნებართვის პროცედურას დაექვემდებაროს.

ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების საკითხთან დაკავშირებით საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებიდან იკვეთება, რომ ამ ღონისძიების განსახორციელებლად გამოიყენება „ე.წ. დავირუსების ტექნიკა.“ თუმცა ამ საკითხთან დაკავშირებით მეტი ინფორმაცია ხელმისაწვდომი არ არის და გაუგებარია, თუ რას გულისხმობს ფრაზა „დავირუსების ტექნიკა“.

ნიშანდობლივია, რომ ზოგადად, კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება (მათ შორის, „დავირუსების“ გზით) ერთ-ერთ პრობლემატურ საკითხად მიიჩნევა ინტერნეტ სივრცეში ინფორმაციის მოპოვების საკითხთან მიმართებით. ამ ღონისძიების განსაკუთრებული ინტენსივობიდან გამომდინარე, რეკომენდებულია მისი გამოყენება მხოლოდ კონკრეტული, სპეციალურად მასზე მორგებული სამართლებრივი რეგულაციების პირობებში. ამდენად, თუკი საქართველოს სამართალდამცავი ორგანოების პრაქტიკაში ასეთი ტიპის ღონისძიების გამოყენება რელევანტურია, აუცილებელია სსსკ-ში, ფარული საგამოძიებო მოქმედებების თავში (თავი XVI[1]) მისი სპეციალურად დარეგულირება და შესაბამისი გარანტიების გათვალისწინებაც.[1110] კვლევაში, საერთაშორისო გამოცდილების მაგალითზე, წარმოდგენილ იქნა ის ძირითადი ასპექტები, რომლებიც ამ შემთხვევაში გათვალისწინებულია საკანონმდებლო დონეზე.

[1110] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 133.

VII. დასკვნა

ამდენად, კვლევაში განხილულ იქნა ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვებასა და სისხლის სამართლის პროცესში გამოყენებასთან დაკავშირებული პრობლემატიკა.

თანამედროვე ტექნოლოგიების პროგრესისა და ამის კვალდაკვალ ფარული მეთვალყურეობის სფეროში სახელმწიფოს შესაძლებლობების განვითარების მასშტაბებიდან გამომდინარე, პირადი ცხოვრების დაცვის საკითხი ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების მიმართულებით აქტუალურია არამარტო საქართველოს, არამედ გლობალურ დონეზე. იმ საფრთხეების გათვალისწინებით, რაც თანამედროვე ტექნოლოგიების სისხლის სამართლის პროცესში გამოყენებას უკავშირდება, აუცილებელია ამ სფეროს ზედმიწევნით დარეგულირება კონსტიტუციური და საერთაშორისო სტანდარტების დაცვით.

ელექტრონული კომუნიკაციის საშუალებებით გადაცემული ინფორმაციის მტკიცებულებითი მნიშვნელობა ფასდაუდებელია; შინაარსობრივი მონაცემების გარდა, თანამედროვე ტექნოლოგიების ეპოქაში უკვე კომუნიკაციის მაიდენტიფიცირებელი მონაცემების სენსიტიურობა და ინფორმაციული ღირებულება იმდენად არის გაზრდილი, რომ მონაცემთა ამ კატეგორიებს შორის სენსიტიურობის თვალსაზრისით განსხვავება უმნიშვნელო გახდა; უფრო მეტიც, კომუნიკაციის მაიდენტიცირებელი მონაცემები, ერთად აღებული, ინდივიდის პიროვნული პორტრეტის, ინტიმური პროფილის განსაზღვრის შესაძლებლობას იძლევა, რაც ბუნებრივია, ისეთივე აქტუალურობით წამოჭრის ამ მონაცემთა შეგროვება/შენახვასთან მიმართებით პირად ცხოვრებასთან დაკავშირებულ ასპექტებს, როგორც შინაარსობრივი მონაცემების შემთხვევაში.

საერთაშორისო გამოცდილების განხილვის გზით გამოიკვეთა, რომ სამართალდამცავ ორგანოებს პირადი ხასიათის ინფორმაციაზე წვდომის მრავალმხრივ შესაძლებლობებზე მიუწვდებათ ხელი, როგორიცაა, მაგალითად, სატელეფონო კომუნიკაციის ფარული მიყურადება და ჩაწერა, პირის ადგილმდებარეობის დადგენა მობილური ტელეფონის საშუალებით, კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება, ელექტრონული კომუნიკაციის კომპანიებისგან ინფორმაციის გამოთხოვა და სხვა. ინფორმაციების მოპოვების

ტექნიკური ასპექტები მჭიდრო კავშირშია და ხშირად განსაზღვრავს კიდევაც მასზე წვდომის სამართლებრივ შესაძლებლობებს; მაგალითად, ინტერნეტსივრცეში ინფორმაციის დაშიფრული სახით არსებობა განაპირობებს იმას, რომ ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნით სხვადასხვა ქვეყნის პრაქტიკაში გამოიყენება კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიება.

აღსანიშნავია, რომ საქართველოს კონსტიტუციაში პირადი ცხოვრებისა და კომუნიკაციის ხელშეუხებლობის უფლებები საგანგებო დაცვით სარგებლობს; ამ უფლებებში ჩარევა მკაცრი წინაპირობების არსებობისას არის შესაძლებელი, რომლებსაც ასევე კონსტიტუცია ადგენს. კონსტიტუციური სტანდარტი მოითხოვს ამ უფლებების შემზღუდველი საპროცესო ღონისძიებების რეგულირებას განჭვრეტადი, ნათელი და მკაფიო სამართლებრივი დებულებებით, პროპორციულობისა და აუცილებლობის მკაცრი დაცვით.

ნიშანდობლივია, რომ კერძო კომუნიკაციის ხელშეუხებლობის შემზღუდველი ღონისძიებების „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონიდან სსსკ-ში ფარული საგამოძიებო მოქმედებების სახით გადატანა სულ რამდენიმე წლის წინ განხორციელდა, შესაბამისად, აღნიშნულ კანონმდებლობას საქართველოში განვითარების საკმაოდ მცირე სამართლებრივი ტრადიცია აქვს. გასათვალისწინებელია ისიც, რომ 2014 წლის 1 აგვისტოდან მოყოლებული მითითებულმა კანონმდებლობამ უკვე არაერთი ცვლილება განიცადა. ეს ყველაფერი ერთი მხრივ, ხაზს უსვამს ამ ღონისძიებებთან დაკავშირებულ პრობლემატიკას, მეორე მხრივ, ამ კუთხით საერთაშორისო გამოცდილების შესწავლის მნიშვნელობას, რაც ისევ და ისევ ქართული კანონმდებლობის დახვეწის მიზნით უნდა იქნეს გამოყენებული.

კვლევაში განხილული საერთაშორისო სტანდარტების (მაგ. ადამიანის უფლებათა ევროპული სასამართლოს, ევროსაბჭოს, ევროკავშირის, გაეროს დონეზე შემუშავებული მოთხოვნების) განხილვის გზით, წარმოჩინდა ის ძირითადი გარანტიები და მოთხოვნები, რომლებიც ჩამოყალიბებულია საერთაშორისო დონეზე, ხოლო ქართული კანონმდებლობის განხილვის დროს შეფასდა ქართული რეგულაციების მიმართება ამ მოთხოვნებთან.

განხილული საერთაშორისო სტანდარტებიდან გამოიკვეთა, რომ კერძო კომუნიკაციის შემზღუდველი საგამოძიებო მოქმედებების ფარული ხასიათიდან

მომდინარე საფრთხეების გათვალისწინებით, აუცილებელია კანონმდებლობა მკაფიო, ნათელი, განჭვრეტადი სამართლებრივი დებულებებითა და საჯაროდ ხელმისაწვდომი ფორმით არეგულირებდეს ამ ღონისძიებებს, პასუხობდეს თანაზომიერების ტესტის ყველა ელემენტს და ითვალისწინებდეს უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგო ადეკვატურ მექანიზმებს. თანაზომიერების პრინციპიდან გამომდინარეობს სხვადასხვა პროცედურული გარანტიების გათვალისწინების აუცილებლობა ფარულ საგამოძიებო მოქმედებებთან მიმართებით, როგორიცაა მაგალითად, ღონისძიების ჩატარებაზე ნებართვის გაცემა დამოუკიდებელი ორგანოს მიერ, საზედამხედველო მექანიზმები, სავარაუდო ღონისძიების ხასიათი, ხანგრძლივობა და ფარგლები, მისი ჩატარების საფუძვლები, მოთხოვნები ფარული მეთვალყურეობის ღონისძიების ჩატარების თაობაზე შუამდგომლობის და სასამართლოს განჩინების მიმართ, მტკიცებულებითი სტანდარტი, შეტყობინების ვალდებულება, გასაჩივრების საშუალებები, გამოყენებული ტექნიკური საშუალებების პოტენციალი უფლებაში ჩარევის კუთხით და სხვ.

ნაშრომში საერთაშორისო დონეზე შემუშავებული კონკრეტული გარანტიების განხილვისა და ქართული კანონმდებლობის აღნიშნულ მოთხოვნებთან შესაბამისობის ჭრილში გაანალიზების გზით გამოიკვეთა შემდეგი პრობლემატური ასპექტები:

2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით ფარული საგამოძიებო მოქმედებების საფუძვლად დადგინდა დანაშაულთა ამომწურავი ჩამონათვალი. ამ დანაშაულთა განსაზღვრის მიზნით კრიტერიუმად გამოყენებულ იქნა ევროპის საბჭოს „დაპატიმრების ორდერის“ ჩარჩო გადაწყვეტილებით დადგენილი დანაშაულების შემადგენლობა; თუმცა აღნიშნულის შემდეგ შეინიშნება სსსკ-ის 143[3] მე-2 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ ჩამონათვალში დანაშაულების დამატების ტენდენცია, რაც სხვადასხვა არგუმენტაციით იყო ახსნილი. ამის ფონზე, თანდათანობით გაურკვეველი ხდება კრიტერიუმი, რომელიც ამ სიის განსაზღვრას უნდა დაედოს საფუძვლად; აღნიშნულ პირობებში, კანონმდებლის მხრიდან განსაკუთრებულად ფრთხილ მიდგომას საჭიროებს ამ დანაშაულებისთვის ახალი შემადგენლობის დამატება, რათა აღნიშნულმა არ გამოიწვიოს ფარული მეთვალყურეობის უფლებამოსილების სამართალდამცავი ორგანოების ხელთ

არსებულ სტანდარტულ საშუალებად გადაქცევა; ხოლო მეორე მხრივ, თვალსაჩინო უნდა იყოს კრიტერიუმი/კრიტერიუმები, რომლებიც დანაშაულთა ახალი შემადგენლობის დამატების საფუძვლად შეიძლება იქნეს გამოყენებული.

გარდა აღნიშნულისა, საერთაშორისო გამოცდილებაზე დაყრდნობით და ასევე იმის გათვალისწინებით, რომ ქართული კანონმდებლობით ფარული საგამოძიებო მოქმედების ჩატარება ნებადართულია ისეთ ნაკლებად მძიმე დანაშაულთა შემთხვევაშიც, რომლებიც სასჯელის სახით თავისუფლების აღკვეთას საერთოდ არ ითვალისწინებს ან ითვალისწინებს მცირე ვადით, მიზანშეწონილია ფარული საგამოძიებო მოქმედების ჩატარების საკითხის გადაწყვეტის მიზნებისათვის სსსკ პირდაპირ განსაზღვრავდეს დანაშაულის სიმძიმის შეფასების მოთხოვნას კონკრეტულ სიტუაციაში საქმის ინდივიდუალური გარემოებებიდან გამომდინარე.

პროკურორის შუამდგომლობასა და სასამართლოს განჩინებაში შესაბამისი რეკვიზიტების დაკონკრეტების მოთხოვნა ერთ-ერთ მნიშვნელოვან გარანტიას წარმოადგენს ღონისძიების ფარგლების შეზღუდვის კუთხით, რამაც თავის მხრივ, უნდა უზრუნველყოს მხოლოდ იმ მოცულობის ინფორმაციის შეგროვება, რაც აუცილებელია კონკრეტულ ვითარებაში ლეგიტიმური მიზნის მისაღწევად; ასეთი კონკრეტიკა განსაკუთრებით მნიშვნელოვანი ინტერნეტკომუნიკაციის მოპოვების დროს შეიძლება იყოს, იქედან გამომდინარე, რომ ინტერნეტსივრცეში განუზომლად დიდი რაოდენობის ინფორმაცია გროვდება. ამდენად, აუცილებელია ღონისძიების ფარგლების თავიდანვე შეძლებისდაგვარად ვიწროდ განსაზღვრა, მათ შორის, ობიექტის ტექნიკური იდენტიფიკატორის/იდენტიფიკატორების მაქსიმალურად დაკონკრეტება; ინტერნეტკომუნიკაციებთან მიმართებით ასევე გამოითქვა შეხედულება სასამართლოს განჩინებაში გამოსაყენებელი ტექნიკური საშუალებების წინასწარ განსაზღვრის შესახებ. ამავდროულად, კომპიუტერულ სისტემაში ფარული შეღწევის კუთხით ასევე მნიშვნელოვანია შესაბამისი კომპიუტერული სისტემის მაქსიმალურად შესაძლო სიზუსტით განსაზღვრა სასამართლოს განჩინებაში.

გამოითქვა აგრეთვე მოსაზრება ფარული საგამოძიებო მოქმედებების ვადის ნათლად დარეგულირების აუცილებლობის თაობაზე, რადგან დღეს არსებული რეგულაცია არ იძლევა ერთმნიშვნელოვან პასუხს ღონისძიების საერთო ვადასთან დაკავშირებით; მიუხედავად იმისა, რომ პრაქტიკაში ეს საკითხი ადამიანის უფლებების დაცვის სასარგებლოდ არის ინტერპრეტირებული, ამ საკითხის

მნიშვნელობიდან გამომდინარე, მისი განჭვრეტადი სახით რეგლამენტაცია აუცილებელია. ასევე მიზანშეწონილია, სსსკ-ის 143[3] მუხლის მე-12 ნაწილი, რომელიც განსაზღვრავს ღონისძიების ვადის გაგრძელების პროცედურას გენერალური პროკურორის მიმართვის საფუძველზე, პირდაპირ აკონკრეტებდეს, რომ ამ შემთხვევაშიც იგივე გარემოებები უნდა დასაბუთდეს შუამდგომლობით, რაც პროკურორის მიმართვის საფუძველზე ვადის გაგრძელების საკითხის გადაწყვეტისას.

როგორც კვლევაში გამოიკვეთა, ევროპული სასამართლოს ჩამოყალიბებული პრაქტიკიდან გამომდინარე, ეროვნული კანონმდებლობა დეტალურად უნდა არეგულირებდეს ფარული მეთვალყურეობის ღონისძიების შედეგად მოპოვებული ინფორმაციის შემოწმების, გამოყენების, შენახვის, სხვა პირებისთვის გადაცემისა და განადგურების წესებს. კვლევაში მნიშვნელოვანი ყურადღება დაეთმო ამ მოთხოვნებთან მიმართებით ქართული კანონმდებლობის გაანალიზებას. ამ მიმართულებით ერთ-ერთ თემატიკას მინიმუმამდე დაყვანის მოთხოვნის პრაქტიკაში იმპლემენტაციასთან დაკავშირებული ასპექტები წარმოადგენდა. როგორც ექსპერტები აღნიშნავენ ევროპის საბჭოს ადამიანის უფლებათა დაცვის და კანონის უზენაესობის გენერალური დირექტორატის დასკვნაში, „ქართულ კანონმდებლობაში ჯერ კიდევ ბევრია გასაკეთებელი მონაცემთა მოპოვებიდან მის განადგურებამდე პროცედურის მოწესრიგების მიზნით.“ ამ კუთხით ერთ-ერთ საკითხს სწორედ მონაცემთა გადარჩევა/დახარისხება წარმოადგენს. მიგვაჩნია, რომ ფარული საგამოძიებო მოქმედებების თავს აკლია სამართლებრივი განჭვრეტადობა მინიმუმამდე დაყვანის მოთხოვნის პრაქტიკაში რეალიზებასთან დაკავშირებული პრინციპებისა და ძირითადი გარანტიების შესახებ, მაგალითად, არ არის განსაზღვრული თუ რა წესით, ვის მიერ, რა ვადაში უნდა მოხდეს ღირებული ინფორმაციის გამიჯვნა გამოძიებისათვის ღირებულების არ მქონე ინფორმაციისგან; რამდენად აღირიცხება ეს პროცედურა ოქმში, რათა შემდგომში გადამოწმებადი იყოს მასთან დაკავშირებული მოთხოვნების შესრულება; ამ კუთხით მნიშვნელოვანია, ფარული საგამოძიებო მოქმედების შესახებ ოქმში აღირიცხოს სსსკ-ის 143[7] მუხლით გათვალისწინებული მინიმუმამდე დაყვანის მოთხოვნის ფარგლებში დაცულ პირებთან დაკავშირებით მონაცემების მოპოვების შესახებ ინფორმაცია, ასევე მოპოვებული მასალის გადარჩევასთან დაკავშირებული მონაცემები. აღნიშნული მოსაზრებები ეხება, მათ შორის, ადვოკატსა და კლიენტს შორის ადვოკატის

პროფესიულ საქმიანობას მიკუთვნებული ინფორმაციის დაცვის საკითხსაც; მიუხედავად იმისა, რომ სსსკ-ის 143[7] მუხლი საგანგებო ყურადღებას ამახვილებს ამ ტიპის ინფორმაციის დაცვაზე, არ განსაზღვრავს შესაბამის პროცედურას, ამ მოთხოვნის პრაქტიკაში ეფექტიანი რეალიზების მიზნით.

გერმანიის გამოცდილების გათვალისწინებით ნაშრომში წარმოდგენილ იქნა რეკომენდაცია პირადი ცხოვრების ინტიმური სფეროს დაცვის მიზნით სსსკ-ში შესაბამისი რეგულაციების გათვალისწინებასთან დაკავშირებით. აღნიშნულ მოსაზრებას საფუძვლად უდევს საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებაში დაფიქსირებული პოზიცია „პირადი ცხოვრების ძირითადი სფეროს სახელმწიფოს ზედამხედველობისგან განსაკუთრებული დაცვის“ აუცილებლობის თაობაზე.

აღსანიშნავია, რომ ევროპული სასამართლოს პრაქტიკიდან გამომდინარე, მნიშვნელოვანია მოპოვებულ მონაცემთა შემდგომი შენახვის რეგულარული გადამოწმების საკითხის რეგლამენტაცია; როგორც უკვე აღინიშნა, შეგროვებულ მონაცემთა შენახვა, პირდაპირ გავლენას ახდენს ინდივიდის პირადი ცხოვრების ინტერესებზე; იქედან გამომდინარე, რომ ამ საკითხის რეგულირების კუთხით სსსკ არაფერს ამბობს, გამოითქვა მოსაზრება აღნიშნული საკითხის საკანონმდებლო წესით მოწესრიგებასთან დაკავშირებით.

ფარული საგამოძიებო მოქმედების განხორციელების დროს შესაძლებელია ადგილი ჰქონდეს მტკიცებულების მოპოვებას „შემთხვევით პირებთან“ ან/და „სხვა დანაშაულთან“ დაკავშირებით, რომელიც არ არის აღნიშნული სასამართლოს ნებართვაში/პროკურორის დადგენილებაში. ზოგადი სტანდარტის მიხედვით, „შემთხვევით მოპოვებულ ინფორმაციასთან“ დაკავშირებით მოქმედებს ისეთივე წესები, როგორიც ფარული საგამოძიებო მოქმედების ჩატარების შესახებ ნებართვის განჩინების მიმართ. საერთაშორისო მიდგომის თანახმად, კანონმდებლობა უნდა ადგენდეს შესაბამის რეგულაციას „შემთხვევით პირებთან მიმართებით“ მოპოვებული მტკიცებულების გამოყენებასთან დაკავშირებით; ასეთი ინფორმაციის მტკიცებულებად გამოყენება არ უნდა იქცეს ზოგად წესად და განსაკუთრებით პრობლემატურია ნებისმიერი კატეგორიის დანაშაულთან მიმართებით მისი გამოყენების შესაძლებლობა; როგორც ქართული კანონმდებლობის განხილვის შედეგად გამოიკვეთა, სსსკ-ში არ არის ნათლად განსაზღვრული იმ ინფორმაციის

მტკიცებულებად გამოყენების საკითხი, რომელიც ღონისძიების ობიექტის გარდა, ავლენს სხვა „შემთხვევითი პირების“ კავშირს სასამართლოს ნებართვაში აღნიშნულ დანაშაულთან; ამდენად, მიზანშეწონილია ამ საკითხის მოწესრიგება საერთაშორისო გამოცდილების გათვალისწინებით, როგორც მინიმუმ, გარკვეული ფარგლებით ასეთი ინფორმაციის სისხლის სამართლის პროცესში გამოყენების შეზღუდვის პირობებში.

რაც შეეხება ისეთ შემთხვევას, როდესაც ღონისძიების განხორციელებისას ვლინდება „სხვა დანაშაულის“ (რომელიც არ არის სასამართლოს ნებართვაში მითითებული) ნიშნები, მართალია აღნიშნულ შემთხვევას ეხება სსსკ-ის 143[3] მუხლის მე-9 ნაწილი, თუმცა არაფერია ნათქვამი იმის შესახებ, როგორ უნდა გაგრძელდეს დაწყებული ღონისძიება როდესაც „სხვა დანაშაულის“ ნიშნები გამოვლინდება, კერძოდ, უნდა შეწყდეს თუ არა ფარული საგამოძიებო მოქმედება და მის გასაგრძელებლად სასამართლოს ახალი განჩინება იქნეს მოპოვებული, თუ გაგრძელდეს სასამართლოს ნებართვით გათვალისწინებული ვადით. ამის გათვალისწინებით, კვლევაში გამოთქმულია შეხედულება აღნიშნული საკითხის სსსკ-ში სათანადოდ მოწესრიგების თაობაზე; რაც შეეხება მოპოვებული მტკიცებულების გამოყენებას იმ დანაშაულებთან დაკავშირებით, რომელთა მიმართებითაც სსსკ-ის მიხედვით არ არის დაშვებული ფარული საგამოძიებო მოქმედების გამოყენება, მიზანშეწონილია გათვალისწინებულ იქნეს მოპოვებული მტკიცებულების შეზღუდულად გამოყენების შესაძლებლობა და როგორც მინიმუმ, გარკვეული ფარგლებით ასეთი ინფორმაციის სისხლის სამართლის პროცესში დაშვების შეზღუდვა.

სახელმწიფო ორგანოებს შორის მონაცემთა გადაცემა კიდევ ერთ საკითხს მიეკუთვნება, რომელიც ასევე საჭიროებს სათანადო რეგლამენტაციას სსსკ-ში. ამ თვალსაზრისით მნიშვნელოვანია ფარული საგამოძიებო მოქმედების ტექნიკურად აღსრულებაზე პასუხისმგებელი ორგანოს - სააგენტოს და შესაბამის საგამოძიებო ორგანოს შორის მოპოვებული ინფორმაციის მიმოცვლის პროცედურის მოწესრიგება. აღნიშნული ეხება სააგენტოს მიერ მოპოვებული ინფორმაციის შესაბამისი საგამოძიებო ორგანოსათვის გადაცემის წესს, სააგენტოში აღნიშნული ინფორმაციის შენახვის ვადას და გამოძიების ორგანოსათვის ინფორმაციის გადაცემის შემდეგ სააგენტოში შენახული ეგზემპლარის განადგურებას მოთხოვნას, ასევე მონაცემთა უსაფრთხოდ გადაცემის მიზნით შესაბამის მოთხოვნებს. რაც შეეხება სხვა

საგამოძიებო ორგანოსათვის მონაცემთა გადაცემას, ევროპული სტანდარტის მიხედვით, ეს საკითხი ასევე ნათლად უნდა იყოს განსაზღვრული; მნიშვნელოვანია მონაცემთა გადაცემის შეზღუდვა დანაშაულთა წრით, გადაცემის პროცედურაზე ეფექტიანი ზედამხედველობის განხორციელება და გადაცემის ფაქტების აღრიცხვა.

ფარული საგამოძიებო მოქმედების განხორციელების თაობაზე ადრესატისათვის შეტყობინების საკითხთან დაკავშირებით მისასალმებელია, რომ ქართული კანონმდებლობა ამ თვალსაზრისით შეესაბამება ევროპულ სტანდარტებს, მათ შორის, გათვალისწინებულია ღონისძიების გადავადების საკითხზე სასამართლოს ზედამხედველობა.

სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების სტატისტიკური ინფორმაციის განხილვის შედეგად გამოიკვეთა აღნიშნული ღონისძიების გამოყენების ზრდის ტენდენცია, რაც მეტყველებს ფარული მეთვალყურეობის უფლებამოსილების სამართალდამცავი ორგანოების ხელთ არსებულ რუტინულ ღონისძიებად გადაქცევის რისკებზე;[1111] აღნიშნული რისკის მინიმალიზება ამ ღონისძიების „მკაცრად აუცილებელ“ შემთხვევებში, მხოლოდ უკიდურესი საშუალების სახით გამოყენების გზით არის შესაძლებელი. ამ მოთხოვნების დაცვის გარეშე, მოცემულ ფარული საგამოძიებო მოქმედებასთან დაკავშირებით სსსკ-ით უზრუნველყოფილი თანაზომიერების პრინციპი მხოლოდ ფორმალურ გარანტიად დარჩება. რაც შეეხება სსსკ-ის 143[1] პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების სტატისტიკას, მართალია განხილული შუამდგომლობების რაოდენობრივი მაჩვენებელი არ არის მაღალი, მაგრამ როგორც ჩანს, თბილისის საქალაქო სასამართლო ამ ღონისძიების ჩატარების შუამდგომლობას ყველა შემთხვევაში აკმაყოფილებს, რაც საყურადღებო ინდიკატორია და შეიძლება მიუთითებდეს სასამართლოს მიერ ამ ღონისძიების ჩატარების საკითხის სათანადოდ განხილვის ხარვეზებზე.

ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით სტატისტიკის წარმოებასთან დაკავშირებით გამოითქვა მოსაზრება, რომ უმჯობესია სსსკ-ის 143[1]

[1111] იხ. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019, 423.

მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებულ ღონისძიებასთან მიმართებით ასევე დამოუკიდებლად ქვეყნდებოდეს რაოდენობრივი მაჩვენებლები, ისევე როგორც დღეს ეს სატელეფონო საუბრის ფარულ მიყურადება/ჩაწერასთან დაკავშირებით ხორციელდება. აღნიშნული ხელს შეუწყობს პროცესის გამჭვირვალობის და საზოგადოების წინაშე ანგარიშვალდებულების გაუმჯობესებას და განსაკუთრებით აქტუალურია მოცემული ფარული საგამოძიებო მოქმედების ინტენსივობისა და უფლებაშემზღუდველი ხასიათის გათვალისწინებით. გამოითქვა ასევე მოსაზრება გადაუდებელი აუცილებლობის საფუძვლით ჩატარებული/მიმდინარე სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული ფარული საგამოძიებო მოქმედებების სტატისტიკური მაჩვენებლების გამოქვეყნების მიზანშეწონილობის შესახებ, რათა საზოგადოებას შეექმნას წარმოდგენა, აღნიშნული საფუძველი რეალურად რამდენად გამოიყენება პრაქტიკაში გადაუდებლად აუცილებელი საშუალების სახით.

სსსკ-ის 136-ე მუხლის საფუძველზე ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების ელექტრონული კომუნიკაციის კომპანიისგან/სააგენტოსგან გამოთხოვის საკითხთან დაკავშირებით დადებითად უნდა შეფასდეს ის გარემოება, რომ მოქმედი კანონმდებლობა მონაცემთა გამოთხოვის შესაძლებლობას ითვალისწინებს იმ დანაშაულებისთვის, რომლებისთვისაც დასაშვებია ფარული საგამოძიებო მოქმედებების განხორციელება. გარდა ამისა, აღნიშნულ მონაცემთა მოპოვება სისხლის სამართლის პროცესში დასაშვებია სასამართლოს განჩინების საფუძველზე და „დასაბუთებული ვარაუდის“ მტკიცებულებითი სტანდარტის არსებობისას. ასევე არსებითად მნიშვნელოვანია, რომ სსსკ-ის მიხედვით, ამ ინფორმაციის მოპოვებაზე ვრცელდება ფარული საგამოძიებო მოქმედებების ჩატარების სტანდარტები და ის გარანტიები, რაც კანონმდებელმა 2014 წლის 1 აგვისტოს საკანონმდებლო პაკეტით გაითვალისწინა. ამ მხრივ შეიძლება ითქვას, რომ ქართული კანონმდებლობა აკმაყოფილებს ევროკავშირის მართლმსაჯულების სასამართლოს პრაქტიკით დადგენილ მოთხოვნებს შენახულ მონაცემთა ხელმისაწვდომობასთან დაკავშირებით, თუმცა სხვა ვითარებაა მონაცემთა შენახვის საკითხთან მიმართებით, ამ კუთხით გამოიკვეთა არაერთი პრობლემატური ასპექტი როგორც ევროკავშირის მართლმსაჯულების სასამართლოს სტანდარტებთან,

ასევე საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებასთან შესაბამისობის თვალსაზრისით.

ნაშრომის ერთ-ერთ ცენტრალურ თემატიკას საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით დადგენილი მოთხოვნების განხილვა და აღნიშნული გადაწყვეტილების შესრულების მიზნით საქართველოს კანონმდებლობაში განხორციელებული ცვლილებების მოცემულ სტანდარტებთან შესაბამისობის შეფასება წარმოადგენდა.

როგორც კვლევაში გამოვლინდა, საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილების შესრულების მიზნით კანონმდებლობაში განხორციელდა გარკვეული პოზიტიური ცვლილებები, თუმცა მიგვაჩნია, რომ ისევ რჩება პრინციპული მნიშვნელობის ასპექტები, რომელთა მიმართება ამ გადაწყვეტილებით დადგენილ სტანდარტებთან პრობლემურია. აღნიშნული, პირველ რიგში, ეხება გარე კონტროლის მექანიზმებს ინტერნეტკომუნიკაციის მონიტორინგის ღონისძიებაზე; ამ თვალსაზრისით შეიძლება ითქვას, რომ 2017 წლის 22 მარტის საკანონმდებლო ცვლილებებს არ შემოუტანია რაიმე ისეთი გარდატეხა, რომლითაც ეს სფერო, რომელიც საკონსტიტუციო სასამართლომ „ფაქტობრივად უკონტროლოდ“ მიიჩნია,[1112] ზედამხედველობის არსებითად განსხვავებული რეჟიმის ქვეშ მოქცეულიყო. დადებით ფაქტორად უნდა შეფასდეს ის გარემოება, რომ ინსპექტორს „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონით მინიჭებული აქვს ფარული საგამოძიებო მოქმედებების განხორციელების მიზნით გამოსაყენებელი ტექნიკური ინფრასტრუქტურის შემოწმების უფლებამოსილება და პრაქტიკაში ახორციელებს კიდევაც ამ ფუნქციას, თუმცა ეს უფლებამოსილება გააჩნდა 2017 წლის 22 მარტის ცვლილებებამდეც და როგორც ირკვევა, იყენებდა კიდევაც მას პრაქტიკაში. ამ თვალსაზრისით, საეჭვოა ინსპექტირების ფუნქციას რაიმე არსებითი სახეცვლილება განეცადა 2017 წლის 22 მარტის საკანონმდებლო ცვლილებების შედეგად. აქედან გამომდინარე, იმის გათვალისწინებით, რომ საკონსტიტუციო სასამართლომ ინსპექტირების მექანიზმი 2016 წლის 14 აპრილის გადაწყვეტილებით არაეფექტიანად მიიჩნია, ინტერნეტკომუნიკაციაზე ზედამხედველობის ეფექტიანობის საკითხი კვლავ

[1112] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება, II-77.

პრობლემატურია. იგივე შეიძლება ითქვას ნახევრად სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში სატელეფონო კომუნიკაციის ფარული მიყურადების განხორციელებაზეც.

რაც შეეხება სატელეფონო კომუნიკაციის ფარული მიყურადება/ჩაწერის ღონისძიებას სტაციონალური ტექნიკური შესაძლებლობის გამოყენების პირობებში, მნიშვნელოვანია, რომ 2017 წლის 22 მარტის ცვლილებებით დაზუსტდა იმ ტექნიკური საშუალებების ჩამონათვალი, რომელიც შეიძლება ამ ღონისძიების ჩასატარებლად იქნეს გამოყენებული, კერძოდ, განისაზღვრა, რომ „სხვა აპარატურა და პროგრამული უზრუნველყოფის საშუალებები“, რომლის გამოყენებაც საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებით ინსპექტორის გვერდის ავლის შესაძლებლობად იქნა ამოკითხული, შინაარსობრივად დაუკავშირდა მართლზომიერი გადაჭერის მენეჯმენტის სისტემას, კერძოდ, აღნიშნული აპარატურა და პროგრამული უზრუნველყოფის საშუალებები უნდა იყოს „მართლზომიერი გადაჭერის მენეჯმენტის სისტემასთან დაკავშირებული ან/და მისი ფუნქციონირებისათვის აუცილებელი.“

რაც შეეხება ინსპექტორის კონტროლის ბერკეტებს, სტაციონალური ტექნიკური შესაძლებლობის ფარგლებში ინსპექტორი ფლობს მეტად მნიშვნელოვან და ქმედით მექანიზმებს ამ ღონისძიების განხორციელებაზე ეფექტიანი ზედამხედველობის თვალსაზრისით, კერძოდ, კონტროლის ელექტრონული საშუალებებით აკონტროლებს სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებას, რომლის ფარგლებშიც გააჩნია ასევე ღონისძიების შეჩერების უფლებამოსილება.

კიდევ ერთი მნიშვნელოვანი საკითხი უკავშირდება ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზების კოპირების უფლებამოსილებას სააგენტოს მიერ. კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის ვადასთან დაკავშირებით უნდა აღინიშნოს, რომ ვინაიდან მონაცემთა შენახვის კონკრეტული ვადა ევროკავშირის მართლმსაჯულების სასამართლოს არ დაუდგენია, რთული სათქმელია, რამდენად პასუხობს თანაზომიერების პრინციპის უზრუნველყოფის კუთხით ევროკავშირის მოთხოვნებს დღევანდელი კანონმდებლობით გათვალისწინებული მონაცემთა შენახვის პერიოდი.

ისევ აქტუალურ საკითხად რჩება შესანახ მონაცემთა მოცულობა. კვლევაში ამ საკითხს მნიშვნელოვანი ყურადღება დაეთმო და გამოიკვეთა, რომ ელექტრონული

კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა „ტოტალური“, „ბლანკეტური“ შენახვა შეუსაბამოა როგორც ევროკავშირის, ასევე კონსტიტუციურ-სამართლებრივ სტანდარტთან. საქართველოს საკონსტიტუციო სასამართლოს შეხედულებით, მონაცემთა „ტოტალური, ბლანკეტური“ შენახვა თავისთავად ზრდის უფლებაში ჩარევის ინტენსივობას, „იმისგან დამოუკიდებლად, ვრცელდება თუ არა ამ პროცესზე ეფექტური გარე კონტროლი.“ ამდენად, ამ საკითხის გადაჭრის თვალსაზრისით მხოლოდ გარე კონტროლის მექანიზმების გაუმჯობესება ვერ ჩაითვლება საკმარისად და აუცილებელია თავად შესანახ მონაცემთა მოცულობის შეზღუდვა „ობიექტური კრიტერიუმით“, რომელიც შესანახ მონაცემთა და „მძიმე დანაშაულთა“ შორის კავშირის (თუნდაც არაპირდაპირი) დადგენის შესაძლებლობას გაითვალისწინებს.

ამ ღონისძიების განხორციელებაზე გარე კონტროლის მექანიზმებთან დაკავშირებით მისასალმებელია, რომ ინსპექტორის ხელთ არსებული ერთ-ერთი ზედამხედველობის ბერკეტი - ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემა ტექნიკური თვალსაზრისით „გამართულად ფუნქციონირებს და მონაცემთა ცენტრალურ ბანკში ნებისმიერი ქმედების განხორციელება ავტომატურად მიეწოდება ინსპექტორს.“[1113] რაც შეეხება თვითონ მონაცემთა კოპირების პროცესზე ზედამხედველობას, რაც 2016 წლის 14 აპრილის გადაწყვეტილებით კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის მარეგულირებელი კანონმდებლობის არაკონსტიტუციურობის ერთ-ერთ მთავარ მიზეზს წარმოადგენდა, მიგვაჩნია, რომ ამ მიმართულებით რაიმე ახლებური მოწესრიგება კანონმდებელს 2017 წლის 22 მარტის ცვლილებებით არ შემოუტანია.

ამასთანავე, ე.წ. „ალტერნატიული ბანკის“ შექმნასთან დაკავშირებული რისკების თაობაზე უნდა აღინიშნოს, რომ ამ საფრთხის დამაბალანსებელ ფაქტორს მონაცემთა კოპირების პროცესზე პასუხისმგებელი ორგანოს - სააგენტოს დამოუკიდებლობის ხარისხი წარმოადგენს.

კვლევაში ასევე ყურადღება დაეთმო სააგენტოს დამოუკიდებლობის გარანტიებს და როგორც გამოიკვეთა, სააგენტო თავის წინამორბედთან - ოპერატიულ-ტექნიკურ დეპარტამენტთან შედარებით აღჭურვილია გაცილებით მეტი ავტონომიურობის

[1113] საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, I-87.

ხარისხით სახელმწიფო უსაფრთხოების სამსახურისგან, თუმცა კვლავ რჩება მეტად მნიშვნელოვანი საკითხები, როდესაც ვლინდება მასზე სახელმწიფო უსაფრთხოების სამსახურის გავლენა და ამ ასპექტებზე საქართველოს საკონსტიტუციო სასამართლოც მიუთითებს 2017 წლის 29 დეკემბრის საოქმო ჩანაწერში. ასეთ საკითხებს მიეკუთვნება, მაგალითად, სააგენტოს უფროსის დანიშვნისა და გათავისუფლების წესი, სახელმწიფო უსაფრთხოების სამსახურის უფლებამოსილება ძალადაკარგულად გამოაცხადოს სააგენტოს უფროსის სამართლებრივი აქტები, მათ შორის, მათი მიზანშეუწონლობის მოტივით; სამსახურის უფროსის მიერ სააგენტოს სტრუქტურის, საშტატო ნუსხის განსაზღვრის, სააგენტოს უფროსისთვის სპეციალური დანამატის დაწესებისა და პრემირების საკითხების გადაწყვეტის, სააგენტოს მოსამსახურეთათვის სპეციალური დანამატის დაწესებისა და პრემირების საკითხების შეთანხმების უფლებამოსილება, ისევე როგოც სამსახურის უფროსის წინაშე ანგარიშვალდებული გენერალური ინსპექციის მიერ სააგენტოს მოსამსახურეების საქმიანობის შესწავლის ფუნქცია. ამდენად, აქტუალურია სააგენტოს დამოუკიდებლობის გარანტიების გაძლიერება აღნიშნულ ასპექტებთან დაკავშირებით და ამ თვალსაზრისით უფრო ხელშესახები ბერკეტების გათვალისწინება კანონმდებლობაში.

ნაშრომის ერთ-ერთ ცენტრალურ საკითხს კომუნიკაციის მონიტორინგის ღონისძიებებზე ზედამხედველობის სისტემა წარმოადგენდა. ამ კუთხით შეფასდა როგორც სასამართლოს კონტროლის ეფექტიანობა, ასევე გარე კონტროლის მექანიზმები. ინსპექტორის უფლებამოსილებასთან დაკავშირებულ ზოგიერთ საკითხზე ზემოთ უკვე ვისაუბრეთ კონსტიტუციურ-სამართლებრივი სტანდარტების შეჯამების დროს, ამდენად, მათზე აღარ შევჩერდებით.

როგორც განხილული საერთაშორისო და კონსტიტუციური სტანდარტებიდან გამოიკვეთა, როდესაც ქვეყანაში აწყობილია სისტემა, სადაც სახელმწიფოს აქვს კავშირგაბმულობის არხებთან პირდაპირი მიერთების შესაძლებლობა, ზედამხედველობის ბერკეტების ეფექტიანობა განსაკუთრებით მნიშვნელოვანია. მართალია დღეის მდგომარეობით ფარული საგამოძიებო მოქმედებების აღსრულების ფუნქცია ახალ ორგანოს - სააგენტოს აქვს დაკისრებული, მაგრამ კომუნიკაციის რეალურ დროში მოპოვების მარეგულირებელი კანონმდებლობის კონსტიტუციურობასთან დაკავშირებით დღესდღეობით მიმდინარე დავა კიდევ ერთხელ უსვამს ხაზს ამ საკითხის აქტუალურობას და სირთულეს. შესაბამისად,

ფარული საგამოძიებო მოქმედებების განხორციელებაზე კონტროლის მექანიზმების გაძლიერებას განსაკუთრებული დატვირთვა აქვს ქართულ რეალობაში.

ფარულ საგამოძიებო მოქმედებებზე სასამართლო კონტროლთან დაკავშირებით გამოიკვეთა, რომ საერთაშორისო სტანდარტის მიხედვით, სასამართლოს ზედამხედველობა განიხილება ზოგად ნორმად, ადამიანის უფლებების დაცვის „საუკეთესო გარანტიად“, თუმცა სასამართლოს კონტროლის ეფექტიანობა მისი კომპეტენციის ფარგლებით იზომება. სწორედ მოსამართლის კომპეტენცია განსაზღვრავს ამ მექანიზმის წარმატებას პრაქტიკაში. მოსამართლის კომპეტენციაზე საუბრისას ერთ-ერთი მნიშვნელოვანი ფაქტორი, რომელსაც ყურადღება ექცევა, უკავშირდება ფარული საგამოძიებო მოქმედების აღსრულების მთელ პროცესზე ზედამხედველობას. ამ კუთხით ევროპული სასამართლო განასხვავებს „ნებართვის გაცემისა“ და „ღონისძიების აღსრულების“ ეტაპებს. სასამართლოს მონაწილეობა აუცილებელია ორივე ამ სტადიაზე. ამ თვალსაზრისით ევროპული სასამართლოს პრაქტიკაში მნიშვნელობა ენიჭება, რამდენად ხდება ღონისძიების დასრულების შემდეგ მოსამართლის ინფორმირება მიღწეული შედეგების შესახებ, რამდენად არის სასამართლო უფლებამოსილი, განახორციელოს განჩინების შესრულებაზე კონტროლი. აღნიშნულ საკითხთან დაკავშირებით, როგორც კვლევაში გამოიკვეთა, ქართული კანონმდებლობით მოსამართლის როლი ნებართვის გაცემის საკითხის გადაწყვეტით შემოიფარგლება და ღონისძიების იმპლემენტაციის ეტაპში მოსამართლე ჩართული არ არის, მაგალითად, ფარული საგამოძიებო მოქმედების შესახებ ოქმი, რომელშიც ჩატარებული ღონისძიების შესახებ გარკვეული ინფორმაცია აღირიცხება და სსსკ-ით განსაზღვრულ სხვადასხვა პირებს მიეწოდებათ, არ ეგზავნება ნებართვის გამცემ სასამართლოს. რაც შეეხება შუალედური ოქმის შედგენასთან დაკავშირებულ ცვლილებას სსსკ-ის 143[6] მუხლის მე-15 ნაწილში, როგორც გამოიკვეთა, ეს ნორმა სასამართლოს განგრძობადი კონტროლის მექანიზმის ნაცვლად, გადაუდებელი აუცილებლობის საფუძვლით დაწყებული ფარული საგამოძიებო მოქმედების გაგრძელების შესახებ გადაწყვეტილების მიღების მიზნით გამოიყენება.

საბოლოო ჯამში, ზედამხედველობის მექანიზმებთან დაკავშირებით ნაშრომში გამოთქმულია შეხედულება მოსამართლის საზედამხედველო ფუნქციის გაძლიერებასთან დაკავშირებით, რაც ღონისძიების აღსრულების სტადიაზე მისი როლის გაძლიერებით უნდა გამოიხატოს. ამ თვალსაზრისით მნიშვნელოვანია

მოსამართლეს მიეწოდებოდეს ღონისძიების დასრულების შესახებ ოქმი; ამასთან, მნიშვნელოვანია აღნიშნულ ოქმში აღირიცხოს მონაცემები ღონისძიების შედეგად მოპოვებული ინფორმაციის შესახებ. ასეთი სახის კონტროლი შემაკავებელი ფუნქციის მატარებელი შეიძლება იყოს მოცემულ ღონისძიებათა განხორციელებისას უფლებამოსილების ბოროტად გამოყენების საწინააღმდეგოდ. ამ კუთხით, ბუნებრივია, საუბარი არ არის მოპოვებული მტკიცებულების ბედის გადაწყვეტაზე სასამართლოს მიერ, არამედ - მხოლოდ მის ინფორმირებულობაზე ღონისძიების შედეგების შესახებ. ამავდროულად, ნაშრომში გამოხატული პოზიციის თანახმად, ღონისძიების დასრულების შესახებ ოქმში მოპოვებული ინფორმაციის შესახებ მონაცემების დაფიქსირება შეუწყობდა ხელს როგორც სასამართლოს მხრიდან ეფექტიან კონტროლს (ოქმის მიწოდების შემთხვევაში), ასევე ინსპექტორის ხელთ არსებული ზედამხედველობის ბერკეტების გაძლიერებას. იმის გათვალისწინებით, რომ ინსპექტორს მიეწოდება ღონისძიების განადგურების შესახებ ოქმი, მოპოვებული ინფორმაციის განადგურების მოთხოვნების დაცვაზე უფრო ქმედითი კონტროლის შესაძლებლობა მიეცემოდა, თუკი თითოეულ ღონისძიებასთან მიმართებით ასევე ინფორმირებული იქნებოდა მოპოვებული მონაცემების მოცულობის შესახებ.

ღონისძიების მთელ პროცესზე ზედამხედველობის უზრუნველყოფასთან დაკავშირებით ასევე უნდა აღინიშნოს, რომ ინსპექტორის მიერ ღონისძიების შეჩერების უფლებამოსილებაც, რომელიც საკმაოდ ეფექტიან მექანიზმს წარმოადგენს სსსკ-ის 143[6] მუხლის პირველი ნაწილის „ა“ ქვეპუნქტით გათვალისწინებულ სატელეფონო კომუნიკაციის ფარული მიყურადების ღონისძიებასთან დაკავშირებით, ძირითადად მოწოდებულია ღონისძიების დასაწყებად შესაბამისი კანონიერი საფუძვლის შესამოწმებლად, ამდენად, ღონისძიების შედეგად მოპოვებული ინფორმაციის ოქმში ასახვა, რომელიც ინსპექტორს ასევე მიეწოდება და დამატებით მოსამართლის მეტი ჩართულობა ზედამხედველობის პროცესში, მხოლოდ დადებითი შედეგის მომტანი შეიძლება იყოს ამ მიმართულებით.

ნაშრომში ასევე მნიშვნელოვანი ყურადღება დაეთმო გარემოებებს, რომლებიც საერთაშორისო გამოცდილების გათვალისწინებით, სასამართლო კონტროლის ეფექტიანობის ხელისშემშლელად განიხილება, როგორიცაა მაგალითად, მოსამართლეთა გადატვირთულობა, შეჯიბრებითი პროცესის ელემენტების ნაკლებობა, მოსამართლეთა კომპეტენციის ნაკლებობა კომუნიკაციის მონიტორინგის

ღონისძიებებთან დაკავშირებულ ტექნიკურ და პრაქტიკულ ასპექტებთან დაკავშირებით. სამოსამართლო კონტროლის ეფექტიანობის ამაღლების კუთხით ძირითად რეკომენდაციებად სახელდება სასამართლოს აღჭურვა შესაბამისი კვალიფიკაციის (ტექნიკურ და სამართლებრივ საკითხებში) პერსონალით, მოსამართლეთა მიერ ფარულ საგამოძიებო მოქმედებებთან დაკავშირებული ფუნქციის ძირითად სამოსამართლო საქმიანობის ნაწილად მიჩნევა, რაც შესაბამის სტატისტიკაში უნდა აისახოს, შეჯიბრებითი პროცესის ელემენტების გაძლიერება. ნიშანდობლივია, რომ შეჯიბრებითი პროცესის ელემენტების არარსებობის დაბალანსების მიზნით ვენეციის კომისიის, გაეროს სპეციალური მომხსენებლის და ევროპის საბჭოს ადამიანის უფლებების კომისრის ანგარიშებში აქტიურად განიხილება ახალი პოზიციის „სპეციალური ადვოკატის“ შემოტანის იდეა. მართალია „სპეციალური ადვოკატების“ მონაწილეობის პრაქტიკა ჯერჯერობით ნაკლებად არის დანერგილი ევროპულ ქვეყნებში, თუმცა სამომავლოდ ამ საკითხს შესაძლებელია გაცილებით მეტი დატვირთვა მიეცეს და იმის გათვალისწინებით, თუ როგორ განვითარდება ამ საკითხთან დაკავშირებით საერთაშორისო პრაქტიკა, სავსებით შესაძლებელია, ვისაუბროთ ქართულ სისხლის სამართლის პროცესში ასეთი სუბიექტის შემოყვანის იდეასა და მიზანშეწონილობაზე.

რაც შეეხება ინსპექტორის საზედამხედველო მექანიზმს, მისი აქტიური ჩართულობა და როლი ფარული საგამოძიებო მოქმედებების ზედამხედველობის კუთხით უდავოდ წარმოადგენს ერთ-ერთ ყველაზე ხელშესახებ გარანტიას ფარულ საგამოძიებო მოქმედებებთან დაკავშირებით. ზოგადად, ზედამხედველობის შერეული მოდელები დადებითად არის შეფასებული საერთაშორისო დონეზე. ამ მხრივ მისასალმებელია, რომ ინსპექტორს საკმაოდ მნიშვნელოვანი ბერკეტები გააჩნია ზედამხედველობის კუთხით, რაზეც კონსტიტუციურ-სამართლებრივ სტანდარტებზე საუბრის დროსაც იქნა ყურადღება გამახვილებული. თუმცა როგორც ზემოთ ვისაუბრეთ, კვლავ არსებობს არაერთი მნიშვნელოვანი პრობლემატური ასპექტი, რომელიც საკონსტიტუციო დავებმა გამოავლინა ინსპექტორის კონტროლთან დაკავშირებით.

ინსპექტორის საზედამხედველო ფუნქციასთან დაკავშირებული ერთ-ერთი მნიშვნელოვანი ასპექტი, რომელიც მიგვაჩნია, რომ უფრო ზედმიწევნით რეგულაციას საჭიროებს, უკავშირდება ინსპექტორის სამსახურის კომპეტენციას ინსპექტირების

პროცესში დარღვევის გამოვლენის შემთხვევაში; ეს საკითხი ითხოვს უფრო დეტალურ და მკაფიო მოწესრიგებას შესაბამის კანონმდებლობაში, რათა დაკონკრეტდეს შემოწმების განმახორციელებელი პირის უფლებების სრულყოფილი ჩამონათვალი და მათ შორის, დაზუსტდეს, თუ რამდენად შეუძლია ინსპექტორს, მოითხოვოს ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული ინფორმაციის განადგურება.

კონკრეტულ პირთა მისამართით ჩატარებული ფარული საგამოძიებო მოქმედებების განხორციელების კანონიერების შესწავლის მიზნით ინსპექტორის სამსახურის მიერ ჩატარებულ შემოწმებებთან დაკავშირებით გამოითქვა მოსაზრება, რომ სასურველი იქნება სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ ფარულ საგამოძიებო მოქმედებებთან მიმართებით ინსპექტორის ინიციატივით დაწყებული ინსპექტირების ფარგლებში ასევე ხდებოდეს შესწავლილი ფარული საგამოძიებო მოქმედებების რაოდენობის, ასევე სასამართლოს განჩინებებისა და პროკურორის დადგენილებების აღრიცხვა, რათა უფრო ნათელი სურათი შეიქმნას იმასთან დაკავშირებით, თუ რამდენად მრავლისმომცველი და გამოყენებადია აღნიშნული მექანიზმი პრაქტიკაში.

საკონსტიტუციო სასამართლო 2016 წლის 14 აპრილის გადაწყვეტილებაში აღნიშნავს, რომ სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ღონისძიება მოიაზრებს „სახელმწიფოს მიერ ნებისმიერი ინფორმაციის მოხსნას და ფიქსაციას ყველა კავშირგაბმულობის საშუალებებიდან, კომპიუტერული ქსელებიდან, კომპიუტერული სისტემიდან, რაც ფაქტობრივად გულისხმობს როგორც ინტერნეტურთიერთობის მონიტორინგს, ისე კომპიუტერულ სისტემებში არსებულ, შექმნილ/შენახულ ინფორმაციაზე ხელმისაწვდომობის უზრუნველყოფას.“ ამდენად, ამ ნორმის ქვეშ თავმოყრილია ინფორმაციულ რესურსზე წვდომის მეტად ფართო შესაძლებლობები, რაც განსაკუთრებული აქტუალურობით წამოჭრის ადამიანის უფლებების დაცვის პრობლემატიკას ამ შემთხვევაში. ამ ნორმის ზოგადი ფორმულირება ვეღარ პასუხობს თანამედროვე ტექნოლოგიური პროგრესის პირობებში ინფორმაციულ რესურსზე შეუზღუდავი წვდომის შესაძლებლობებიდან მომდინარე გამოწვევებს. ციფრულ ეპოქაში პირადი ხასიათის ინფორმაციის ელექტრონული საშუალებებით მოპოვების შესაძლებლობების მრავალფეროვანი ხასიათი განაპირობებს, რომ პირადი ცხოვრების უფლებაზე მათი შესაძლო გავლენა და ჩარევის ხარისხი ხშირ შემთხვევაში განსხვავებულია, რაც კონკრეტულ

ვითარებაში თანაზომიერების ტესტის განსხვავებულ შეფასებას შეიძლება მოითხოვდეს[1114]. შესაბამისად, ინტერნეტთან მიმართებით ფარული მეთვალყურეობის ღონისძიებების მკაფიო, კონკრეტული მოწესრიგება განსაკუთრებულ მნიშვნელობას იძენს.[1115]

განხილული საერთაშორისო გამოცდილების გათვალისწინებით გამოიკვეთა, რომ ინტერნეტკომუნიკაციის მოპოვების ღონისძიების მკაფიოდ რეგლამენტაციის აუცილებლობა კიდევ უფრო აქტუალურია „დავირუსების“ ღონისძიებასთან მიმართებაში - საერთაშორისო სტანდარტების მიხედვით, იმ შემთხვევაში, როდესაც დღის წესრიგში დგას კომპიუტერულ სისტემაში ფარულად შეღწევის ღონისძიების განსხვავებული ფუნქციური შესაძლებლობების გამოყენების საკითხი, რეკომენდებულია, ტექნიკური თვალსაზრისით ძირითადი შესაძლებლობები საკანონმდებლო დონეზე გაიმიჯნოს და მათი ჩატარება ცალ-ცალკე ნებართვის პროცედურის ფარგლებში წარიმართოს.

ყოველივე აქედან გამომდინარე, გამოითქვა მოსაზრება, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული კომუნიკაციის რეალურ დროში მოპოვებისა და კომპიუტერულ სისტემაში შენახულ ინფორმაციაზე წვდომის უფლებამოსილებების გამიჯვნასთან დაკავშირებით.

ამავდროულად, ინტერნეტკომუნიკაციებზე წვდომის შესაძლებლობების ტექნიკური თვალსაზრისით კომპლექსური ხასიათი განაპირობებს სასამართლოს მეტად ინფორმირების აუცილებლობას იმასთან დაკავშირებით, თუ რა საშუალებით უნდა განხორციელდეს კონკრეტული ღონისძიება პრაქტიკაში. აღნიშნული მნიშვნელოვანია იმდენად, რამდენადაც გამოყენებულ ტექნიკურ საშუალებებს მოსაპოვებელი ინფორმაციის მოცულობასა და პირადი ცხოვრების უფლების შეზღუდვის ინტენსივობაზე არსებითი ზეგავლენის მოხდენა შეუძლია. მოთხოვნილი ღონისძიების განხორციელების მეთოდის შესახებ სასამართლოს ინფორმირების აუცილებლობა აქტიურად განიხილება ასევე „კომპიუტერულ სისტემაში ფარული შეღწევის“ ღონისძიების შემთხვევაში, ვინაიდან ამ საგამოძიებო მოქმედების განხორციელებასთან დაკავშირებული ტექნიკური ასპექტები თანაზომიერების

[1114] *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1, 132-133.
[1115] იქვე.

პრინციპის მნიშვნელოვან საზომად მიიჩნევა. ამდენად, სსსკ-ის 143[1] მუხლის პირველი ნაწილის „ბ“ ქვეპუნქტით გათვალისწინებული ფარული საგამოძიებო მოქმედების შემთხვევაში სასამართლოს ინფორმირება (პროკურორის დადგენილებაში და შემდეგ - სასამართლოს განჩინებაში აღნიშვნა) იმასთან დაკავშირებით, თუ რა ტექნიკური საშუალებები იქნება გამოყენებული ღონისძიების ფარგლებში, მნიშვნელოვნად შეუწყობს ხელს მოსამართლის მხრიდან ღონისძიების აუცილებლობასა და პროპორციულობასთან დაკავშირებული ასპექტების ადეკვატურ შეფასებას და ასევე არანაკლებ მნიშვნელოვანია ღონისძიების ფარგლების დაკონკრეტების თვალსაზრისით.

კვლევის ფარგლებში მნიშვნელოვანი ყურადღება იქნა გამახვილებული საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებაში არსებულ ჩანაწერზე იმასთან დაკავშირებით, რომ ინტერნეტკომუნიკაციის რეალურ დროში მოპოვების მიზნით „მიმართავენ ე.წ. დავირუსების ტექნიკას“. იმის გათვალისწინებით, რომ ამ „ტექნიკაზე“ სხვა რაიმე ინფორმაცია გადაწყვეტილებაში არ არის მოცემული, ბუნდოვანია თუ რა ტექნიკური შესაძლებლობა მოიაზრება მითითებული ღონისძიების ქვეშ. როგორც უკვე აღინიშნა, ზოგადი თვალსაზრისით, კომპიუტერულ სისტემაში ფარული შეღწევის ღონისძიების გამოყენების პრაქტიკა არ არის უჩვეულო საერთაშორისო დონეზე და ზოგიერთი ევროპული სახელმწიფო პირდაპირ არეგულირებს კანონმდებლობით ამ ღონისძიების კონკრეტული ფუნქციური შესაძლებლობების განხორციელების საკითხს და შესაბამის გარანტიებს. მოცემული ღონისძიება აერთიანებს ფუნქციურად განსხვავებულ შესაძლებლობებს და სხვადასხვა სახის ინფორმაციების მოპოვების მრავალფეროვან ტექნიკურ საშუალებებს. ადამიანის უფლებებში ჩარევის თვალსაზრისით მისი განსაკუთრებული ინტენსივობიდან გამომდინარე, საერთაშორისო დონეზე განვითარდა შეხედულება, რომ ამ ღონისძიებასთან დაკავშირებული ასპექტების სათანადოდ რეგულირება მოითხოვს უშუალოდ მასზე მორგებულ სამართლებრივ ნორმებს და უფრო მკაცრ მიდგომას, ამდენად, რეგულაციები, რომლებიც აწესრიგებს ტრადიციული ფარული მეთვალყურეობის უფლებამოსილებას (მაგ. სატელეფონო კომუნიკაციის ფარული მიყურადება) არ არის საკმარისი ამ კუთხით. აქედან გამომდინარე, იმ შემთხვევაში, თუკი საქართველოს რეალობაშიც დგას დღის წესრიგში „ე.წ. დავირუსების ტექნიკის“ პრაქტიკაში გამოყენების საკითხი,

გათვალისწინებული უნდა იქნეს კონკრეტული, სპეციალური ნორმები, განსხვავებული, მკაცრი მიდგომა და უფლების დაცვის საიმედო გარანტიები.

საერთაშორისო პრაქტიკის გათვალისწინებით, ნაშრომში წარმოდგენილი იქნა ცალკეული ძირითადი გარანტიები, რომლებიც ამ შემთხვევაში არის გათვალისწინებული, როგორიცაა, მაგალითად, ამ ღონისძიების განხორციელების შესაძლებლობა მხოლოდ „მძიმე დანაშაულის“ წინააღმდეგ ბრძოლის ინტერესებისათვის; ღონისძიების ჩატარების მეთოდისა და ფარგლების შესახებ სასამართლოს ინფორმირება, რაც შეიძლება განხორციელდეს, მაგალითად, იმ ტექნიკური საშუალებების აღნიშვნით, რომლითაც უნდა ჩატარდეს ეს საგამოძიებო მოქმედება; ტექნიკურ საკითხებში სპეციალისტის მონაწილეობა ნებართვის გაცემის პროცედურის ფარგლებში; შესაბამისი კომპიუტერული სისტემის წინასწარ მაქსიმალურად დაზუსტება სასამართლოს განჩინების ფარგლების დაკონკრეტების მიზნით; ასევე ღონისძიების დასრულების შემდეგ მასთან დაკავშირებული ინფორმაციის დეტალური აღრიცხვა, რაც მოიცავს, მათ შორის, კომპიუტერულ სისტემაში განხორციელებულ ცვლილებებსა და მოპოვებული ინფორმაციის შესახებ მონაცემებს.

საბოლოო ჯამში, შეიძლება ითქვას, რომ მოქმედი კანონმდებლობა ითვალისწინებს არაერთ მნიშვნელოვან გარანტიას ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის მოპოვების/გამოყენების თვალსაზრისით; თუმცა ეს თემა იყო და კვლავაც რჩევა ერთ-ერთ ყველაზე სენსიტიურ და პრობლემატურ საკითხად სისხლის სამართლის პროცესში, რასაც საკონსტიტუციო დავებიც ადასტურებს. როგორც გამოიკვეთა, ქართულ კანონმდებლობაში არსებობს მრავალი პრობლემატური ასპექტი საერთაშორისო და კონსტიტუციურ-სამართლებრივ სტანდარტებთან შესაბამისობის კუთხით; ნიშანდობლივია ისიც, რომ საქართველოს ევროკავშირთან ასოცირების შეთანხმების ფარგლებში აღებული აქვს ვალდებულება, პერსონალურ მონაცემთა დაცვის სფეროში ეროვნული კანონმდებლობა დაუახლოვოს ევროპულ სტანდარტებს, აქედან გამომდინარე, მეტად მნიშვნელოვანია, მოცემულ სფეროში ქართული კანონმდებლობის საერთაშორისო მიდგომებისა და მოთხოვნების შესაბამისად რეგულირება.

ბიბლიოგრაფია

ქართულენოვანი წყაროები:

1. ავტორთა კოლექტივი, საქართველოს კონსტიტუციის კომენტარი, *(რედ.)*, თბ., 2013.
2. ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი, *(რედ.)*, თბ., 2015.
3. *ალბრეხტი, ჰ.-ი.,* დასკვნა საქართველოს კანონმდებლობით ევროკავშირის 2006/24/EC დირექტივის დებულებათა გაზიარების და ფარული საგამოძიებო მოქმედებების ახლებურად მოწესრიგების საკითხზე, 2014, <https://info.parliament.ge/file/1/BillReviewContent/13275?> [04.06.2021].
4. ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ, 2018, <https://personaldata.ge/ka/press/post/5047> [25.06.2020].
5. *აქუბარდია ი.,* წიგნში: სისხლის სამართლის პროცესი (ზოგადი ნაწილის ცალკეული ინსტიტუტები), *(რედ.)*, თბ., 2009.
6. *გეგეშიძე. თ.,* ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება – ქართული სამართალი და საერთაშორისო სტანდარტები, DGStZ, №2, 2017, <http://www.dgstz.de/storage/documents/uyXdgF3kEMpfvqb91SMMjM0iGVsLRQQcFf6p04rK.pdf> [10.06.2020].
7. *გეგეშიძე თ.,* ინტერნეტკომუნიკაციის მონიტორინგი სისხლის სამართლის პროცესში, სამართლის ჟურნალი, 2019, №1.
8. *დემეტრაშვილი/კობახიძე,* კონსტიტუციური სამართალი, თბ., 2014.
9. *ერემაძე ქ.* წიგნში: საქართველოს საკონსტიტუციო სამართალი, თბ., 2017.
10. თბილისის საქალაქო სასამართლოს 2019 წლის 14 აგვისტოს N2058-19 წერილი.
11. *თუმანიშვილი გ., გეგეშიძე თ.,* მტკიცებულებათა სახეები და დასაშვებობასთან დაკავშირებული ზოგადი წესები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *(რედ.)*, თბ., 2019.
12. *თუმანიშვილი გ.,* სისხლის სამართლის პროცესი, ზოგადი ნაწილის მიმოხილვა, თბ., 2014.

13. *კილკელი უ.,* პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის განხორციელება, გზამკვლევი, *(რედ.),* ევროპის საბჭო, თბ., 2005.

14. *კორკელია კ.,* პირადი ცხოვრების, მიმოწერისა და საცხოვრებლის ხელშეუხებლობის უფლებები საქართველოს კონსტიტუციის მიხედვით, ქართული სამართლის მიმოხილვა, 7/2004-1.

15. *კუბლაშვილი კ.,* ძირითადი უფლებები, 2008, თბ.

16. *ლომთათიძე ე., ხანთაძე ნ., ზედელაშვილი დ.,* პირადი თავისუფლება და ავტონომია, 2018, <http://ewmi-prolog.org/images/files/5844ResearchRighttoPrivacyFINAL.pdf> [25.06.2020].

17. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის საჯარო ინფორმაციაზე პასუხისმგებელი პირის 2019 წლის 21 იანვრის წერილი (№: PDP 7 19 00000216).

18. პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები, 2017, <http://www.supremecourt.ge/files/upload-file/pdf/piradi-da-ojaxuri-cxovrebis-pativiscemis-upleba-da-saxelmwipo-valdebulebebi.pdf> [18.06.2020].

19. სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, 2019, <https://personaldata.ge/ka/about-us> [25.06.2020].

20. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 23 ივნისის წერილი (№ SIS 8 20 00009512).

21. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 5 მაისის წერილი (№:SIS 5 20 00006422).

22. სახელმწიფო ინსპექტორის სამსახურის 2019 წლის 18 სექტემბრის წერილი (№SIS 1 19 00003946).

23. *ტრექსელი შ.,* ადამიანის უფლებები სისხლის სამართლის პროცესში, *(რედ.),* თბ., 2009.

24. *ტულუში თ., ბურჯანაძე გ., მშვენიერაძე გ., გოცირიძე გ., მენაბდე ვ.,* ადამიანის უფლებები და საქართველოს საკონსტიტუციო სასამართლოს სამართალწარმოების პრაქტიკა, თბ., 2013.

25. *უსენაშვილი ჯ.* პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციის პრობლემა სასამართლოს კონტროლს დაქვემდებარებული ოპერატიულ-სამძებრო ღონისძიებების წარმოებისას, „სამართლის ჟურნალი,“ N2, 2012.

26. *ფაფიაშვილი ლ.* პირადი ცხოვრების ხელშეუხებლობა პირადი ჩხრეკისას მობილურ ტელეფონებთან მიმართებით, საკონსტიტუციო სამართლის მიმოხილვა, VIII, 2015.

27. *ფაფიაშვილი ლ.,* სისხლის სამართალწარმოებაში პერსონალური მონაცემების დაცვის ევროპეიზაციის ტენდენციები, წიგნში: ევროპული და საერთაშორისო სამართლის ზეგავლენა ქართულ სისხლის საპროცესო სამართალზე, *(რედ.)*, თბ., 2019.

28. *ხოდელი მ.,* სატელეფონო საუბრის ფარული მიყურადება სისხლის სამართლის პროცესში (ქართული და გერმანული სამართლის მიხედვით), თბ., 2019.

29. IDFI, ფარული საგამოძიებო მოქმედებების სტატისტიკა საქართველოში: 2015-2018; 2019, <https://idfi.ge/public/upload/IDFI_2019/General/surveillance_geo_final.pdf> [25.06.2020].

30. IDFI, სატელეფონო საუბრის ფარული მიყურადებისა და ფარული საგამოძიებო მოქმედებების 2016 წლის სტატისტიკური მონაცემები, 2017, <https://idfi.ge/public/upload/IDFI_FOTOS_2016/surveillance_regulation/surveillance-update-statistics-03.02.2017-2.pdf> [25.06.2020].

31. <http://www.supremecourt.ge/farulebi> [25.06.2020].

32. <http://www.supremecourt.ge/statistics/> [25.06.2020].

33. <https://idfi.ge/ge/decreased-motions> [25.06.2020].

ნორმატიული მასალა:

1. საქართველოს კონსტიტუცია, საქართველოს პარლამენტის უწყებები, 31-33, 24/08/1995.

2. ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია, 04/11/1950.

3. ევროპის საბჭოს კონვენცია „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ,“ 08/11/2001.

4. „პერსონალურ მონაცემთა ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციის დამატებითი ოქმი ზედამხედველობით ორგანოებთან და მონაცემთა ტრანსსასაზღვრო გადადინებასთან დაკავშირებით, 01/07/2004.

5. კონვენცია კომპიუტერული დანაშაულის შესახებ, ევროპის საბჭო, 23/11/2001.

6. საქართველოს სისხლის სამართლის კოდექსი, სსმ, 41(48), 22/07/1999.

7. საქართველოს სისხლის სამართლის საპროცესო კოდექსი, სსმ, 31, 09/10/2009.

8. „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონი, სსმ, 26, 02/06/2005.

9. „ოპერატიულ-სამძებრო საქმიანობის შესახებ” საქართველოს კანონი, 30/04/1999.

10. „საჯარო სამართლის იურიდიული პირის - ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონი, matsne.gov.ge, 27/03/2017.

11. „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონი, matsne.gov.ge, 21/07/2018.

12. „პერსონალურ მონაცემთა დამუშავების კანონიერების შემოწმების (ინსპექტირების) წესის დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 2 ივლისის N2 ბრძანება, www.matsne.gov.ge, 03/07/2019.

13. „საქართველოს სახელმწიფო უსაფრთხოების სამსახურის დებულების დამტკიცების შესახებ“ საქართველოს მთავრობის 2015 წლის 30 ივლისის N385 დადგენილებით დამტკიცებული დებულება, www.matsne.gov.ge, 30/07/2015.

14. „სახელმწიფო ინსპექტორის სამსახურის დებულების დამტკიცების შესახებ“ სახელმწიფო ინსპექტორის 2019 წლის 22 მაისის N1 ბრძანება.

15. „ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლის წესის დამტკიცების შესახებ 2017 წლის 28 დეკემბრის N01/338 ბრძანების არასაიდუმლო N1 დანართი - „ფარული საგამოძიებო მოქმედებებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკში განხორციელებული აქტივობების კონტროლთან დაკავშირებული ცალკეული ღონისძიებები და პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის ინფორმაციული ტექნოლოგიებისა და ინსპექტირების დეპარტამენტის ფუნქციები.“

16. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „ოპერატიულ-სამძებრო საქმიანობის შესახებ.“

17. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“, <https://info.parliament.ge/#law-drafting/1317> [10.06.2020].

18. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში“ ცვლილების შეტანის თაობაზე“ <https://info.parliament.ge/#law-drafting/24>, [12.06.2020].

19. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/#law-drafting/15289> [20.06.2020].

20. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/#law-drafting/16624> [20.06.2020].

21. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „საქართველოს სისხლის სამართლის საპროცესო კოდექსში ცვლილების შეტანის შესახებ“, <https://info.parliament.ge/file/1/BillReviewContent/142892?> [20.06.2020].

საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილებები:

1. საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.

2. საქართველოს საკონსტიტუციო სასამართლოს წევრების – ირინე იმერლიშვილის, გიორგი კვერენჩხილაძის და მაია კოპალეიშვილის განსხვავებული აზრი საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერზე.

3. საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის №1/1/650,699 გადაწყვეტილება.

4. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625, 640 გადაწყვეტილება.

5. საქართველოს საკონსტიტუციო სასამართლოს 2014 წლის 23 მაისის №3/1/574 გადაწყვეტილება.

6. საქართველოს საკონსტიტუციო სასამართლოს 2012 წლის 24 ოქტომბრის N1/2/519 გადაწყვეტილება.

7. საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის 1/3/407 გადაწყვეტილება.

8. საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 2 ივლისის N1/2/384 გადაწყვეტილება.

9. საქართველოს საკონსტიტუციო სასამართლოს 2006 წლის 15 დეკემბრის N1/3/393,397 გადაწყვეტილება.

უცხოენოვანი წყაროები:

1. *Abel W., Schafer B.,* The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822, SCRIPTed, Vol. 6, No 1, 2009.

2. Access Now, A Human Rights Response to Government Hacking, 2016, <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf> [17.06.2020].

3. *Barak A.* Proportionality - Constitutional Rights and their Limitations, Cambridge, 2012.

4. *Bloom R. M., Clark W. T.,* Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and The Need for Fourth Amendment Protection, The Journal of Criminal Law & Crimininology, Vol.106, No.2.

5. *Boehm F.,* Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes, European Data Protection Law Review, Vol. 2, No 2, 2016.

6. *Brkan M.*, The Essence of The Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the Cjeu's Constitutional Reasoning, German Law Journal, Vol. 20, 2019.

7. *Bumke C., Vosskuhle H.C.A.,* German Constitutional Law, Introduction, Cases, Principles, 2019.

8. *Clough J.,* Principles of Cybercrime, New York, 2010.

9. *Cobley P., Schulz P.J.,* Introduction, წიგნში: Theories and Models of Communication, *(ed.),* Berlin/Boston, 2013.

10. *Cohen-Eliya M., Porat I.,* American Balancing and German Proportionality: The Historical Origins, International Journal of Constitutional Law, Vol 8, No 2, 2010, <https://academic.oup.com/icon/article/8/2/263/699991> [18.06.2020].

11. *Corn G.S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017.

12. Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime, UN Office on Drugs and Crime, 2009, <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf> [25.06.2020].

13. *Dempsey J., X.; Gate F., H.,* Recommendations for Government and Industry, წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.),* Oxford, 2017.

14. Encryption and Anonymity follow-up report, Special Rapporteur On The Promotion and Protection of The Right to Freedom of Opinion and Expression, 2018, <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, [17.06.2020].

15. *Etteldorf C.,* Higher Administrative Court of Northrhine Westphalia Declares German Data Retention Law Violates EU Law, European Data Protection Law Review, Vol. 3, No 3, 2017.

16. European Commission for Democracy through Law (Venice Commission), On the Democratic Oversight of Signal Intelligence Agencies, 15.12.2015, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e> [20.06.2020].

17. European Commission for Democracy Through Law (Venice Commission), Poland, Opinion on The Act of 15 January 2016 Amending The police Act and Certain Other Acts, 2016, <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)012-e> [25.06.2020].

18. *Forcese C.*, Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Initiatives, წიგნში: Law, Privacy and Surveillance in Canada in the Post-Snowden Era, *Geist M., (ed.),* 2015.

19. *Galletta A., Hert P.D.,* Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance, Utrecht Law Review, 2014, Vol. 10, No 1.

20. *Ghanayim K.,* Human Dignity in Criminal Procedure: A comparative Overview of Israeli and German Law, Israel Law Review, Vol.44.

21. *Gray D.* The Fourth Amendment in an Age of Surveillance, Cambridge, 2017.

22. Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence, Council of Europe, 31.08.2019, <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> [18.06.2020].

23. *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf [25.06.2020].

24. *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017.

25. Handbook on European Data Protection Law, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> [25.06.2020].

26. *Hert P. D.,* Balancing Security and Liberty within The European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11, Utrecht L. Rev. Vol. 1, No 1, 2005.

27. *Hert P. D.,* Court, Privacy and Data Protection in Belgium: Fundamental Rights that Might as well Be Struck from the Constitution, წიგნში: Court, Privacy and Data Protection in The Digital Environment, *Brkan M., Psychogiopoulou E. (eds.),* Cheltenham, UK, 2017.

28. *Hosein G., Palow C. W.,* Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques, Ohio State Law Journal, Vol. 74, No6, <https://kb.osu.edu/bitstream/handle/1811/71608/OSLJ_V74N6_1071.pdf> [12.06.2020].

29. *Hyat S. M.,* Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirement, Vanderbilt Law Review, Vol. 64, No4, 2011.

30. *Israel J. H., LaFave W. R.,* Criminal Procedure, Constitutional Limitations in a Nutshell, 8th Ed. 2014.

31. *Jacoby N.,* Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States, Georgia Journal of International and Comparative Law, Vol. 35, No.3, 2007.

32. *Kerr, O. S.* Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, Northwestern University Law Review, 2003, Vol. 97, No.2.

33. *Kerr O.S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014.

34. *Korff D., Cannataci, J. A., Sutton G.,* Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Strasbourg, 14.02.2014, <https://rm.coe.int/16806af19b> [20.06.2020].

35. *LaFave W. R., Israel J. H., King N.J.,* Criminal Procedure, 4th Ed, 2004.

36. *LaFave W., R., Israel J., H., King N., J., Kerr O., S.,* Principles of Criminal Procedure: Investigation, 2nd Ed., 2009.

37. Landau S., Surveillance or Security? The Risks Posed by New Wiretapping Technologies, 2013.

38. *Lindemann M., Toor D. V.,* Protection of a Suspect's Privacy in Criminal Procedures, Does the Conceptual Approach of the German Federal Constitutional Court Make a Difference? *Ars Aequi,* Issue 5, 2018.

39. *Lippman M.,* Criminal Procedure, 3rd Edition, Los Angeles, 2017.

40. *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No 2, 2015.

41. *Malgieri, G., Hert, P. D.,* European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges, The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017.

42. *Malgieri, G., Hert, P. D.,* European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges, The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017.

43. *McArthur E. D.,* The Search and Seizure of Privileged Attorney-Client Communications, The University of Chicago Law Review, Vol. 72, No. 2, 2005.

44. *McIntyre TJ,* Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective, წიგნში: Judges as Guardians of Constitutionalism and Human Rights, Ed. by *Scheinin M., Krunke H., Aksenova M. (eds.),* 2016.

45. Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, Commissioner for Human Rights, Council of Europe, 17.05.2016, <https://rm.coe.int/16806db72c> [20.06.2020].

46. *Michaelsen C.,* The Proportionality Principle, Counter-Terrorism Laws and Human Rights: A German-Australian Comparison, City U. H.K. L. Rev. 19, 2010.

47. *Milaj. J.,* Invalidation Data Retention Directive – Extending the Proportionality Test, Computer Law & Security Review, 31, 2015.

48. *Milaj J.,* Privacy, Surveillance, and The Proportionality Principle: The Need for A Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No 3, 2016.

49. *Murphy, M. H.,* The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases, 3(2) Irish Journal of Legal Studies, 2013.

50. Necessary & Proportionate, International Principles on the Application of Human Rights Law to Communications Surveillance, 2014, <https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf> [15.06.2020].

51. *Nohlen N.,* Germany: The Electronic Eavesdropping Case, International Journal of Constitutional Law, Vol. 3, No. 4.

52. *Ohm P.,* The Surveillance Regulation b: Thinking Beyond Probable Cause, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E. (eds),* New York, 2017.

53. Opinion of Advocate General, Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, 12.12.2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0293> [20.06.2020].

54. Opinion of Advocate General, Tele2 Sverige AB v Post- och Telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, 19.07.2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CC0203> [20.06.2020].

55. *Pedersen A.M., Udsen H., Jakobsen S. S.,* Data Retention in Europe—the Tele 2 Case and Beyond, International Data Privacy Law, Vol. 8, No 2, 2018.

56. *Pell S. K.,* Location Tracking, წიგნში: The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S.E., (eds.),* New York, 2017.

57. *Petersen J.K.,* Handbook of Surveillance Technologies, 3rd edition, 2012.

58. Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgement, 2017, <https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf> [15.06.2020].

59. Privacy International, Submission to the UN Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression: Study on Telecommunications and Internet Access Sector, 2016, <https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/PrivacyInternational.pdf> [17.06.2020].

60. Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf> [17.06.2020].

61. *Psychogiopoulou E.,* The European Couts of Human Rights, Privacy and Data Protection in the Digital Era, წიგნში: Court, Privacy and Data Protection in The Digital Environment, *Brkan M., Psychogiopoulou E. (eds.),* Cheltenham, UK, 2017.

62. Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc> [05.06.2020].

63. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 28.12.2009, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement> [18.06.2020].

64. Report of the Special Rapporteur On the Promotion and Protection of the Right to Freedom of Opinion and Expression, 17.04.2013, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> [05.06.2020].

65. *Roberts A.,* Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v. Minister for Communications, Modern Law Review, Vol.78, No3, 2015.

66. *Rodríguez K.,* Principled Fight Against Surveillance, Global information Society Watch, Communications Surveillance in the Digital Age, *Finlay A. APC and Hivos (eds.),* 2014, <https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf> [18.06.2020].

67. *Sagers G.,* The Role of Security in Wireless Privacy, წიგნში: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, *Lind N.S., Rankin E. (eds.),* Vol.2, California, 2015.

68. *Schwartz, P.M.*, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, Hastings Law Journals, Vol. 54.

69. *Schwartz P. M.,* Systematic Government Access to Private-sector Data in Germany წიგნში: Bulk Collection, Systematic Government Access to Private-Sector Data, *Dempsey J., X.; Gate F., H. (eds.)*, 2017.

70. *Schweda S.,* Parliament Adopts New Data Retention Law, European Data Protection Law Review, Vol. 1, No3, 2015.

71. *Signorelli W. P.,* Criminal Law, Procedure, and Evidence, New York, 2011.

72. *Slobogin C.,* Privacy at Risk, The New Government Surveillance and The Fourth Amendment, Chicago, 2007.

73. *Solove D. J.,* Reconstructing Electronic Surveillance Law, Geo. Wash. L. Rev, Vol. 72, 2004.

74. *Solove D.J., Rotenberg M., Schwartz P. M.* Privacy, Information, and Technology, New York, 2006.

75. *Solove D.J., Schwartz P. M.,* Information Privacy Law, 5th Edition, New York, 2015.

76. *Solove D. J., Schwartz P. M.*, Privacy, Information, and Technology, 2nd edition, 2008.

77. *Somody B., Szabo M., D., Szekely I.,* Moving Away from The Security–Privacy Trade-off: The Use of The Test of Proportionality in Decision Support, წიგნში: Surveillance, Privacy and Security, Citizens' Perspectives, *Friedewald M., Burgess J. P., Čas J., Bellanova R., Peissl W. (eds.),* London, New York, 2017.

78. *Stalla-Bourdillon S., Phillips J., Ryan M.D.*, Privacy vs. Security, Springer, 2014.

79. *Stoeva E.,* The Data Retention Directive and the Right to Privacy, ERA Forum, 2014, 15.

80. *Swire. P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012.

81. *Taylor N.,* To Find the Needle Do You need The Whole Haystack? Global Surveillance and Principled Regulation, The International Journal of Human Rights, Vol. 18, No 1, 2014.

82. *Tracol X.,* The judgment of the Grand Chamber dated 21 December 2016 in the Two Joint *Tele2 Sverige* and *Watson* Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level, Computer Law & Security Review: The International Journal of Technology Law and Practice, 2017.

83. *Tranberg C. B.,* Proportionality and Data Protection in The Case Law of The European Court of Justice, International Data Privacy Law, 2011, Vol. 1, No. 4.

84. *Tzanou M.,* The Fundamental Right to Data Protection, Normative Value in the Context of Counter-Terrorism Surveillance, Oxford, 2017.

85. *Tzanou M.,* Data Protection in Eu Law After Lisbon: Challenges, Developments and Limitations, წიგნში: Cyber Law, Privacy and Security: Concepts, Methodologies, Tools and Applications, Hershey PA, 2019.

86. United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration On Surveillance Programs and Their Impact on Freedom of Expression, 21/06/2013, <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1>[18.06.2020].

87. *Vaciago G., Ramalho D.S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital

Evidence and Electronic Signature Law Review, 13, 2016, http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252> [17.06.2020].

88. *Winter L.B.,* Remote Computer Searches Under Spanish Law: The Proportionality Principle and The Protection of Privacy, ZStW, Vol.129, No 1, 2017.

89. *Wright J.,* Necessary and inherent limits to internet surveillance, Internet Policy Review,Vol. 2, No. 3, 2013.

90. *Zigerell L. J.,* Maintaining the Technological Neutrality of the Fourth Amendment, წიგნში: Privacy in the Digital Age, 21st – Century Challenges to the Fourth Amendments, *Lind N., S., Rankin E., Praeger (eds.),* California, 2015, Vol. 2.

91. <https://www.merriam-webster.com/dictionary/communication> [10.06.2020].

92. <https://privacyinternational.org/explainer/1309/communications-surveillance> [05.06.2020].

93. <https://privacyinternational.org/explainer/1640/phone-monitoring> [15.06.2020].

94. <https://theconversation.com/rise-and-fall-of-the-landline-143-years-of-telephones-becoming-more-accessible-and-smart-113295> [15.06.2020].

95. <https://searchmobilecomputing.techtarget.com/definition/smartphone> [15.06.2020].

96. <https://www.eff.org/criminaldefender/cell-site-location> [15.06.2020].

97. <https://privacyinternational.org/blog/1296/lawful-interception-russian-approach> [15.06.2020].

98. <https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/> [17.06.2020].

99. <https://privacyinternational.org/feature/827/how-bulk-interception-works> [17.06.2020].

100. <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> [17.06.2020].

101. <https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/> [17.06.2020].

102. <https://www.bverwg.de/pm/2019/66> [20.06.2020].

103. <https://eucrim.eu/news/federal-administrative-court-refers-german-data-retention-law-european-court-justice/> [20.06.2020].

104. <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html> [25.06.2020].

ნორმატიული მასალა:

1. Charter of Fundamental Rights of The European Union, 18/12/2000, <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [18.06.2020].

2. International Covenant on Civil and Political Rights, 16/12/1966.

3. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 08/04/1988, <https://www.refworld.org/docid/453883f922.html> [18.06.2020].

4. Council Resolution On Lawful Interception of Telecommunications, 17/01/1995 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104> [15.06.2020].

5. Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Committee of Ministers, 11/06/2013, <https://www.garanteprivacy.it/documents/10160/2603116/Declaration+of+the+Committee.pdf> [05.06.2020].

6. Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 12/07/2002, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058> [15.06.2020].

7. Directive 2006/24/EC of the European Parliament and of the Council On the Retention of Data Generated or Processed in connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 15/03/2006 <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32006L0024> [20.06.2020].

8. EU General Data Protection Regulation (EU) 2016/679 (GDPR); <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

9. General Assembly, United Nations, Resolution on "The Right to Privacy in The Digital Age", 21/01/2013, <https://undocs.org/A/RES/68/167> [05.06.2020].

10. EU Data Protection Directive for Police and Criminal Justice Authorities (EU) 2016/680 („Police Directive“), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680> [12.06.2020].

11. Recommendation R(87)15of the Committee of Ministers Regulating The Use of Personal Data in The Police Sector, Council of Europe, 17/09/1987.

12. Recommendation No R (95) 13 of The Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology, Council of Europe, 11/09/1995, <https://rm.coe.int/native/09000016804f6e76> [20.06.2020].

13. Proposal for a Regulation of The European Parliament and of The Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10/01/2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> [20.06.2020].

14. StPO (Strafprozessordnung), 07/04/1987.

სასამართლოს გადაწყვეტილებები:

1. Liblik and others v. Estonia, [2019], ECtHR.

2. Case C-207/16, Ministerio Fiscal, [2018], Court of Justice.

3. Benedik v. Slovenia; [2018], ECtHR.

4. Big Brother Watch and Others v. United Kingdom, [2018] ECtHR.

5. Bărbulescu v. Romania, [2017], ECtHR.

6. Mustafa Sezgin Tanrikulu v. Turkey, [2017], ECtHR.

7. *Matanović v. Croatia,* [2017], ECtHR.

8. Bašić v. Croatia, [2017], ECtHR.

9. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice.

10. Versini-Campinchi and Crasnianski v. France, [2016], ECtHR.

11. Šantare and Labaznikovs v. Latvia, [2016], ECtHR.

12. Szabo and Vissy v. Hungary, [2016] ECtHR.

13. BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09.

14. Roman Zakharov v. Russia, [2015] ECtHR.

15. Uzun v. Germany, [2015], ECtHR.

16. Dragojević v. Croatia, [2015], ECtHR.

17. Case NC-293/12 and C-594/12, Digital Rights Ireland ltd and Seitlinger and others, [2014], Court of Justice.

18. Khodorkovskiy and Lebedev v. Russia, [2013], ECtHR.

19. Kennedy v. United Kingdom, [2010] ECtHR.

20. Özpınar v. Turkey, [2010], ECtHR.

21. BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08.

22. Bigaeva v. Greece, [2009], ECtHR.

23. BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08.

24. Iordachi and others v. Moldova, [2009], ECtHR.

25. Liberty and others v. United Kingdom, [2008], ECtHR.

26. S and Marper v. United Kingdom, [2008], ECtHR.

27. BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07.

28. Copland v. the United Kingdom, [2007], ECtHR 2007-I.

29. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR.

30. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI.

31. Aalmoes and others v. The Netherlands, [2004], ECtHR.

32. Doerga v. The Netherlands, [2004], ECtHR.

33. Prado Bugallo v. Spain, [2003], ECtHR.

34. Peck v the United Kingdom, [2003] ECHR.

35. Greuter v. the Netherlands, [2002], ECtHR.

36. Rotaru v. Romania, [2000], ECHR 2000-V.

37. Amman v. Switzerland, [2000], ECHR 2000-II.

38. Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V.

39. Kopp v Switzerland, [1998], ECtHR, Reports 1998-II.

40. Costello-Roberts v. the United Kingdom, [1993], ECtHR, (Series A).

41. Campbell v. United Kingdom, [1992], ECtHR, (Series A no. 233).
42. S. v. Switzerland, [1991], ECtHR, (Series A no.220).
43. Huvig v. France, [1990], ECtHR, (Ser. A.).
44. Kruslin v. France, [1990], ECtHR, (Ser. A.).
45. Leander v. Sweden, [1987] ECtHR, (Ser. A.).
46. Malone v. United Kingdom, [1984], ECtHR (Ser. A.).
47. Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.).
48. Katz v. United States, (1967), 389 U.S. 347.