JUNE 2024 (№30)
Volume 10; Issue 2; Page No. 96-122
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/10.2.9 Licensed under: CC BY-SA

COPYING AND STORING OF ELECTRONIC COMMUNICATION IDENTIFYING DATA AS ELECTRONIC EVEDENCE THE STORAGE PROBLEM IN THE GEORGIAN CRIMINAL JUSTICE PROCESS – IN RELATION TO ARTICLE 8 OF THE EUROPEAN CONVENTION

Dodo Jugheli
Master of Criminal Law, Ivane Javakhishvili Tbilisi State University, Association of Personal Data Protection Officers of Georgia, Labor Inspection Office, Georgia

ARTICLE INFO

Article History:

Received	19.04.2024
Accepted	29.05.2024
Published	30.06.2024

Keywords:

Evidence, Limitation, Copying, Storage

ABSTRACT

The current standard of criminal procedural law of Georgia, along with the danger of illegally copying information obtained from electronic means of communication, envisages collecting such information in the hands of a professionally interested body, which is naturally a big challenge for criminal procedural law. The reason for this is the important fact that the information obtained by the investigation in this way is used as electronic evidence during the substantive consideration of the case in court.

Accordingly, the case concerns information that the court must rely on in making a decision "beyond a reasonable doubt standard". Thus, when deciding the fate of the accused, it is especially important that there are no doubts regarding the legality, truthfulness and inviolability of such evidence. The above-mentioned is particularly noteworthy in the circumstances when the above-mentioned approach, according to European human rights jurisprudence, is incompatible with the right to respect for private life protected by Article 8 of the European Convention.

INTRODUCTION

Relevance of the topic. The Criminal Procedure Legislation of Georgia refers to the use of the existing norms for the purpose of obtaining electronic records, their storage and, accordingly, the legality of attaching them to the case for the implementation of secret investigative actions, which, as explained by the Constitutional Court, carries the threat of interfering with human rights and freedoms with increased intensity. In addition, the appeal to the Constitutional Court regarding compliance with the issue of copying and storage of identifying data of electronic communication obtained as a result of secret investigative activities with the Constitution of Georgia has not been stopped. There is a difference of opinion regarding the aforementioned among the judges of the Constitutional Court, some of whom consider the norms regulating the above-mentioned issue to be "overriding norms" of the norms known as unconstitutional by the decision of the Constitutional Court of Georgia dated April 14, 2016, N1/1/625,640.

In addition, the new edition of the Law of Georgia, "On Personal Data Protection," is particularly relevant in this regard, as it defines the standards in the field of personal data protection and the control of conducting secret investigative activities. It is interesting to see whether recent legislative changes are in line with the current international approach to copying and storing personally identifiable communications data. Thus, in relation to the aforementioned data copying and storage in the criminal justice process, the need for an in-depth study of the issue is particularly apparent for protecting human rights and freedoms.

Research subject. The subject of the study is the challenges related to the storage and copying of identifying communication data obtained through the implementation of undercover investigative activities in the criminal process, which are used as electronic evidence in the substantive consideration of the case in court.

The purpose and objectives of the research. The purpose of the research is to outline and analyze the separate legal problems in the storage and copying of identifying data of electronic communication in the criminal justice process. The set task will be achieved both by presenting the issue in terms of historical precedents and constitutional-legal perspective, as well as by using the norms and practices of European human rights law.

Research novelty. The novelty of scientific research is expressed in the fact that the article defines "electronic evidence" as the final result of obtaining communication identifying data, as well as its nature and differences. Also, the content of the legislative changes implemented after the decision of the Constitutional Court of Georgia on April 14, 2016, N1/1/625,640 will be discussed, to what extent it is of "substantial" importance and whether it still creates a threat of interfering with the right to respect for private life.

Research stages. At the beginning of this article, the essence of electronic evidence is presented, and the purpose of obtaining identifiable communication data is defined. The main part is also devoted to sub-chapters, which refer to the existing legal threats related to the storage of information transmitted through electronic communication created under the current legislation. In particular, the issue of gathering and illegal copying of obtained information in the hands of a professionally interested body (creating the so-called "alternative bank") in relation to the right to respect for private life is discussed. The conclusion presents the author's point of view and summary to solve the problems discussed in the article.

1. NATURE AND RELATIONSHIP OF ELECTRONIC EVIDENCE AND ELECTRONIC COMMUNICATION IDENTIFIABLE DATA

The global technological progress made in the XXI century brought great change in all spheres of public life. As communication has become easier, every person, state or private institution has faced so many challenges in terms of information protection. The mentioned progress also affected the criminal procedural legislation, especially from the point of view of the development of evidence.[1] The rate of use of the computer system in the process of committing a crime has increased significant-

1 Carrera S., Stefan M., Mitsilegas V., (2020). Cross-border data access in criminal proceedings and the future of digital justice, p. 1.

ly. It has become quite relevant the issue of using "digital" evidence in criminal proceedings, which has become a new type of evidence.[2]

Electronic evidence[3] is any data stored or transmitted using computer technology that supports a theory about how a crime occurred.[4] According to Article 1 of the Council of Europe Convention on "Computer Crime", a computer system means "any mechanism or a group of interconnected or interconnected mechanisms, one or more of which, through a program, performs automatic data processing.[5] Computer data itself is "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program that ensures the functioning of a computer system".[6]

Despite the fact that electronic proof is so-called While it has similar characteristics to "traditional" proof, there are a number of aspects that make it unique.[7] First of all, it should be noted the "fragility" of digital data,[8] what makes it stand out, for example, from a document created in material form, on paper. This refers to the nature of information obtained from electronic communication, which can be easily deleted,[9] change etc. Another important circumstance is its decentralized storage. It is possible that information stored outside the country's borders can be used remotely by criminals,[10] Which makes the investigation process even more difficult. Thus, determining the reliability and authenticity of such data mining, electronic nature of evidence is quite a challenge for the criminal procedural laws of all countries.[11]

However, the Explanatory Report (N187) to the Convention on Computer Crime states that additional procedural safeguards are required for the effective collection of communications identifying data[12]. There are several reasons for this. The first is that the mentioned information is presented in an immaterial, electromagnetic form. The second reason is the different standards of its touch. In particular, computer data cannot be confiscated or seized in the same way as a paper document.

In 2016, the Constitutional Court of Georgia deliberated on the procedural guarantees of the storage of communication identifying data obtained by the investigation.[13] At what time should the standards be used by the state when copying and storing information from electronic means of communication were determined.[14]

On the basis of the mentioned decision, certain changes were made in the legislation of Georgia, and the issue of compliance of the contents with

2 Training of Judges on Computer Crime, (2010). France, Strasbourg, p.75 <https://rm.coe.int/16802fa028> [Last accessed: April 15, 2024].

3 In the criminal procedural legislation of Georgia, we do not find the definition of electronic evidence as an independent category of evidence, but the regulatory norms of the mentioned issue are mainly presented in the Criminal Procedure Code of Georgia, the Law of Georgia "On Operative-Search Activity", the Law of Georgia "On Electronic Communications" and others.

4 Casey E., (2004). Digital Evidence and Computer Crime, p.12. The admissibility of electronic evidence in court: fighting against high-tech crime, 2005.

5 Council of Europe Convention on Computer Crime (23.11.2001), Article 1 <https://rm.coe.int/16802fa423> [Last accessed: 15 April 2024].

6 *Ibid*.

7 Training of Judges on Computer Crime, (2010). France, Strasbourg, p.76 <https://rm.coe.int/16802fa028> [Last accessed: April 15, 2024].

8 Casey, Digital Evidence and Computer Crime, 2004, p.16; Vacca, Computer Forensics, Computer Crime Scene Investigation, Second Edition, 2005, p.39.

9 Moore, (2004). To View or not to View: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, #1, p. 58.

10 Training of Judges on Computer Crime, (2010). France, Strasbourg, p.76 <https://rm.coe.int/16802fa028> [Last accessed: April 15, 2024].

11 Stephen M., Allison S., (2017). Electronic Evidence, p. 193.

12 A striking example of the need for additional procedural norms regarding the development of electronic evidence into a "new type" of evidence and the acquisition of personally identifiable communications data is the investigation conducted by German law enforcement several decades ago, during which the identities of criminals who purchased and downloaded child pornography were established through credit card companies. from one of the websites (see: Spiegel Online, Fahnder überprüfen erstmals alle deutschen Kreditkarten, 08.01.2007).

13 Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chitidze, Lasha Tugushi, Zviad Koridze, "Open Society Foundation Georgia", "Transparency International – Georgia", "Young Lawyers Association of Georgia", "International Society for Fair Elections and Democracy" and "Human Rights Center" against the Parliament of Georgia".

14 Acquisition/storage/destruction of digital evidence is carried out according to the standard established by the Constitutional Court for covert investigative actions, since according to the criminal procedural legislation, the rules established for covert investigative actions apply to investigative actions related to computer data.

the Constitution of Georgia caused a difference of opinion among the judges of the Constitutional Court itself.[15]

One of the reasons for the difference of opinion was the problem of copying and storing information from modern electronic means of communication. In particular, a part of the judges of the Constitutional Court drew attention to gathering the obtained data in the hands of the professionally interested body and the so-called On the dangers of creating "alternative banks".

2. THE SO-CALLED DANGER OF CREATING "ALTERNATIVE BANKS"

As emphasized in the decision of the Constitutional Court, "it is technically possible to create the so-called "Alternative bank", the existence of which may not be known to anyone, and the personal data protection inspector may not even have access to it.[16] This implies total access to the information obtained by the investigation, without any content separation: who connected where, when, by what technical means, from which location and for how long.

It should be noted the mechanisms of supervision, which were created for the purpose of preventing the copying of the obtained information. As noted by the Constitutional Court, in the Law of Georgia "On Personal Data Protection"[17] the changes made on March 22, 2017, did not introduce any new regulation in terms of controlling the data copying process by the inspector.[18] A positive innovation was that one of the levers of existing control – the electronic system of control of the central bank of identifying data of electronic communication has already been fixed from a technical point of view, and with its help the inspector could control the actions carried out in the copied data bank.[19] As for the process of copying data from electronic communication companies by the agency, the only lever of supervision was the inspection. This type of supervision was deemed ineffective by the Constitutional Court in its decision of April 14, 2016, due to the method of its implementation, which was based on the "principle of random selection". The mentioned approach excludes absolutely all data control, therefore, the possibility of detecting absolutely all violations, and such "selective control is practically impossible to produce tangible results".[20]

Regarding the regulatory norms of the above-mentioned issue, it should be emphasized that the current version of the Law of Georgia "On Personal Data Protection" does not provide provisions that are significantly different from the previous version of the law regarding the field of data protection and the control of conducting secret investigative activities. In particular, Chapter VII of the current edition of the Law of Georgia "On Personal Data Protection" textually and, accordingly, in terms of content V2 of the previous edition of the Law of Georgia "On Personal Data Protection" ("Powers of the Personal Data Protection Service in the field of data protection and control of the conduct of covert investigative actions"). It is identical to itself.

15 The minutes of the Constitutional Court of Georgia dated December 29, 2017. No. 3/4/885-1231.

16 Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chitidze, Lasha Tugushi, Zviad Koridze, Open Society Foundation Georgia ", AIP "Transparency International – Georgia", AIP "Young Lawyers Association of Georgia", AIP "International Society for Fair Elections and Democracy" and AIP "Human Rights Center" against the Parliament of Georgia", II-100.

17 The first law on personal data protection was adopted on 28.12.2011, and the new law on 14.06.2023, which came into effect on 01.03.2024, and after its implementation, the law of 28.12.2011 lost its force. Here, it should be noted that control over personal data processing has been implemented in Georgia since 2013. Since 2015, there has been direct supervision of covert investigative actions. In 2013-2019, the personal data protection inspector's office carried out the above-mentioned activities, in 2019-2022, its successor – the state inspector's office. From March 1, 2022, the said mandate was assigned to the Personal Data Protection Service.

18 Minutes of the Constitutional Court No. 3/4/885-1231 of December 29, 2017. II-84.

19 *Ibid*., II – 96.

20 Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chitidze, Lasha Tugushi, Zviad Koridze, "Open Society Foundation Georgia", "Transparency International – Georgia", "Young Lawyers Association of Georgia", "International Society for Fair Elections and Democracy" and "Human Rights Center" against the Parliament of Georgia", II-104.

Thus, the existing lever of inspection is still the bearer of the "random selection principle", which allows the possibility that during the operation of the mentioned control mechanism, the personal data protection service will completely detect and, therefore, eliminate violations of the law in relation to the issues within its competence.

In addition, since the so-called In the presence of threat of creating "alternative banks", it is possible to copy absolutely all the obtained information without any selection, it is interesting to see what changes the legislation has undergone in this regard after the implementation of the new law "On Personal Data Protection".

As mentioned in the explanatory note of the aforementioned law, the data "should be processed only to the extent necessary to achieve the relevant legal purpose". In addition, we read here that information can be stored "only for the period necessary to achieve the purpose of data processing". The explanatory note also emphasizes the importance of the safe storage of information and that appropriate measures should be taken to prevent "unauthorized or illegal" processing of data.[21] The above-mentioned goals, elaborated in the explanatory card, were formulated in the form of principles of data processing in Article 4 of the mentioned law.

However, on the part of the legislator, in terms of information storage and protection, despite the above-mentioned clear, obvious readiness to protect human rights, the mentioned approach has little effect on the storage period of information obtained from electronic communication through covert investigative actions. After the decision of the Constitutional Court, the period of storage of identifiable data of electronic communication was reduced from two years to 12 months.[22] Despite the mentioned change, there is no periodic verification of the above term. Accordingly, there is no provision in the legislation to determine whether the obtained information is still relevant to the case and whether there is a need to keep it. Thus, everything, including information not important to the case, can be stored for the period established by law, without any selection or justification. Thus, the current legislation "provides absolutely unlimited copying and storage of such information for a period of one year depending on the circle of persons and location.[23]

Based on all of the above, the danger of creating "alternative banks" is problematic in the sense that it is possible to store such information that is not important for the investigation, but in the absence of the law, it is not destroyed by the authorized persons.

3. COLLECTION OF DATA IN THE HANDS OF PROFESSIONALLY INTERESTED BODY

According to the Law of Georgia "About the Legal Entity of Public Law – Operative-Technical Agency of Georgia", the Operative-Technical Agency is a legal entity under public law responsible for the processing, storage, issuance and destruction of identifiable data of electronic communication.[24] Before the decision of the Constitutional Court of Georgia on April 14, 2016, the agency was represented as a department within the State Security Service. According to the position expressed by the witness at the mentioned session of the Constitutional Court, the transformation of the operational-technical department into a legal entity under public law was named as the only lever to prevent the creation of "alternative banks". In this case, the collection of obtained data in the hands of the professionally interested body, the State Security Service, of which the agency was an integral part, was excluded.

21 Parliament of Georgia. Explanatory card on the draft law "On personal data protection" <https://info.parliament.ge/file/1/BillReviewContent/222087> [Last accessed: April 15, 2024].

22 "On the Legal Entity of Public Law – Operational-Technical Agency of Georgia", Law of Georgia. Article 15. Legislative Gazette of Georgia <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [Last accessed: April 15, 2024].

23 Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chititdze, Lasha Tugushi, Zviad Koridze, "Open Society Foundation Georgia", "Transparency International – Georgia", "Young Lawyers Association of Georgia", "International Society for Fair Elections and Democracy" and "Center for Human Rights" against the Parliament of Georgia", II-91.

24 Article 15 of the Law of Georgia "On Legal Entity of Public Law – Operational-Technical Agency of Georgia".

After the formation of the mentioned approach of the Constitutional Court, regardless of the transformation of the operational-technical agency into a legal entity under public law, it should be noted that it is still subject to the "effective control" of the State Security Service.[25]

According to Article 3 of the Law of Georgia, "On Legal Entity of Public Law – Operative-Technical Agency of Georgia", the agency, as a legal entity of public law, is created in the system of the State Security Service and functions in this system as a part of a unified and centralized service. In particular:

- The head of the agency "will develop proposals for the agency's material and technical support and financing (including the agency's budget) and submit the relevant projects to the head of the service"[26].
- "Before submitting the statistical and generalized report of the agency's activities to the Prime Minister of Georgia, the head of the agency will submit this report to the head of the service".[27]
- The head of the State Security Service decides on the issues of establishing a special allowance and determining bonuses for the head of a legal entity under public law.[28]
- "The state control of the agency's activities is carried out by the head of the service".[29]

It should be emphasized that by the decision of the Constitutional Court of April 14, 2016, the Operational-Technical Department was considered a professionally interested body, not because this department directly had any kind of investigative function but due to the fact that it represented the State Security Service. The unit and the functions of the service made it an investigative function.[30] The Constitutional Court emphasized that "when the technical capabilities of direct and immediate access to personal information are at the disposal of the State Security Service (or another body with an investigative function), which, as we have already mentioned, immeasurably increases the risks of arbitrary, excessive interference with the right, it becomes objectively very difficult if not impossible, effective control of the authorities authorized to investigate"[31].

In the conditions of the current legal regulation, it is clear that the issue of the transformation of the mentioned department into a legal entity under public law is of a formal nature since the activity of the operational-technical agency depends on the decision taken by the head of the State Security Service, both in terms of financial and functional management.

The so-called possibility of creating "alternative banks" and collecting data in the hands of an interested body on a professional basis, according to the Constitutional Court, "both cumulatively and separately create a danger of excessive, groundless interference in a person's personal space, therefore, a violation of fundamental rights".[32]

Especially in circumstances where covert investigative actions are concerned, the risk of taking arbitrary action is obvious. In addition, since, in this case, we are talking about obtaining electronic evidence, the issue of authenticity of which is closely related to technological progress, the need for clear and detailed rules in this regard is even more evident.[33]

Since, both at the national and international level, great importance is attached to the inviolability of a person's intimate life, to personal connections with a certain circle of people with the intensity necessary for his personal perfection.[34],

25 The minutes of the Constitutional Court of Georgia dated December 29, 2017. No. 3/4/885-1231.

26 "On the Legal Entity of Public Law – Operational-Technical Agency of Georgia", Law of Georgia. Article 20, Paragraph 2. Legislative Gazette of Georgia <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [Last accessed: April 15, 2024].

27 *Ibid*. Article 29, Paragraph 2.

28 *Ibid*. Article 20, Paragraph 2, subsection 1.

29 *Ibid*. Article 29, Paragraph 1. Legislative Gazette of Georgia <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [Last accessed: April 15, 2024].

30 Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chitidze, Lasha Tughushi, Zviad Koridze, "Foundation Open Society Georgia", "Transparency International – Georgia", "Young Lawyers Association of Georgia", "International Society for Fair Elections and Democracy" and "Human Rights Center" against the Parliament of Georgia", II-55.

31 *Ibid*.

32 *Ibid*., II-95.

33 Decision of the European Court of Human Rights in the case: Kopp v. Switzerland (25.03.1998), §46.

34 Decision No. 2/1/536 of the Constitutional Court of Georgia dated February 4, 2014 in the case "Citizens of Georgia Levan Asatiani, Irakli Vacharadze, Levan Berianidze, Beka

It is necessary to have such a set of legal norms at the national level that will not create doubts about the disproportionate interference with the above-mentioned rights by unauthorized persons.

Thus, since the threats that have been discussed above can have a great impact on the freedom of human behavior, it is necessary to determine whether the current legal regulation in this regard leads to the limitation of such an important right as respect for private life.

4. THE ISSUE OF COMPLIANCE WITH THE RIGHT TO RESPECT FOR PRIVATE LIFE PROTECTED BY ARTICLE 8 OF THE EUROPEAN CONVENTION

It is interesting to see what approach the European Court of Human Rights takes in terms of the right to respect for private life and whether the criminal procedural legislation of Georgia in relation to the safe storage of identifiable data of electronic communication is consistent with the above-mentioned right protected by Article 8 of the European Convention.

The Strasbourg Court explains that the concept of private life is broad and cannot be subject to an exhaustive definition.[35] The concept of respect for private life includes the right to the free development of the individual, as well as the establishment of relationships with others.[36]

In the case of A v. France,[37] the French government argued that the recorded conversations related to the commission of the murder did not concern private life. The commission found the following: the fact that the conversation was a matter of public interest did not deprive it of its private character. The court shared the mentioned argument and explained that the collection of information about an individual without his consent by state officials always refers to a person's personal life and, therefore, falls within the scope of Article 8, Paragraph 1. In order to determine the compatibility of the issue of copying and storage of information obtained from electronic communication in criminal proceedings with the right to respect for private life protected by Article 8 of the European Convention, the following must be determined:

a) Was the restriction implemented in accordance with the law?

The approach of the European Court, according to which the existence of a norm at the legislative level does not mean that the restriction will be in accordance with the same law, is particularly interesting in terms of determining "compliance with the law". In the case of Bykov v. Russia [38] the European Court noted that for national legislation to comply with the "quality of law" requirement, the scope of discretion of the authorities must be taken into account. In addition, attention was drawn to the importance of the participation of an independent and impartial body and the fact that the involvement of an impartial body in the implementation of undercover investigative activities is important to the extent that, in this way, the individual will have an adequate means of protection against arbitrary interference.[39]

In addition, since "undercover surveillance or communication monitoring by government bodies does not produce public control regarding interference with the right,[40] "the law should exhaustively define the procedures for the investigation, use and storage of information obtained as a result of covert surveillance, as well as the procedures for transferring information obtained as a result of covert surveillance to third parties"[41]. The mentioned approach excludes "abuse or arbitrary use of authority by government bodies"[42].

Buchashvili and Gocha Gabodze against the Minister of Labor, Health and Social Protection of Georgia" II-55.

35 Decision of the European Court of Human Rights in the case: Costello-Roberts v. The United Kingdom (25.03.1993), §36.

36 Kilkelly U., The Right to Respect for Private and Family Life, Human Rights Implementation of Article 8 of the European Convention, Guide, (ed.), Council of Europe, Tb., 2005, p.14.

37 Decision of the European Court of Human Rights in the case: A v. France (07.04.2022).

38 Decision of the European Court of Human Rights in the case: Bykov v. Russia (10.03.2009).

39 Decision of the European Court of Human Rights in the case: Huvig v. France (24.04.1990), § 29; Decision of the European Court of Human Rights in the case: Amann v. Switzerland (16.02.2000), §56.

40 Decision of the European Court of Human Rights in the case: Klass and Others v. Germany (06.09.1978), §54-56.

41 Decision of the European Court of Human Rights in the case: Weber and Saravia v. Germany (29.06.2006), § 95.

42 Decision of the European Court of Human Rights in the

Accordingly, interference with the right to respect for private life is not "in accordance with the law" when the national legislation does not provide adequate protection of the applicant against the interference of law enforcement officers in the aforementioned right.[43]

b) Does the restriction serve a legitimate purpose?

Regarding the legal objective, the Strasbourg Court explains that the respondent state itself is obliged to determine the objectives of the legal restriction. In most cases, the court believes that the states are acting with a proper purpose, therefore, the claimant's request in this section is rarely granted.[44]

Even in the case discussed by us, there are such legitimate goals as ensuring the necessary state or public security in a democratic society, protecting the rights of others.[45] However, it is one thing to have said legal objectives and another question is whether the existing legislation is necessary to achieve these objectives in a democratic society.

c) Is it necessary in a democratic society?

Regarding digital data obtained through covert investigative action, the European Court of Human Rights explained that the power of secret surveillance under the European Convention is permissible only when it is strictly necessary to protect democratic institutions. However, the concept of necessity implies that the restriction must represent an urgent social necessity, in particular, it must be proportionate to the legitimate aim.[46].

In the case "Klass v. Germany",[47] German law allowed the opening of letters and wiretapping to protect national security and prevent disorder and crime. The system of state supervision of the implementation of the mentioned actions was carried out not in the court but in the Parliamentary Council, and the body called the G10 Commission, which was approved by the Council. The above-mentioned control system was acceptable to the European Court since both bodies were independent of the supervisory authorities and were given sufficient powers to carry out effective and continuous control. Accordingly, the Strasbourg Court did not find a violation of Article 8 of the European Convention in this case.

The above-mentioned decision is noteworthy in that the European Court here emphasized not only the importance of supervision by an independent body but also noted that judicial control or supervision in the implementation of the above-mentioned actions is desirable but not necessary. Therefore, it is important that the body, which will be equipped with supervisory functions, meets the standards of independence and impartiality. However, it should also be noted here that it would be inappropriate if this authority, without any criteria and in the form of unlimited discretion, is granted even to a judge.[48]

As for determining the appropriateness of storing and destroying the obtained information, in the case of Iodachi v. Moldova[49], the Moldovan legislation did not provide for the procedure for selecting secretly obtained information, which should be kept and which not, what procedure should be implemented in terms of protecting the confidentiality of said information and in what cases such information should be destroyed. The European Court found a violation of Article 8 of the European Convention in this case.

CONCLUSION

Based on all of the above, it can be said that the Criminal Procedure Legislation of Georgia cannot provide adequate protection of the right to respect for private life in the process of storing identifying data of electronic communication and,

case: Klass and Others v. Germany (06.09.1978), § 54-56.

43 Decision of the European Court of Human Rights in the case: Halford v. the United Kingdom (25.06.1997).

44 For example, The judgment of the European Court of Human Rights in Handyside v. the United Kingdom (07.12.1976).

45 Constitution of Georgia. Article 15, Paragraph 1. Legislative Gazette of Georgia. <https://matsne.gov.ge/ka/document/view/30346?publication=36> [Last accessed: April 15, 2024].

46 Decision of the European Court of Human Rights in the case: Olsson v. Sweden (24.03.1988).

47 Decision of the European Court of Human Rights in the case: Klass v. Germany (06.09.1978).

48 Decision of the European Court of Human Rights in the case: Silver and others v. the United Kingdom (25.03.1983).

49 Decision of the European Court of Human Rights in the case: Iodachi v. Moldova (10.02.2009).

therefore, in the presentation of digital evidence during the substantive consideration of the case in court. Despite the standards established by Strasbourg and the Constitutional Court, national legislation still has norms that contain threats to protecting the right. In particular, despite the change in legal form, the operational-technical agency, which collects the identifying data of electronic communication, is still under the authority of the professionally interested body – the State Security Service, which does not correspond to the practice established by the European Court of Human Rights. In addition, the system of supervision over the obtained information has some shortcomings, which creates the danger of creating an "alternative bank" and does not determine the possibility of selecting the data obtained through covert investigative actions based on the need, which also contradicts the right to respect for private life protected by the European Convention.

Under these conditions, if there are no clear and predictable rules that exclude the collection of such information in the hands of the professionally interested body, the issue of using the obtained data for other illegal purposes by unauthorized persons will become uncontrolled under the threat of creating an "alternative bank". It is clear that such threats will significantly damage the fundamental right of a person to respect for private life protected by the European Convention and the Constitution of Georgia, as well as the principles, goals and interests of criminal procedural law.

BIBLIOGRAPHY

Books:

1. Carrera S., Stefan M., Mitsilegas, V., (2020). Cross-border data access in criminal proceedings and the future of digital justice.
2. Casey, Digital Evidence and Computer Crime, 2004, p.12; The admissibility of electronic evidence in court: fighting against high-tech crime, 2005, Cybex, <http://www.cybex.es/agis2005/elegir_idioma_pdf.htm> [Last accessed: April 15, 2024]
3. Casey, Digital Evidence and Computer Crime, 2004, p.16; Vacca, Computer Forensics, Computer Crime Scene Investigation, Second Edition, 2005, p.39
4. Stephen M., Allison S., (2017). Electronic Evidence.
5. Spiegel Online, (08.01.2007). Fahnder überprüfen erstmals alle deutschen Kreditkarten
6. Kilkelly U., The Right to Respect for Private and Family Life, Human Rights Implementation of Article 8 of the European Convention, Guide, (ed.), Council of Europe, Tbilisi, 2005, 117-118.

Articles:

1. Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Volume 29, #1, 2004.

Normative materials:

1. Council of Europe Convention on Computer Crime (23.11.2001), Article 1 <https://rm.coe.int/16802fa423> [Last accessed: April 15, 2024].
2. "On Personal Data Protection" of December 28, 2011, which entered into force on 14.06.2023 N3144.
3. Parliament of Georgia. Explanatory card on the draft law "On personal data protection" <https://info.parliament.ge/file/1/BillReviewContent/222087> [Last accessed: April 15, 2024].
4. "On the Legal Entity of Public Law – Operational-Technical Agency of Georgia", Law of Georgia. Legislative Gazette of Georgia <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [Last accessed: April 15, 2024].

5. Constitution of Georgia. Legislative Gazette of Georgia. <https://matsne.gov.ge/ka/document/view/30346?publication=36> [Last accessed: April 15, 2024].

Court decisions:

1. Decision No. 1/1/625,640 of the Constitutional Court of Georgia dated April 14, 2016 in the case "Public Defender of Georgia, Citizens of Georgia – Giorgi Burjanadze, Lika Sajaia, Giorgi Gotsiridze, Tatia Kinkladze, Giorgi Chitidze, Lasha Tughushi, Zviad Koridze, "Open Foundation "Society Georgia", "Transparency International – Georgia", "Young Lawyers Association of Georgia", "International Society for Fair Elections and Democracy" and "Human Rights Center" against the Parliament of Georgia.
2. The minutes of the Constitutional Court of Georgia dated December 29, 2017. No. 3/4/885-1231.
3. Decision No. 2/1/536 of the Constitutional Court of Georgia dated February 4, 2014 in the case "Georgian citizens Levan Asatiani, Irakli Vacharadze, Levan Berianidze, Beka Buchashvili and Gocha Gabodze against the Minister of Labor, Health and Social Protection of Georgia", II-55.
4. The decision of the European Court of Human Rights in the case: Kopp v. Switzerland (25.03.1998).
5. Decision of the European Court of Human Rights in the case: Costello-Roberts v. The United Kingdom (25.03.1993).
6. Decision of the European Court of Human Rights in the case: A v. France (07.04.2022).
7. Decision of the European Court of Human Rights in the case: Bykov v. Russia (10.03.2008).
8. Decision of the European Court of Human Rights in the case: Huvig v. France (24.04.1990).
9. Decision of the European Court of Human Rights in the case: Amann v. Switzerland (16.02.2000).
10. Decision of the European Court of Human Rights in the case: Klass and Others v. Germany (06.09.1978).
11. Decision of the European Court of Human Rights in the case: Weber and Saravia v. Germany (29.06.2006).
12. Decision of the European Court of Human Rights in the case: Halford v. the United Kingdom (25.06.1997).
13. Decision of the European Court of Human Rights in the case: Handyside v. the United Kingdom (07.12.1976).
14. Decision of the European Court of Human Rights in the case: Olsson v. Sweden (24.03.1988).
15. Decision of the European Court of Human Rights in the case: Klass v. Germany (06.09.1978).
16. Decision of the European Court of Human Rights in the case: Silver and others v. the United Kingdom (25.03.1983).
17. Decision of the European Court of Human Rights in the case: Iodachi v. Moldova (10.02.2009).

Additional material:

1. Training of Judges on Computer Crime, (2010). France, Strasbourg <https://rm.coe.int/16802fa028> [Last accessed: April 15, 2024].

ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა კოპირებისა და შენახვის პრობლემა ქართულ სისხლის სამართლის პროცესში – ევროპული კონვენციის მე-8 მუხლთან მიმართებაში

დოდო ჯუღელი
სისხლის სამართლის მაგისტრი, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, საქართველოს პერსონალურ მონაცემთა დაცვის ოფიცერთა ასოციაცია, სსიპ შრომის ინსპექციის სამსახური, საქართველო

აბსტრაქტი

საქართველოს სისხლის სამართლის საპროცესო სამართლის მოქმედი კანონმდებლობით არსებული სტანდარტი, რომელიც ელექტრონული კომუნიკაციის საშუალებებიდან მოპოვებული ინფორმაციის უკანონოდ კოპირების საფრთხესთან ერთად ასეთი ინფორმაციის პროფესიულად დაინტერესებული ორგანოს ხელში თავმოყრას ითვალისწინებს, ბუნებრივია, დიდი გამოწვევაა სისხლის სამართლის საპროცესო კანონმდებლობისათვის. აღნიშნულის მიზეზს წარმოადგენს ის მნიშვნელოვანი გარემოება, რომ ამ გზით გამოძიების მიერ მოპოვებულ მონაცემთა გამოყენება ხდება ელექტრონული მტკიცებულების სახით, საქმის არსებითი განხილვის დროს სასამართლოში.

შესაბამისად, საქმე ეხება ინფორმაციას, რომელსაც "გონივრულ ეჭვს მიღმა სტანდარტით" სასამართლო უნდა დაეყრდნოს გადაწყვეტილების მიღებისას. ამდენად, ბრალდებულის ბედის გადაწყვეტისას განსაკუთრებით მნიშვნელოვანია, რომ არ არსებობდეს ეჭვები ასეთ მტკიცებულებათა კანონიერებას, უტყუარობასა და ხელშეუხებლობასთან დაკავშირებით. აღნიშნული საკითხი საყურადღებოა განსაკუთრებით იმ პირობებში, როდესაც ზემოხსენებული მიდგომა, ადამიანის უფლებათა ევროპული სასამართლო პრაქტიკის თანახმად, შეუსაბამოა ევროპული კონვენციის მე-8 მუხლით დაცული პირადი ცხოვრების პატივისცემის უფლებასთან.

საკვანძო სიტყვები: მტკიცებულება, შეზღუდვა, კოპირება, შენახვა

შესავალი

თემის აქტუალობა. საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობა ელექტრონულ მტკიცებულებათა მოპოვების, მათი შენახვისა და, შესაბამისად, საქმეზე დამაგრების კანონიერების მიზნებისთვის, ფარული საგამოძიებო მოქმედებების განხორციელებისთვის არსებული ნორმების გამოყენებაზე მიუთითებს, რაც, როგორც საკონსტიტუციო სასამართლო განმარტავს, ადამიანის უფლებებსა და თავისუფლებებში მომეტებული ინტენსივობით ჩარევის საფრთხის მატარებელია. ამასთან, არ წყდება საკონსტიტუციო სასამართლოსადმი მიმართვა, ფარული საგამოძიებო მოქმედებების განხორციელების შედეგად მოპოვებული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა კოპირებისა და შენახვის საკითხის საქართველოს კონსტიტუციასთან შესაბამისობასთან დაკავშირებით. აღნიშნულის თაობაზე აზრთა სხვადასხვაობაა თავად საკონსტიტუციო სასამართლოს მოსამართლეთა შორის, რომელთა ნაწილს ზემოხსენებული საკითხის მარეგულირებელი ნორმები საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625,640 გადაწყვეტილებით არაკონსტიტუციურად ცნობილი ნორმების „დამძლევ ნორმებად" მიაჩნია.

ამასთანავე, განსაკუთრებით აქტუალურია ამ კუთხით "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის ახალი რედაქცია, რომლითაც განისაზღვრა სტანდარტი პერსონალურ მონაცემთა დაცვის სფეროსა და ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის მიმართულებით. საინტერესოა, შეესაბამება თუ არა ახლახან განხორციელებული საკანონმდებლო ცვლილებები კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა კოპირებასა და შენახვასთან დაკავშირებით არსებულ საერთაშორისო მიდგომას.

ამდენად, სისხლის სამართლის პროცესში ზემოხსენებულ მონაცემთა კოპირებასა და შენახვასთან მიმართებით, ადამიანის უფლებათა და თავისუფლებათა დაცვის მიზნებისთვის, განსაკუთრებულად იკვეთება საკითხის სიღრმისეული კვლევის საჭიროება.

კვლევის საგანი. კვლევის საგანია ფარული საგამოძიებო მოქმედებების განხორციელების გზით მოპოვებული კომუნიკაციის მაიდენტიფიცირებელი მონაცემების შენახვასთან და კოპირებასთან დაკავშირებული გამოწვევები სისხლის სამართლის პროცესში, რომელთა გამოყენება ხდება ელექტრონული მტკიცებულების სახით საქმის არსებითი განხილვისას სასამართლოში.

კვლევის მიზანი და ამოცანები. კვლევის მიზანს სისხლის სამართლის პროცესში ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემებთა შენახვისას და კოპირებისას ცალკეულ სამართლებრივ პრობლემათა გამოკვეთა და ანალიზი წარმოადგენს. დასახული ამოცანის მიღწევა მოხდება როგორც ისტორიული წინამძღვრებისა და კონსტიტუციურ-სამართლებრივ ჭრილში საკითხის წარმოდგენით, ასევე, ადამიანის უფლებათა ევროპული სამართლის ნორმებისა და პრაქტიკის მოშველიებით.

კვლევის სიახლე. მეცნიერული კვლევის სიახლე გამოიხატება იმაში, რომ სტატიაში ჩამოყალიბებულია „ელექტრონული მტკიცებულების", როგორც კომუნიკაციის მაიდენტიფიცირებელი მონაცემის მოპოვების საბოლოო შედეგის, განმარტება, მისი ბუნება და განსხვავება ე. წ. „ტრადიციული" სახის მტკიცებულებებისაგან. ასევე, განხილული იქნება, საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625,640 გადაწყვეტილების მიღების შემდგომ განხორციელებული საკანონმდებლო ცვლილებების შინაარსი, თუ რამდენად არის იგი „არსებითი" მნიშვნელობის მქონე და კვლავ ხომ არ ქმნის პირადი ცხოვრების პატივისცემის უფლებაში ჩარევის საფრთხეს.

კვლევის ეტაპები. წინამდებარე სტატიის დასაწყისში წარმოდგენილია ელექტრონული მტკიცებულების არსი და განსაზღვრულია, თუ რა მიზანს ისახავს კომუნიკაციის მაიდენტიფიცირებელი მონაცემების მოპოვება. ძირითადი ნაწილი ეთმობა, ასევე, ქვეთავებს, რომლებიც ეხება ელექტრონული კომუნიკაციის საშუალებით გადაცემული ინფორმაციის შენახვასთან დაკავშირებით არსებულ სამართლებრივ საფრთხეებს, რაც მოქმედი კანონმდებლობის პირობებში იქმნება. კერძოდ, განხილულია მოპოვებული ინფორმაციის პროფესიულად დაინტერესებული ორგანოს ხელში თავმოყრისა და უკანონო კოპირების

(ე.წ. "ალტერნატიული ბანკის" შექმნა) საკითხი პირადი ცხოვრების პატივისცემის უფლებასთან მიმართებით. დასკვნაში წარმოდგენილია ავტორის შეხედულება და შეჯამება სტატიაში განხილულ პრობლემათა გადაწყვეტის მიზნით.

1. ელექტრონული მტკიცებულებისა და ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა არსი და ურთიერთმიმართება

XXI საუკუნეში განხორციელებულმა გლობალურმა ტექნოლოგიურმა პროგრესმა დიდი გარდატეხა შეიტანა საზოგადოებრივი ცხოვრების ყველა სფეროში. რამდენადაც გამარტივდა კომუნიკაცია, იმდენად დიდი გამოწვევების წინაშე დადგა თითოეული პიროვნება, სახელმწიფო თუ კერძო დაწესებულება ინფორმაციის დაცვის კუთხით. აღნიშნული პროგრესი შეეხო სისხლის სამართლის საპროცესო კანონმდებლობასაც, განსაკუთრებით, მტკიცებულებათა განვითარების თვალსაზრისით[1]. დანაშაულის ჩადენის პროცესში საგრძნობლად იმატა კომპიუტერული სისტემის გამოყენების მაჩვენებელმა. შესაბამისად, საკმაოდ აქტუალური გახდა ელექტრონული, ანუ ე. წ. „ციფრული" მტკიცებულებების გამოყენების საკითხი სისხლის სამართალწარმოებაში, რომელიც ახალი ტიპის მტკიცებულებად ჩამოყალიბდა[2].

ელექტრონულ მტკიცებულებას წარმოადგენს[3] ნებისმიერი მონაცემი, რომელიც ინახება ან რომლის გადაცემაც ხდება კომპიუტერული ტექნოლოგიის გამოყენებით და მხარს უჭერს თეორიას იმის შესახებ, თუ როგორ მოხდა დანაშაული.[4] „კომპიუტერული დანაშაულის შესახებ" ევროსაბჭოს კონვენციის 1-ლი მუხლის თანახმად, კომპიუტერულ სისტემაში იგულისხმება „ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელთაგან ერთი ან მეტი, პროგრამის მეშვეობით, ასრულებს მონაცემთა ავტომატურ დამუშავებას".[5] თავად კომპიუტერული მონაცემი კი არის „ფაქტების, ინფორმაციის ან კონცეფციათა ნებისმიერი გამოსახვა კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ფორმით, მათ შორის პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას".[6]

მიუხედავად იმისა, რომ ელექტრონულ მტკიცებულებას ე.წ. "ტრადიციული" მტკიცებულების მსგავსი მახასიათებლები აქვს, არსებობს მთელი რიგი ასპექტები, რომლებიც მას უნიკალურს ხდის.[7] პირველ რიგში, უნდა აღინიშნოს ციფრულ მონაცემთა "სიმყიფე"[8], რაც მას განსაკუთრებულად გამოარჩევს, მაგალითად, ქაღალდზე, მატერიალური სახით შექმნილი დოკუმენტისაგან. აღნიშნული გულისხმობს ელექტრონული კომუნიკაციის საშუალებიდან მოპოვებული ინფორმაციის ბუნებას, რომ იგი ადვილად შეიძლება წაიშალოს[9], შეიცვალოს და ა.შ. კიდევ ერთი მნიშვნელოვანი გარემოება მისი დეცენტრალიზებული შენახვაა. შესაძლებელია, ქვეყნის

1 Carrera S., Stefan M., Mitsilegas V., Cross-border data access in criminal proceedings and the future of digital justice, 2020, გვ. 1.

2 მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.75 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

3 საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში ელექტრონული მტკიცებულების, როგორც მტკიცებულების დამოუკიდებელი კატეგორიის განმარტებას არ ვხვდებით, მაგრამ აღნიშნული საკითხის მარეგულირებელი ნორმები ძირითადად წარმოადგენილია საქართველოს სისხლის სამართლის საპროცესო კოდექსში, „ოპერატიულ-სამძებრო საქმიანობის შესახებ" საქართველოს კანონში, „ელექტრონული კომუნიკაციების შესახებ" საქართველოს კანონში და სხვ.

4 Casey E., Digital Evidence and Computer Crime, 2004, გვ.12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005.

5 ევროპის საბჭოს კონვენცია „კომპიუტერული დანაშაულის შესახებ" (23.11.2001), მუხლი 1. <https://rm.coe.int/16802fa423> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

6 *იქვე.*

7 მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.76 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

8 Casey E., Digital Evidence and Computer Crime, 2004, გვ.16; Vacca, Computer Forensics, Computer Crime Scene Investigation, 2005.

9 Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, #1, 2004, გვ. 58.

საზღვრებს გარეთ შენახული ინფორმაცია დანაშაულის ჩამდენი პირების მიერ დისტანციურად იქნეს გამოყენებული,[10] რაც უფრო მეტად ართულებს გამოძიების პროცესს. ამდენად, ასეთ მონაცემთა მოპოვების, ელექტრონულ მტკიცებულებათა ბუნების სანდოობისა და ავთენტურობის საკითხის დადგენა საკმაოდ დიდი გამოწვევაა ყველა ქვეყნის სისხლის სამართლის საპროცესო კანონმდებლობისთვის.[11]

ამასთან, კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა – განმარტებით ანგარიშში (N187) მითითებულია, რომ კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ეფექტიანი მოპოვებისათვის საჭიროა დამატებითი პროცესუალური გარანტიები[12]. ამის რამდენიმე მიზეზი არსებობს. პირველი ის, რომ აღნიშნული ინფორმაცია არამატერიალური, ელექტრომაგნიტური ფორმითაა წარმოდგენილი. მეორე მიზეზს კი მისი შემხებლობის განსხვავებული სტანდარტი წარმოადგენს. კერძოდ, კომპიუტერული მონაცემი ვერ იქნება კონფისკირებული ან ჩამორთმეული ისე, როგორც ქაღალდზე ნაბეჭდი დოკუმენტი.

სწორედ გამოძიების მიერ მოპოვებულ, კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის პროცესუალურ გარანტიებთან დაკავშირებით იმსჯელა საქართველოს საკონსტიტუციო სასამართლომ 2016 წელს[13], რა დროსაც განსაზღვრა ის სტანდარტები, რომელიც სახელმწიფოს მიერ ელექტრონული კომუნიკაციის საშუალებიდან ინფორმაციის კოპირებისა და შენახვისას უნდა იქნეს გამოყენებული[14].

აღნიშნული გადაწყვეტილების საფუძველზე საქართველოს კანონმდებლობაში განხორციელდა გარკვეული ცვლილებები, რომელთა შინაარსის საქართველოს კონსტიტუციასთან შესაბამისობის საკითხმა აზრთა სხვადასხვაობა გამოიწვია თავად საკონსტიტუციო სასამართლოს მოსამართლეთა შორის[15].

აზრთა სხვადასხვაობის ერთ-ერთ მიზეზს თანამედროვე ელექტრონული კომუნიკაციის საშუალებებიდან ინფორმაციის კოპირებისა და შენახვის პრობლემა წარმოადგენდა. კერძოდ, საკონსტიტუციო სასამართლოს მოსამართლეთა ნაწილის მიერ ყურადღება იქნა გამახვილებული მოპოვებულ მონაცემთა პროფესიულად დაინტერესებული ორგანოს ხელში თავმოყრისა და ე.წ. "ალტერნატიული ბანკების" შექმნის საფრთხეებზე.

2. ე.წ. "ალტერნატიული ბანკების" შექმნის საფრთხე

როგორც საკონსტიტუციო სასამართლოს გადაწყვეტილებაშია ხაზგასმული, „ტექნიკურად შესაძლებელია, მაიდენტიფიცირებელი მონაცემის კოპირების და შენახვის პროცესში შეიქმნას ე.წ. „ალტერნატიული ბანკი", რომლის არსებობის შესახებ შესაძლოა არავინ იცოდეს და მასზე დაშვება არც პერსონალურ

10 მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.76 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

11 Stephen M., Allison S., Electronic Evidence, 2017, გვ. 193

12 ელექტრონულ მტკიცებულებათა "ახალი ტიპის" მტკიცებულებებად ჩამოყალიბების და კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა მოპოვების საკითხთან დაკავშირებით დამატებითი პროცესუალური ნორმების საჭიროების თვალსაჩინო მაგალითია გერმანიის სამართალდამცავთა მიერ რამდენიმე ათეული წლის წინათ ჩატარებული გამოძიება,, რა დროსაც საკრედიტო ბარათების გამცემი კომპანიების მეშვეობით დადგინდა იმ დამნაშავეთა ვინაობა, რომლებმაც შეიძინეს და ჩამოტვირთეს ბავშვთა პორნოგრაფია ერთ-ერთი ვებგვერდიდან (იხ., Spiegel Online, Fahnder überprüfen erstmals alle deutschen Kreditkarten,08.01.2007).

13 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ"

14 ციფრულ მტკიცებულებათა მოპოვება/შენახვა/განადგურება ხორციელდება ფარული საგამოძიებო მოქმედებებისთვის საკონსტიტუციო სასამართლოს მიერ დადგენილი სტანდარტით, ვინაიდან სისხლის სამართლის საპროცესო კანონმდებლობის თანახმად, კომპიუტერულ მონაცემთან დაკავშირებულ საგამოძიებო მოქმედებებზე ვრცელდება ფარული საგამოძიებო მოქმედებებისთვის დადგენილი წესები.

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

მონაცემთა დაცვის ინსპექტორს ჰქონდეს“[16]. აღნიშნული გულისხმობს ტოტალურ წვდომას გამოძიების მიერ მოპოვებულ ინფორმაციაზე, ყოველგვარი შინაარსობრივი გამიჯვნის გარეშე: ვინ სად, როდის, რა ტექნიკური საშუალებით, რომელი ლოკაციიდან და როგორი ხანგრძლივობით მოახდინა დაკავშირება.

უნდა აღინიშნოს ზედამხედველობის იმ მექანიზმებზე, რომელიც მოპოვებული ინფორმაციის კოპირების თავიდან აცილების მიზნებისთვის შეიქმნა. როგორც საკონსტიტუციო სასამართლომ აღნიშნა, “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონში[17] განხორციელებულ 2017 წლის 22 მარტის ცვლილებებს რაიმე ახლებური რეგულირება არ შემოუტანია ინსპექტორის მიერ მონაცემთა კოპირების პროცესის გაკონტროლების თვალსაზრისით.[18] დადებითი ნოვაცია იყო ის, რომ არსებული კონტროლის ერთ-ერთი ბერკეტი – ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის კონტროლის ელექტრონული სისტემა – ტექნიკური თვალსაზრისით უკვე გამართულ იქნა და მისი საშუალებით ინსპექტორს შეეძლო კოპირებულ მონაცემთა ბანკში განხორციელებული ქმედებების კონტროლი.[19] რაც შეეხება ელექტრონული კომუნიკაციის კომპანიებისგან სააგენტოს მიერ მონაცემთა კოპირების პროცესს, აღნიშნულზე ზედამხედველობის ერთადერთ ბერკეტს ინსპექტირება წარმოადგენდა. ზედამხედველობის ეს სახე საკონსტიტუციო სასამართლომ 2016 წლის 14 აპრილის გადაწყვეტილებით არაეფექტიანად მიიჩნია მისი განხორციელების მეთოდის გამო, რაც „შემთხვევითი შერჩევის პრინციპში“ მდგომარეობდა. აღნიშნული მიდგომა გამორიცხავს აბსოლუტურად ყველა მონაცემთა კონტროლის, შესაბამისად, აბსოლუტურად ყველა დარღვევის აღმოჩენის შესაძლებლობას, ხოლო ასეთმა “შერჩევითმა კონტროლმა, ფაქტობრივად, შეუძლებელია ხელშესახები შედეგები გამოიღოს“[20].

ზემოხსენებული საკითხის მარეგულირებელ ნორმებთან დაკავშირებით ხაზგასასმელია ის გარემოება, რომ “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მოქმედი რედაქცია მონაცემთა დაცვის სფეროსა და ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის სფეროსთან დაკავშირებით, კანონის წინა რედაქციისგან არსებითად განმასხვავებელ დანაწესებს არ ითვალისწინებს. კერძოდ, “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მოქმედი რედაქციის VII თავი ტექსტობრივად და, შესაბამისად, შინაარსობრივადაც “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის წინა რედაქციის V^2 (“პერსონალურ მონაცემთა დაცვის სამსახურის უფლებამოსილებები მონაცემთა დაცვის სფეროსა და ფარული საგამოძიებო მოქმედებების ჩატარების კონტროლის სფეროში”) თავის იდენტურია.

16 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-100.

17 საუბარია “პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს 2011 წლის 28 დეკემბრის კანონზე, რომელიც ძალადაკარულია – 14.06.2023 N3144. აქვე, უნდა აღინიშნოს, რომ პერსონალურ მონაცემთა დამუშავების საკითხზე კონტროლი საქართველოში 2013 წლიდან ხორციელდება.2015 წლიდან კი, ადგილი აქვს უშუალოდ ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობას. ზემოთხსენებულ საქმიანობას 2013-2019 წლებში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი ახორციელებდა, 2019-2022 წლებში მისი უფლებამონაცვლე – სახელმწიფო ინსპექტორის სამსხური. 2022 წლის 1 მარტიდან კი აღნიშნული მანდატი პერსონალურ მონაცემთა დაცვის სამსახურს მიენიჭა.

18 საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II – 84.

19 *იქვე*, II – 96

20 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-104.

ამდენად, ინსპექტირების არსებული ბერკეტი კვლავ "შემთხვევითი შერჩევის პრინციპის" მატარებელია, რაც უშვებს იმის ალბათობას, რომ კონტროლის აღნიშნული მექანიზმის მოქმედებისას იმთავითვე გამორიცხულია პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მის კომპეტენციას მიკუთვნებულ საკითხებთან დაკავშირებით კანონდარღვევათა სრულად აღმოჩენა და, შესაბამისად, აღმოფხვრაც.

ამასთან, ვინაიდან ე.წ. "ალტერნატიული ბანკების" შექმნის საფრთხის არსებობის პირობებში შესაძლებელია კოპირებულ იქნას აბსოლუტურად ყველა მოპოვებული ინფორმაცია ყოველგვარი გადარჩევის გარეშე, საინტერესოა, თუ რა ცვლილებები განიცადა ამ კუთხით კანონმდებლობამ "პერსონალურ მონაცემთა დაცვის შესახებ" ახალი კანონის ამოქმედების შემდგომ.

როგორც ზემოთ ხსენებული კანონის განმარტებით ბარათშია აღნიშნული, მონაცემები "უნდა დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად". ამასთან, აქვე ვკითხულობთ, რომ ინფორმაცია შესაძლებელია შენახულ იქნას "მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად". განმარტებით ბარათში, ასევე, ხაზგასმულია ინფორმაციის უსაფრთხო შენახვის მნიშვნელობა, რომ მიღებულ უნდა იქნას სათანადო ზომები მონაცემთა "უნებართვო ან უკანონო" დამუშავების თავიდან ასაცილებლად.[21] განმარტებითი ბარათში განსაზღვრული ზემოთ ხსენებული მიზნები აღნიშნული კანონის მე-4 მუხლში, მონაცემთა დამუშავების პრინციპების სახით იქნა ჩამოყალიბებული.

თუმცა, კანონმდებლის მხრიდან, ინფორმაციის შენახვისა და დაცვის კუთხით, ზემოთ ხსენებული, ადამიანის უფლებათა დაცვის მკაფიო, აშკარა მზადყოფნის მიუხედავად, აღნიშნული მიდგომა ნაკლებად შეეხო ფარული საგამოძიებო მოქმედებების გზით ელექტრონული კომუნიკაციის საშუალებიდან მოპოვებული ინფორმაციის შენახვის ვადას. საკონსტიტუციო სასამართლოს მიერ გადაწყვეტილების მიღების შემდეგ, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის ვადა ორი წლიდან 12 თვემდე შემცირდა[22]. მიუხედავად აღნიშნული ცვლილებისა, არ ხდება ზემოხსენებული ვადის პერიოდული გადამოწმება. შესაბამისად, არ არსებობს დანაწესი კანონმდებლობაში, რომელიც გაითვალისწინებს იმის დადგენას, კვლავ არის თუ არა მოპოვებული ინფორმაცია საქმისთვის მნიშვნელოვანი და არსებობს თუ არა მისი შენახვის საჭიროება. ამდენად, შეიძლება შენახულ იქნას ყველაფერი, მათ შორის, საქმისთვის მნიშვნელობის არმქონე ინფორმაცია, კანონით დადგენილი ვადით, ყოველგვარი გადარჩევისა და დასაბუთების გარეშე. ამდენად, მოქმედი კანონმდებლობა დღემდე ითვალისწინებს, აბსოლუტურად შეუზღუდავად, პირთა წრის და ლოკაციის მიხედვით ასეთი ინფორმაციის კოპირებასა და შენახვას[23] ერთი წლის ვადით.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, ე. წ. "ალტერნატიული ბანკების" შექმნის საფრთხე პრობლემურია, იმ კუთხითაც, რომ შესაძლებელია შენახულ იქნეს ისეთი ინფორმაცია, რომელიც გამოძიებისთვის არ იყოს მნიშვნელოვანი, მაგრამ კანონის დანაწესის არარსებობის პირობებში არ ნადგურდება საამისოდ უფლებამოსილ პირთა მიერ.

21 საქართველოს პარლამენტი. განმარტებითი ბარათი კანონპროექტზე "პერსონალურ მონაცემთა დაცვის შესახებ" <https://info.parliament.ge/file/1/BillReviewContent/222087> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

22 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 15. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

23 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ", II-91.

3. მონაცემთა პროფესიულად დაინტერესებული ორგანოს ხელში თავმოყრა

"საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ" საქართველოს კანონის თანახმად ოპერატიულ-ტექნიკური სააგენტო არის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა დამუშავებაზე, შენახვაზე, გაცემასა და განადგურებაზე პასუხისმგებელი საჯარო სამართლის იურიდიული პირი.[24] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილებამდე სააგენტო დეპარტამენტის სახით იყო წარმოდგენილი სახელმწიფო უსაფრთხოების სამსახურის შემადგენლობაში. საკონსტიტუციო სასამართლოს აღნიშნულ სხდომაზე მოწმის მიერ გაჟღერებული პოზიციით, "ალტერნატიული ბანკების" შექმნის თავიდან აცილების ერთადერთ ბერკეტად ოპერატიულ-ტექნიკური დეპარტამენტის საჯარო სამართლის იურიდიულ პირად გარდაქმნა დასახელდა. ამ შემთხვევაში გამოირიცხებოდა მოპოვებულ მონაცემთა თავმოყრა პროფესიულად დაინტერესებული ორგანოს – სახელმწიფო უსაფრთხოების სამსახურის ხელში, რომლის განუყოფელ ნაწილსაც სააგენტო წარმოადგენდა.

საკონსტიტუციო სასამართლოს აღნიშნული მიდგომის ჩამოყალიბების შემდეგ, ოპერატიულ-ტექნიკური სააგენტოს საჯარო სამართლის იურიდიულ პირად გარდაქმნის მიუხედავად, უნდა აღინიშნოს, რომ იგი შინაარსობრივად დღემდე სახელმწიფო უსაფრთხოების სამსახურის "ეფექტიან კონტროლს" არის დაქვემდებარებული.[25]

„საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ" საქართველოს კანონის მე-3 მუხლის თანახმად სააგენტო, როგორც საჯარო სამართლის იურიდიული პირი არის სახელმწიფო უსაფრთხოების სამსახურის სისტემაში შექმნილი და სწორედ ამ სისტემაში ფუნქციონირებს როგორც ერთიანი და ცენტრალიზებული სამსახურის ნაწილი. კერძოდ:

- სააგენტოს უფროსი „შეიმუშავებს წინადადებებს სააგენტოს მატერიალურ-ტექნიკური უზრუნველყოფისა და დაფინანსების (მათ შორის, სააგენტოს ბიუჯეტის) შესახებ და შესაბამის პროექტებს წარუდგენს სამსახურის უფროსს"[26].
- „სააგენტოს მიერ გაწეული საქმიანობის სტატისტიკური და განზოგადებული ანგარიშის საქართველოს პრემიერ-მინისტრისთვის წარდგენამდე სააგენტოს უფროსი ამ ანგარიშს წარუდგენს სამსახურის უფროსს".[27]
- სახელმწიფო უსაფრთხოების სამსახურის უფროსი წყვეტს შემავალი საჯარო სამართლის იურიდიული პირის ხელმძღვანელისთვის სპეციალური დანამატის დაწესებისა და პრემიების განსაზღვრის საკითხებს[28]
- „სააგენტოს საქმიანობის სახელმწიფო კონტროლს ახორციელებს სამსახურის უფროსი".[29]

ხაზი უნდა გაესვას იმ გარემოებას, რომ 2016 წლის 14 აპრილის საკონსტიტუციო სა-

24 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 15. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

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

26 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 20, პუნქტი 2. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

27 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 29, პუნქტი 2. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

28 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 20, პუნქტი 2, ქვეპუნქტი „ლ". საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

29 "საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ", საქართველოს კანონი. მუხლი 29, პუნქტი 1. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

სამართლოს გადაწყვეტილებით ოპერატიულ-ტექნიკური დეპარტამენტი პროფესიულად დაინტერესებულ ორგანოდ მიჩნეულ იქნა არა იმის გამო, რომ უშუალოდ ამ დეპარტამენტს გააჩნდა რაიმე სახის საგამოძიებო ფუნქცია, არამედ იმ გარემოებიდან გამომდინარე, რომ ის წარმოადგენდა სახელმწიფო უსაფრთხოების სამსახურის სფეროში არსებულ ერთეულს და სწორედ სამსახურის ფუნქციები აქცევდა მას გამოძიების ფუნქციის მქონედ.[30] საკონსტიტუციო სასამართლომ ხაზგასმით აღნიშნა, რომ „როდესაც პირად ინფორმაციაზე პირდაპირი და უშუალო წვდომის ტექნიკური შესაძლებლობები სახელმწიფო უსაფრთხოების სამსახურის (ან გამოძიების ფუნქციის მქონე სხვა ორგანოს) ხელთაა, რაც, როგორც უკვე აღვნიშნეთ, თავისთავად განუზომლად ზრდის უფლებაში თვითნებურად, გადამეტებულად ჩარევის რისკებს, ობიექტურად ძალიან რთული ხდება, თუ შეუძლებელი არა, გამოძიებაზე უფლებამოსილი ორგანოების ეფექტიანი კონტროლი"[31].

მოქმედი საკანონმდებლო რეგულაციის პირობებში, ნათელია, რომ აღნიშნული დეპარტამენტის საჯარო სამართლის იურიდიულ პირად გარდაქმნის საკითხი ფორმალური ხასიათის მატარებელია, ვინაიდან შინაარსობრივად ოპერატიულ-ტექნიკური სააგენტოს საქმიანობა როგორც საფინანსო, ისე ფუნქციური მმართველობის კუთხით სახელმწიფო უსაფრთხოების სამსახურის ხელმძღვანელის მიერ მიღებულ გადაწყვეტილებაზეა დამოკიდებული.

ე.წ. "ალტერნატიული ბანკების" შექმნისა და მონაცემების პროფესიული ნიშნით დაინტერესებული ორგანოს ხელში თავმოყრის შესაძლებლობა, საკონსტიტუციო სასამართლოს განმარტებით, "როგორც კუმულაციაში, ისე ცალ-ცალკე ქმნიან საფრთხეს ადამიანის პირად სივრცეში გადამეტებული, უსაფუძვლო ჩარევისთვის, შესაბამისად, ფუნდამენტური უფლებების დარღვევისთვის"[32].

განსაკუთრებით იმ პირობებში, როდესაც საქმე ეხება ფარულ საგამოძიებო მოქმედებებს, თვითნებურ ქმედებათა განხორციელების რისკი აშკარაა. ამასთანავე, ვინაიდან მოცემულ შემთხვევაში, საუბარია ელექტრონულ მტკიცებულებათა მოპოვებაზე, რომლის ავთენტურობის საკითხი მჭიდროდაა დაკავშირებული ტექნოლოგიურ პროგრესთან, კიდევ უფრო მეტად იკვეთება ამ კუთხით ნათელი და დეტალური წესების არსებობის საჭიროება[33].

ვინაიდან, როგორც ეროვნულ, ისე საერთაშორისო დონეზე დიდი მნიშვნელობა ენიჭება პიროვნების ინტიმური ცხოვრების ხელშეუვალობას, ადამიანთა გარკვეულ წრესთან პერსონალურ კავშირებს იმ ინტენსივობით, რაც აუცილებელია მისი პიროვნული სრულყოფისთვის[34], საჭიროა ეროვნულ დონეზე არსებობდეს ისეთ სამართლებრივ ნორმათა ერთობლიობა, რომელიც არ შექმნის ეჭვებს ზემოხსენებულ უფლებებში არაუფლებამოსილი პირების მიერ არაპროპორციული ჩარევის შესახებ.

ამდენად, ვინაიდან საფრთხეებმა, რომლებიც ზემოთ იქნა განხილული, დიდი გავლენა შეიძლება იქონიოს ადამიანის ქცევის თავისუფლებაზე, საჭიროა დადგინდეს – იწვევს თუ არა ამ კუთხით არსებული მოქმედი საკა-

30 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ", II-55.

31 საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ", II-55.

32 *იქვე*, II-95.

33 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Kopp v. Switzerland (25.03.1998), §46.

34 საქართველოს საკონსტიტუციო სასამართლოს 2014 წლის 4 თებერვლის №2/1/536 გადაწყვეტილება საქმეზე "საქართველოს მოქალაქეები ლევან ასათიანი, ირაკლი ვაჭარაძე, ლევან ბერიანიძე, ბექა ბუჩაშვილი და გოჩა გაბოძე საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის წინააღმდეგ" II-55.

ნონმდებლო რეგულაცია ისეთი მნიშვნელოვანი უფლების შეზღუდვას, როგორიცაა პირადი ცხოვრების პატივისცემა.

4. ევროპული კონვენციის მე-8 მუხლით დაცული პირადი ცხოვრების პატივისცემის უფლებასთან შესაბამისობის საკითხი

საინტერესოა, რა მიდგომას აყალიბებს პირადი ცხოვრების პატივისცემის უფლების კუთხით ადამიანის უფლებათა ევროპული სასამართლო და შეესაბამება თუ არა მოპოვებული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა უსაფრთხო შენახვასთან დაკავშირებით საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობა ევროპული კონვენციის მე-8 მუხლით დაცულ ზემოაღნიშნულ უფლებას.

სტრასბურგის სასამართლო განმარტავს, რომ პირადი ცხოვრების ცნება არის ფართო და არ შეიძლება ექვემდებარებოდეს ამომწურავ განმარტებას.[35] პირადი ცხოვრების პატივისცემის კონცეფცია მოიცავს პიროვნების თავისუფალი განვითარების უფლებას, ისევე როგორც ურთიერთობების დამყარებას სხვებთან.[36]

საქმეში A v. France[37] საფრანგეთის მთავრობა ამტკიცებდა, რომ ჩაწერილი საუბრები, რომლებიც დაკავშირებული იყო მკვლელობის ჩადენასთან, არ ეხებოდა პირად ცხოვრებას. კომისიამ დაადგინა შემდეგი: ის ფაქტი, რომ საუბარი წარმოადგენდა საზოგადოებრივი ინტერესის საგანს, არ უკარგავდა მას პირად ხასიათს. სასამართლომ აღნიშნული არგუმენტი გაიზიარა და განმარტა, რომ ინდივიდის თანხმობის გარეშე სახელმწიფო თანამდებობის პირთა მხრიდან მასზე ინფორმაციის შეგროვება ყოველთვის ეხება პირის პირად ცხოვრებას და, შესაბამისად, ხვდება მე-8 მუხლის 1-ლი პუნქტის მოქმედების ფარგლებში.

სისხლის სამართლის პროცესში ელექტრონული კომუნიკაციის საშუალებიდან მოპოვებული ინფორმაციის კოპირებისა და შენახვის საკითხის ევროპული კონვენციის მე-8 მუხლით დაცულ პირადი ცხოვრების პატივისცემის უფლებასთან შესაბამისობის განსაზღვრისთვის უნდა დადგინდეს შემდეგი:

ა) შეზღუდვა განხორციელდა თუ არა კანონის შესაბამისად?

"კანონის შესაბამისობის" დადგენის კუთხით განსაკუთრებით საინტერესოა ევროპული სასამართლოს მიდგომა, რომლის თანახმად, საკანონმდებლო დონეზე ნორმის არსებობა არ ნიშნავს იმას, რომ შეზღუდვა იმთავითვე კანონის შესაბამისი იქნება. საქმეში Bykov v. Russia [38] ევროპულმა სასამართლომ აღნიშნა, რომ იმისათვის, რათა ეროვნული კანონმდებლობა შეესაბამებოდეს „კანონის ხარისხის" მოთხოვნას, ის უნდა ითვალისწინებდეს ხელისუფლების ორგანოების დისკრეციის ფარგლებს. ამასთანავე, ყურადღება იქნა გამახვილებული დამოუკიდებელი და მიუკერძოებელი ორგანოს მონაწილეობის მნიშვნელობაზე და ხაზი გაესვა იმ გარემოებას, რომ ფარული საგამოძიებო მოქმედებების განხორციელებისას მიუკერძოებელი ორგანოს ჩართვა მნიშვნელოვანია იმდენად, რამდენადაც ამ გზით ინდივიდს ექნება ადეკვატური დაცვის საშუალება თვითნებური ჩარევისაგან[39].

ამასთან, ვინაიდან "ხელისუფლების ორგანოების მხრიდან ფარული თვალთვალის ან კომუნიკაციის მონიტორინგის განხორციელებისას არ წარმოებს უფლებაში ჩარევასთან დაკავშირებით საჯარო კონტროლი,[40]" "კანონი ამომწურავად უნდა განსაზღვრავდეს ფარული თვალთვალის შედეგად მოპოვებული ინფორ-

35 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Costello-Roberts v. The United Kingdom (25.03.1993), §36.

36 კილკელი უ., პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის განხორციელება, გზამკვლევი, ლ.ჭელიძის, ბ. ბოხაშვილის, თ. მამუკელაშვილის თარგმანი, ლ. ჭელიძის რედაქტორობით, ევროპის საბჭო, 2005, გვ.14.

37 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: A v. France (07.04.2022).

38 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Bykov v. Russia (10.03.2009).

39 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Huvig v. France (24.04.1990), § 29; ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Amann v. Switzerland (16.02.2000) §56.

40 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass and Others v. Germany (06.09.1978), §54-56.

მაციის გამოკვლევის, გამოყენებისა და შენახვის, ისევე როგორც ფარული თვალთვალის შედეგად მოპოვებული ინფორმაციის მესამე მხარისათვის გადაცემის პროცედურებს"[41]. აღნიშნული მიდგომა გამორიცხავს "ხელისუფლების ორგანოების მხრიდან უფლებამოსილების ბოროტად ან თვითნებურად"[42] გამოყენებას.

შესაბამისად, პირადი ცხოვრების პატივისცემის უფლებაში ჩარევა არ არის "კანონის შესაბამისი მაშინ", როდესაც ეროვნული კანონმდებლობით ზემოხსენებულ უფლებაში სამართალდამცავთა ჩარევისგან მომჩივნის ადეკვატური დაცვა არ არის უზრუნველყოფილი.[43]

ბ) შეზღუდვა შეესაბამება თუ არა კანონიერ მიზანს?

კანონიერ მიზანთან დაკავშირებით სტრასბურგის სასამართლო განმარტავს, რომ თავად მოპასუხე სახელმწიფოა ვალდებული განსაზღვროს კანონიერი შეზღუდვის მიზნები. უმრავლეს საქმეებში სასამართლოს მისაღებად მიაჩნია, რომ სახელმწიფოები სათანადო მიზნით მოქმედებენ, შესაბამისად, იშვიათად კმაყოფილდება ხოლმე მოსარჩელის მოთხოვნა ამ ნაწილში. [44]

ჩვენ მიერ განხილულ შემთხვევაშიც არსებობს ისეთი ლეგიტიმური მიზნები, როგორიცაა: დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფა, სხვათა უფლებების დაცვა.[45] თუმცა ერთია ხსენებული კანონიერი მიზნების არსებობა და მეორე საკითხია ის, არის თუ არა ამ მიზნების მისაღწევად არსებული კანონმდებლობა აუცილებელი დემოკრატიულ საზოგადოებაში.

გ) აუცილებელია თუ არა დემოკრატიულ საზოგადოებაში?

ფარული საგამოძიებო მოქმედების გზით მოპოვებულ ციფრულ მონაცემებთან დაკავშირებით ადამიანის უფლებათა ევროპულმა სასამართლომ განმარტა, რომ საიდუმლო მეთვალყურეობის უფლებამოსილება ევროპული კონვენციის თანახმად დასაშვებია მხოლოდ იმ შემთხვევაში, როდესაც იგი მკაცრად აუცილებელია დემოკრატიული ინსტიტუტების დაცვის მიზნით. ამასთან, აუცილებლობის ცნება გულისხმობს იმას, რომ შეზღუდვა უნდა წარმოადგენდეს გადაუდებელ სოციალურ აუცილებლობას, განსაკუთრებით პროპორციული უნდა იყოს კანონიერ მიზანთან [46].

საქმეში "Klass v. Germany"[47] გერმანიის კანონმდებლობა ეროვნული უშიშროების დაცვის, უწესრიგობისა და დანაშაულის თავიდან აცილების მიზნით უშვებდა წერილის გახსნასა და სატელეფონო მოსმენებს. აღნიშნულ ქმედებათა განხორციელების სახელმწიფო ზედამხედველობის სისტემა ხორციელდებოდა არა სასამართლოში, არამედ საპარლამენტო საბჭოში და ორგანოში, სახელწოდებით G10 კომისია, რომელიც საბჭომ დაამტკიცა. ევროპული სასამართლოსთვის მისაღები იყო ზემოხსენებული კონტროლის სისტემა, ვინაიდან ორივე ორგანო დამოუკიდებელი იყო მეთვალყურეობის განმახორციელებელი ორგანოებისგან და მინიჭებული ჰქონდა საკმარისი უფლებამოსილებები ეფექტიანი და განგრძობადი კონტროლის განსახორციელებლად. შესაბამისად, სტრასბურგის სასამართლომ მოცემულ საქმეში ევროპული კონვენციის მე-8 მუხლის დარღვევა არ დაადგინა.

საყურადღებოა ზემოხსენებული გადაწყვეტილება იმ კუთხითაც, რომ ევროპულმა სასამართლომ აქ ხაზი გაუსვა არა მარტო დამოუკიდებელი ორგანოს მხრიდან ზედამხედველობის განხორციელების მნიშვნელობაზე, არამედ, ასევე აღნიშნა, რომ სასამართლო კონტროლი თუ ზედამხედველობა ზემოხსენებულ ქმედებათა განხორციელებისას სასურველია, მაგრამ არა აუცილებელი. შესაბამისად, მთავარია ორგანო, რომელიც საზედამხედვე-

41 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Weber and Saravia v. Germany (29.06.2006), § 95.

42 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass and Others v. Germany (06.09.1978), §54-56.

43 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Halford v. the United Kingdom (25.06.1997).

44 მაგ., ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Handyside v. the United Kingdom (07.12.1976).

45 საქართველოს კონსტიტუცია. მუხლი 15, პუნქტი 1. საქართველოს საკანონმდებლო მაცნე. <https://matsne.gov.ge/ka/document/view/30346?publication=36> [ბოლო ნახვა: 15 აპრილი, 2024წ.].

46 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Olsson v. Sweden (24.03.1988).

47 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass v. Germany (06.09.1978).

ლო ფუნქციებით იქნება აღჭურვილი, აკმაყოფილებდეს დამოუკიდებლობისა და მიუკერძოებლობის სტანდარტებს. თუმცა, აქვე ისიც უნდა აღინიშნოს, რომ შეუსაბამო იქნება, თუ ეს უფლებამოსილება, რაიმე კრიტერიუმების გარეშე და შეუზღუდავი დისკრეციის სახით, მიენიჭება თუნდაც მოსამართლეს.[48]

რაც შეეხება მოპოვებული ინფორმაციის შენახვისა და განადგურების მიზანშეწონილობის საკითხის განსაზღვრას, საქმეში Iodachi v. Moldova[49], მოლდოვის კანონმდებლობა არ ითვალისწინებდა პროცედურას თუ რა წესით უნდა გადარჩეულიყო ფარულად მოპოვებული ინფორმაცია, რომელი უნდა შენახულიყო და რომელი არა, რა პროცედურა უნდა განხორციელებულიყო აღნიშნული ინფორმაციის კონფიდენციალურობის დაცვის კუთხით და რა შემთხვევაში უნდა განადგურებულიყო ასეთი ინფორმაცია. ევროპულმა სასამართლომ მოცემულ საქმეში ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა.

დასკვნა

ყოველივე ზემოაღნიშნულიდან გამომდინარე, შეიძლება ითქვას, რომ საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობა ვერ უზრუნველყოფს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა შენახვის პროცესში და, შესაბამისად, სასამართლოში საქმის არსებითი განხილვის დროს ციფრულ მტკიცებულებათა წარდგენისას პირადი ცხოვრების პატივისცემის უფლების ადეკვატურ დაცვას. სტრასბურგისა და საკონსტიტუციო სასამართლოს მიერ ჩამოყალიბებული სტანდარტის მიუხედავად, ეროვნულ კანონმდებლობაში კვლავ არსებობს ისეთი ნორმები, რომელიც შეიცავს საფრთხეებს აღნიშნული უფლების დაცვის კუთხით. კერძოდ, ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა მომპოვებელი – ოპერატიულ-ტექნიკური სააგენტო, სამართლებრივი ფორმის ცვლილების მიუხედავად, კვლავ პროფესიულად დაინტერესებული ორგანოს – სახელმწიფო უსაფრთხოების სამსახურის დაქვემდებარებაშია, რაც არ შეესაბამება ადამიანის უფლებათა ევროპული სასამართლოს მიერ ჩამოყალიბებულ პრაქტიკას. ამასთან, მოპოვებულ ინფორმაციაზე ზედამხედველობის სისტემას აქვს გარკვეული ხარვეზები, რომელიც ქმნის "ალტერნატიული ბანკის" შექმნის საფრთხეს და არ განსაზღვრავს ფარული საგამოძიებო მოქმედებების გზით მოპოვებულ მონაცემთა საჭიროების საფუძვლით გადარჩევის შესაძლებლობას, რაც ასევე, წინააღმდეგობაში მოდის ევროპული კონვენციით დაცულ პირადი ცხოვრების პატივისცემის უფლებასთან.

იმ პირობებში, თუკი არ იარსებებს ნათელი და განჭვრეტადი წესები, რომელიც გამორიცხავს პროფესიულად დაინტერესებული ორგანოს ხელში ასეთი ინფორმაციის თავმოყრას, "ალტერნატიული ბანკის" შექმნის საფრთხის პირობებში უკონტროლო გახდება მოპოვებულ მონაცემთა სხვა, არაკანონიერი მიზნებისთვის გამოყენების საკითხი საამისოდ არაუფლებამოსილ პირთა მიერ. ცალსახაა, რომ მსგავსი საფრთხეების არსებობა მნიშვნელოვნად დააზიანებს როგორც ევროპული კონვენციითა და საქართველოს კონსტიტუციით დაცულ ადამიანის ფუნდამენტურ – პირადი ცხოვრების პატივისცემის უფლებას, ისე, სისხლის სამართლის საპროცესო სამართლის პრინციპებს, მიზნებსა და ინტერესებს.

48 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Silver and others v. the United Kingdom (25.03.1983).

49 ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Iodachi v. Moldova (10.02.2009).

ბიბლიოგრაფია

1. Carrera S., Stefan M., Mitsilegas V., Cross-border data access in criminal proceedings and the future of digital justice, 2020, გვ. 1.
2. მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.75 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.].
3. საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში ელექტრონული მტკიცებულების, როგორც მტკიცებულების დამოუკიდებელი კატეგორიის განმარტებას არ ვხვდებით, მაგრამ აღნიშნული საკითხის მარეგულირებელი ნომები ძირითადად წარმოადგენილია საქართველოს სისხლის სამართლის საპროცესო კოდექსში, „ოპერატიულ-სამძებრო საქმიანობის შესახებ" საქართველოს კანონში, „ელექტრონული კომუნიკაციების შესახებ" საქართველოს კანონში და სხვ.
4. Casey E., Digital Evidence and Computer Crime, 2004, გვ.12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005.
5. ევროპის საბჭოს კონვენცია „კომპიუტერული დანაშაულის შესახებ" (23.11.2001), მუხლი 1. <https://rm.coe.int/16802fa423> [ბოლო ნახვა: 15 აპრილი, 2024წ.].
6. *იქვე.*მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.76 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.].Casey E., Digital Evidence and Computer Crime, 2004, გვ.16; Vacca, Computer Forensics, Computer Crime Scene Investigation, 2005. Moore, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, #1, 2004, გვ. 58.
7. მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, საფრანგეთი, სტრასბურგი, 2010 წ. გვ.76 <https://rm.coe.int/16802fa028> [ბოლო ნახვა: 15 აპრილი, 2024წ.]. Stephen M., Allison S., Electronic Evidence, 2017, გვ. 193
8. ელექტრონულ მტკიცებულებათა "ახალი ტიპის" მტკიცებულებებად ჩამოყალიბების და კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა მოპოვების საკითხთან დაკავშირებით დამატებითი პროცესუალური ნორმების საჭიროების თვალსაჩინო მაგალითია გერმანიის სამართალდამცავთა მიერ რამდენიმე ათეული წლის წინათ ჩატარებული გამოძიება,, რა დროსაც საკრედიტო ბარათების გამცემი კომპანიების მეშვეობით დადგინდა იმ დამნაშავეთა ვინაობა, რომლებმაც შეიძინეს და ჩამოტვირთეს ბავშვთა პორნოგრაფია ერთ-ერთი ვებ-გვერდიდან (იხ., Spiegel Online, Fahnder überprüfen erstmals alle deutschen Kreditkarten,08.01.2007).
9. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ"
10. ციფრულ მტკიცებულებათა მოპოვება/შენახვა/განადგურება ხორციელდება ფარული საგამოძიებო მოქმედებებისთვის საკონსტიტუციო სასამართლოს მიერ დადგენილი სტანდარტით, ვინაიდან სისხლის სამართლის საპროცესო კანონმდებლობის თანახმად, კომპიუტერულ მონაცემთან დაკავშირებულ საგამოძიებო მოქმედებებზე ვრცელდება ფარული საგამოძიებო მოქმედებებისთვის დადგენილი წესები. საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.
11. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო", ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო", ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია", ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება" და ააიპ „ადამიანის უფლებათა ცენტრი" საქართველოს პარლამენტის წინააღმდეგ, II-100
12. საუბარია "პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს 2011 წლის 28 დეკემბრის კანონზე, რომელიც ძალადაკარულია – 14.06.2023 N3144. აქვე, უნდა აღინიშნოს, რომ პერსონალურ

მონაცემთა დამუშავების საკითხზე კონტროლი საქართველოში 2013 წლიდან ხორციელდება. 2015 წლიდან კი, ადგილი აქვს უშუალოდ ფარულ საგამოძიებო მოქმედებებზე ზედამხედველობას. ზემოთხსენებულ საქმიანობას 2013-2019 წლებში პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი ახორციელებდა, 2019-2022 წლებში მისი უფლებამონაცვლე – სახელმწიფო ინსპექტორის სამსხური. 2022 წლის 1 მარტიდან კი აღნიშნული მანდატი პერსონალურ მონაცემთა დაცვის სამსახურს მიენიჭა.საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი, II – 84.*იქვე*, II – 96საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-104.

13. საქართველოს პარლამენტი. განმარტებითი ბარათი კანონპროექტზე “პერსონალურ მონაცემთა დაცვის შესახებ” <https://info.parliament.ge/file/1/BillReviewContent/222087> [ბოლო ნახვა: 15 აპრილი, 2024წ.]. “საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 15. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.]. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-91.
14. “საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 15. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 29 დეკემბრის №3/4/885-1231 საოქმო ჩანაწერი.
15. “საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 20, პუნქტი 2. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].
16. “საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 29, პუნქტი 2. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].“საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 20, პუნქტი 2, ქვეპუნქტი „ლ“. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.].
17. “საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ”, საქართველოს კანონი. მუხლი 29, პუნქტი 1. საქართველოს საკანონმდებლო მაცნე <https://matsne.gov.ge/ka/document/view/3625121?publication=0> [ბოლო ნახვა: 15 აპრილი, 2024წ.]. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-55.საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ“, II-55.*იქვე*, II-95.
18. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Kopp v. Switzerland (25.03.1998), §46.საქართველოს საკონსტიტუციო სასამართლოს 2014 წლის 4 თებერვლის №2/1/536

გადაწყვეტილება საქმეზე “საქართველოს მოქალაქეები ლევან ასათიანი, ირაკლი ვაჭარაძე, ლევან ბერიანიძე, ბექა ბუჩაშვილი და გოჩა გაბოძე საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის წინააღმდეგ” II-55.
19. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Costello-Roberts v. The United Kingdom (25.03.1993), §36.კილკელი უ.,პირადი და ოჯახური ცხოვრების პატივისცემის უფლება, ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის განხორციელება, გზამკვლევი, ლ. ჭელიძის, ბ. ბოხაშვილის, თ. მამუკელაშვილის თარგმანი, ლ. ჭელიძის რედაქტორობით, ევროპის საბჭო, 2005, გვ.14.
20. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: A v. France (07.04.2022).
21. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Bykov v. Russia (10.03.2009).
22. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Huvig v. France (24.04.1990), § 29; ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Amann v. Switzerland (16.02.2000) §56.
23. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass and Others v. Germany (06.09.1978), §54-56.
24. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Weber and Saravia v. Germany (29.06.2006), § 95.
25. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass and Others v. Germany (06.09.1978), §54-56.
26. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Halford v. the United Kingdom(25.06.1997). მაგ., ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Handyside v. the United Kingdom (07.12.1976).საქართველოს კონსტიტუცია. მუხლი 15, პუნქტი 1. საქართველოს საკანონმდებლო მაცნე. <https://matsne.gov.ge/ka/document/view/30346?publication=36 > [ბოლო ნახვა: 15 აპრილი, 2024წ.].
27. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Olsson v. Sweden (24.03.1988).
28. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Klass v. Germany (06.09.1978).
29. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Silver and others v. the United Kingdom (25.03.1983).
30. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე: Iodachi v. Moldova (10.02.2009).