ზურაბ ჩიტაშვილი

# ინფორმაციული უსაფრთხოების პოლიტიკის გავლენა საჯარო სექტორში პერსონალურ მონაცემთა დაცვის ხარისხზე

წარმოდგენილია საჯარო მმართველობის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

აღმოსავლეთ ევროპის უნივერსიტეტი
თბილისი, 0178, საქართველო
2019 წელი

აღმოსავლეთ ევროპის უნივერსიტეტი

იურიდიული ფაკულტეტი

ვადასტურებ, რომ გავეცანი ზურაბ ჩიტაშვილის მიერ შესრულებულ სამაგისტრო ნაშრომს დასახელებით: ,,ინფორმაციული უსაფრთხოების პოლიტიკის გავლენა საჯარო სექტორში პერსონალურ მონაცემთა დაცვის ხარისხზე“ და ვაძლევ რეკომენდაციას აღმოსავლეთ ევროპის უნივერსიტეტის იურიდიული ფაკულტეტის დასკვნითი გამოცდის/სამაგისტრო ნაშრომის დაცვის სპეციალური კომისიაში მის განხილვას საჯარო მმართველობის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი:  კახაბერ გოშაძე

თარიღი: 04.07.2019

# რეზიუმე

პერსონალურ მონაცემთა დაცვის უზრუნველყოფა ერთ-ერთ უმნიშვნელოვანეს ამოცანად რჩება თანამედროვე მსოფლიო საზოგადოებაში, რომლის შესახებ არაერთი კვლევაა ჩატარებული. განსაკუთრებით მნიშვნელოვანია ამ მიმართულებით საქართველოში არსებული ამჟამად არსებული პრობლემების გააზრება, რადგან აღნიშნული მიმართულებით საკანონმდებლო რეგულაციები სულ რამოდენიმე წელია ამოქმედდა.

განსაკუთრებით საყურადღებოა საჯარო სამსახურში პერსონალური მონაცემების დაცვის კუთხით ამჟამად არსებული მდგომარეობის შეფასება, განსახილველია რა განსაკუთრებულ მიდგომებს აწესებს კანონმდებლობა, როგორ მიმდინარეობს აღსრულება და რა გამოწვევების წინაშეა საჯარო სექტორი, რაც მომავალში გაუმჯობესებისაკენ გადასადგმელ ნაბიჯებს დაგვანახებს.

წინამდებარე ნაშრომის მიზანია გამოკვეთოს საჯარო სექტორში არსებული მდგომარეობა და ტენდენციები ინფორმაციული უსაფრთხოების კუთხით, მის პერსონალურ მონაცემთა დაცვის გავლენაზე აქცენტირებით.

ნაშრომი მოიცავს ამჟამად მოქმედი კანონმდებლობის ანალიზს, მისი აღსრულების მდგომარეობას და შემაფერხებელ გარემოებებს, სამეცნიერო ლიტერატურაზე დაყრდნობით მიმოხილულია რა არის საუკეთესო პრაქტიკა ამ მიმართულებით.

სრულად და ყოველმხრივ შესწავლის მიზნით მიმოიხილავს ასევე ანგარიშებს, კანონქვემდებარე ნორმატიულ აქტებს და მათ საფუძვლებს, ასევე ნაშრომში წარმოდგენილია პრობლემის გააზრება კონკრეტულ მტკიცებულებებსა და ფაქტობრივ მდგომარეობაზე დაყრდნობით, გამოკვლეულია კრიტიკული ინფორმაციული სისტემის სუბიექტების განხორციელებული აქტივობები ამ მიმართულებით და ამ სუბიექტების წილი საჯარო სექტორში.

ამასთან, ნაშრომი აანალიზებს საჯარო სამსახურში არსებულ პრობლემებს მონაცემთა უსაფრთხოების უზრუნველსაყოფად გადასადგმელი ნაბიჯების მიმართულებით.

# Abstract

Ensuring the protection of personal data remains one of the most important tasks in modern world society, since a number of studies are being conducted. It is especially important to understand the current problems that exist in Georgia in this direction, since legislative acts have been in force for several years.

It is especially important to assess the current situation in the field of personal data protection in the public service, which specific approaches the legislation implies, how the execution takes place and what tasks the public sector faces, which will show us steps for improvement in the future.

The purpose of this paper is to outline the current situation and trends in the public sector in terms of information security, paying particular attention to the impact of personal data protection.

The work includes an analysis of current legislation, the state of its implementation and circumstances based on scientific literature with an overview of what is best practiced in this direction.

In order to study it, it also considers reports, subordinate normative acts and their bases, and also studies the problem based on specific facts and actual circumstances, actions of the subjects of the critical information system in this direction and the share of these entities in the public sector.

Finally, the study analyzes the problems of public service in the direction of taking measures to ensure data security.

# შინაარსი

აბსტრაქტი ..... 3

Abstract .....

4

შესავალი .....7

ლიტერატურის მიმოხილვა .....10

**თავი I. პერსონალურ მონაცემთა დაცვის კონცეფცია და მიზანი** .....12

1. საქართველოში მოქმედი ძირითადი რეგულაციები პერსონალურ მონაცემთა დაცვის სფეროში და მათი გავრცელების არეალები .....12

1.1 თანამედროვე გამოწვევები პერსონალურ მონაცემთა დაცვის მიმართულებით .....16

1.2 მონაცემთა დაცვის ოფიცერი და მონაცემთა უსაფრთხოების მენეჯერი .....18

2. მონაცემთა დამუშავების პრინციპები და საფუძვლები, როგორც კონფიდენციალურობის განმაპირობებელი ფაქტორები .....

21

**თავი II. პერსონალურ მონაცემთა უსაფრთხოების სტანდარტების დანერგვა საჯარო სამსახურში** ..... 24

1. პერსონალურ მონაცემთა ორგანიზაციული და ტექნიკური
უსაფრთხოების სტანდარტების დაცვა, როგორც პრინციპი ..... 24
1.1 მონაცემთა უსაფრთხოების დანერგვის პროცესი ..... 28
1.2 პროპორციულობის პრინციპის დაცვა საჯარო სამსახურში
მონაცემთა დამუშავებისას ..... 30
**თავი III. კონფიდენციალურობა, როგორც პერსონალურ მონაცემთა კანონიერი დამუშავების გარანტია საჯარო სამსახურში** ..... 34
1. კონფიდენციალურობის უზრუნველყოფა მონაცემთა
დამუშავებაში ჩართული პირების მიერ ..... 34
2. მონაცემთა მიმართ შესრულებული ქმედებების
აღრიცხვა კრიტიკული ინფორმაციული სისტემის სუბიექტში ..... 35
3. მონაცემთა უსაფრთხოება საჯარო დაწესებულებათა
ვიდეოთვალთვალის დროს .....
38
4. პერსონალურ მონაცემთა დაცვის უზრუნველყოფა
საჯარო სამსახურში განსაკუთრებული კატეგორიის
მონაცემთა დამუშავებისას ..... 40
**თავი IV. პერსონალურ მონაცემთა კონფიდენციალურობის უზრუნველყოფის მექანიზმები** ..... 43
1. ინდივიდუალური ანალიზი მონაცემთა დამუშავებისას ..... 43
2. ინფორმაციული უსაფრთხოების მართვის სისტემის საფუძვლები
და მათი სახეები ..... 45
3. საფრთხეები მონაცემთა გასაჯაროების მნიშვნელოვანი
ლეგიტიმური მიზნების არსებობისას ..... 48
4. საჯარო ელექტრონული მონაცემთა ბაზები ..... 49
5. მონაცემთა შენახვის ვადები ..... 52
6. მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი
პროდუქტის ან მომსახურების შექმნის პროცესში

(„Data Protection by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Data Protection by Default“) ..... 55

**შედეგები და მათი განსჯა** ..... 58

**დასკვნა** ..... 60

გამოყენებული ლიტერატურა ..... 66

# შესავალი

სახელმწიფოში დემოკრატიის განვითარების გზაზე სასიცოცხლოდ მნიშვნელოვანია ადამიანის უფლებების დაცვა, სადაც გარდაუვლად მოიაზრება პერსონალურ მონაცემთა დაცვაც, როგორც თანამედროვე ტექნოლოგიური პროგრესიდან გამომდინარე გამოწვევა. ამ მხრივ განსაკუთრებით მნიშვნელოვანია საჯარო სექტორში ინფორმაციული უსაფრთხოების პოლიტიკის დანერგვა, რაც პირდაპირ კავშირშია პერსონალური მონაცემების დაცვასთან.

2012 წლის 5 ივნისს, საქართველოს პარლამენტმა მიიღო კანონი ,,ინფორმაციული უსაფრთხოების შესახებ“, რომლის მიზანია ,,ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დააწესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების სახელმწიფო კონტროლის მექანიზმები“[1].

კანონის მოქმედება გავრცელდა კრიტიკული ინფორმაციული სისტემის სუბიექტებზე, რომლის ნუსხა დამტკიცებულია საქართველოს მთავრობის დადგენილებით და აღნიშნულ სუბიექტებად განსაზღვრულია ის სახელმწიფო ორგანიზაციები, ,,რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის“[2].

აღნიშნული კანონის მიღებით საქართველომ კიდევ ერთი ნაბიჯი გადადგა ,,ერთის მხრივ, საქართველოსა და მეორეს მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის ასოცირების შესახებ“ შეთანხმებით დადგენილ სამართლებრივ პრინციპებთან თავსებადობის მიმართულებით. აღნიშნული შეთანხმებით განსაზღვრული ევროკავშირის, ევროპის საბჭოსა და საერთაშორისო

[1] ,,ინფორმაციული უსაფრთხოების შესახებ” საქართველოს კანონის პირველი მუხლი.
[2] იქვე, მუხ. 2.

სამართლებრივი დოკუმენტებისა და სტანდარტების დანერგვით, უზრუნველყოფილი უნდა იქნეს პერსონალურ მონაცემთა მაღალ დონეზე დაცვა, მათ შორისაა ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია, რომლის ერთ-ერთ მთავარ პრინციპს წარმოადგენს სწორედ ის, რომ ,,ავტომატიზირებულ ფაილებში შენახული მონაცემების დაცვის მიზნით, მიღებულ უნდა იქნას უსაფრთხოების შესაბამისი ზომები მათი შემთხვევითი თუ არასანქცირებული დარღვევის, შემთხვევითი დაკარგვის, ასევე მათთან არასანქცირებული შეღწევის, შეცვლის ან გავრცელების წინააღმდეგ“[3], რაც ასევე ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის ამოცანებში მოიაზრება.

ამრიგად, პერსონალურ მონაცემთა დაცვის სამართალში, ერთ-ერთ საკვანძო საკითხად განიხილება მონაცემთა უსაფრთხოება, რაც გულისხმობს მონაცემთა დამმუშავებელის ვალდებულებას ,,მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან“[4].

მით უფრო, მსოფლიოს თანამედროვე ცხოვრების პირობებში ერთ-ერთ მთავარ გამოწვევად რჩება ადამიანთა პერსონალური მონაცემების დაცვის უზრუნველყოფა, რადგან ტექნოლოგიების ელვის სისწრაფით განვითარების პირობებში, პერსონალური მონაცემების დაცვის გარანტიები სულ უფრო სუსტდება და ყოველი ახალი ტექნოლოგიის ბაზარზე შემოსვლისას, საჭიროა პერსონალურ მონაცემთა დაცვის მიმართულებით მასზე მორგებული მექანიზმების დროულად დანერგვა.

მიუხედავად კანონმდებლობის მკაფიო მიზნებისა და ამოცანებისა, მთავარ კითხვად რჩება, რამდენად ზედმიწევნით სრულდება საჯარო სექტორში კანონმდებლობის ნორმები ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით, რა გავლენა აქვს აღნიშნულს საჯარო ორგანიზაციაში დაცული

[3] ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენციის მე-7 მუხლი.

[4] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი.

პერსონალური მონაცემების უსაფრთხოებაზე, რამდენად ქმედითი და ეფექტურია ის მექანიზმები, რაც საჯარო სამსახურებში, მათ შორის კრიტიკული ინფორმაციული სისტემის სუბიექტებშია დანერგილი.

ამასთან, მნიშვნელოვანია გაანალიზებული იქნეს, რა ვალდებულებებს აწესებს პერსონალურ მონაცემთა დაცვის კანონმდებლობა, რას ადგენს იმპერატიულად, სად იძლევა ლავირების საშუალებას და სად გვევლინება ურთიერთგამომრიცხავი პრინციპები, რაც საშუალებას მოგვცემს ვიმსჯელოთ გასაუმჯობესებელ მხარეებზე.

წინამდებარე ნაშრომი ეხება სწორედ საჯარო სექტორში პერსონალური მონაცემების დაცვის საკითხს ინფორმაციული უსაფრთხოების სისტემის დანერგვის პროცესში, ვინაიდან ზემოხსენებული საკანონმდებლო ნორმებიდან გამომდინარე, საჯარო სექტორს უფრო მაღალი პასუხისმგებლობა აკისრია მონაცემთა უსაფრთხოების საკითხში, მით უფრო ყურადსაღებია ის ნიუანსები, გამოწვევები და პროცესების ელემენტები, რომლებიც ამ მიმართულებით ახლავს საჯარო სექტორს და მნიშვნელოვანია პრევენციული ღონისძიებების გატარების მიზნით განხორციელდეს რისკების იდენტიფიცირება, რაც მრავლადაა საკითხის მრავალმხრივობიდან და სიმძაფრიდან გამომდინარე. ნაშრომში კონკრეტული მაგალითების მოყვანით განხილულია, რა შეიძლება იყოს მიზეზი საჯარო სექტორში პერსონალურ მონაცემთა დაცვის ხარისხის დაქვეითებისა და რა შეიძლება წარმოადგენდეს პრევენციულ მექანიზმებს, პერსონალურ მონაცემთა დაცვის გარანტიების უზრუნველყოფის მიზნით.

ნაშრომი ეფუძნება პერსონალურ მონაცემთა დაცვის მიმართულებით არსებულ საერთაშორისო კვლევებს, ანგარიშებს, სამეცნიერო ლიტერატურას, სამართლებრივ ანალიზს და ამ მხრივ საჯარო დაწესებულებებში არსებულ ფაქტობრივ მტკიცებულებებს.

# ლიტერატურის მიმოხილვა

პერსონალურ მონაცემთა დაცვის ინსპექტორის ბოლო წლების ანგარიშები მრავლად მიუთითებს საჯარო სექტორში პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ პრობლემებზე და მათი აღმოფხვრის მექანიზმებზე. ვინაიდან პერსონალურ მონაცემთა დაცვის ინსპექტორი 2013 წლის აგვისტოდან ახორციელებს უფლებამოსილებებს, დღემდე წარმოდგენილია 6 წლიური ანგარიში, თუმცა წინამდებარე ნაშრომში ძირითადი აქცენტები გაკეთებულია ბოლო წლების ანგარიშებზე: <https://personaldata.ge/ka/about-us>.

მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის მხარდაჭერისათვის მონაცემთა გაცვლის სააგენტოს ფუნქციონირება, რომლის საქმიანობის საგანია სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული ტექნოლოგიების (სისტემების) და ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა. ამ მხრივ, გამოყენებულია ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და მისი ქვემდებარე საკანონმდებლო აქტები. ამასთან, ვინაიდან ნაშრომი ძირითადად ინფორმაციულ უსაფრთხოებასთან დაკავშირებული კანონმდებლობის ანალიზს მოიცავს, გამოყენებულია საქართველოს არაერთი საკანონმდებლო ნორმა ვებ გვერდიდან - <https://matsne.gov.ge/ka>.

მონაცემთა დაცვის ძირითადი ევროპული რეგულაცია (GDPR) მთავარი დოკუმენტია თანამედროვე სამყაროში პერსონალურ მონაცემთა დაცვის პრინციპების დანერგვის ასპექტში. მნიშვნელოვანია რეგულაციის განმარტებები (Recitals): <https://gdpr-info.eu/>.

ევროკავშირის მიერ აღიარებულ, სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) მონაცემთა უსაფრთხოების სტანდარტების ჯგუფს წარმოადგენს ISO270000, რომლის გავრცელება საქართველოს კრიტიკულ ინფორმაციულ სუბიექტებზე ერთ-ერთ უმთავრეს მიმართულებას წარმოადგენს მონაცემთა

დაცვის საქმეში. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>.

პერსონალურ მონაცემთა დაცვის პრობლემატური საკითხების მიმოხილვისა და მათი გადაჭრის გზების საუკეთესო გამოცდილების კუთხით გამოყენებულია სხვადასხვა მკვლევარის ნაშრომები: ,,Data science ethics in government", ,,The Digital Persona and Its Application to Data Surveillance", ,,Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", ,,Guidelines on the protection of personal data in IT governance and I management of EU institutions", ,,The Architecture of Privacy" და სხვა.

# თავი I. პერსონალურ მონაცემთა დაცვის კონცეფცია და მიზანი

## 1. საქართველოში მოქმედი ძირითადი რეგულაციები პერსონალურ მონაცემთა დაცვის სფეროში და მათი გავრცელების არეალები

ძირითადი საერთაშორისო სამართლებრივი დოკუმენტებით, როგორებიცაა ,,ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია“ და ,,გაეროს საერთაშორისო პაქტი სამოქალაქო და პოლიტიკურ უფლებათა შესახებ“, პირადი ცხოვრების პატივისცემის უფლება აღიარებულია როგორც ადამიანის ერთ-ერთი უმნიშვნელოვანესი და ფუნდამენტური უფლება, ადამიანის უფლებათა შორის, რაც ასევე დაცულია საქართველოს კონსტიტუციით[5].

თანამედროვე ცხოვრებაში, ადამიანის პერსონალური მონაცემები მუშავდება ადამიანის ყოფა-ცხოვრებისათვის აუცილებელი საჭიროებებისათვის, რასაც პერმანენტული ხასიათი აქვს და ყველასათვის მისაღები მოვლენაა, თუმცა აღნიშნული პროცესში არაკეთილსინდისიერმა ჩარევამ შესაძლებელია გამოიწვიოს ადამიანის ღირსებისა და პატივის შელახვა, მატერიალური თუ სხვა სახის ზიანი, ხოლო არაკეთილსინდისიერი ჩარევა შესაძლოა მოხდეს გარკვეული ანგარებიანი მიზნებისათვის, თუმცა ასევე შესაძლებელია არამიზნობრივი ჩარევა წარმოადგენდეს უბრალო შეცდომას[6].

აღნიშნულიდან გამომდინარე, ყველა დემოკრატიული სახელმწიფოს ამოცანაა ქვეყანაში შექმნას გარემო, სადაც ,,ადამიანთა პერსონალური მონაცემები დამუშავებული იქნება

[5] საქართველოს კონსტიტუციის მე-15 მუხლი.

[6] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2016, 69.

სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად, მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის, იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად, მონაცემები იქნება იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი, იქნება ნამდვილი, ზუსტი და განახლებადი, ხოლო უკანონოდ შეგროვებული და დამუშავების მიზნის შეუსაბამო მონაცემები დაიბლოკება, წაიშლება და განადგურდება. ასევე, შენახული იქნება მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად, ხოლო მიზნის მიღწევის შემდეგ დაიბლოკება, წაიშლება, განადგურდება ან შენახული იქნება პირის იდენტიფიცირების გამომრიცხავი ფორმით“[7].

ზემოაღნიშნული ფუნდამენტური მიზნის მისაღწევად, აუცილებელია ქვეყანაში შეიქმნას პერსონალურ მონაცემთა დაცვის ადეკვატური მარეგულირებელი ნორმები და მათი აღსრულების ეფექტური მექანიზმები.

2012 წლამდე საქართველოში არ არსებობდა სპეციალური კანონი პერსონალურ მონაცემთა დაცვის შესახებ და ამ მიმართულებით გარკვეული მარეგულირებელი მწირი ნორმები მიმოფანტული იყო სხვადასხვა საკანონმდებლო რეგულაციებში, ხოლო საჯარო სამსახურში პერსონალურ მონაცემთა დაცვის საკითხი ზოგადი ადმინისტრაციული კოდექსით შემოიფარგლებოდა, რომლის მიხედვითაც პერსონალური მონაცემების შემცველი ინფორმაცია წარმოადგენს საიდუმლო ინფორმაციას[8]. ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონმა ერთიან სივრცეში მოაქცია საჯარო და კერძო სექტორების საქმიანობა პერსონალური მონაცემების დამუშავების კუთხით, თუმცა ვინაიდან საჯარო სექტორს მოქალაქეთა ცხოვრებაში უფრო მაღალი პასუხისმგებლობა აკისრია მონაცემთა უსაფრთხოების მიმართულებით, ამჟამად, მრავალი სპეციალური საკანონმდებლო რეგულაცია მოქმედებს და მათი აღსრულება განსაკუთრებით მნიშვნელოვანია.

თუ ევროპულ საუკეთესო გამოცდილებას დავეყრდნობით, მონაცემთა დაცვის ძირითადი ევროპული რეგულაცია (GDPR)

[7] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი.

[8] იხ. <https://info.parliament.ge/file/1/BillReviewContent/63200> [25.06.2019]

აწესებს, რომ უახლესი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მოცულობის, კონტექსტისა და მიზნების, ასევე მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისათვის სავარაუდო რისკების გათვალისწინებით, მონაცემთა დამმუშავებელმა და უფლებამოსილმა პირმა უსაფრთხოების უზრუნველსაყოფად უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები, კერძოდ, მოახდინონ პერსონალურ მონაცემთა ფსევდონიმიზაცია და დაშიფვრა, დამუშავების სისტემებისა და სერვისების მუდმივი კონფიდენციალურობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა, ფიზიკური ან ტექნიკური ინციდენტის შემთხვევაში პერსონალურ მონაცემებთან წვდომისა და ხელმისაწვდომობის დროული აღდგენის შესაძლებლობა, დამუშავების უსაფრთხოების უზრუნველყოფის ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარული შემოწმება და შეფასება[9].

ამ მხრივ, საქართველოს კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ“ შემოიფარგლება დებულებით, რომ მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან[10], ხოლო აღნიშნული მიზნების შესასრულებლად საჭირო გასატარებელ კონკრეტულ ღონისძიებებს არ აწესებს, მაგალითად როგორიცაა ინფორმაციის დამმუშავებლის მიერ ,,დამუშავების უსაფრთხოების უზრუნველყოფის ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარული შემოწმება და შეფასება“ (GDPR).

თუმცა, მონაცემთა დაცვის მიმართულებით განსახორციელებელ კონკრეტულ ღონისძიებებსა და მექანიზმებს მოიცავს ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი და მისი ქვემდებარე ნორმატიული აქტები, რომლებიც ვრცელდება საქართველოს მთავრობის N312 დადგენილებით დამტკიცებულ კრიტიკული ინფორმაციული სისტემის სუბიექტებზე (ჯამში 40

[9] General Data Protection Regulation; May 25th, 2018; Article 32(1)

[10] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი.

სახელმწიფო ორგანიზაცია). მათ შორის არიან ის სახელმწიფო ორგანიზაციები, რომლებიც განსაკუთრებით მჭიდრო კავშირში არიან საზოგადოებრივ ცხოვრებასთან, კერძოდ, როგორიცაა შინაგან საქმეთა სამინისტრო, ქალაქ თბილისის მერია, საჯარო სამართლის იურიდიული პირი – სოციალური მომსახურების სააგენტო; საჯარო სამართლის იურიდიული პირი – შეფასებისა და გამოცდების ეროვნული ცენტრი; საჯარო სამართლის იურიდიული პირი – საჯარო რეესტრის ეროვნული სააგენტო, საჯარო სამართლის იურიდიული პირი – საქართველოს შინაგან საქმეთა სამინისტროს მომსახურების სააგენტო, საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი და სხვა. აღნიშნულ ორგანიზაციებზე ელვის სისწრაფით მოქმედებს ტექნოლოგიების განვითარება, რადგან მათი მუშაობა მთლიანად დაფუძნებულია მოცულობით მონაცემთა ბაზებზე და ამ პირობებში ერთ-ერთი მთავარი გამოწვევაა მონაცემთა უსაფრთხოების უზრუნველყოფისათვის ბრძოლა[11].

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მიხედვით, კრიტიკული ინფორმაციული სისტემის სუბიექტებში, ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს (კრიტიკული ინფორმაციული სისტემის სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით), რომლებსაც განსაზღვრავს სსიპ მონაცემთა გაცვლის სააგენტო[12] სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO)[13] და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA)[14] მიერ დადგენილი სტანდარტებისა და მოთხოვნების შესაბამისად.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მოთხოვნები ეფუძნება უსაფრთხოების სტანდარტს ISO 27001:2011[15].

---

[11] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 29.

[12] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-4 მუხლის მე-2 პუნქტი.

[13] იხ. <https://www.iso.org/about-us.html> [25.06.2019]

[14] იხ. <https://www.isaca.org/about-isaca/Pages/default.aspx> [25.06.2019]

[15] იხ. <https://www.iso.org/about-us.html> [25.06.2019]

კრიტიკული ინფორმაციული სისტემის სუბიექტებად განსაზღვრული სახელმწიფო ორგანიზაციები ვალდებულნი არიან მიიღონ ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები, რომლებიც ემსახურებიან ,,ინფორმაციული უსაფრთხოების შესახებ“ კანონის დებულებათა აღსრულებას და განსაზღვრავენ ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას, რაშიც დახმარებას უწევს საჯარო სამართლის იურიდიული პირი - მონაცემთა გაცვლის სააგენტო[16].

კრიტიკული ინფორმაციული სისტემის სუბიექტის თანხმობით, მონაცემთა გაცვლის სააგენტო ან მონაცემთა გაცვლის სააგენტოს მიერ ავტორიზებულ პირთაგან კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ შერჩეული პირი ან ორგანიზაცია ატარებს ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების, მონაცემთა გაცვლის სააგენტოს მიერ დადგენილ უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შეფასებას - ინფორმაციული უსაფრთხოების აუდიტს, რის შემდგომაც დგება დასკვნა და მისი მოთხოვნების შესრულება სავალდებულოა[17].

ამდენად, მონაცემთა დაცვის ევროპული რეგულაციის მოთხოვნებით (რომელიც საქართველოს საჯარო სექტორზე არ ვრცელდება), მონაცემთა დამმუშავებელი ვალდებულია მონაცემთა დამუშავების უსაფრთხოების უზრუნველსაყოფად მოახდინოს ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარული შემოწმება და შეფასება, ხოლო ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით კრიტიკული ინფორმაციული სისტემის სუბიექტი უფლებამოსილია და არა ვალდებული ჩაატაროს ინფორმაციული უსაფრთხოების აუდიტი.

ამასთან მნიშვნელოვანია აღინიშნოს, რომ ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონმდებლობა მხოლოდ 40 სახელმწიფო ორგანიზაციაზე ვრცელდება, რაც სახელმწიფო უწყებების დაახლოებით ერთი მეხუთედი ნაწილია[18], ხოლო

---

[16] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-4 მუხლი.

[17] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლი.

[18] საქართველოს მთავრობის დადგენილება №427 ,,საჯარო მმართველობის განხორციელების სტრატეგიული დოკუმენტების - „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020-ისა“ და „პოლიტიკის დაგეგმვის სისტემის რეფორმის სტრატეგია 2015-2017-ის“ დამტკიცების თაობაზე“, დანართი: „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020“ გვ.27

დანარჩენი სახელმწიფო ორგანიზაციებისათვის არ არის სავალდებულო ინფორმაციული უსაფრთხოების კანონმდებლობის გავრცელება[19].

## 1.1 თანამედროვე გამოწვევები პერსონალურ მონაცემთა დაცვის მიმართულებით

ევროკავშირის ქვეყნებისათვის, 2018 წლის 25 მაისიდან ამოქმედდა ევროპარლამენტისა და ევროსაბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 ,,პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“ (მონაცემთა დაცვის ძირითადი რეგულაცია (General Data Protection Regulation)), რომელმაც ჩაანაცვლა თანამედროვე ცხოვრებისათვის მოძველებული, 1995 წელს მიღებული მონაცემთა დაცვის დირექტივა (Data Protection Directive 95/46/ec).

მონაცემთა დაცვის ძირითადი რეგულაციის მიღების ერთ-ერთ მთავარ საფუძვლად დასახელდა სწრაფი ტექნოლოგიური განვითარება და გლობალიზაცია, რის გამოც წარმოიქმნა პერსონალური მონაცემების დაცვის ახალი გამოწვევები. პერსონალურ მონაცემთა შეგროვებისა და გაცვლის მასშტაბი მნიშვნელოვნად გაიზარდა. ტექნოლოგია, როგორც კერძო, ასევე საჯარო უწყებებს, თავისი საქმიანობის განხორციელებისას პერსონალური მონაცემების უპრეცენდენტო მასშტაბით გამოყენების შესაძლებლობებს აძლევს. ფიზიკური პირები თავის პერსონალურ მონაცემებს უფრო ხშირად ასაჯაროვებენ და გლობალურად ხელმისაწვდომს ხდიან. ტექნოლოგიამ გარდაქმნა როგორც ეკონომიკა, ისე საზოგადოებრივი ცხოვრება და მომავალში კიდევ უფრო გააადვილებს ინფორმაციის თავისუფალ მიმოცვლას ევროკავშირის შიგნით და მის მიღმა არსებულ ქვეყნებსა და საერთაშორისო ორგანიზაციებს შორის. ამავდროულად

[19] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-3 მუხლის მე-4 პუნქტი.

ტექნოლოგია პერსონალური მონაცემების დაცვის საშუალებებსაც იძლევა[20].

ვინაიდან სახელმწიფო სერვისების უდიდესი ნაწილი ელექტრონული ფორმით ხორციელდება, მონაცემების ელექტრონული სისტემების მეშვეობით დამუშავებისას, მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, შეაფასოს რისკები და მონაცემთა უსაფრთხოების დასაცავად მიიღოს შესაბამისი ორგანიზაციული და ტექნიკური ზომები[21].

## 1.2 მონაცემთა დაცვის ოფიცერი და მონაცემთა უსაფრთხოების მენეჯერი

მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით, მონაცემთა დამმუშავებელს და უფლებამოსილ პირს აქვთ ვალდებულება ორგანიზაციაში დანიშნონ მონაცემთა დაცვის ოფიცერი, იმ შემთხვევაში, თუ მონაცემთა დამმუშავებელი არის სახელმწიფო უწყება, გარდა სასამართლოებისა, რომლებიც მოქმედებენ სასამართლო კომპეტენციის ფარგლებში, ასევე, როდესაც მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითადი საქმიანობა, რომელიც თავისი ხასიათით, მასშტაბითა და/ან მიზნებით მოიცავს მონაცემთა სუბიექტების რეგულარულ და სისტემატურ მონიტორინგს ფართო მასშტაბებით, ან მონაცემთა დამმუშავებლის ან უფლებამოსილი პირის ძირითად საქმიანობას წარმოადგენს განსაკუთრებული კატეგორიის მონაცემთა ფართო მასშტაბით დამუშავება[22].

მონაცემთა დაცვის ოფიცერის ფუნქციები მოიცავს მონაცემთა დამმუშავებლის ან უფლებამოსილი პირისათვის, ასევე დამუშავების

[20] იხ. <https://gdpr-info.eu/recitals/no-6/> [25.06.2019]

[21] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 23.

[22] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 37(1).

პროცესში ჩართული თანამშრომლებისთვის მონაცემთა დამუშავებასთან დაკავშირებული კანონმდებლობით დადგენილი ვალდებულებების გაცნობას და რჩევების მიცემას, ევროკავშირის და წევრი სახელმწიფოების პერსონალურ მონაცემთა დაცვის კანონმდებლობის მონაცემთა დამმუშავებლის/ უფლებამოსილი პირის შიდა რეგულაციების შესრულების მონიტორინგს, პასუხისმგებლობის გადანაწილების, ცნობიერების ამაღლების, მონაცემთა დამუშავებაში ჩართული თანამშრომლების გადამზადების და ასევე შესაბამისი აუდიტის მეშვეობით. მოთხოვნის შემთხვევაში ახორციელებს მონაცემთა დაცვის რისკების შეფასებასთან დაკავშირებული რჩევის გაცემას და მისი შესრულების მონიტორინგს, პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოსთან თანამშრომლობას, საზედამხედველო ორგანოსთან მიმართებაში მთავარი საკონტაქტო პირის ფუნქციის შესრულებას მონაცემთა დამუშავების საკითხებზე, ასევე წინასწარი კონსულტაციისას, საჭიროების შემთხვევაში კონსულტაციების გავლას სხვა საკითხებთან დაკავშირებით. ამ ფუნქციების შესრულებისას მონაცემთა დაცვის ოფიცერი სათანადო ყურადღებას აქცევს დამუშავებასთან დაკავშირებულ რისკებს, დამუშავების ხასიათის, ფარგლების, კონტექსტის და მიზნების გათვალისწინებით[23].

საქართველოს კანონმდებლობაში მონაცემთა დაცვის ოფიცერის მსგავსი ინსტიტუტი ჩამოყალიბებულია ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით, რომლის მიხედვით, კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს ინფორმაციული უსაფრთხოების მენეჯერი კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის[24]. ინფორმაციული უსაფრთხოების მენეჯერის შესარჩევად კი განსაზღვრულია კრიტერიუმები, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის №4 ბრძანებით[25], თუმცა როგორც ზემოთ აღინიშნა, აღნიშნული რეგულაციები სავალდებულოდ ვრცელდება საჯარო

[23] იქვე, მუხლი 39.

[24] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-7 მუხლი.

[25] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის №4 ბრძანება ,,კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“.

უწყებების მცირე (40 სუბიექტი) ჩამონათვალზე და უცნობია რამდენად ხორციელდება ამ უწყებებში ინფორმაციული უსაფრთხოების მენეჯერის ინსტიტუტის დანერგვა.

მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით, მონაცემთა დაცვის ოფიცერს შეუძლია შეითავსოს სხვა ფუნქციები და მოვალეობები, თუმცა მონაცემთა დამმუშავებელმა ან უფლებამოსილმა პირმა უნდა უზრუნველყონ ინტერესთა კონფლიქტის თავიდან აცილება[26].

ინტერესთა კონფლიქტის თავიდან ასაცილებლად, მონაცემთა დაცვის ოფიცერს არ შეუძლია იმავე ორგანიზაციაში დაიკავოს ისეთი პოზიცია, რომლის ფუნქციებშიცაა პერსონალური მონაცემების დაცვის მექანიზმების შემუშავება. ასეთი პოზიციები შესაძლებელია იყოს მაღალი მენეჯერული თანამდებობები, მაგალითად ადამიანური რესურსების, ინფორმაციული ტექნოლოგიების, ლოჯისტიკის, საფინანსო ან სხვა სამსახურის ხელმძღვანელის თანამდებობები მისი ფუნქციებიდან გამომდინარე[27].

მონაცემთა დაცვის ძირითადი რეგულაციით, მონაცემთა დამმუშავებლის და უფლებამოსილი პირის მიერ, რეგულაციასთან შესაბამისობის დემონსტრირების უზრუნველსაყოფად, წევრმა სახელმწიფოებმა, საზედამხედველო ორგანომ, საბჭომ და ევროკომისიამ, ევროკავშირის დონეზე უნდა წაახალისონ მონაცემთა დაცვის სერტიფიცირების მექანიზმის და მონაცემთა დაცვის ბეჭდისა და ნიშნების მიღება[28]. სერტიფიცირება ნებაყოფლობითია და ხელმისაწვდომია გამჭვირვალე პროცესის საშუალებით[29]. უფლებამოსილების მინიჭება ხორციელდება EN-ISO/IEC 17065/2012 სტანდარტის შესაბამისად[30]. თუმცა უსაფრთხოების სტანდარტების დანერგვა (სერტიფიცირება) არ ამცირებს დამმუშავებლის ან

[26] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 38(6).

[27] A Closer Look At Data Protection Officer; Information commissioner; September 2017 V1; (12). იხ. <https://www.inforights.im/media/1416/dpo.pdf > [25.06.2019]

[28] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 42(1).

[29] იქვე, მუხლი 42(3).

[30] იქვე, მუხლი 43(1).

უფლებამოსილი პირის რეგულაციასთან შესაბამისობის პასუხისმგებლობას[31].

ორგანიზაციაში მონაცემთა დაცვის ძირითადი რეგულაციით გათვალისწინებული მონაცემთა უსაფრთხოების სტანდარტის დანერგვის შემთხვევაში, მონაცემთა დაცვის ოფიცერთან ერთად ინფორმაციული უსაფრთხოების დაცვის მიმართულებით განსაზღვრული იქნება ასევე ინფორმაციული უსაფრთხოების მენეჯერის პოზიცია, რაც უმაღლეს სტანდარტებზე აყენებს ორგანიზაციის ინფორმაციული უსაფრთხოების გარემოს.

ამდენად, მონაცემთა უსაფრთხოების სტანდარტების დანერგვა საჯარო სამსახურებში, ყველაზე საუკეთესო გზაა მონაცემთა დაცვის თვალსაზრისით, რაც ქვეყანაში ადამიანის უფლებების დაცვის მდგომარეობას ერთიორად გააუმჯობესებს.

2019 წლის 22 მაისს სახელმწიფო ინსპექტორის სამსახურის ინიციატივით, საქართველოს პარლამენტში შეტანილი იქნა კანონპროექტი ,,პერსონალურ მონაცემთა დაცვის შესახებ“[32], რომელიც მიზნად ისახავს პერსონალურ მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოებას, საქართველოს მიერ საერთაშორისო ვალდებულებების შესრულებასა და საერთაშორისოდ აღიარებული პრინციპებისა და საუკეთესო პრაქტიკის დამკვიდრებას[33].

აღნიშნული კანონპროექტის ამოცანად დასახელდა ევროპის პარლამენტისა და საბჭოს მიერ მიღებულ 2016/679(GDPR) მონაცემთა დაცვის ძირითად რეგულაციასთან და ევროკავშირის კანონმდებლობასთან ჰარმონიზაცია, ახალი დემოკრატიული სტანდარტების იმპლემენტაცია ეროვნულ კანონმდებლობაში, მათ შორის მონაცემთა დაცვის ოფიცერის ინსტიტუტის დანერგვა იმ დაწესებულებებში რომელიც მომსახურებას უწევს წელიწადში არანაკლებ 10000 მონაცემთა სუბიექტს, ასევე, ის მონაცემთა დამმუშავებელი/უფლებამოსილი პირი, რომელიც ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს[34].

---

[31] იქვე, მუხლი 42(4).

[32] იხ. <https://info.parliament.ge/#law-drafting/18184> [25.06.2019]

[33] იხ. <https://info.parliament.ge/file/1/BillReviewContent/222087?> [25.06.2019]

[34] იქვე, გვ.2

პერსონალურ მონაცემთა დაცვის ოფიცერის ინსტიტუტის საქართველოს კანონმდებლობაში დანერგვა ხელს შეუწყობს ინფორმაციული უსაფრთხოების საერთაშორისოდ აღიარებული სტანდარტების მსგავსი მექანიზმების დანერგვას, რაც ცალსახად წინგადადგმული ნაბიჯი იქნება საქართველოში პერსონალურ მონაცემთა დაცვის ხარისხის ამაღლების კუთხით, თუმცა გამოწვევები ამ მიმართულებით კვლავ უამრავია და ტექნოლოგიების განვითარებასთან ერთად პრობლემური საკითხები მომავალშიც მრავლად წამოიჭრება, მონაცემთა უსაფრთხოების მაღალი სენსიტიური ხასიათიდან გამომდინარე.

## 2. მონაცემთა დამუშავების პრინციპები და საფუძვლები, როგორც კონფიდენციალურობის განმაპირობებელი ფაქტორები

საქართველოს კანონმდებლობით, მონაცემთა დამუშავების პრინციპები და საფუძვლები ემსახურება მთავარ მიზანს, რომ მონაცემების დამუშავებისას აღმატებულ ხარისხზე იქნეს აყვანილი მონაცემთა სუბიექტის კანონიერი ინტერესები, რისი მიღწევაც კონფიდენციალურობის მკაცრი დაცვითაა შესაძლებელი.

მონაცემთა კონფიდენციალურობის სათანადო დონის უზრუნველყოფად შესაძლებელია ჩაითვალოს ვითარება, როდესაც მონაცემები მუშავდება მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის, მუშავდება მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად, დამუშავება ხორციელდება სათანადო ტექნიკურ-ორგანიზაციული მექანიზმების პირობებში და მიზნის მიღწევის შემდგომ წაიშლება ან ინახება პირის იდენტიფიცირების გამომრიცხავი ფორმით[35].

აღნიშნული დებულებებიდან ერთ-ერთის შელახვის შემთხვევაში მწვავედ დგება რისკის ქვეშ მონაცემთა კონფიდენციალურობის საკითხი.

როგორც ზემოთ აღინიშნა, ტექნოლოგიების განვითარება წარმოშობს ახალ რისკებს პერსონალურ მონაცემთა დაცვის

[35] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი.

უზრუნველყოფის საქმეში. ჯერ კიდევ ათიოდე წლის წინ ამერიკელი ადვოკატი და მკვლევარი - ლოურენს ლესიგი აცხადებდა, რომ მონაცემთა დაცვის უზრუნველსაყოფად ყველაზე მიზანშეწონილი ინფორმაციის კოდირებაა („Encryption“). ამ სისტემის მეშვეობით ინდივიდებს საშუალება ეძლევათ ეფექტურად დამალონ ფაქტები საკუთარი თავის შესახებ, რომელთა გახმაურებაც მათ არ სურთ. მაგრამ კოდირების მეშვეობით არ იმალება, მაგალითად, მონაცემები ტრანსზაქციების შესახებ, ტელეფონით საუბრის ხანგრძლივობა და სხვა. ცხადია, კოდირებით ასევე არ იმალება მესამე პირების მიერ ჩვენს შესახებ შექმნილი პერსონალური მონაცემებიც. უფრო მეტიც, კოდირების მეშვეობით იზრდება მონიტორინგისა და ძიების ტექნოლოგიები, რადგან კოდირების მეშვეობით იმალება როგორც გარკვეული მონაცემები პირის შესახებ, ასევე შესაძლებელია პირის იდენტიფიკაციაც. საერთო ჯამში კოდირების ტექნოლოგიები გაზრდის პირადი მონაცემების დაცვის ხარისხს[36].

მონაცემთა დაცვის ძირითადი რეგულაციით მნიშვნელოვანი ყურადღება დაეთმო მონაცემთა ფსევდონიმიზაციას, რაც გულისხმობს პერსონალური მონაცემების იმგვარ დამუშავებას, როდესაც დამატებითი ინფორმაციის გამოყენების გარეშე შეუძლებელია პერსონალური მონაცემების დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან, იმ პირობით, რომ ეს დამატებითი ინფორმაცია შენახულია ცალკე და ტექნიკური და ორგანიზაციული ზომების მეშვეობით მონაცემების დაკავშირება არ ხდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან[37].

ფსევდონიმიზაციის გამოყენების შემთხვევაში დამმუშავებელი თავისუფლდება ამავე რეგულაციით განსაზღვრული ვალდებულებისაგან, უსაფრთხოების დარღვევის მაღალი რისკის თაობაზე შეატყობინონ მონაცემთა დაცვის ორგანოს და მონაცემთა სუბიექტს, რაც ფსევდონიმიზაციის განსაკუთრებულ მნიშვნელობაზე მეტყველებს[38].

საქართველოს კანონმდებლობაში, ფსევდონიმიზაციის მსგავსი რეგულირება წარმოდგენილია დეპერსონალიზაციის სახით, რაც

---

[36] Lessig L., The Architecture of Privacy, 1998, 15,16.

[37] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 4(5).

[38] იქვე, მუხლი 32(1a); 33(1); 34(1).

გულისხმობს მონაცემთა იმგვარ მოდიფიკაციას, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებსა და დროს საჭიროებდეს[39].

ხშირად, საჯარო ინტერესის გათვალისწინებით, საჯარო სამსახურები სისხლის სამართლის დანაშაულის გამოძიების შესახებ ინფორმაციას აქვეყნებენ საჯაროდ, თუმცა ამ დროს ხდება დანაშაულთან დაკავშირებული პირების დეპერსონალიზაცია, ვინაიდან ასეთ შემთხვევაში შესაძლებელია კანონიერი მიზნის მიღწევა მონაცემთა დეპერსონალიზაციით, ანუ პირთა იდენტიფიცირების გამომრიცხავი ფორმით ინფორმაციის გავრცელების გზით[40], რაც არსებული პრაქტიკით, ხორციელდება პირის სახელისა და გვარის ინიციალების გამოქვეყნებით.

პერსონალური მონაცემების დაშიფრული იდენტიფიკატორიებით გამოქვეყნება მრავალ შემთხვევაში გამოიყენება, როგორც პიროვნების ვინაობის საიდუმლოდ შენახვის საშუალება. აღნიშნული განსაკუთრებით საჭიროა იმ შემთხვევაში, როდესაც გამოქვეყნების მიზანი მონაცემთა სუბიექტის ნამდვილი ვინაობის გასაჯაროების გარეშეც მიიღწევა, ამასთან უზრუნველყოფილია პერსონალურ მონაცემთა დაცვა[41].

თუმცა მნიშვნელოვანია აღინიშნოს, რომ ვინაიდან პერსონალურ მონაცემთა დაცვის შესახებ კანონის მოქმედება არ ვრცელდება მონაცემთა მედიასაშუალებების მიერ საზოგადოების ინფორმირების მიზნით დამუშავებაზე[42], როდესაც მასმედია აქვეყნებს ინფორმაციას საგამოძიებო სამსახურებში მიმდინარე სისხლის სამართლის დანაშაულის გამოძიების თაობაზე, ზოგიერთ შემთხვევაში ასაჯაროებს დანაშაულთან დაკავშირებული პირების პერსონალურ მონაცემებს, პირის სახელს და გვარს და სხვა, ამ დროს შესაძლებელია მასმედიის მიერ გასაჯაროებული ინფორმაცია

[39] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის ,,რ“ ქვეპუნქტი.

[40] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 21, იხ. <https://personaldata.ge/cdn/2018/12/angarishi_2017.pdf> [25.06.2019]

[41] გოშაძე კახაბერ. მონაცემთა დაცვის ევროპული სამართალი. თარგმანი, თბილისი 2015 იურისტის გამომცემლობა. © ძირითადი უფლებების ევროპული კავშირის სააგენტო, 2014 ევროპის საბჭო, 2014. გვ 60.

[42] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის მე-4 პუნქტი.

მონაცემთა სუბიექტის სახელისა და გვარის შესახებ, მარტივად იქნეს დაკავშირებული საჯარო სამსახურის(ების) მიერ დეპერსონალიზაციის გათვალისწინებით გამოქვეყნებულ სუბიექტთა ინიციალებთან, რითაც ირღვევა დეპერსონალიზაციის პრინციპები და ამიტომ მნიშვნელოვანია საჯარო სამსახურებმა უზრუნველყონ მონაცემთა დეპერსონალიზაცია იმგვარად, რომ ,,შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებსა და დროს საჭიროებდეს“. მაგალითად, ინიციალების ნაცვლად შესაძლებელია გამოყენებული იქნეს ციფრები ან სხვა სიმბოლოები[43].

# თავი II. პერსონალურ მონაცემთა უსაფრთხოების სტანდარტების დანერგვა საჯარო სამსახურში

## 1. პერსონალურ მონაცემთა ორგანიზაციული და ტექნიკური უსაფრთხოების სტანდარტების დაცვა, როგორც პრინციპი

ვინაიდან, საჯარო დაწესებულებებში ძირითად სიმდიდრეს წარმოადგენს არამატერიალური აქტივები, ინტელექტუალური საკუთრება, ინფორმაცია, ცოდნა, გამოცდილება, რეპუტაცია, ნდობა და ა.შ. ,,ინფორმაციული უსაფრთხოების შესახებ” კანონმა და კანონქვემდებარე საკანონმდებლო ნორმებმა კრიტიკული ინფორმაციული სისტემის სუბიექტებში დაცულ ინფორმაციულ აქტივთა შორის მოაქციეს პერსონალურ მონაცემების შემცველი ინფორმაციაც, რადგან ცალსახაა, რომ ინფორმაციული უსაფრთხოება მნიშვნელოვანწილად მოიცავს პერსონალურ მონაცემთა უსაფრთხოებას. ,,ინფორმაციული უსაფრთხოების შესახებ” საქართველოს კანონის დებულებები გავლენას არ ახდენს საქართველოს კანონმდებლობით გათვალისწინებული იმ ნორმების მოქმედებაზე, რომლებიც არეგულირებს ინფორმაციის

[43] Handbook on European Data Protection Law – 2018 edition, FRA, CoE, ECHR. 2018, 132

თავისუფლებას, პერსონალური მონაცემის დამუშავებას, სახელმწიფო, კომერციული და პირადი საიდუმლოებების დაცვას[44].

ამგვარად, ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის და მისი ქვემდებარე ნორმატიული აქტების დებულებები, შესაძლებელია ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის დამატებით დებულებებად მოვიაზროთ, დაწესებულების მიერ პერსონალურ მონაცემთა დასაცავად, სათანადო ტექნიკურ-ორგანიზაციული ზომების მიღების კუთხით.

ინფორმაციული უსაფრთხოების სტანდარტი ISO 27001:2011, მოიცავს ყველა ტიპის ორგანიზაციას და განსაზღვრავს ინფორმაციული უსაფრთხოების მართვის სისტემის ჩამოყალიბების, დანერგვის, ფუნქციონირების, მონიტორინგის, განხილვის, მხარდაჭერის და გაუმჯობესების დოკუმენტირებულ მოთხოვნებს ორგანიზაციაში არსებული ზოგადი საქმიანობის რისკების გათვალისწინებით, ხოლო ინფორმაციული უსაფრთხოების მართვის სისტემის დანიშნულებაა ინფორმაციული აქტივების დამცავი, ადეკვატური და პროპორციული კონტროლის მექანიზმების დანერგვა.

,,ინფორმაციული უსაფრთხოების შესახებ” კანონის შესაბამისად, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის მიერ დამტკიცებულია ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“, რომელიც 27001:2011 სტანდარტზე დაყრდნობით აღწერს ორგანიზაციაში კონტროლის მექანიზმების და კონტროლის მიზნების ზოგად ჩამონთვალს და აღნიშნული მიჩნეულია შერჩევის საწყის წერტილად, რათა არ მოხდეს მნიშვნელოვანი კონტროლის მექანიზმების გამოტოვება. შესაბამისად, ბუნებრივია, აღნიშნულ სტანდარტში მოცემული კონტროლის მექანიზმები და კონტროლის მიზნები არ წარმოადგენს ამომწურავ ჩამონათვალს და შესაძლებელია შეირჩეს დამატებითი კონტროლის მექანიზმები[45].

[44] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-3 მუხლის მე-6 პუნქტი.

[45] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1; 4.2.1 ,,ზ“

,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის N2 ბრძანების დანართი ,,ა“-ს შესაბამისად (27002:2011 სტანდარტი), ორგანიზაციაში ყველა დასაქმებული, კონტრაქტორი და მესამე მხარე დასაქმების შეწყვეტის შედეგად ვალდებულია დააბრუნოს მათ დაქვემდებარებაში არსებული ორგანიზაციის ყველა აქტივი[46]. სტანდარტის აღნიშნული პუნქტი განსაკუთრებით სენსიტიურია, რადგან ყოველთვის არსებობს რისკი იმისა, რომ ორგანიზაციის თანამშრომელი სამსახურიდან გათავისუფლებისას ფარულად დაეუფლება ორგანიზაციის ინფორმაციულ აქტივს გარკვეული არამართლზომიერი მიზნებისათვის, რომლის კონტროლის მექანიზმის დანერგვა განსაკუთრებულ სირთულეს წარმოადგენს, ხოლო დაუფლებული ინფორმაციული აქტივი მაღალი რისკის ქვეშ დგება, მისი უკანონო გამოყენების თვალსაზრისით.

ზემოაღნიშნული საკითხის პრობლემურობას ადასტურებს ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ“ 2018 წლის ანგარიში, რომლის მიხედვით ერთ-ერთი საჯარო უწყების ყოფილმა ხელმძღვანელმა სოციალურ ქსელ „ფეისბუქ“-ის გვერდზე გაასაჯაროვა მისი ყოფილი თანამშრომელების შესახებ მის უწყებაში დაცული პერსონალური მონაცემები, რაც როგორც თავად განმარტა მას ჰქონდა კანონიერი ინტერესი, მედიაში გავრცელებული ინფორმაციის საფუძველზე საზოგადოებისათვის მიეწოდებინა სწორი ინფორმაცია, თუმცა უწყების ყოფილი ხელმძღვანელის ქმედება არ იქნა მიჩნეული კანონიერ და პროპორციულ ზომად და ცნობილი იქნა სამართალდამრღვევად, ხოლო საჯარო უწყებას მიეცა რეკომენდაცია განესაზღვრა შიდა რეგულაციების დარღვევის შემთხვევაში რეაგირების სამართლებრივი ბერკეტები[47].

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად, ინფორმაცია, რომელიც განკუთვნილია

[46] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი ,,ა“ 8.3.2

[47] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 31.

მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტის თანამშრომლისათვის ან/და მასთან სახელშეკრულებო ურთიერთობის მქონე პირისათვის, წარმოადგენს შინასამსახურებრივი გამოყენების ინფორმაციას, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა, სავარაუდოდ, გამოიწვევს კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ თავისი ფუნქციების შესრულების მნიშვნელოვან შეფერხებას ან ზიანს მიაყენებს სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოებას, სახელმწიფო ინტერესს ან კერძო პირის საქმიან რეპუტაციას[48].

გარდა აღნიშნულისა, ,,საჯარო სამსახურის შესახებ“ და ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონებით განსაზღვრულია თანამშრომლის ვალდებულებები, გამჟღავნებისგან დაიცვას სხვისი პერსონალური მონაცემები, სახელმწიფო, კომერციული და პროფესიული საიდუმლოებები, რომლებიც მისთვის სამსახურებრივი მოვალეობის შესრულებისას გახდა ცნობილი, ასევე, როგორც სამსახურებრივი უფლებამოსილების განხორციელებისას, ისე სამსახურიდან გათავისუფლების შემდეგ არ გაავრცელოს სახელმწიფო, კომერციული და პროფესიული საიდუმლოებები, სხვა პირის ოჯახურ და პირად ცხოვრებასთან დაკავშირებული ინფორმაცია, აგრეთვე სხვა ინფორმაცია, რომლებიც მისთვის სამსახურებრივი მოვალეობის შესრულებასთან დაკავშირებით გახდა ცნობილი[49].

ამდენად, მიზანშეწონილია უწყებაში დასაქმებული თანამშრომელის დაკავებული თანამდებობიდან გათავისუფლებისას, ჩამოერთვას ხელწერილი კონფიდენციალური ინფორმაციის არამიზნობრივად გამოყენების შესახებ პასუხისმგებლობაზე, რაც დამატებით ღონისძიებად ჩაითვლება.

მსგავსი გარემოებების თავიდან ასაცილებლად, ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის N2 ბრძანების დანართი ,,ა“-ს სტანდარტის

[48] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-2 მუხლის ,,ი“ ქვეპუნქტი.

[49] ,,საჯარო სამსახურის შესახებ“ საქართველოს კანონი მუხ.74, ,,გ“ მუხ. 75. ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მუხ.17; მე-4 პ.

შესაბამისად, ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის ფარგლებში, უნდა განისაზღვროს ინფორმაციული უსაფრთხოების ამსახავი შეთანხმებები კონფიდენციალურობის და გაუმჟღავნებლობის შესახებ, რაც პერიოდულად უნდა გადაიხედოს[50].

ამავე სტანდარტის მიხედვით, ტერმინი ,,ინფორმაციული აქტივის მფლობელი“ გამოიყენება ინდივიდის ან ობიექტის აღსაწერად, რომელსაც გააჩნია აქტივის წარმოების, შენარჩუნების ან დაცვის მოვალეობა. ,,მფლობელი” არ ნიშნავს, იმას, რომ პიროვნებას გააჩნია აქტივზე საკუთრების უფლება[51].

## 1.1 მონაცემთა უსაფრთხოების დანერგვის პროცესი

,,ინფორმაციული უსაფრთხოების შესახებ” კანონით გათვალისწინებული ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების დასანერგად აუცილებელია ორგანიზაციაში ინფორმაციული ციკლის აღწერა, რომელიც თავის მხრივ მოიცავს ინფორმაციის შექმნას, შენახვას, დამუშავებას, გადაცემას, გამოყენებას, დაზიანებას, დაკარგვას, დატაცებას და განადგურებას. ამ დროს მნიშვნელოვანია იდენტიფიცირებული იქნეს ინფორმაციის ტიპები, ესენია ქაღალდზე ნაბეჭდი და ნაწერი, თუ ელექტრონულად შენახული, ფოსტის ან ელექტრონული საშუალებებით გადაცემული, ნაჩვენები ვიდეოში, ნაჩვენები/გამოქვეყნებული ქსელის მეშვეობით, ზეპირსიტყვიერი და სხვა. რა სახითაც არ უნდა იყოს წარმოდგენილი და რა სახითაც არ უნდა ინახებოდეს ან ხდებოდეს მისი გაზიარება, ინფორმაცია ყოველთვის საჭიროებს სათანადო დაცვას.

ასევე მნიშვნელოვანია შეფასებული იქნეს რისკები, რომლებიც შესაძლოა იყოს თანამშრომლების უსაფრთხოების საკითხებში დაბალი ინფორმირებულობა, არაფორმალიზებული ორგანიზაციული პროცესები და კონტროლის მექანიზმები,

[50] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი ,,ა“ 6.1.5.

[51] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1, 4.2.1; ,,დ“ შენიშვნა

საკანონმდებლო და საკონტრაქტო მოთხოვნები, ტექნოლოგიების არასათანადო გამოყენება და დაცვა, ჰაკერების ხელსაწყოების და ვირუსების სირთულისა და ეფექტურობის ზრდა, ბუნებრივი მოვლენები (მაგ. ხანძარი, წყალდიდობა, მიწისძვრა), სოციალური ინჟინერია და სხვა.

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 აწესებს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის, აღნიშნული მარეგულირებელი აქტის მიხედვით კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ ეტაპობრივად სამი წლის განმავლობაში გასატარებელია სავალდებულო ღონისძიებები, ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის შესახებ[52], მაგრამ როგორ მიმდინარეობს კრიტიკული ინფორმაციული სისტემის სუბიექტებში ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით და მისი ქვემდებარე აქტებით განსაზღვრული მექანიზმების დანერგვა უცნობია, რადგან აღნიშნულზე სრული ინფორმაცია საჯაროდ ხელმისაწვდომი არ არის, თუმცა რამდენიმე კრიტიკული ინფორმაციული სისტემის სუბიექტი საჯაროდ აცხადებს სისტემაში ინფორმაციული უსაფრთხოების სტანდარტის დანერგვის შესახებ, მაგალითად, საქართველოს ეროვნული ბანკი, რომელიც ინფორმაციული უსაფრთხოების მართვის სისტემის ISO/IEC 27001: 2013 სტანდარტთან შესაბამისობაზე დასერტიფიცირდა[53]. ცხადია მისასალმებელია საქართველოს ეროვნული ბანკის მიერ ISO/IEC 27001: 2013 ინფორმაციული უსაფრთხოების სტანდარტის დანერგვა, თუმცა მსგავსი მაგალითები საქართველოს საჯარო სექტორში ბევრი არ მოიძებნება.

როგორც აღინიშნა, ,,ინფორმაციული უსაფრთხოების შესახებ” კანონის მოთხოვნები ეფუძნება სტანდარტს ISO 27001:2011, რომელიც წარმოადგენს ISO 27001:2005-ის ლოკალიზებულ ვერსიას[54]. ISO 27001:2013 ინფორმაციული უსაფრთხოების

[52] ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2, 2013 წლის 4 თებერვალი, ქ. თბილისი

[53] იხ. <https://www.nbg.gov.ge/index.php?m=340&newsid=2670> [25.06.2019]

[54] იხ. <http://dea.gov.ge/?action=page&p_id=249&lang=geo> [25.06.2019]

განახლებული სტანდარტია, რომელმაც უფრო მოქნილი გახდა ორგანიზაციაში უსაფრთხოების პროცესების დანერგვა, დააზუსტა ინფორმაციული უსაფრთხოების საბჭოსა და მენეჯმენტის ინფორმაციული უსაფრთხოების მართვის სისტემისადმი დამოკიდებულება, რაც დიდ ორგანიზაციებში როლების მკაფიოდ გამიჯვნის საშუალებას იძლევა და სხვა[55].

ამდენად, მიზანშეწონილია ,,ინფორმაციული უსაფრთხოების შესახებ“ კანონის ცვლილება ISO 27001:2013 სტანდარტის საფუძველზე, რაც გააუმჯობესებს ინფორმაციული უსაფრთხოების დაცვის ხარისხს.

## 1.2 პროპორციულობის პრინციპის დაცვა საჯარო სამსახურში მონაცემთა დამუშავებისას

საკანონმდებლო ნორმები განსაზღვრავენ, რომ პერსონალურ მონაცემთა დამუშავებისას აუცილებელია დაცული იქნეს პროპორციულობის პრინციპი, რაც გულისხმობს, რომ მონაცემთა დამმუშავებელმა პირის პერსონალური მონაცემები დაამუშაოს იმ დოზით, რამდენადაც ეს ესაჭიროება შესაბამისი ამოცანის შესრულებას[56].

ზემოაღნიშნულიდან გამომდინარე, სწორედ პერსონალურ მონაცემთა დამმუშავებელია მონაცემთა დამუშავების მიზნებისა და პროპორციულობის განმსაზღვრელი სუბიექტი და პასუხისმგებელია აღნიშნულზე, თუმცა აუცილებელია მონაცემთა დამმუშავებლის კონტროლი, რათა არ მოხდეს პერსონალური მონაცემების გამოყენების დამმუშავებლის კეთილსინდისიერების ამარა დატოვება, რაც ხელს შეუშლის ამ მიმართულებით რისკების შემცირებას.

მიუხედავად იმისა, რომ პერსონალური მონაცემების დაცვის კონტროლს ახორციელებენ კონკრეტული უწყებები (სახელმწიფო ინსპექტორის სამსახური, არასამთავრობო ორგანიზაციები და სხვ.) და კანონმდებლობით განსაზღვრულია სანქციები პერსონალურ მონაცემთა დაცვის პრინციპების დარღვევისათვის, მაინც რჩება

[55] იხ. <https://www.linkedin.com/pulse/difference-between-iso-270012005-270012013-nutshell-manish-mishra> [25.06.2019]

[56] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი.

რისკები, როგორც ზემოთ აღინიშნა - პერსონალური მონაცემების დამმუშავებლის კეთილსინდისიერების ამარა დარჩენისა. ამ მხრივ განსაკუთრებით მნიშვნელოვანია განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების საკითხი, ვინაიდან კანონმდებლობით აკრძალულია ამ მონაცემთა დამუშავება, მონაცემთა სუბიექტის წერილობითი თანხმობის გარეშე, კანონმდებლობამ დაუშვა გამონაკლისები და სუბიექტის წერილობითი თანხმობის გარეშე დამუშავების საფუძვლებში მოიხსენია გარემოებები, რომელიც საკმაოდ ფართოა, მაგალითად ნასამართლობასთან და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება, მონაცემთა დამუშავება მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დასაცავად, მონაცემთა დამუშავება ბრალდებულთა / მსჯავრდებულთა პირადი საქმეებისა და რეესტრების წარმოების, მსჯავრდებულის მიმართ მის მიერ სასჯელის მოხდის ინდივიდუალური დაგეგმვის ან/და მსჯავრდებულის სასჯელის მოხდისგან პირობით ვადამდე გათავისუფლებასთან და მისთვის სასჯელის მოუხდელი ნაწილის უფრო მსუბუქი სახის სასჯელით შეცვლასთან დაკავშირებული საკითხების განხილვის მიზნით და სხვა[57].

სახელმწიფო შესყიდვების ვებ-გვერდზე (www.tenders.procurement.gov.ge), სახელმწიფო შემსყიდველი ორგანიზაციების მიერ გამოცხადებული შესყიდვებს შორისაა ტენდერები დროის საკონტროლო სისტემების ან სამუშაო საათების აღრიცხვის სისტემის შესყიდვის შესახებ[58]. აღნიშნული შესყიდვების შედეგად დადებული ხელშეკრულებების ტექნიკური დავალებები, ხშირად მოიცავენ, ადმინისტრაციულ შენობაში პირთა შესვლისა და გასვლის რეგისტრაციის სისტემების (დაშვების სისტემა) მონტაჟს, რომელსაც ექნება თითის ანაბეჭდებით რეგისტრაციის ფუნქციონალი, დასაქმებულთა სამსახურში გამოცხადების აღრიცხვის მიზნით.

როგორც ზემოთ აღინიშნა, ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიხედვით, განსაკუთრებული

[57] იქვე, მუხ. 6

[58] იხ. <http://procurement.gov.ge/> CPV 35100000; 35125200, მაგალითად: <https://tenders.procurement.gov.ge/public/library/contract.php?go=274176> [25.06.2019]

კატეგორიის პერსონალურ მონაცემს წარმოადგენს ბიომეტრიული მონაცემი, მათ შორის თითის ანაბეჭდი[59]. საჯარო დაწესებულების მიერ ბიომეტრიულ მონაცემთა დამუშავება შეიძლება მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნებისათვის, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით, თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან[60].

ასევე გასათვალისწინებელია, რომ ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მიხედვით საჯარო და კერძო დაწესებულებებს შენობაში შესვლისა და შენობიდან გასვლის აღრიცხვის მიზნით შეუძლიათ შეაგროვონ შემდეგი მონაცემები: სახელი, საიდენტიფიკაციო დოკუმენტის ნომერი და სახე, მისამართი, შესვლისა და გასვლის თარიღები და დრო, ასევე შენობაში შესვლისა და შენობიდან გასვლის მიზეზები[61].

თანამშრომელთა სამსახურში გამოცხადების აღრიცხვის მიზნით ბიომეტრიული მონაცემების დამუშავება წარმოადგენს პროპორციულობის პრინციპის დარღვევას, რადგან აღნიშნული მიზნის მიღწევა შესაძლებელია სხვა საშუალებებით, რომლებიც არ საჭიროებენ ,,არაპროპორციულად დიდ ძალისხმევას"[62].

ამდენად, აღნიშნული მაგალითი მიუთითებს, თუ რამდენად საჭიროა საჯარო სამსახურებში ინფორმაციული უსაფრთხოების კანონმდებლობის მოთხოვნების სავალდებულოდ გავრცელება, თუმცა სამწუხაროდ, ინფორმაციული უსაფრთხოების შესახებ საქართველოს საკანონმდებლო გავრცელების არეალი შეზღუდულია და ამასთან კანონის ზოგიერთი დებულება არ არის სავალდებულოდ შესასრულებელი და პერსონალურ მონაცემთა დაცვის კუთხით საჯარო დაწესებულების უმეტესობა ექვემდებარება კანონს ,,პერსონალურ მონაცემთა დაცვის შესახებ", რომელიც თავისთავად დამმუშავებელს ინფორმაციული უსაფრთხოების სტანდარტების დანერგვას არ ავალდებულებს.

---

[59] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-2 მუხლის ,,გ" ქვეპუნქტი.

[60] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-9 მუხლი.

[61] იქვე, მე-14 მუხლი.

[62] რეკომენდაციები ბიომეტრიულ მონაცემთა დამუშავების შესახებ, გვ.3 იხ. <http://manage.personaldata.ge/res/docs/recommendation/Guidelines%20on%20Biometric%20Data.pdf> [25.06.2019]

პროპორციულობის პრინციპის დაცვისათვის მონაცემთა დამმუშავებელმა არ უნდა დაამუშავოს მიზნის მისაღწევად საჭირო მონაცემებზე მეტი და შენახული მონაცემები არ უნდა შეიცავდეს იმაზე მეტ დეტალებს, რაც საჭიროა მიზნის მისაღწევად. ასევე მნიშვნელოვანია დამმუშავებელმა ყოველი კონკრეტული სუბიექტის მონაცემები დაამუშაოს ინდივიდუალური შეფასების საფუძველზე, ვინაიდან შეუძლებელია მონაცემთა დამუშავებისას, ყველა ინდივიდის შემთხვევაში საჭირო იყოს ერთიდაიგივე მიდგომების გავრცელება[63].

ასევე მნიშვნელოვანია დამუშავებული მონაცემები იყოს ზუსტი, რადგან არაზუსტი განსაკუთრებული კატეგორიის პერსონალური მონაცემის გამჟღავნების შედეგად შესაძლოა გაცილებით მეტი ზიანი მიადგეს მონაცემთა სუბიექტს, ვიდრე ეს ზუსტი მონაცემით შეიძლებოდა.

ამ მხრივ საინტერესოა ესტონეთის კანონმდებლობა, რომლის მიხედვითაც არაზუსტი პერსონალური მონაცემები შენახული უნდა იქნეს ზუსტ პერსონალურ მონაცემებთან ერთად და მითითებული უნდა იყოს მათი მოქმედების პერიოდი[64]. აღნიშნულით კანონმდებელმა განსაზღვრა, რომ იმ შემთხვევაში თუ არაზუსტი პერსონალური მონაცემი იქნება დამუშავებული იგი უნდა დაფიქსირდეს, არ უნდა წაიშალოს სწორედ ზუსტი მონაცემის გასამყარებლად, რადგან კანონმდებელმა დაინახა რისკები, რომ იმ შემთხვევაში თუ არაზუსტი მონაცემი წაიშლება და ახლით ჩანაცვლდება, შესაძლოა ეს უფრო მეტად ზიანის მომტანი აღმოჩნდეს სუბიექტისათვის, ვიდრე ზუსტ მონაცემებთან ერთად არაზუსტი მონაცემის შენახვა, კანონით გათვალისწინებული სათანადო პერიოდის განმავლობაში.

[63] პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.18-19.

[64] პერსონალურ მონაცემთა დაცვის აქტი; 1992 წლის 28 ივნისი, ესტონეთი, მუხ.11

# თავი III. კონფიდენციალურობა, როგორც პერსონალურ მონაცემთა კანონიერი დამუშავების გარანტია საჯარო სამსახურში

## 1. კონფიდენციალურობის უზრუნველყოფა მონაცემთა დამუშავებაში ჩართული პირების მიერ

ამჟამად საქართველოში ფუნქციონერებს ათი სამინისტრო[65], დაახლოებით ორასი სახელმწიფო დაწესებულება და სახელმწიფო საწარმო, რომლებიც ჯამში ათასობით სახის მომსახურების მიწოდებას ახორციელებენ[66]. საერთო ჯამში სახელმწიფო სექტორში დასაქმებულთა რაოდენობა 283 800 ადამიანს შეადგენს[67], რაც ისეთი პატარა ქვეყნისათვის როგორიც საქართველოა მნიშვნელოვანი წილია და საზოგადოებრივ ცხოვრებაში მის განსაკუთრებულ როლზე მეტყველებს.

საქართველოს მთავრობის მიერ გაცხადებულია, რომ სწორი და ეფექტური სახელმწიფო მართვა ხელს უწყობს და აძლიერებს დემოკრატიული სახელმწიფოს მშენებლობას. საზოგადოების ნდობა პოლიტიკური სისტემის მიმართ ზრდის მთავრობის ლეგიტიმურობას, როდესაც მმართველობა ზოგადად, და კერძოდ კი სახელმწიფო

[65] საქართველოს კანონი ,,საქართველოს მთავრობის სტრუქტურის, უფლებამოსილებისა და საქმიანობის წესის შესახებ“, მე-14 მუხ., მე-2 პ.

[66] საქართველოს მთავრობის დადგენილება №427 ,,საჯარო მმართველობის განხორციელების სტრატეგიული დოკუმენტების - „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020-ისა“ და „პოლიტიკის დაგეგმვის სისტემის რეფორმის სტრატეგია 2015-2017-ის“ დამტკიცების თაობაზე“ იხ. დანართი „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020“ გვ.27

[67] იხ. <https://www.geostat.ge/ka/modules/categories/38/dasakmeba-da-umushevroba> [25.06.2019]

მომსახურების მიწოდება არის ეფექტური, საჯარო პირები მოქალაქეებისთვის არიან ხელმისაწვდომნი, სამთავრობო უწყებები და დეპარტამენტები მუშაობენ ერთობლივად, კოორდინირებული და თანმიმდევრული გზით. არანაკლებ მნიშვნელოვანია „მართვის უნარი“, რათა მოხდეს სწორი გადაწყვეტილებების მიღება პოლიტიკისა და პროგრამების დაგეგმვის პროცესში, დასახული მიზნების მისაღწევად, და, ასევე, შესაძლებელი იყოს მოსალოდნელი ტენდენციებისა და გამოწვევების პროგნოზირება[68].

ზემოაღნიშნული ამოცანების მისაღწევად ერთ-ერთი უმნიშვნელოვანესია საჯარო სამსახურში კონფიდენციალურობის იმ დოზით დაცვა, რომლითაც უზრუნველყოფილი იქნება საზოგადოების პირადი ცხოვრების ხელშეუხებლობა და ამასთანავე შეუფერხებლად იფუნქციონირებს საჯარო სამსახური მისი მიზნების შესაბამისად.

კლასიკური გაგებით, კონფიდენციალურობა არის იმის უზრუნველყოფა, რომ ინფორმაცია მისაწვდომი გახდეს მხოლოდ იმათთვის, ვისთვისაც ის არის განკუთვნილი. იგი წარმოადგენს ინფორმაციის უსაფრთხოების დაცვის ერთ-ერთ ქვაკუთხედს. კონფიდენციალურობა არის ძირითადი ეთიკური პრინციპი მრავალი პროფესიისთვის[69].

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონმა კონფიდენციალური ინფორმაცია განმარტა, როგორც ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ, მოჰყვება კრიტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი და რომლის კონფიდენციალურ ინფორმაციად კლასიფიცირების მიზანია ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც

[68] საქართველოს მთავრობის დადგენილება №427 ,,საჯარო მმართველობის განხორციელების სტრატეგიული დოკუმენტების - „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020-ისა“ და „პოლიტიკის დაგეგმვის სისტემის რეფორმის სტრატეგია 2015-2017-ის“ დამტკიცების თაობაზე“ იხ. დანართი „საქართველოს საჯარო მმართველობის რეფორმის გზამკვლევი 2020“ გვ.3

[69] იხ. <http://www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=165891> [25.06.2019]

საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას[70].

## 2. მონაცემთა მიმართ შესრულებული ქმედებების აღრიცხვა კრიტიკული ინფორმაციული სისტემის სუბიექტში

როგორც საერთაშორისო პრაქტიკა მიუთითებს საპოლიციო სექტორში პერსონალური ინფორმაციის დაცვის ხარისხი, ყველაზე პრობლემატურ საკითხს წარმოადგენს[71], მით უფრო სამართალდამცავი უწყებები დიდი მოცულობით ამუშავებენ განსაკუთრებული კატეგორიის პერსონალურ მონაცემებსაც.

სამართალდამცავ ორგანოებში პერსონალურ მონაცემთა დაცვის კანონმდებლობის პრინციპების დარღვევის მაღალ რისკზე მიუთითებს პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017 წლის ანგარიში[72], რომლის მიხედვით, საქართველოს შინაგან საქმეთა სამინისტროს, კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად შექმნილი აქვს ცენტრალური საინფორმაციო ბანკი, სადაც ხელმისაწვდომია პირთა პერსონალური (მათ შორის, განსაკუთრებული კატეგორიის) მონაცემები, რომელზედაც წვდომა გააჩნიათ შინაგან საქმეთა სამინისტროს ცალკეულ თანამშრომელებს ერთჯერადი რიცხვითი პაროლის გენერირების მოწყობილობის (ე.წ. DIGIPASS) მეშვეობით, ხოლო როგორც შემოწმებით გაირკვა ამონაწერი სამინისტროს ცენტრალური საინფორმაციო ბანკიდან არ შეიცავდა ინფორმაციას წვდომის დროს დამუშავებული მონაცემების თაობაზე, შესაბამისად კონტროლს მიღმა რჩებოდა საკითხი - მონაცემთა დამმუშავებელმა თუ რა სახის პერსონალური ინფორმაცია დაამუშავა, რათა მომხდარიყო შეფასება რამდენად მიზნობრივი და პროპორციული იყო იგი. შესაბამისად, პერსონალურ მონაცემთა დაცვის ინსპექტორის

[70] ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-2 მუხლის ,,თ“ ქვეპუნქტი.

[71] ადამიანის უფლებათა ევროპული სასამართლო, S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 დეკემბერი 2008

[72] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 46.

აპარატის მიერ აღინიშნა, რომ მნიშვნელოვანია სამინისტრომ უზრუნველყოს ცენტრალურ მონაცემთა ბანკებში განხორციელებული წვდომის დროს დამუშავებული მონაცემების აღრიცხვა, ასევე, მოახდინოს მუდმივი და განგრძობადი კონტროლი საინფორმაციო ბაზების გამოყენებაზე, რათა ყოველ კონკრეტულ შემთხვევაში ცენტრალური საინფორმაციო ბანკის მონაცემთა ინფორმაციულ რესურსებზე დაშვება განხორციელდეს კანონით განსაზღვრული საფუძვლითა და პრინციპების დაცვით, იმისათვის, რომ არასანქცირებულმა წვდომამ ზიანი არ მიაყენოს მონაცემთა სუბიექტის კანონიერ ინტერესებს.

პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2018 წლის ანგარიშის მიხედვით, მომდევნო წელს, კვლავ იქნა შემოწმებული შინაგან საქმეთა სამინისტროს ცენტრალური საინფორმაციო ბანკის უსაფრთხოების დაცვის მიზნით გატარებული ღონისძიებები, რის შედეგადაც დადგინდა, რომ სამინისტროს დანერგილი აქვს შემდეგი ორგანიზაციულ-ტექნიკური ზომები: ცენტრალურ საინფორმაციო ბანკში არსებულ მონაცემზე სამინისტროს თანამშრომლები დაიშვებიან სამინისტროს სტრუქტურული ქვედანაყოფების, ტერიტორიული ორგანოების, სამინისტროს სახელმწიფო საქვეუწყებო დაწესებულებისა და სამინისტროს სისტემაში შემავალი საჯარო სამართლის იურიდიული პირების ხელმძღვანელთა დასაბუთებული წერილობითი მიმართვის საფუძველზე, გაპიროვნებული მომხმარებლის სახელის, პაროლისა და ერთჯერადი რიცხვითი პაროლის გენერირების მოწყობილობის (ე.წ. DIGIPASS) საშუალებით.

ცენტრალურ საინფორმაციო ბანკში არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედება, ამჯერად ექვემდებარება აღრიცხვას, რაც შესაძლებელს ხდის როგორც წვდომის განმახორციელებელი სამინისტროს თანამშრომლის ვინაობის, ასევე მის მიერ მონაცემთა მიმართ შესრულებული ყველა ქმედების დადგენას. სამინისტროს თანამშრომლებს ეკრძალებათ ცენტრალურ საინფორმაციო ბანკში არსებული მონაცემების მოპოვება, გამოყენება ან გავრცელება არასამსახურებრივი მიზნით, აღნიშნულის კონტროლის ვალდებულება კი ეკისრებათ როგორც სამინისტროს სტრუქტურული ქვედანაყოფების, ტერიტორიული

ორგანოების, სამინისტროს სახელმწიფო საქვეუწყებო დაწესებულებისა და სამინისტროს სისტემაში შემავალი საჯარო სამართლის იურიდიული პირების ხელმძღვანელებს, ასევე, სამინისტროს საინფორმაციო-ანალიტიკურ დეპარტამენტსა და სამინისტროს გენერალურ ინსპექციას (დეპარტამენტს). ცენტრალურ საინფორმაციო ბანკში არსებული მონაცემების არასამსახურებრივი მიზნით დამუშავება წარმოშობს კანონმდებლობით დადგენილი პასუხისმგებლობის ზომების ან/და მკაცრი დისციპლინური პასუხისმგებლობის დაკისრების წინაპირობას[73].

საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალურ საინფორმაციო ბანკში არსებული მონაცემების უსაფრთხოების მიზნით გატარებული ორგანიზაციულ-ტექნიკური ღონისძიებები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისია, თუმცა მონაცემთა უსაფრთხოებისთვის დანერგილი ორგანიზაციულ-ტექნიკური ზომები წარმოადგენს კომპლექსურ ღონისძიებათა ერთობლიობას და მათი ადეკვატურობა და ეფექტიანობა ფასდება ყოველ კონკრეტულ შემთხვევაში საქმის გარემოებების სრული, ყოველმხრივი და ობიექტური გამოკვლევის შედეგად[74].

ზემოაღნიშნული მაგალითი მიუთითებს, რომ პერსონალურ მონაცემთა დამუშავებისას ყოველთვის რჩება თანმდევი რისკები იმისა, რომ პერსონალური მონაცემები არამიზნობრივად იქნეს გამოყენებული, ისე, რომ შემდგომი რეაგირების გასატარებლად მისი გამოვლენა ვერ განხორციელდეს.

ვინაიდან არ არსებობს პერსონალური მონაცემების დაცვის აბსოლუტური გარანტიები, საბოლოოდ რჩება მონაცემთა დამმუშავებლის როლი, რომელსაც უდიდესი პასუხისმგებლობა ეკისრება ამ საქმეში და ამ შემთხვევაში, ერთადერთი მნიშვნელოვანი დაცვის მექანიზმი რჩება ის, რომ პერსონალურ მონაცემებზე, განსაკუთრებით კი განსაკუთრებული კატეგორიის პერსონალურ მონაცემებზე წვდომის სუბიექტი წარმოადგენდეს მაღალი მორალისა და ეთიკის მქონე პირს, რომელსაც გააზრებული ექნება თუ რა

[73] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 65.

[74] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 64,65.

შეიძლება გამოიწვიოს პერსონალური მონაცემების არამიზნობრივმა გამოყენებამ[75].

## 3. მონაცემთა უსაფრთხოება საჯარო დაწესებულებათა ვიდეოთვალთვალის დროს

უსაფრთხოებისა და საკუთრების დაცვის მიზნით, თითქმის ყველა სახელმწიფო უწყება იყენებს ადმინისტრაციული შენობის პერიმეტრზე ვიდეოსათვალთვალო მოწყობილობების ფუნქციონირებას. ამ დროს მნიშვნელოვანია კანონით დადგენილი მოთხოვნების შესრულების საკითხი.

კრიტიკული ინფორმაციული სისტემის სუბიექტის - ქალაქ თბილისის მუნიციპალიტეტის მერიის მიერ, ვიდეოთვალთვალის სისტემის მეშვეობით მონაცემთა დამუშავების კანონიერება პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა შეამოწმა[76].

შემოწმებით დადგინდა, რომ ვიდეოსათვალთვალო კამერების ელექტრონული სისტემა არ აღრიცხავდა მონაცემთა მიმართ შესრულებულ ყველა მოქმედებას. სისტემაში აღირიცხებოდა მხოლოდ კონკრეტულ კამერებთან დაკავშირებისა და მომხმარებლის სისტემაში შესვლისა და გამოსვლის ფაქტები. არ აღირიცხებოდა, ვინ, რომელი კამერიდან, როდის და რა მიზნით დაამუშავა ვიდეოჩანაწერი.

,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, საჯარო და კერძო დაწესებულებებს შესაბამისი მონიტორინგის განხორციელების მიზნით შეუძლიათ განახორციელონ თავიანთი შენობების ვიდეოთვალთვალი, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვისათვის.

მონაცემთა დამმუშავებელის ვალდებულება, ,,უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა“[77], ემსახურება მიზანს,

---

[75] Drew C., Data science ethics in government (Published: 28 December 2016), 3, იხ. <https://doi.org/10.1098/rsta.2016.0119> [25.06.2019]

[76] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 22.

[77] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის მე-2 პუნქტი.

რომ შემოწმებას ექვემდებარებოდეს მონაცემების დამუშავების მიზნობრიობა. ვიდეოთვალთვალის შემთხვევაში, შეფასებას უნდა ექვემდებარებოდეს, ხომ არ ხორციელდება ვიდეოთვალთვალი პირთა ქცევის აღრიცხვისა ან რაიმე არალეგიტიმური მიზნით, რაც სცილდება პირის უსაფრთხოებისა და საკუთრების, ასევე საიდუმლო ინფორმაციის დაცვის ფარგლებს.

ვიდეოთვალთვალი უნდა განხორციელდეს მხოლოდ კანონით განსაზღვრული მიზნებისათვის და იმ მოცულობით, რომელიც აუცილებელია კანონით განსაზღვრული მიზნის მისაღწევად.

ამასთან მნიშვნელოვანია ვიდეოჩანაწერების შენახვის ვადები, რაც მიზნის ადეკვატური უნდა იყოს. მით უმეტეს, თუ არ არის მიღებული სათანადო ორგანიზაციული და ტექნიკური ზომები, იზრდება პერსონალური მონაცემების უკანონო გამჟღავნების საფრთხე[78].

ვიდეოთვალთვალის განხორციელებისას მნიშვნელოვანია მონიტორინგის არეალში მოხვედრილ პირთა ინფორმირება კანონით დადგენილი წესით. კერძოდ, აუცილებელია შესაბამისი გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილზე განთავსება, ორგანიზაციაში დასაქმებულთა წერილობითი ინფორმირება ვიდეოთვალთვალის მიმდინარეობისა და მათი უფლებების შესახებ. უწყებებმა მონაცემთა უსაფრთხოების დაცვის უზრუნველსაყოფად უნდა შეიმუშაონ შესაბამისი წესები და განსაზღვრონ ვიდეოთვალთვალის სისტემაზე პერსონიფიცირებული და დიფერენცირებული წვდომის დონეები, საჭიროებისა და მათი უფლებამოსილების შესაბამისად[79].

კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის განსაზღვრული ინფორმაციული უსაფრთხოების სტანდარტით, ვიდეოთვალთვალის გამოყენების წესები დარეგულირებული არ არის, თუმცა ასახულია მინიმალური რეგულირება, ინფორმაციის დამუშავების საშუალებათა არამიზნობრივად გამოყენების აღკვეთის

[78] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 98.

[79] იქვე, გვ. 99.

შესახებ, უსაფრთხოების მოთხოვნების დარღვევის თავის არიდების მიზნით[80].

## 4. პერსონალურ მონაცემთა დაცვის უზრუნველყოფა საჯარო სამსახურში განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისას

პერსონალურ მონაცემთა დაცვის სამართლებრივი ნორმები მკაფიოდ განსაზღვრავენ თუ რა წარმოადგენს განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, ესენია მონაცემები რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში გაწევრებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა, ხოლო ბიომეტრიული და გენეტიკური მონაცემები განმარტებულია როგორც ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი). ასევე მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემი გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება[81]. ამ მონაცემების განსაკუთრებული მნიშვნელობის

[80] ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2, დანართი ,,ა“; ,,ა15.1.5“ 2013 წლის 4 თებერვალი, ქ. თბილისი

[81] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის ,,ბ“, ,,გ”, ,,გ[1]“ პუნქტები.

გამო, პერსონალურ მონაცემთა დაცვის კანონმდებლობა მკაცრ შეზღუდვებს აწესებს მის დამუშავებასთან დაკავშირებით[82].

მონაცემთა უსაფრთხოებისათვის მიღებული ზომები რისკების ადეკვატური და პროპორციული უნდა იყოს. რისკების შეფასებისას მხედველობაში მიიღება დამუშავებული მონაცემების კატეგორია და შინაარსი, ორგანიზაციის თანამშრომელთა რაოდენობა და მონაცემებთან მათი წვდომის ხარისხი, მონაცემთა ბაზაზე წვდომის უფლების მქონე მესამე პირები და მათი რაოდენობა[83].

პერსონალური მონაცემების დაცულობის ხარისხი მჭიდრო კავშირშია დამუშავების საშუალებებთან. კერძოდ, მნიშვნელოვანია რა სახით მუშავდება ინფორმაცია, ესაა არაავტომატური, ნახევრად ავტომატური თუ ავტომატური საშუალებები.

თანამედროვე ცხოვრების პირობებში მონაცემთა ნახევრად ავტომატური და ავტომატური დამუშავება ყველაზე გავრცელებულ ფორმას წარმოადგენს, რასაც თან ახლავს რისკი დაიკარგოს ინფორმაცია, რითაც შესაძლოა მონაცემთა სუბიექტის პირადი ცხოვრების ხელშეუხებლობა შეილახოს. თანამედროვე ტექნოლოგიების მეშვეობით, როგორც კი კომპიუტერში ჩნდება მონაცემები, მაშინვე ჩნდება შესაძლებლობა მისი გადაგზავნის, შედარების თუ კოპირებისა. ბუნებრივია, ციფრული ტექნოლოგიების გამოგონებამდე პერსონალური თუ სხვა მონაცემების ამგვარი მოძრაობა შეუძლებელი იყო, შესაბამისად პერსონალური მონაცემების დაცვა თანამედროვე ტექნოლოგიებმა ერთიორად გაართულა და მისი განვითარების ტემპების გათვალისწინებით შეუქცევადი ხასიათი აქვს[84].

პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ ევროპის საბჭოს 108-ე კონვენცია მკაფიოდ განსაზღვრავს, რომ დაუშვებელია შესაბამისი სამართლებრივი დაცვის მექანიზმის გარეშე განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება.

---

[82] იქვე, მე-6 მუხლი.

[83] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 47.

[84] იხ. <http://www.nplg.gov.ge/gsdl/cgi-bin/library.exe?e=d-01000-00---off-0samartal--00-1----0-10-0---0---0prompt-10---4-------0-1l--11-ka-50---20-about---00-3-1-00-0-0-11-1-0utfZz-8-00&cl=CL4.3&d=HASH01ffaf957157488e546f5b51.2.1&gt=1> [25.06.2019]

ამ მხრივ განსაკუთრებით რისკის შემცველია განსაკუთრებული კატეგორიის პერსონალური მონაცემების ტრანსფერირება. საჯარო დაწესებულებები ხშირად აგზავნიან განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს ელექტრონული ფოსტის საშუალებით, ამ დროს მნიშვნელოვანია დამმუშავებელმა უზრუნველყოს ინფორმაციის დაბლოკვა გარეშე წვდომისაგან, შეიმუშაოს რამდენიმე საფეხურიანი დაცვის სისტემა, მაგალითად, გასაგზავნ ფაილს დაადოს პაროლი, ადრესატთან მობილურ ტელეფონზე აღნიშნული პაროლის გაგზავნით[85] და შეიმუშაოს სხვა ადეკვატური ღონისძიებები ინფორმაციის გარეშე წვდომისაგან დაცვის მიზნით[86]. მით უმეტეს, როდესაც ელექტრონულ ფოსტაზე სენსიტიური პერსონალური ინფორმაციის შემცველი ფაილის გაგზავნა შეიცავს რისკს, ინფორმაციის დამმუშავებელის მიერ შეცდომით იქნეს მითითებული ელექტრონული ფოსტის მისამართი.

განსაკუთრებული კატეგორიის პერსონალური მონაცემების გაგზავნის შედარებით დაცულ ფორმად შეიძლება ჩაითვალოს ინფორმაციის პორტალზე ატვირთვა, რომელიც ავტომატურად უზრუნველყოფს ინფორმაციის განადგურებას, როდესაც ფაილს ადრესატი ჩამოტვირთავს.

ინფორმაციული უსაფრთხოების სტანდარტის მიხედვით, ელექტრონულ მიმოწერაში მოხვედრილი ინფორმაცია უნდა იყოს სათანადოდ დაცული[87].

თუმცა მონაცემთა ავტომატური დამუშავებისას არ არსებობს ჩამოყალიბებული მექანიზმი იმისა, რომ ციფრული ტექნოლოგიებით დამუშავებული მონაცემები აბსოლუტურად დაცული იქნება.

ამდენად, თანამედროვე ცხოვრებაში ადამიანი ერთგვარ ციფრულ პერსონად ჩამოყალიბდა, რომლის შესახებ მონაცემებიც გამუდმებით მუშავდება ავტომატურად თუ ნახევრდავტომატურად,

---

[85] რეკომენდაცია ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, მაისი, 2016, 5

[86] Guidelines on the protection of personal data in IT governance and IT management of EU institutions; 23 March 2018; 19; 35
იხ. <https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf> [25.06.2019]

[87] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1, 10.8.4

,,ციფრული ადამიანი“ ორ ნაწილადაა გაყოფილი, ერთი რომელზე ზემოქმედებაც მხოლოდ თვითონ შეუძლია, და მეორე, რომელიც იქმნება მესამე პირების მიერ შექმნილი მონაცემებით, რომელზე ზემოქმედების მოხდენაც ამ მონაცემების სუბიექტს არ ძალუძს[88].

სწორედ ,,ციფრული ადამიანის“ მეორე ნაწილი წარმოადგენს განსაკუთრებული საფრთხის შემცველ ობიექტს, რაც გულისხმობს საფრთხეს, იმისა, რომ მასზე დამუშავებული განსაკუთრებული კატეგორიის პერსონალური მონაცემი გამოყენებული იქნეს არამიზნობრივად და ამით მძიმე მატერიალური თუ მორალური ზიანი მიადგეს.

# თავი IV. პერსონალურ მონაცემთა კონფი-დენციალურობის უზრუნველყოფის მექანიზმები

## 1. ინდივიდუალური ანალიზი მონაცემთა დამუშავებისას

როგორც აღინიშნა, საჯარო სამსახურში კონფიდენციალურობის მაღალი ხარისხით უზრუნველსაყოფად საჭიროა უსაფრთხოების სათანადო სტანდარტების დანერგვა, თუმცა აღნიშნული სტანდარტები გულისხმობენ მხოლოდ მინიმალურ ღონისძიებებს და თუ საჭიროა უფრო მეტი გადაწყვეტილებები კონფიდენციალურობის უზრუნველსაყოფად, უწყებამ უნდა შეაფასოს აღნიშნული გარემოება და იმოქმედოს შესაბამისად[89].

კრიტიკული ინფორმაციული სისტემის სუბიექტმა ყოველწლიურად უნდა ჩაატაროს ინფორმაციული უსაფრთხოების აუდიტი უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობის შესაფასებლად, ხოლო აუდიტის დასკვნის მოთხოვნების შესრულება სავალდებულოა[90].

---

[88] Clarke R., The Digital Persona and Its Application to Data Surveillance, The Info. Soc.,10,2 (June 1994).

[89] ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2, დანართი ,,ა“; ,,ა1“ 2013 წლის 4 თებერვალი, ქ. თბილისი

[90] ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესი, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N1, მუხ. 1,3

ამდენად, ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებთან თავსებადობა არ ნიშნავს უსაფრთხოების სრულყოფილად დაცვას, მით უმეტეს, როდესაც გარე შემფასებელი (აუდიტი)[91] მხოლოდ უსაფრთხოების მინიმალურ მოთხოვნებთან თავსებადობას ამოწმებს, ხოლო ფაქტობრივად შესაძლოა საჭირო იყოს უფრო მეტი ღონისძიებები მონაცემთა კონფიდენციალურობის უზრუნველსაყოფად.

ინფორმაციული უსაფრთხოების მართვის სისტემების მთავარ ორიენტირს წარმოადგენს რისკების იდენტიფიცირება და პრევენცია[92], რადგან რასაკვირველია ორგანიზაციისათვის უმთავრესია უარყოფითი მოვლენის დადგომამდე მოახდინოს მისი გამომწვევი ფაქტორების ლიკვიდაცია, რაც პროცესებისადმი ინდივიდუალურ მიდგომებს საჭიროებს, მით უმეტეს, როდესაც რისკის აღმოცენების წყარო ხშირად წინასწარ უცნობია[93]. მაგალითად, თუ გარეშე პირი უწყებისაგან ითხოვს საჯარო ინფორმაციას კონკრეტულ ფაქტზე და უწყება აღნიშნულ ინფორმაციას მომთხოვნ პირს გაუგზავნის პერსონალური მონაცემების დაფარვით, შესაძლოა მაინც დაირღვეს პერსონალური ინფორმაციის კონფიდენციალურობა, იმ შემთხვევაში, თუ უწყებას არ შეუფასებია გარემოება, რამდენად იძლეოდა მის მიერ შერჩეული ფორმით ინფორმაციის გაცემა პირის იდენტიფიცირების საშუალებას[94]. თუ პირი ინფორმაციის მოთხოვნის წერილში უთითებს რაიმე ისეთ დეტალს, რაც იძლევა ვარაუდის საფუძველს, რომ მას აქვს საქმესთან დაკავშირებით გარკვეული ინფორმაცია და მისთვის დეპერსონალიზებული ინფორმაციის მიწოდების შემთხვევაშიც იქნება გასაგები, თუ რომელ კონკრეტულ პირს ეხება იგი[95].

მიუხედავად იმისა, თუ რამდენად ზედმიწევნით იცავს ორგანიზაცია მონაცემთა უსაფრთხოების სტანდარტებს, მსგავსი რისკები შესაძლოა მანამდე ვერ იქნეს იდენტიფიცირებული, სანამ

---

[91] იქვე, მუხ. 1

[92] Privacy by Design Setting a new standard for privacy certification; © Deloitte LLP and affiliated entities, 2, <www.deloitte.com> [25.06.2019]

[93] იხ. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en> [25.06.2019]

[94] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2015, 27.

[95] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი; სასამართლო გადაწყვეტილებათა ხელმისაწვდომობა საქართველოში: საერთო სასამართლოების პრაქტიკის ანალიზი; გვ. 14

უშუალოდ ფაქტი არ დადგება. ამიტომ, მნიშვნელოვანია ყოველი საკითხის ინდივიდუალური შესწავლა და კრიტიკული ანალიზი. თუ ქმედება კანონიერია, არ ნიშნავს, რომ ინფორმაციული უსაფრთხოების დარღვევას არ გამოიწვევს ისე, რომ მისი გამოვლენა შესაძლოა ვერც კი განხორციელდეს.

## 2. ინფორმაციული უსაფრთხოების მართვის სისტემის საფუძვლები და მათი სახეები

ინფორმაციული უსაფრთხოების მართვის სისტემის საფუძველს წარმოადგენს აქტივები, რომლის დანიშნულებაა აქტივების დამცავი და ადექვატური უსაფრთხოების კონტროლის მექანიზმების დანერგვა და დაინტერესებული მხარეების ნდობის გამყარება[96].

ინფორმაციული აქტივია ყველა ინფორმაცია და ცოდნა, ინფორმაციის შენახვის, დამუშავებისა და გადაცემის ტექნოლოგიური საშუალებები, თანამშრომლები და მათი ცოდნა ინფორმაციის დამუშავების შესახებ, ასევე ნებისმიერი რამ, რაც ღირებულია კრიტიკული ინფორმაციული სისტემის სუბიექტისათვის. ინფორმაციული აქტივი შეუძლებელია არსებობდეს დამოუკიდებლად, მასთან დაკავშირებული აქტივის გარეშე[97].

აქტივზე წვდომა, ფაქტობრივად წარმოადგენს ორგანიზაციაში მიმდინარე მთავარ პროცესს, აქტივების ერთ-ერთი ძირითადი შემადგენელია პერსონალურ მონაცემები, რომელიც საერთო ჯამში უკავშირდება ორგანიზაციის ფუნქციების შესრულებას. აქტივების სრულყოფილი მართვა წარმოადგენს ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის და წარმატებული ფუნქციონირების მნიშვნელოვან ფაქტორს[98].

კრიტიკული ინფორმაციული სისტემის ერთ-ერთ სუბიექტს წარმოადგენს საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი. ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად, ცენტრალური საარჩევნო კომისიის აპარატის სტრუქტურული ერთეული - ამომრჩეველთა სიების ფორმირებისა

[96] ,,ინფორმაციული აქტივების მართვის წესების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N7; მუხ.2
[97] იქვე, მუხ. 1.
[98] იქვე, მუხ. 2.

და საინფორმაციო ტექნოლოგიების დეპარტამენტი და ინფორმაციული უსაფრთხოების მენეჯერი უზრუნველყოფენ „პერსონალურ მონაცემთა დაცვის შესახებ" და „ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონების მოთხოვნების შესრულებასა და დაცვას[99].

მნიშვნელოვანია აღინიშნოს, რომ ,,პერსონალურ მონაცემთა დაცვის მდგომარეობისა და ინსპექტორის საქმიანობის შესახებ" 2018 წლის ანგარიშში აღნიშნულია[100], რომ გამოვლინდა საქართველოს ცენტრალური საარჩევნო კომისიის (ცესკო) ვებგვერდზე[101] ამომრჩეველთა ერთიანი სიის მონაცემების (ფოტოსურათის, რეგისტრაციის მისამართისა და მასთან ერთად ამავე მისამართზე რეგისტრირებული პირების შესახებ) სხვა მიზნებით გამოყენების არაერთი შემთხვევა. აღნიშნულ ბაზას აქტიურად იყენებენ ე.წ. სესხის ამომღები ორგანიზაციები და კერძო დეტექტივები. მართალია, ამომრჩეველთა ერთიანი სიის გადამოწმებისთვის განკუთვნილ გვერდზე მითითებულია, რომ: „ვებგვერდი განკუთვნილია მხოლოდ ამომრჩეველთათვის საკუთარი და ოჯახის წევრების მონაცემების გადასამოწმებლად!", თუმცა კანონმდებლობა არ შეიცავს დათქმას, გამოქვეყნებული მონაცემების შემდგომი დამუშავების შეზღუდვის თაობაზე[102].

,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ" მონაცემთა გაცვლის სააგენტოს თავმჯდომარის N2 ბრძანების დანართი ,,ა"-ს (27002:2011 სტანდარტი), ა.15 პუნქტით განსაზღვრულია იურიდიულ მოთხოვნებთან შესაბამისობა, რაც გულისხმობს, რომ კრიტიკული ინფორმაციული სისტემის სუბიექტი (ამ შემთხვევაში ცენტრალური საარჩევნო კომისიის აპარატი), უნდა ახორციელებდეს ნებისმიერი იურიდიული, მარეგულირებელი და საკონტრაქტო ვალდებულებების და უსაფრთხოების მოთხოვნების დარღვევის თავიდან არიდებას. ამავე პუნქტის ა.15.1.4 და ა.15.1.5 პუნქტებით

[99] საქართველოს ცენტრალური საარჩევნო კომისიის რეგლამენტი, მუხ. 15, პუნქტი 19. საქართველოს ცენტრალური საარჩევნო კომისიის დადგენილება №54/2015 2015 წლის 25 ნოემბერი ქ. თბილისი

[100] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 35.

[101] იხ. <https://voters.cec.gov.ge/> [25.06.2019]

[102] საქართველოს ორგანული კანონი, საქართველოს საარჩევნო კოდექსი მუხ.14

განსაზღვრულია, რომ მონაცემთა დაცვა და საიდუმლოება უნდა იყოს უზრუნველყოფილი იურიდიული, მარეგულირებელი და საჭიროების შემთხვევაში საკონტრაქტო ვალდებულებების შესაბამისად, ინფორმაციის დამუშავების საშუალებების არამიზნობრივად გამოყენება მომხმარებლის მიერ უნდა აღიკვეთოს[103].

აღნიშნულიდან გამომდინარე, ცენტრალური საარჩევნო კომისიის აპარატის მიერ ირღვევა ინფორმაციული უსაფრთხოების სტანდარტები, ვინაიდან ნებისმიერ ფიზიკურ პირს, ყოველგვარი კონტროლის მექანიზმების გარეშე, იმ შემთხვევაში თუ მას მოპოვებული აქვს სხვისი გვარი და პირადი ნომერი, შეუძლია მოიპოვოს მასზე უფრო მეტი პერსონალური ინფორმაცია, კერძოდ, სახელი, დაბადების თარიღი, ფოტოსურათი, რეგისტრაციის მისამართი და მასთან ერთად ამავე მისამართზე რეგისტრირებული პირების ინფორმაცია და სხვა, რაც ასევე ცალსახად არღვევს პერსონალურ მონაცემთა დაცვის საერთაშორისოდ აღიარებულ პრინციპებს, რომ ავტომატიზებულ ფაილებში შენახული მონაცემების დაცვის მიზნით, მიღებული უნდა იქნეს უსაფრთხოების შესაბამისი ზომები მათი შემთხვევითი თუ არასანქცირებული დარღვევის, ასევე მათთან არასანქცირებული შეღწევის ან გავრცელების წინააღმდეგ[104]. ამასთან ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიხედვით, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისაგან, ხოლო მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს[105].

ცენტრალური საარჩევნო კომისიის აპარატის მიერ, ამომრჩეველთა მონაცემების უსაფრთხოებისათვის მიღებულ ადეკვატურ ზომად ჩაითვლებოდა მაგალითად, თითოეული

[103] ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის N2 ბრძანების დანართი ,,ა“, ა.15; ა.15.1.4; ა.15.1.5

[104] ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია, მუხ.7

[105] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი.

ამომრჩევლისათვის ერთჯერადად უნიკალური კოდების გადაცემა, რომლის ცენტრალური საარჩევნო კომისიის ოფიციალურ ვებ გვერდზე, შესაბამის ველში აუცილებლად შეყვანით იქნებოდა შესაძლებელი ამომრჩევლის მიერ, მისი პირადი მონაცემების გადამოწმება. ხოლო ამომრჩევლის მიერ კოდის დაკარგვის შემთხვევაში, შესაძლებელი იქნებოდა მისი აღდგენა ცენტრალური საარჩევნო კომისიის აპარატთან სათანადო პერსონალიზებული კომუნიკაციით.

## 3. საფრთხეები მონაცემთა გასაჯაროების მნიშვნელოვანი ლეგიტიმური მიზნების არსებობისას

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის სხვა საჯარო სამსახურებზე სავალდებულო გავრცელების საჭიროებაზე მიუთითებს სახელმწიფო აუდიტის სამსახურის სსიპ საჯარო აუდიტის ინსტიტუტის მიერ, ოფიციალურ ვებ გვერდზე გამოქვეყნებულ სერტიფიცირებულ პირთა სია, რომელიც შეიცავს სახელებს გვარებს და მათ პირად ნომრებს[106].

ამ შემთხვევაში ირღვევა პერსონალურ მონაცემთა დაცვის კანონმდებლობის პრინციპი, რომლის მიხედვით ,,მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი“[107].

ვინაიდან საჯარო სექტორის აუდიტორთა რეესტრის გამოქვეყნება ინსტიტუტის ან/და სახელმწიფო აუდიტის სამსახურის ვებგვერდზე გამოქვეყნება სავალდებულოა ,,საჯარო სექტორში აუდიტორული მომსახურების გაწევის უფლების მოპოვების მსურველ პირთა სერტიფიცირების წესით“[108], საჯარო აუდიტის ინსტიტუტის მიერ, მიზნის ადეკვატურ და პროპორციულ ზომად ჩაითვლებოდა

[106] იხ. <https://sao.ge/lepl-pai/lepl-pai-certification/lepl-pai-list-of-certified-people> [25.06.2019]

[107] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის ,,გ“ ქვეპუნქტი.

[108] ,,საჯარო სექტორში აუდიტორული მომსახურების გაწევის უფლების მოპოვების მსურველ პირთა სერტიფიცირების წესისა და პირობების დამტკიცების შესახებ“ სახელმწიფო აუდიტის სამსახურის გენერალური აუდიტორის ბრძანება №71/37, 2013 წლის 12 აპრილი, ქ. თბილისი, მუხ.26

სერტიფიცირებულ პირთა მხოლოდ სახელებისა და გვარების გამოქვეყნება. პირადი ნომრებისა და გვარების საჯაროდ გამოქვეყნება პერსონალურ მონაცემთა დაცვის თვალსაზრისით განსაკუთრებით სარისკოა, მით უმეტეს იმ პირობებში, როდესაც ცენტრალური საარჩევნო კომისიის ოფიციალურ ვებ გვერდზე არსებულ, ამომრჩეველთა ერთიან სიაში გადასამოწმებელ პორტალზე, პირადი ნომრისა და გვარის გამოყენების შემთხვევაში ხელმისაწვდომია სხვა უამრავი პერსონალური ინფორმაცია. ამასთან, თუ გავითვალისწინებთ, რომ პირადი ნომერი ხშირად საჯაროდ ხელმისაწვდომია[109] და აღნიშნულ გარემოებებს ერთიან სიბრტყეში განვიხილავთ, შეგვიძლია დავასკვნათ, რომ ქვეყანაში პერსონალურ მონაცემთა დაცვის მდგომარეობა არ შეესაბამება თანამედროვე გამოწვევებს.

## 4. საჯარო ელექტრონული მონაცემთა ბაზები

საქართველოს კანონმდებლობით საჯაროდ არის მიჩნეული ისეთი მონაცემთა ბაზები, რომელში დაცული ინფორმაციის მიმართაც არსებობს მაღალი საჯარო ინტერესი. შესაბამისად, უწყებები უზრუნველყოფენ მათ ხელმისაწვდომობას შესაბამის ვებგვერდებზე გამოქვეყნებით (მაგალითად, napr.gov.ge; voters.cec.gov.ge; declaration.gov.ge; privatization.ge და სხვა). ნიშანდობლივია, რომ აღნიშნული ბაზების მარეგულირებელი კანონმდებლობა, როგორც წესი, არ ითვალისწინებს შეზღუდვას ბაზებში განთავსებული პერსონალური მონაცემების გამოყენებასთან დაკავშირებით, შესაბამისად, ვებგვერდების ტექნიკური ფუნქციონალიც ნაკლებად შეიცავს მონაცემთა მოპოვების შემზღუდავ მექანიზმებს[110].

მონაცემთა გასაჯაროების მნიშვნელოვანი ლეგიტიმური მიზნების არსებობის მიუხედავად, პერსონალური მონაცემების ინტერნეტსივრცეში ხელმისაწვდომობა ხშირად გარკვეული

[109] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2017, 13.

[110] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 33.

უხერხულობის, ზოგიერთ შემთხვევაში კი, ზიანის მომტანია მონაცემთა სუბიექტებისთვის[111].

კრიტიკული ინფორმაციული უსაფრთხოების ერთ-ერთი ყველაზე სენსიტიური სუბიექტია საჯარო სამართლის იურიდიული პირი - საჯარო რეესტრის ეროვნული სააგენტო, რადგან კანონიერი საჯარო ინტერესებიდან გამომდინარე ოფიციალურ ვებ გვერდზე - ,,napr.gov.ge“ ასაჯაროვებს პერსონალური მონაცემების შემცველ დიდი მოცულობის მონაცემებს.

ასეთ შემთხვევაში, კანონმდებლობა და ინფორმაციული უსაფრთხოების სტანდარტები ითვალისწინებენ გამონაკლისებს რისკების მიღების კუთხით, კერძოდ, როდესაც მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად, მნიშვნელოვანი საჯარო ინტერესის დასაცავად, კრიტიკული ინფორმაციული სისტემის სუბიექტი განსაზღვრავს ინფორმაციული უსაფრთხოების რისკების დასაშვებ დონეებს და მათი მიღების კრიტერიუმებს[112].

ევროკავშირის ან წევრი სახელმწიფოს კანონმდებლობის შესაბამისადაც დასაშვებია პერსონალური მონაცემების გამჟღავნება, საზოგადოებრივი ინტერესების გამო, სახელმწიფო უწყების მიერ საჯარო ფუნქციების შესასრულებლად, ოფიციალური დოკუმენტების საჯაროდ ხელმისაწვდომობის თვალსაზრისით, მაგრამ ევროკავშირის კანონმდებლობითვე მკაცრად დარეგულირებულია, რომ ამ დროს უზრუნველყოფილი უნდა იქნეს ოფიციალურ დოკუმენტების საჯაროდ ხელმისაწვდომობისა და პერსონალური მონაცემების დაცვას შორის ბალანსი[113].

ამდენად, მიუხედავად მნიშვნელოვანი საჯარო ინტერესის გამო მონაცემთა დამუშავების აუცილებლობისა (საჯარო რეესტრის წარმოება და ინფორმაციის ხელმისაწვდომობა[114]), აუცილებელია მონაცემთა დამმუშავებელმა მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც ადეკვატურად უზრუნველყოფს

---

[111] იქვე, გვ.33

[112] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1; 4.2.1 ,,გ“

[113] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) მუხლი 86.

[114] ,,საჯარო რეესტრის შესახებ“ საქართველოს კანონი, მუხ. 3; 1პუნქტი

მონაცემთა უსაფრთხოებას ნებისმიერი ფორმით უკანონო გამოყენებისაგან[115].

საჯარო რეესტრის ვებ გვერდზე - ,,napr.gov.ge“, ყოველგვარი მნიშვნელოვანი დაცვის მექანიზმების გარეშე, შესაძლებელია ისეთი პერსონალური მონაცემების მოპოვება, როგორიცაა მოქალაქის სახელი, გვარი, მისამართი როგორც ფაქტობრივი, ისე რეგისტრაციის, ტელეფონის ნომერი, ზოგიერთ შემთხვევაში პირადობის მოწმობის ასლი და ხელმოწერის ნიმუშიც კი. აღნიშნული უდავოდ იწვევს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების შელახვის რისკებს.

პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2018 წლის ანგარიშის მიხედვით გამოვლინდა, რომ ერთ-ერთი არაკომერციული ორგანიზაცია სპეციალური ალგორითმის საშუალებით მოიპოვებს საჯარო რეესტრის ეროვნული სააგენტოს ვებგვერდზე განთავსებულ მონაცემებს და რეესტრისგან განსხვავებული, შედარებით მარტივად ხელმისაწვდომი ფორმით ათავსებს ვებგვერდზე, ძებნის პარამეტრებში პირის საიდენტიფიკაციო მონაცემების მითითებით კი, ერთიანად არის შესაძლებელი მასთან დაკავშირებული სრული ინფორმაციის მიღება. ,,napr.gov.ge“ -სგან განსხვავებით, ორგანიზაციის ვებგვერდს არ გააჩნია საძიებო სისტემების წვდომის შეზღუდვის ტექნიკური ფუნქციონალი და ინფორმაცია ხელმისაწვდომი ხდება ნებისმიერ საძიებო სისტემაში პირის სახელისა და გვარის მითითების შემთხვევაშიც[116].

კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების სტანდარტის მიხედვით, ორგანიზაციის ინფორმაციისა და მისი დამუშავების საშუალებებზე მესამე მხარის მიერ წვდომის შემთხვევაში, ინფორმაციასთან დაკავშირებული რისკები უნდა იქნეს გამოვლენილი და დაინერგოს შესაბამისი კონტროლის მექანიზმები, წვდომის უფლების მინიჭებამდე[117].

---

[115] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი.

[116] პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის ანგარიში, თბილისი, 2018, 34.

[117] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1; ა.6.2.

საჯარო რეესტრის ვებ გვერდზე (napr.gov.ge) ინფორმაციული უსაფრთხოების უზრუნველყოფის ტექნიკურ-ორგანიზაციულ ადეკვატურ ზომად ჩაითვლებოდა, მომხმარებლის მიერ, ინფორმაციის მოპოვებამდე მინიმალური საიდენტიფიკაციო პროცედურის გავლა, მაგალითად, მობილური ტელეფონის საშუალებით SMS რეგისტრაცია, საჯარო რეესტრის სააგენტოს მხრიდან ავტომატურად, სათანადო კოდის გაგზავნით. ხოლო საჯარო რეესტრის ეროვნული სააგენტო მოახდენდა ამ სატელეფონო ნომრების ავტომატურ აღრიცხვას, იმ შემთხვევისათვის თუ ადგილი ექნებოდა მომხმარებლის მხრიდან კანონმდებლობის დარღვევას, მისი ვინაობის მარტივად დადგენის მიზნით. აღნიშნულ მექანიზმს ასევე ექნებოდა პრევენციული ხასიათი, ვებ-გვერდის მომხმარებლის პერსონალიზაციის გამო, მისი პასუხისმგებლობის განცდის ამაღლების კუთხით, მონაცემთა ბაზების მხოლოდ კანონიერი მიზნით გამოყენებისათვის.

ამდენად, პერსონალურ მონაცემთა დამუშავება უნდა ემსახურებოდეს კაცობრიობას. პერსონალურ მონაცემთა დაცვის უფლება არ არის აბსოლუტური უფლება, ის უნდა განიხილებოდეს საზოგადოებაში მისი ფუნქციის შესაბამისად და დაცული უნდა იქნეს ბალანსი ამ უფლებასა და სხვა ფუნდამენტურ უფლებებს შორის, პროპორციულობის პრინციპის შესაბამისად[118].

## 5. მონაცემთა შენახვის ვადები

,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ“ ბოლო წლების ანგარიშებში, მწვავედ დგას საკითხი პერსონალური მონაცემების შენახვის ვადებთან დაკავშირებით. საჯარო სამსახურებში ხშირად ირღვევა პრინციპი, რომ მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად[119].

---

[118] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს).Recital 4 Data protection in balance with other fundamental rights* იხ. <https://gdpr-info.eu/recitals/no-4/> [25.06.2019]

[119] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის ,,ე” ქვეპუნქტი.

მონაცემთა დაცვის ევროპული ძირითადი რეგულაციის მიხედვით, პერსონალური მონაცემების შენახვის ვადა, უნდა იყოს მკაცრად მინიმალური პერსონალური მონაცემების გაუმართლებლად ხანგრძლივი პერიოდის განმავლობაში შენახვის თავიდან ასაცილებლად. დამმუშავებელმა უნდა განსაზღვროს ვადა, რომლის გასვლის შემდეგ მოხდება მონაცემების წაშლა ან პერიოდული გადახედვა[120].

რეგულაცია აძლიერებს ინდივიდის უფლებებს და განსაზღვრავს მონაცემთა სუბიექტის ახალ შესაძლებლობებს, მონაცემთა დამმუშავებელ ორგანიზაციებს კი აკისრებს შესაბამის ვალდებულებებს, სუბიექტის მონაცემების წაშლის უფლების მიმართულებით. მაგალითად თუ მონაცემები აღარ არის საჭირო იმ მიზნის მისაღწევად, რისთვისაც მოხდა მათი შეგროვება ან დამუშავება. თუ დამუშავება განხორციელდება არაკანონიერად ან/და პირი გაითხოვს თანხმობას, რომლის საფუძველზეც მუშავდებოდა მონაცემები, ორგანიზაცია ვალდებულია წაშალოს მონაცემები. ამასთან, თუ ეს არ მოითხოვს არაპროპორციულად დიდ ძალისხმევას, ორგანიზაციამ უნდა აცნობოს მონაცემთა ყველა მიმღებს მონაცემთა წაშლის საჭიროების თაობაზე, ხოლო როდესაც ორგანიზაციას პირის მოთხოვნის საფუძველზე ევალება საჯაროდ (მაგალითად ინტერნეტში) გამოქვეყნებული მონაცემების წაშლა, მან ამის შესახებ, არსებული ტექნოლოგიებისა და ხარჯების გათვალისწინებით, უნდა აცნობოს სხვა ორგანიზაციებს, რომლებიც ამავე მონაცემებს ამუშავებენ[121].

მნიშვნელოვანია უსაფრთხოების სტანდარტებით გათვალისწინებული ბერკეტები პერსონალური მონაცემების შენახვის ვადებთან დაკავშირებით. ISO27000 უსაფრთხოების სტანდარტით დადგენილია, რომ აქტივების მართვის ფარგლებში აუცილებელია ყველა აქტივის აღწერა და მნიშვნელოვანი აქტივების ინვენტარიზაცია. ინფორმაციის და ინფორმაციის დამუშავებასთან

---

[120] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) Recital 39; იხ. <https://gdpr-info.eu/recitals/no-39/> [25.06.2019]

[121] ,,რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ“ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი; გვ. 11; იხ. <https://www.undp.org/content/dam/georgia/docs/publications/DG/UNDP_GE_DG_PDPI_GDPR_geo.pdf> [25.06.2019]

დაკავშირებული აქტივების დასაშვები მართვის წესები უნდა ჩამოყალიბდეს, მოხდეს მისი დოკუმენტირება და დანერგვა[122].

აქტივების ინვენტარიზაციისას აუცილებლობას წარმოადგენს ინფორმაციის კლასიფიცირება. ინფორმაციის კლასიფიკაცია უნდა მოხდეს მისი ორგანიზაციაში ღირებულების, საკანონმდებლო მოთხოვნების, მგრძნობიარობისა და კრიტიკულობის გათვალისწინებით. ჩამოყალიბდეს და დაინერგოს ინფორმაციის მარკირებისა და მისი მოპყრობის სათანადო პროცედურები ორგანიზაციაში მიღებული კლასიფიკაციის სქემის შესაბამისად[123].

აღნიშნული მექანიზმების გამოყენებით, პერსონალური ინფორმაციის შემცველი მასალები, გარდა იმისა, რომ დაცული უნდა იყოს არამიზნობრივი გამოყენებისაგან, მისი მგრძნობიარობისა და კრიტიკულობის გათვალისწინებით, მნიშვნელოვანია შენახული იქნეს აუცილებლად იმ ვადით, რა ვადითაც საჭიროა შენახვის მიზნების მიღწევა. ამისათვის აუცილებელია მონაცემთა შენახვის საჭიროების საკითხის პერიოდული გადახედვა, რასაც როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშებიდან ჩანს საჯარო უწყებები ნაკლებ ყურადღებას უთმობენ. ამდენად, მნიშვნელოვანია უწყებაში შიდა რეგულაციის დამტკიცება, რომლის მიხედვითაც განისაზღვრება მონაცემთა შენახვის ვადების მონიტორინგზე პასუხისმგებელი პირი და გაიწერება წესები ვადების გადახედვის პერიოდულობასთან დაკავშირებით, ხოლო თუ დამმუშავებელს სურს მათი შენახვა იმ ვადის გასვლის შემდეგ, რაც საჭირო იყო საწყისი მიზნის მისაღწევად, ამ შემთხვევაში მონაცემი უნდა იქნეს ანონიმირებული[124].

თავის მხრივ მონაცემთა დაცვის პრინციპები არ ვრცელდება ანონიმურ ინფორმაციაზე, კერძოდ, ინფორმაციაზე, რომელიც არ შეეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს ან პერსონალურ მონაცემებზე, რომელიც ანონიმიზებულია იმგვარად,

---

[122] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1; ა.7.1

[123] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი, დანართი N1; ა.7.2

[124] გოშაძე კ., მონაცემთა დაცვის ევროპული სამართალი. თარგმანი, თბილისი 2015, იურისტის გამომცემლობა. © ძირითადი უფლებების ევროპული კავშირის სააგენტო, 2014 ევროპის საბჭო, 2014. გვ. 58.

რომ მონაცემთა სუბიექტის იდენტიფიცირება აღარ არის შესაძლებელი[125].

## 6. მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Data Protection by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Data Protection by Default“)

ახალი პროდუქტის ან მომსახურების შექმნის პროცესში მონაცემთა დაცვის სტანდარტების გათვალისწინების კონცეფცია - „Privacy by Design“, 2009 წელს შეიმუშავა ინფორმაციისა და პირადი ცხოვრების დაცვის ყოფილმა კომისარმა - ანა კავუკიანმა (ონტარიო, კანადა), რომლის მიხედვითაც მოქმედების შვიდი ძირითადი პრინციპია განსაზღვრული, ესენია: პროაქტიული და არა რეაქტიული, ანუ პროფილაქტიკური და არა გამოსწორებაზე ორიენტირებული მიდგომა; მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“), რაც გულისხმობს საწყის ეტაპზე მინიმალური მონაცემების დამუშავებას და მონაცემთა სუბიექტისათვის საშუალების მიცემას თავად განკარგოს მონაცემების ღიაობა; კონფიდენციალურობის უზრუნველყოფა; სრული ფუნქციონალურობა - დადებითი თანხა არ არის ნულოვანი თანხა, რაც გულისხმობს არასაჭირო კომპრომისების გამორიცხვას კონფიდენციალურობის და უსაფრთხოების დასაცავად; მუდმივი უსაფრთხოება; გამჭვირვალობა; მომხმარებლის კონფიდენციალურობის პატივისცემა[126].

დროთა განმავლობაში ზემოაღნიშნული პრინციპები მონაცემთა დაცვის უმთავრეს მიდგომებად გარდაიქმნა და მონაცემთა დაცვის ევროპული რეგულაციის საფუძვლებში იქნა წარმოდგენილი.

---

[125] General Data Protection Regulation, (EU) 2016/679, (მიღებულია 2016 წლის 27 აპრილს, ძალაში შევიდა 2018 წლის 25 მაისს) Recital 26; იხ. <https://gdpr-info.eu/recitals/no-26/> [25.06.2019]

[126] Cavoukian A., Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices; Ph.D. Information & Privacy Commissioner, Ontario, Canada, იხ. <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> [25.06.2019]

მონაცემთა დაცვის ევროპული ძირითადი რეგულაციის მიხედვით, მონაცემთა კატეგორიის, მოცულობის, დამუშავების მიზნების, საფუძვლების, ტექნიკური საშუალებებისა და რისკების გათვალისწინებით, ორგანიზაციებს ევალებათ მონაცემთა დაცვისთვის საჭირო ტექნიკური და ორგანიზაციული ზომების მიღება დამუშავების საშუალებების განსაზღვრის ეტაპზევე. ამ ზომების მიღება უნდა მოხდეს უშუალოდ დამუშავების საშუალებების, მაგალითად, ელექტრონული პროგრამის შექმნისას.

ორგანიზაციებს საწყის ეტაპზევე ევალებათ კონკრეტულ კანონიერ მიზანთან მონაცემთა მოცულობისა და დამუშავების ვადის შესაბამისობის უზრუნველყოფა. მონაცემები თავისთავად („by default“) არ უნდა იყოს ხელმისაწვდომი პირთა განუსაზღვრელი წრისთვის. მაგალითად, სოციალური ქსელის ან აპლიკაციის ოპერატორმა უნდა უზრუნველყოს, რომ მომხმარებლის მიერ ფოტოს გამოქვეყნებისას პირველადი პარამეტრი იყოს პრივატული და მხოლოდ მაშინ გახდეს საჯარო, თუ პირი თავად შეცვლის შესაბამის პარამეტრს[127].

აღნიშნულ პრინციპებს ეფუძნება მონაცემთა დაცვის ევროპული ძირითადი რეგულაცია და ინფორმაციული უსაფრთხოების სტანდარტები[128].

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით დადგენილი უსაფრთხოების სტანდარტის (ISO27001) შესაბამისად, ახალი ინფორმაციული სისტემის დანერგვის, ან არსებული სისტემის გაუმჯობესების ფარგლებში, უზრუნველყოფილი უნდა იყოს უსაფრთხოების კონტროლის მოთხოვნები[129].

კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ, ახალი სერვისების დანერგვის პროცესში აუცილებელია მკაცრად იქნეს გათვალისწინებული აღნიშნული პრინციპები, რაც უსაფრთხოების სტანდარტების დამატებით დებულებად შეიძლება განიხილებოდეს.

---

[127] ,,რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ“ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი; გვ. 15 იხ. <https://www.undp.org/content/dam/georgia/docs/publications/DG/UNDP_GE_DG_PDPI_GDPR_geo.pdf> [25.06.2019]

[128] <https://gdpr-info.eu/issues/privacy-by-design/> [25.06.2019]

[129] მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანება N2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ 2013 წლის 4 თებერვალი; დანართი N1; ა.12

მნიშვნელოვანია მონაცემთა დაცვის პროცესის საწყის ეტაპზე შეფასება, რათა უწყებაში პროფილაქტიკური და არა გამოსწორებაზე ორიენტირებული მიდგომა იყოს უზრუნველყოფილი. 2019 წლის 22 მაისს, სახელმწიფო ინსპექტორის სამსახურის ინიციატივით, საქართველოს პარლამენტში შეტანილი ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონპროექტის 31-ე მუხლით, დარეგულირებულია მონაცემთა დამუშავების ზეგავლენის შეფასება დამმუშავებლის მიერ, იმ შემთხვევაში, როდესაც მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნების და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებების შელახვის საფრთხე[130].

ასევე, მონაცემთა დამუშავების ზეგავლენის შეფასების განხორციელება სავალდებულოა თუ მონაცემთა დამმუშავებელი, მონაცემთა სუბიექტისათვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს პროფილირების საფუძველზე, ან/და ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს ან ახორციელებს მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში[131].

ზეგავლენის შეფასების დოკუმენტში უნდა აისახოს მონაცემთა კატეგორიის, მათი დამუშავების მიზნების, პროპორციულობის, პროცესისა და საფუძვლების აღწერა, ასევე ადამიანის ძირითადი უფლებების შელახვის შესაძლო საფრთხეების შეფასება და მონაცემთა უსაფრთხოების დაცვის მიზნით გათვალისწინებული ორგანიზაციულ-ტექნიკური ზომების აღწერა. ხოლო თუ აღმოჩნდება, რომ ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითად უფლებათა შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს[132].

---

[130] იხ. <https://info.parliament.ge/#law-drafting/18184> [25.06.2019]

[131] იხ. <https://info.parliament.ge/file/1/BillReviewContent/222089?> [25.06.2019] 31-ე მუხლის მე-2 პუნქტის ,,ბ“ ქვეპუნქტი.

[132] იხ. <https://info.parliament.ge/file/1/BillReviewContent/222089?> [25.06.2019] 31-ე მუხლის მე-5 პუნქტი

მნიშვნელოვანია მონაცემთა დამუშავების ზეგავლენის შეფასების დოკუმენტში აისახოს თუ რამდენად ხორციელდება მონაცემთა დამმუშავებლის მიერ მონაცემთა დამუშავების უსაფრთხოების უზრუნველყოფის ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარული შემოწმებისა და შეფასების ღონისძიებები. ასევე, საჭიროა წარმოდგენილი იქნეს ინფორმაცია, რამდენად ხორციელდება ელექტრონული სისტემის მეშვეობით დამუშავებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, ფსევდონიმიზაციის ან დეპერსონალიზაციის გამოყენების შემთხვევები, ინფორმაციის მესამე პირზე გადაცემისას მიღებული ზომები პერსონალურ მონაცემთა დაცვის უზრუნველსაყოფად, ინფორმაციის ინტერნეტსივრცეში გასაჯაროებისას დანერგილი მექანიზმები, გამოქვეყნებული ინფორმაციის მხოლოდ მიზნობრივად გამოყენების უზრუნველსაყოფად და მონაცემთა შენახვის ვადების მონიტორინგის მდგომარეობა.

მონაცემთა დამუშავების ზეგავლენის შეფასების დოკუმენტში ზემოაღნიშნული ინფორმაციის ასახვა, აუცილებელია ადამიანის ძირითადი უფლებების შელახვის საფრთხის თავიდან ასაცილებლად.

## შედეგები და მათი განსჯა

საქართველოს საჯარო სექტორში, პერსონალური მონაცემების დაცვის მდგომარეობა გაუმჯობესების ტენდენციით ხასიათდება, თუმცა, ნაშრომში მოყვანილი პრობლემებისა და მათი აქტუალობის შინაარსიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის საუკეთესო პრაქტიკის დანერგვამდე, კვლავ დიდი გზაა გასავლელი.

მისასალმებელია ქვეყანაში ,,პერსონალურ მონაცემთა დაცვის“ ახალი კანონის ინიცირება, რომელიც გარკვეულწილად შესაბამისობაშია მონაცემთა დაცვის ევროპულ ძირითად რეგულაციასთან, აღნიშნული კანონის დანერგვა და აღსრულების უზრუნველყოფა, ერთიორად აამაღლებს ქვეყანაში პერსონალურ მონაცემთა დაცვის მდგომარეობას, თუმცა წინასწარ იმის ვარაუდი, რომ პერსონალურ მონაცემთა დაცვის ახალი კანონმდებლობა ერთი ხელის მოსმით გამოასწორებს ნაშრომში ასახულ პრობლემებს

- არ იქნება მართლზომიერი, რადგან ამ მხრივ ყოველი დეტალი ფასდება გარკვეული შედეგის საფუძველზე.

კრიტიკული ინფორმაციული სისტემის სუბიექტების მიერ მართვადი საჯარო ელექტრონული მონაცემთა ბაზები, კვლავ რჩება მთავარ პრობლემად პერსონალურ მონაცემთა დაცვის პროცესში. საჭიროა ადეკვატური ღონისძიებები პერსონალურ მონაცემებზე საჯარო წვდომის შეზღუდვის თვალსაზრისით. აუცილებელია მაქსიმალურად იქნეს შემცირებული მონაცემთა ბაზებზე არამიზნობრივი წვდომის შესაძლებლობა, რისთვისაც ნაშრომში წარმოდგენილი იქნა პრობლემის გადაჭრის გზები. ვებ გვერდზე მინიშნებული გამაფრთხილებელი ინფორმაცია, მონაცემების მხოლოდ მიზნობრივად გამოყენების შესახებ, რასაკვირველია ვერ იქნება საკმარისი ღონისძიება, მით უმეტეს იმ პირობებში, როდესაც მომხმარებელი სრულიად ანონიმურია და ბუნებრივია მონაცემებთან მოპყრობის კუთხით მისი პასუხისმგებლობის განცდა მინიმალური იქნება.

არანაკლებ მნიშვნელოვანია საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალურ მონაცემებთან მოპყრობის საკითხი. ბიომეტრიული მონაცემების დამუშავება თანამშრომელთა სამუშაო საათების აღრიცხვის მიზნით ცალსახად გადაჭარბებული მეთოდია, მაშინ როდესაც არსებობს სხვა უამრავი გზა იგივე მიზნის მისაღწევად, რომელიც არ საჭიროებს განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებას.

ასევე, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კუთხით, საყურადღებოა შინაგან საქმეთა სამინისტროს ცენტრალურ საინფორმაციო ბანკზე წვდომის საკითხი. მართალია გასულ წლებთან შედარებით ამ მხრივ ვითარება რადიკალურად გაუმჯობესებულია, თუმცა საჭიროა პერმანენტული მონიტორინგი რათა თავი არ იჩინოს ახალმა პრობლემებმა, მონაცემთა არამიზნობრივ გამოყენებასთან დაკავშირებით.

ამასთან, აღსანიშნავია პრობლემები საჯარო სექტორში მონაცემთა დეპერსონალიზაციის გამოყენებასთან დაკავშირებით. მაღალი საზოგადოებრივი ინტერესის შემცველი ინფორმაცია უნდა გასაჯაროვდეს იმგვარად, რომ პერსონალური მონცემები იყოს

დაშიფრული ყოველგვარი მიმანიშნებელი სიმბოლოების გარეშე, რათა მისი დაკავშირება კონკრეტულ პირთან იყოს შეუძლებელი.

ასევე, არ არის საკმარისი საჯარო უწყებამ, დაინტერესებულ პირს ინფორმაცია მიაწოდოს პერსონალური მონაცემების დაფარვით (ე.წ. ,,დაშტრიხული“ ფორმით), აუცილებელია ამასთანავე განხორციელდეს ყოველი ცალკეულ საკითხის ინდივიდუალურად შეფასება, თუ რა ინფორმაციას ფლობს, ან შესაძლოა ფლობდეს დაინტერესებული მხარე პერსონალურ მონაცემთა სუბიექტთან დაკავშირებით და არ გაიცეს ინფორმაცია, თუ არსებობს საფრთხე პერსონალურ მონაცემთა გამჟღავნებისა.

როდესაც არსებობს პერსონალურ მონაცემთა გასაჯაროების საფუძვლები, უნდა გასაჯაროვდეს მხოლოდ ის პერსონალური მონაცემები რაც საკმარისი იქნება მიზნის მისაღწევად, კერძოდ, არ არის აუცილებელი სახელსა და გვართან ერთად გასაჯაროვდეს მონაცემთა სუბიექტის პირადი ნომერი, ან პირიქით.

აუცილებელია ყველა საჯარო უწყებამ დანერგოს მონაცემთა შენახვის ვადების მონიტორინგის სისტემა, რათა შენახვის მიზნის მიღწევის შემთხვევაში დროულად მოახდინოს პერსონალური ინფორმაციის შემცველი მონაცემების წაშლა, ან საჭიროების შემთხვევაში მისი შენახვა პირის იდენტიფიცირების გამომრიცხავი ფორმით. მოახდინოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.

ამ და ნაშრომში ასახული სხვა პრობლემების ერთობლიობით გამოიკვეთა, რომ საჯარო სექტორში ინფორმაციული უსაფრთხოების კუთხით კვლავ უამრავი პრობლემაა გადასაჭრელი, რათა მათი გავრცელება პერსონალურ მონაცემთა დაცვის ხარისხზე იყოს ეფექტიანი, საკანონმდებლო აქტების მიზნების გათვალისწინებით.

## დასკვნა

ნაშრომში მოყვანილმა არგუმენტებმა, დაგვანახა, რომ მიუხედავად საჯარო სამსახურების ინფორმაციული უსაფრთხოების კუთხით მაღალი პასუხისმგებლობისა და კერძო სექტორისაგან განსხვავებით უფრო მაღალი სტანდარტის დანერგვის ვალდებულებისა, მრავლად გვევლინება რისკები პერსონალურ

მონაცემთა დაცვის პრინციპების დარღვევის თვალსაზრისით. ზემოაღნიშნულმა მაგალითებმა წარმოაჩინა, რომ პერსონალურ მონაცემთა დაცვა ცოცხალი პროცესია და ყოველ დეტალს სათანადო, ხშირ შემთხვევაში კი ინდივიდუალური მიდგომა სჭირდება.

პრობლემებს შორისაა ის, რომ საქართველოს კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ“ არ აწესებს ინფორმაციის დამმუშავებლის მიერ დამუშავების უსაფრთხოების უზრუნველყოფის ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარულ შემოწმებასა და შეფასებას, როგორც ეს ევროპულ კანონმდებლობაშია.

მართალია მსგავსი რეგულირება წარმოდგენილია ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით, თუმცა იგი არ არის სავალდებულოდ შესასრულებელი, ვინაიდან კრიტიკული ინფორმაციული სისტემის სუბიექტი უფლებამოსილია და არა ვალდებული ჩაატაროს ინფორმაციული უსაფრთხოების აუდიტი. აღნიშნულს ასევე აუარესებს ის გარემოება, რომ ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, საჯარო სექტორის დაახლოებით ერთ მეხუთედ ნაწილზე ვრცელდება.

ინფორმაციული უსაფრთხოების შესახებ საკანონმდებლო აქტებში, ნორმების არასავალდებულოდ შესასრულებელი ფორმულირებით ჩამოყალიბება, ასუსტებს კანონის მიზნების აღსრულების ხარისხს. აუცილებელია კრიტიკული ინფორმაციული სისტემის სუბიექტებისათვის კანონის ზედმიწევნით შესრულების უზრუნველყოფის მკაცრად ჩამოყალიბებული მიდგომები და ანგარიშგების მოთხოვნა. მით უმეტეს, მცირეა იმ უწყებათა ჩამონათვალი, რომელთაც ევალებათ ინფორმაციული უსაფრთხოების სტანდარტების დანერგვა.

სახელმწიფო სერვისებისა და სამსახურებრივი უფლებამოსილების შესრულების ელექტრონული ფორმით განხორციელების ფარგლებში, პრობლემას წარმოადგენს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვის პროცესი. როგორც ნაშრომშია ასახული, ამ მიმართულებით ბოლო წლებში მრავლად გამოვლინდა პერსონალურ მონაცემთა დაცვის პრინციპების

დარღვევის ფაქტები, რაც ცალსახად მიუთითებს, რომ აუცილებელია მონაცემთა დამმუშავებელმა უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა, რათა შემოწმებას ექვემდებარებოდეს, ხომ არ ხორციელდება მონაცემთა დამუშავება რაიმე არალეგიტიმური მიზნით, რაც აუცილებელია დროული რეაგირებისა და პრევენციული ღონისძიებების გატარების თვალსაზრისით.

ბუნდოვანია საჯარო უწყებებში მონაცემთა დაცვაზე პასუხისმგებელი პირის განსაზღვრის საკითხი. ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, ითვალისწინებს უსაფრთხოების მენეჯერის ინსტიტუტის დანერგვას ორმოც კრიტიკულ ინფორმაციულ სუბიექტში, უცნობია რამდენად ასრულებენ კრიტიკული ინფორმაციული სუბიექტები აღნიშნულ მოთხოვნას, თუმცა ამ მხრივ პოზიტიური მაჩვენებლის შემთხვევაშიც კი, აღნიშნული საკანონმდებლო ნორმა უმეტეს სახელმწიფო უწყებებზე არ ვრცელდება. აღნიშნულ მდგომარეობას აუარესებს ასევე ის გარემოება, რომ ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი არ ითვალისწინებს მონაცემთა დამმუშავებლის მიერ მონაცემთა დაცვის ოფიცერის ინსტიტუტის დანერგვას.

ამდენად, აუცილებელია დროულად ამოქმედდეს მონაცემთა დაცვის ევროპულ რეგულაციაზე დაფუძნებული ახალი კანონი ,,პერსონალურ მონაცემთა დაცვის შესახებ“, რაც იძლევა მოცემულობას, რომ კრიტიკული ინფორმაციის სუბიექტებში, ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით გათვალისწინებული მონაცემთა უსაფრთხოების სტანდარტების დანერგვის შემთხვევაში, მონაცემთა დაცვის ოფიცერთან ერთად, ინფორმაციული უსაფრთხოების დაცვის მიმართულებით, განსაზღვრული იქნება ასევე ინფორმაციული უსაფრთხოების მენეჯერის პოზიცია, რაც უმაღლეს სტანდარტებზე დააყენებს უწყებაში მონაცემთა უსაფრთხოების გარემოს.

აქტუალურია საჯარო სამსახურების მხრიდან მონაცემთა დეპერსონალიზაციისადმი მიდგომები. ინფორმაციის საჯაროდ გამოქვეყნებისას, მონაცემთა სუბიექტის სახელისა და გვარის ინიციალებით აღნიშვნა იწვევს მაღალ რისკს, შესაძლებელი გახდეს მათი დაკავშირება მონაცემთა სუბიექტთან, ინფორმაციის სხვა

წყაროებიდან მიღების შემთხვევაში. ამისათვის, მსგავს შემთხვევაში, აუცილებელია საჯარო სამსახურებმა უზრუნველყონ მონაცემთა დაშიფრვა იმგვარად, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან, ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებსა და დროს საჭიროებდეს. აღნიშნულის განხორციელება კი შესაძლებელია ინიციალების ნაცვლად პირობითი სიმბოლოების გამოყენებით.

როგორც საჯარო სამსახურების პრაქტიკა გვიჩვენებს, საფრთხის შემცველია უწყების თანამშრომელის სამსახურიდან გათავისუფლებისას, მის მიერ ინფორმაციული აქტივის დაუფლება შემდგომში რაიმე არამართლზომიერი გამოყენების მიზნით, რომლის კონტროლის მექანიზმის დანერგვა განსაკუთრებულ სირთულეს წარმოადგენს. მეტიც, ხშირ შემთხვევაში შესაძლოა შეუძლებელიც იყოს. ამ მხრივ რისკების შესამცირებლად, მიზანშეწონილია უწყებაში დასაქმებულ თანამშრომელს, მის მიერ დაკავებული თანამდებობიდან გათავისუფლებამდე, ჩამოერთვას ხელწერილი კონფიდენციალური ინფორმაციის არამიზნობრივად გამოყენების შესახებ პასუხისმგებლობის თაობაზე.

მნიშვნელოვანია მონაცემთა დამუშავების თანამედროვე მიდგომების სწრაფად გავრცელება საჯარო უწყებებზე და მიზანშეწონილია ,,ინფორმაციული უსაფრთხოების შესახებ“ კანონის ცვლილება ISO 27001:2013 სტანდარტის საფუძველზე, რაც გააუმჯობესებს ინფორმაციული უსაფრთხოების დაცვის ხარისხს.

,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონმდებლობის პრინციპების დარღვევას წარმოადგენს, საჯარო უწყების თანამშრომელთა სამსახურში გამოცხადების აღრიცხვის მიზნით, სენსიტიური მონაცემების (თითის ანაბეჭდი) დამუშავება. აღნიშნული მიზნის მიღწევა ცალსახად შესაძლებელია სხვა ტექნიკური საშუალებებით, რომლებიც არ საჭიროებენ სენსიტიური მონაცემების დამუშავებას.

მონაცემთა დაცვის თვალსაზრისით, მაღალი მგრძნობიარობით გამოირჩევა ინფორმაციის მესამე პირებისათვის მიწოდების საკითხი. ელექტრონულ მიმოწერაში მოხვედრილი ინფორმაცია უნდა იყოს ადეკვატურად დაცული ადამიანური შეცდომებისაგან. ინფორმაციის პერსონალური მონაცემების დაფარვით გაგზავნის შემთხვევაში, დამმუშავებელმა უნდა შეაფასოს რამდენად იძლევა აღნიშნული

ფორმით ინფორმაციის მიწოდება ანონიმირებული პირის იდენტიფიცირების შესაძლებლობას. შეფასება თავის მხრივ მოიცავს დამმუშავებლის ხელთ არსებული, ადრესატისათვის ცნობილი ინფორმაციების ანალიზს, რაც საშუალებას მისცემს მონაცემთა დამმუშავებელს, დაასკვნას თუ რამდენად შესაძლებელია ადრესატისათვის ცნობილი იყოს საკითხთან დაკავშირებული პერსონალური მონაცემები. სწორედ აღნიშნული შეფასების შედეგად უნდა მიიღოს დამმუშავებელმა გადაწყვეტილება ადრესატისათვის ინფორმაციის მიწოდების თაობაზე.

განსაკუთრებით პრობლემატურია საჯარო ელექტრონული მონაცემთა ბაზები. როგორც ნაშრომში მოყვანილი არგუმენტები გვიჩვენებს, მიუხედავად იმისა, რომ საზოგადოებრივი ცხოვრებისათვის აუცილებელია გარკვეული ინფორმაციის ინტერნეტსივრცეში ხელმისაწვდომობა, სასიცოცხლოდ მნიშვნელოვანია დაცული იქნეს ბალანსი ოფიციალურ დოკუმენტებზე საჯაროდ ხელმისაწვდომობასა და პერსონალურ მონაცემთა დაცვას შორის.

უწყებებმა არ უნდა გაასაჯაროონ მიზნის მისაღწევად საჭიროზე მეტი პერსონალური ინფორმაცია. დაუშვებელია ცენტრალური საარჩევნო კომისიის ვებ გვერდის ამჟამინდელი ფორმით ფუნქციონირება, ვინაიდან ნებისმიერ ფიზიკურ პირს, ყოველგვარი კონტროლის მექანიზმების გარეშე, იმ შემთხვევაში თუ მას მოპოვებული აქვს სხვისი გვარი და პირადი ნომერი, ვებ გვერდზე არსებულ საძიებო ველში შეყვანით, შეუძლია მოიპოვოს უამრავი პერსონალური ინფორმაცია, რაც ცალსახად არღვევს პერსონალურ მონაცემთა დაცვის საერთაშორისოდ აღიარებულ პრინციპებს.

მით უმეტეს, აღნიშნული პრობლემის გადაჭრა არ წარმოადგენს განსაკუთრებულ სირთულეს. მაგალითად, ვებ გვერდის ფუნქციონირების, მხოლოდ მიზნობრივად გამოსაყენებლად, შესაძლებელია თითოეულ ამომრჩეველს ერთჯერადად გადაეცეს უნიკალური კოდი, რომლის ცენტრალური საარჩევნო კომისიის ოფიციალურ ვებ გვერდზე, შესაბამის ველში აუცილებლად შეყვანით იქნებოდა შესაძლებელი ამომრჩევლის მიერ, მისი პირადი მონაცემების გადამოწმება.

ანალოგიური პრობლემა გვევლინება საჯარო რეესტრის ვებ გვერდის შემთხვევაში, სადაც ყოველგვარი მნიშვნელოვანი დაცვის

მექანიზმების გარეშე, შესაძლებელია უამრავი პერსონალური მონაცემის შემცველი ინფორმაციის მოპოვება.

ამ შემთხვევაში, ინფორმაციული უსაფრთხოების უზრუნველყოფის ტექნიკურ-ორგანიზაციულ ადეკვატურ ზომად ჩაითვლებოდა, მომხმარებლის მიერ, ინფორმაციის მოპოვებამდე, მინიმალური საიდენტიფიკაციო პროცედურის გავლა, მობილური ტელეფონის საშუალებით.

ნაშრომში ასახული აქტუალური პრობლემათაგანია, პერსონალური მონაცემების გაუმართლებლად ხანგრძლივი პერიოდის განმავლობაში შენახვა. აღნიშნული შეიცავს რისკებს ადამიანის პირადი ცხოვრების შელახვის კუთხით. ამისათვის მნიშვნელოვანია უწყებაში შიდა რეგულაციის დამტკიცება, რომლის მიხედვითაც განისაზღვრება მონაცემთა შენახვის ვადების მონიტორინგზე პასუხისმგებელი პირი და გაიწერება წესები ვადების გადახედვის პერიოდულობასთან დაკავშირებით, რაც თავის მხრივ მოემსახურება მიზანს, მონაცემთა შენახული იყოს დამუშავების ამოცანისათვის საჭირო ვადით.

როგორც ნაშრომში აღინიშნა, სახელმწიფო ინსპექტორის სამსახურის ინიციატივით, 2019 წლის 22 მაისს, საქართველოს პარლამენტში შეტანილი ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონპროექტი, ითვალისწინებს დამმუშავებლის მიერ მონაცემთა დამუშავების ზეგავლენის შეფასების დოკუმენტის შედგენას (31-ე მუხლი), იმ შემთხვევაში, თუ იქმნება ადამიანის ძირითადი უფლებების შელახვის საფრთხე. ვინაიდან, წინამდებარე ნაშრომში ასახული პრობლემატური საკითხებიდან, ცალსახად გამოიკვეთა ადამიანის ძირითად უფლებათა შელახვის საფრთხე, მონაცემთა დამუშავების ზეგავლენის შეფასების დოკუმენტის აუცილებელ შემადგენელად უნდა განისაზღვროს: მონაცემთა დამუშავების უსაფრთხოების უზრუნველყოფის ტექნიკური და ორგანიზაციული საშუალებების ეფექტიანობის რეგულარული შემოწმებისა და შეფასების ღონისძიებების დეტალური აღწერა; ელექტრონული სისტემის მეშვეობით დამუშავებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვის მდგომარეობა; დამმუშავებლის მიერ ფსევდონიმიზაციის ან დეპერსონალიზაციის გამოყენების შემთხვევების დეტალური აღწერა; ინფორმაციის მესამე პირზე გადაცემისას მიღებული ზომები პერსონალურ მონაცემთა

კონფიდენციალურობის უზრუნველსაყოფად; ინფორმაციის ინტერნეტსივრცეში გასაჯაროებისას გამოყენებული მექანიზმები, გამოქვეყნებული ინფორმაციის მხოლოდ მიზნობრივად გამოყენების უზრუნველსაყოფად და მონაცემთა შენახვის ვადების მონიტორინგის აღწერა.

ნაშრომში ასახული პრობლემების ერთობლიობა გვიჩვენებს, რომ უწყებებმა ახალი სერვისების დანერგვის პროცესში უნდა გაითვალისწინონ მონაცემთა დაცვის საერთაშორისოდ აღიარებული პრინციპები, წინააღმდეგ შემთხვევაში თავს იჩენს პერსონალურ მონაცემთა არამართლზომიერი ხელყოფის შემთხვევები, რაც უარყოფითად აისახება ქვეყანაში პერსონალურ მონაცემთა დაცვის ხარისხზე და ადამიანის უფლებათა დაცვის მდგომარეობაზე.

ამდენად, თანამედროვე გამოწვევები მუდმივად ითხოვს პერსონალურ მონაცემთა დაცვის ახალი მექანიზმების დანერგვას, მონიტორინგს და შეფასებას. ვინაიდან ქვეყნის განვითარების პროცესში უმთავრესია ადამიანის უფლებების დაცვის ხარისხი, აუცილებელია საზოგადოების თითოეულ წევრი ცხოვრობდეს ისეთ გარემოში, სადაც პირადი ცხოვრებისა და ღირსების შელახვისაგან ადეკვატურად იქნება დაცული.

## გამოყენებული ლიტერატურა

### სამეცნიერო ნაშრომები


*გოშაძე კახაბერ,* მონაცემთა დაცვის ევროპული სამართალი, თარგმა-

ნი, იურისტის გამომცემლობა. © ძირითადი უფლე-
ბების ევროპული კავშირის სააგენტო, ევროპის
საბჭო 2014, თბილისი, 2015

*Clarke Roger*, The Digital Persona and Its Application to Data Surveillance,

The Info. Soc. June 1994

*Cavoukian Ann*, Privacy by Design The 7 Foundational Principles Imple-
Mentation and Mapping of Fair Information Practices,

Information & Privacy Commissioner, Ontario, Canada, 2010

*Drew Cat,* Data science ethics in government, Published: 28 December 2016

*Lessig Lawrence*, The Architecture of Privacy, April 3, 1998

Handbook on European Data Protection Law, FRA, CoE, ECHR. – 2018

Edition, 2018

Guidelines on the protection of personal data in IT governance and IT management of EU institutions, 23 March 2018

A Closer Look At Data Protection Officer, Information commissioner, V1 September, 2017

ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, სასამართლო გადაწყვეტილებათა ხელმისაწვდომობა საქართველოში: საერთო სასამართლოების პრაქტიკის ანალიზი, 2017

რა უნდა ვიცოდეთ ევროკავშირის მონაცემთა დაცვის რეგულაციის შესახებ, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2018

## სამართლებრივი აქტები და ანგარიშები

საქართველოს 1995 წლის 24 აგვისტოს კონსტიტუცია

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

,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია

მონაცემთა დაცვის ძირითადი ევროპული რეგულაცია

,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი

,,საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“ საქართველოს კანონი

საქართველოს იუსტიციის მინისტრის 2009 წლის 22 დეკემბრის ბრძანება N228 ,,საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს დებულების დამტკიცების შესახებ“

,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი

საქართველოს მთავრობის 2014 წლის 29 აპრილის დადგენილება N312 ,,კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ”

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანება №4 ,,კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერისათვის მინიმალური სტანდარტების დამტკიცების შესახებ“

,,ინფორმაციის ერთიანი სახელმწიფო რეესტრის შესახებ“ საქართველოს კანონი

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანება №5 ,,მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“

საქართველოს მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2011 წლის 13 ივლისის ბრძანება №52/ს „მონაცემთა გაცვლის სააგენტოსთვის ინფორმაციის ერთიან სახელმწიფო რეესტრში შესატანად ინფორმაციის მიწოდების პროცედურების, ტექნიკური სტანდარტების, ფორმატისა და მიწოდების გზების შესახებ“ ინსტრუქციის დამტკიცების თაობაზე

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანება №2 ,,ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანება №3 ,,ქსელური სენსორის კონფიგურაციის წესების დამტკიცების შესახებ“

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 7 თებერვლის ბრძანება №7 ,,ინფორმაციული აქტივების მართვის წესების დამტკიცების შესახებ“

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლისბრძანება №1 ,,ინფორმაციული უსაფრთხოების აუდიტის ჩატარების წესის დამტკიცების შესახებ“

მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის ბრძანება №6 ,,ინფორმაციული უსაფრთხოების აუდიტის ჩატარების უფლებამოსილების მქონე პირთა და ორგანიზაციათა მიერ ავტორიზაციის გავლის წესის, ავტორიზაციის პროცედურების და ავტორიზაციის საფასურის დამტკიცების შესახებ“
საქართველოს მთავრობის 2013 წლის 19 ივლისის დადგენილება №180 ,,პერსონალურ მონაცემთა დაცვის ინსპექტორის საქმიანობისა და მის მიერ უფლებამოსილების განხორციელების წესის შესახებ“ დებულების დამტკიცების თაობაზე
,,საჯარო სამსახურის შესახებ“ საქართველოს კანონი
,,საერთაშორისო დაცვის შესახებ“ საქართველოს კანონი

## ელექტრონული წყაროები

<http://parliament.ge/ge/kanonmdebloba/announcements-all/gancxadebebi-mimartvebi-da-dadgenilebebi> [10.06.2019]
<http://www.dea.gov.ge/?action=0&lang=geo> [04.05.2019]
<https://gdpr-info.eu/> [07.06.2019]
<https://info.parliament.ge/file/1/BillReviewContent/63200> [10.06.2019]
<https://gdpr-info.eu/recitals/no-6/> [02.06.2019]
<https://doi.org/10.1098/rsta.2016.0119> [10.06.2019]
<http://www.nplg.gov.ge/gsdl/cgi-bin/library.exe?e=d-01000-00---off-0samartal--00-1----0-10-0---0---0prompt-10---4-------0-1l--11-ka-50---20-about---00-3-1-00-0-0-11-1-0utfZz-8-00&cl=CL4.3&d=HASH01ffaf957157488e546f5b51.2.1&gt=1> [09.06.2019]
<https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf> [12.06.2019]
<https://www.geostat.ge/ka/modules/categories/38/dasakmeba-da-umushevroba> [01.05.2019]
<http://www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=16589> [10.06.2019]
<https://www.inforights.im/media/1416/dpo.pdf> [14.06.2019]
<https://info.parliament.ge/#law-drafting/18184> [14.06.2019]

<https://info.parliament.ge/file/1/BillReviewContent/222087?> [11.06.2019]
<https://personaldata.ge/cdn/2018/12/angarishi_2017.pdf> [10.06.2019]
<https://www.iso.org/about-us.html> [10.05.2019]
<https://www.nbg.gov.ge/index.php?m=340&newsid=26701> [04.06.2019]
<http://procurement.gov.ge/> [02.06.2019]
<https://tenders.procurement.gov.ge/public/library/contract.php?go=274176> [02.06.2019]
<http://manage.personaldata.ge/res/docs/recommendation/Guidelines%20on%20Biometric%20Data.pdf> [10.06.2019]
<www.deloitte.com> [10.06.2019]
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en> [09.06.2019]
<https://voters.cec.gov.ge/> [25.06.2019]
<https://sao.ge/lepl-pai/lepl-pai-certification/lepl-pai-list-of-certified-people> [22.06.2019]
<https://gdpr-info.eu/recitals/no-4/> [20.06.2019]
<https://gdpr-info.eu/recitals/no-39/> [11.06.2019]
<https://www.undp.org/content/dam/georgia/docs/publications/DG/UNDP_GE_DG_PDPI_GDPR_geo.pdf> [08.06.2019]
<https://www.undp.org/content/dam/georgia/docs/publications/DG/UNDP_GE_DG_PDPI_GDPR_geo.pdf> [14.06.2019]
<https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf> [10.06.2019]