

# პერსონალურ მონაცემთა დაცვის ქირითადი უფლება



თბილისი  
2020

წინამდებარე ნაშრომი გამოცემულია ევროპის უნივერსიტეტის ფინანსური მხარდაჭერით. ევროპის უნივერსიტეტი ხელს უწყობს იურიდიული ლიტერატურის შექმნასა და პერსონალურ მონაცემთა დაცვის პოპულარიზაციას. უნივერსიტეტი პასუხს არ აგებს წიგნში მოცემულ შინაარსზე.

**ავტორი:** კახაბერ გოშაძე, სამართლის დოქტორი,  
ევროპის უნივერსიტეტის ასოცირებული პროფესორი.

**სამეცნიერო რედაქტორი:** მალხაზ ბეგიაშვილი, სამართლის  
დოქტორი, საქართველოს უნივერსიტეტის პროფესორი

© კახაბერ გოშაძე, 2020



**გამომცემლობა „იურისტების სამყარო“**

თბილისი, მ. კოსტავას №75; 0171

ტელ.: (+995 032) 238 35 99; (+995) 557 51 51 34

ვებ-გვერდები: [www.law.ge](http://www.law.ge)

ელ-ფოსტა: [Info@law.ge](mailto:Info@law.ge)

[www.facebook.com/PublishingWorldofLawyers](https://www.facebook.com/PublishingWorldofLawyers)

ISBN 978-9941-9698-4-3

## შინაარსი

|                                                                                                                                                                                     |           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>შესავალი.....</b>                                                                                                                                                                | <b>6</b>  |
| <b>თავი I. პირადი ცხოვრების უფლების<br/>კონცეპტუალური საფუძვლები და სამართლებრივი<br/>მონესრიგება .....</b>                                                                         | <b>8</b>  |
| 1.1. პირადი ცხოვრების უფლების არსი და კონცეფცია.....                                                                                                                                | 8         |
| 1.2. პირადი ცხოვრების უფლებით დაცული სფერო და<br>ჩარევის ფარგლები.....                                                                                                              | 15        |
| 1.2.1. პირადი ცხოვრების უფლების სამართლებრივი<br>მონესრიგება საქართველოში .....                                                                                                     | 16        |
| 1.2.2. პირადი ცხოვრების უფლების დაცვის ევროპული<br>სტანდარტი .....                                                                                                                  | 25        |
| 1.2.3. პირადი ცხოვრების დაცული სფერო<br>ადამიანის უფლებათა ევროპული სასამართლოს<br>გადაწყვეტილებათა მიხედვით.....                                                                   | 29        |
| 1.2.4. პირადი ცხოვრების უფლების დაცული სფერო<br>ამერიკული პრეცედენტული სამართლის<br>მიხედვით.....                                                                                   | 34        |
| <b>თავი II. პერსონალურ მონაცემთა დაცვის<br/>უფლება .....</b>                                                                                                                        | <b>42</b> |
| 2.1. დაცული სფერო.....                                                                                                                                                              | 43        |
| 2.2. პერსონალურ მონაცემთა დაცვის მარეგულირებელი<br>ძირითადი საერთაშორისო და<br>შიდასახელმწიფოებრივი ინსტრუმენტები.....                                                              | 56        |
| 2.3. პერსონალურ მონაცემთა დაცვის უფლების<br>სამართლებრივი და ინსტიტუციური გარანტიები .....                                                                                          | 78        |
| 2.3.1. საერთაშორისო სასამართლოების მიერ პერსონალურ<br>მონაცემთა დაცვის უფლების თაობაზე მიღებული<br>ზოგიერთი მნიშვნელოვანი გადაწყვეტილება .....                                      | 78        |
| 2.3.2. საქართველოს პერსონალურ მონაცემთა დაცვის<br>ინსპექტორის და თბილისის საქალაქო სასამართლოს<br>მიერ პერსონალურ მონაცემთა დაცვის უფლების<br>თაობაზე ჩამოყალიბებული პრაქტიკა ..... | 91        |

|                                                                                                                                               |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 2.3.3. 2017 წლის 13 ოქტომბრის კონსტიტუციური<br>ცვლილებები - გარანტია პერსონალურ მონაცემთა<br>დაცვისთვის? .....                                | 104        |
| <b>თავი III. პერსონალურ მონაცემთა დაცვის,<br/>როგორც ძირითადი უფლების კონსტიტუციით<br/>დამოუკიდებლად მონაცემების<br/>მიზანშეწონილობა.....</b> | <b>108</b> |
| 3.1. ტექნოლოგიური პროგრესის გავლენის ზოგადი<br>თავისებურებები პერსონალურ მონაცემთა<br>დაცვაზე .....                                           | 108        |
| 3.2. პერსონალურ მონაცემთა დაცვა, როგორც ძირითადი<br>უფლება .....                                                                              | 122        |
| 3.3. პერსონალურ მონაცემთა დაცვის ძირითადი<br>უფლების კონსტიტუციურად დამოუკიდებელი<br>მონაცემების თეორიული და პრაქტიკული<br>ასპექტები.....     | 126        |
| მაგალითი №1.....                                                                                                                              | 138        |
| მაგალითი №2.....                                                                                                                              | 140        |

## წინასიტყვაობა

პერსონალური მონაცემების დაცვა თითოეული ინდივიდის ყურადღების საგანი უნდა იყოს, განსაკუთრებით მაშინ, თუ ხდება ჩვენს შესახებ არსებული ინფორმაციის გამოყენება. მონაცემთა დაცვა, როგორც უკვე არც თუ ისე უცხო უფლება, გამონეგების წინაშე დგას საქართველოში, ასევე – მსოფლიოში. ამის მიზეზად, მრავალი რამ შეიძლება დასახელდეს, მაგალითად, ცნობიერების არასათანადო დონე, ტექნოლოგიური პროგრესის სწრაფი ტემპები, არაეფექტური სამართლებრივი რეგულირება ან მათი არაეფექტური აღსრულება და სხვა. მნიშვნელოვანია გავიაზროთ, რომ თითოეული დასახელებული გამონეგვა საფრთხის წინაშე აყენებს პერსონალურ მონაცემთა დაცვის ძირითადი უფლების დაცვის უზრუნველყოფას, ხოლო ამ რისკების ერთობლიობა კი – განსაკუთრებით დიდი ზიანის მომტანი შეიძლება იყოს.

უდავოა, რომ ძირითადი უფლებების დაცვა სახელმწიფოს ვალდებულებაა, მას გააჩნია, კომპეტენცია, რესურსი, მექანიზმები და უზრუნველყოფის მეთოდები ამ მიზნის მისაღწევად. მეორე მხრივ, მნიშვნელოვანია, რომ თავად ინდივიდი იყოს დაინტერესებული მისი ძირითადი უფლებების დაცვით, მათ შორის, პერსონალური მონაცემების დაცვის უზრუნველყოფით, ვინაიდან, ამით იგი მეტად მომთხოვნი გახდება სახელმწიფოს მიმართ, ხოლო ასეთ მოთხოვნათა სიმრავლე კი – უზრუნველყოფს სახელმწიფოს ანგარიშვალდებულების ზრდას საზოგადოების წინაშე.

ვფიქრობ, ცნობიერების ამაღლება სანინდარია თითოეული საკითხის ადეკვატური გააზრებისთვის და შესაძლო გადანეგების გზების მოძიებისთვის. მეორე მხრივ, პერსონალურ მონაცემთა დაცვის მიმართულებით, საქართველოში ისევ შეინიშნება ცნობიერების არასაკმარისი დონე, რაც, ზოგადად, ხელისშემშლელი ფაქტორია ამ უფლების ეფექტური რეალიზებისთვის. შესაბამისად, ამ პუბლიკაციით შევეცდები მცირე წვლილი შევიტანო არსებული მდგომარეობის გაუმჯობესების მიზნით.

კახაბერ გოშაძე,  
28 იანვარი, 2020

პერსონალურ მონაცემთა დაცვა XXI საუკუნის ერთ-ერთი გამოწვევაა. რთულია მონაცემთა დაცვასთან დაკავშირებულ აქტუალურ საკითხებს მოეძებნოს ის ათვლის წერტილი, რომელიც დასაბამს მისცემს ამ საკითხების ირგვლივ არსებულ დისკუსიას, თუმცა ის, თუ რატომ არის ამ სამართლებრივი სიკეთის დაცვა აუცილებელი არაერთი მაგალითით შეიძლება აიხსნას. მიუხედავად ამისა, ამ ეტაპზე მხოლოდ იმის აღნიშვნა იქნება საკმარისი, რომ პერსონალური მონაცემების მეშვეობით ინდივიდი საზოგადოებაში ახდენს ინტეგრაციას, ამდენად, ამ მონაცემთა გამორყენება სხვების მიერ ნებისმიერი ადამიანის გარდაუჭელი „ხვედრია.“ აღნიშნული არგუმენტი საკმარისია, რათა წარმოდგენა შეგვექმნას პერსონალური მონაცემების გამოყენების მასშტაბების შესახებ. ეს კი, ხაზს უსვამს იმ გარემოებას, რომ ინდივიდის პერსონალური მონაცემები მრავალგზის დამუშავებას ექვემდებარება, სხვადასხვა მეთოდისა თუ კონცეფციის გამოყენებით.

გამოწვევების პარალელურად ვითარდება ამ სფეროს მომწესრიგებელი ნორმატიული ბაზისიც, როგორც საერთაშორისო ისე ადგილობრივ დონეზე. XXI საუკუნის II ნახევარში მონაცემთა დაცვის მარეგულირებელი აქტების შემუშავება და მიღება ცხადყოფს, რომ აღნიშნული პრობლემატიკა თანამედროვეობის, კერძოდ, ინფორმაციული ტექნოლოგიების განვითარების შედეგია. ელექტრული კომუნიკაციით, ინტერნეტით და, ზოგადად, ციფრული ტექნოლოგიებით სარგებლობას ბევრი დადებითი მხარე გააჩნია, როგორიცაა კომუნიკაციის სიმარტივე, დროის უკეთესი მენეჯმენტი, საყოველთაო საზოგადოებრივ ინტერესებსა და უსაფრთხოებაზე ზრუნვა და ა.შ. ამ ფაქტორებიდან გამომდინარე, ერთი შეხედვით, პერსონალური მონაცემების გამოყენება შესაძლოა მეორეხარისხოვან საზრუნავად იქცეს, თუმცა ეს იმთავითვე მცდარი შეხედულებაა. მონაცემთა დაცვა და საყოველთაო სიკეთეებით სარგებლობა არ უნდა განვაცალკევოთ ერთმანეთისგან, სხვა სიტყვებით, ეს არ არის ორი დაპირისპირებული „ბანაკი.“ პერსონალურ მონაცემთა დაცვის წინამედროვე კონცეფცია ისწრაფვის იმისკენ, რომ მოხდეს ამ უფლების დაცვა სხვა სიკეთეების სათანადო დონეზე უზრუნ-

ველყოფის პარალელურად.

წინამდებარე პუბლიკაცია ეხება პერსონალურ მონაცემთა დაცვის უფლებას, როგორც ძირითადს და თავს უყრის პერსონალურ მონაცემთა დაცვის კონცეფციასთან დაკავშირებულ საკითხებს – დაწყებული პირადი ცხოვრების კონცეფციის განხილვითა და მონაცემთა დაცვის უფლების წარმოშობით და დამთავრებული მონაცემთა დამუშავების კონკრეტული საკითხებით.

მნიშვნელოვანია გავიაზროთ, რომ პერსონალურ მონაცემთა დაცვასა და დამუშავებასთან დაკავშირებული წესები მეტად თუნაკლებად თითოეულმა ადამიანმა უნდა იცოდეს, რამდენადაც არ აქვს მნიშვნელობა თუ რა პროფესიის წარმომადგენელია იგი ან საქმიანობის რა სფეროში მოღვაწეობს – მონაცემთა დაცვა თითოეული ინდივიდის საზრუნავი და ყურადღების ობიექტი უნდა იყოს. შესაბამისად, მოცემული პუბლიკაცია განკუთვნილია ნებისმიერი იმ პირისთვის, ვინც დაინტერესებულია სამართლებრივი ურთიერთობების ამ სეგმენტით ანდა მასთან დაკავშირებული საკუთარი საქმიანობიდან გამომდინარე.

# თავი I. პირადი ცხოვრების უფლების კონცეპტუალური საფუძვლები და სამართლებრივი მონუსხვა

## 1.1. პირადი ცხოვრების უფლების არსი და კონცეფცია

სიტყვა “privacy” (პრივატულობა) ხშირად გამოიყენება საუბარში, ფილოსოფიურ, პოლიტიკურ და სამართლებრივ დებატში. ამ ცნებას ფართო ისტორიული ფესვები გააჩნია სოციოლოგიურ და ანთროპოლოგიურ ქრილში.<sup>1</sup> პირადი ცხოვრების უფლება ინდივიდებს საშუალებას აძლევს მოიხსნან „საჯარო ნიღბები“ და კერძო სივრცეში განსხვავებულად მოიქცნენ; იგი ფესვგადგმულია ადამიანურ ღირსებასა და მის პატივისცემაში.<sup>2</sup> პირადი ცხოვრების განმარტებები იცვლება მოცემულობისა და გარემოს გათვალისწინებით. იგი ადამიანის ერთ-ერთი ყველაზე მნიშვნელოვანი ბერკეტია თანამედროვე ეპოქაში.<sup>3</sup> თუ პირის პირადი ცხოვრება მუდმივ დარღვევას განიცდის, მაშინ ინდივიდი ვერ ცხოვრობს მშვიდი და თავისუფალი ცხოვრებით. შესაბამისად, პირადი ცხოვრების დაცვა მნიშვნელოვანია ინდივიდის უსაფრთხო ცხოვრების უზრუნველსაყოფად.<sup>4</sup> ამ უფლებით დაცულია პირის კერძო სფერო, რაც მოიცავს კერძო ტერიტორიას, ადგილს, ნებისმიერ საგანს პიროვნების მფლობელობაში, ასევე, პირთა წრეს, რომელთანაც აქვს მას კომუნიკაცია.<sup>5</sup> ეს უფლება იცავს პიროვნების ხელშეუვალობას, მის დამოუკიდებლობას, ღირსებასა და არსებობას. ამიტომ, ზოგჯერ, მათ ერთიანობას მოიხსენიებენ არა პირადი ცხოვრების უფლებად, არამედ, რო-

1 Stanford Encyclopedia of Philosophy, *Privacy*, 2013 [<http://plato.stanford.edu/entries/privacy/>].

2 Parliament of the UK, *Privacy and Injunction*, 2013. [<http://www.publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/27305.htm>].

3 Marshall, J., *Personal Freedom through Human Rights Law?*, Martinus Nijhoff Publishers, 2009, p. 50.

4 Benedek, W. (ed.), *Understanding Human Rights, Manual on Human Rights Education*. European Training and Research Centre for Human Rights and Democracy (ETC), Wien – Graz: NWV Neuer Wissenschaftlicher Verlag, 2012, p. 359.

5 კუბლაშვილი, კ., *ადამიანის ძირითადი უფლებები და თავისუფლებები*, იურიდიული სახელმძღვანელო, „იურისტების სამყარო“, თბილისი, 2019, გვ. 146-147.

გორც ავტონომიურობისა და დამოუკიდებლობის უფლებას.<sup>6</sup> რა თქმა უნდა, იგი მოიცავს საკუთარ (პერსონალურ) ინფორმაციაზე კონტროლის შესაძლებლობას. დამატებით, ეს უფლება პიროვნების თავისუფალი განვითარების შემადგენელ ნაწილად გვევლინება. მასში ერთიანდება ისეთი უფლებები, როგორიცაა თვითგამორკვევის, მათ შორის, საკუთარი წარმოშობის გარკვევის უფლება, საკუთარი პიროვნების შეგრძნების უფლება, ინფორმაციული თვითგამორკვევის, ასევე, თვითგამოსახვის უფლება, მათ შორის, უფლება საკუთარ სიტყვაზე, საკუთარ სურათზე, საკუთარი პიროვნების წარმოსახვაზე, სანინალმდებარე შინაარსის ინფორმაციის გავრცელებაზე.<sup>7</sup>

იმის გათვალისწინებით, რომ პირადი ცხოვრება ვერ იქნება თითოეული ინდივიდის მიერ იდენტიურად აღქმული, შესაძლებელია გამოიყოს მისი გააზრების სუბიექტური და ობიექტური მეთოდი. სუბიექტური გააზრება აქცენტს აკეთებს საკითხზე, თუ რა არის პირადი ცხოვრება კონკრეტული პირისთვის, რა ელემენტებს შეიცავს იგი და რა მოლოდინი გააჩნია პიროვნებას საკუთარი პირადი ცხოვრების დაცვის მიმართ. ამ შემთხვევაში სამართლებრივ რეგულირებაზე საუბარი ნაკლებადაა შესაძლებელი, ვინაიდან ეს მიდგომა პიროვნების სუბიექტურ აღქმაზეა დამოკიდებული. ამის საპირისპიროდ, ობიექტური მიდგომის თანახმად, საკითხი დაიყვანება პირადი ცხოვრების ამა თუ იმ ასპექტის სამართლებრივი დაცვის შესაძლებლობამდე, კანონმდებლობის აბსტრაქტულ და კონკრეტულ დანაწესზე დაყრდნობით.<sup>8</sup> მაგალითად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად „ვიდეოთვათვალის განხორციელება დაუშვებელია გამოსაცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში.“<sup>9</sup> აღნიშნული ჩანაწერი კონკრეტულ აკრძალვას აწესებს. შესაბამისად, იგი აღარ საჭიროებს

6 Marshall, p. 51.

7 კუბლაშვილი, გვ. 96-100.

8 შეად. Gavison, R., *Privacy and the Limits of Law*, The Yale Law Journal (Vol. 89, No. 3), 1980 და Nissenbaum, H., *Privacy in Context*, Stanford University Press, 2010. სადაც ავტორები განიხილავენ პირადი ცხოვრების ნეიტრალურ და ნორმატიულ კონცეფციებს.

9 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 12, პ. 4.

ინტერპრეტირებასა და სხვადასხვა მეთოდურ განმარტებას. მეორე შემთხვევაში, როდესაც ნორმა აბსტრაქტულია იგი უნდა განიმარტოს ყოველი კონკრეტული შემთხვევის მიხედვით. მაგალითად, ამავე კანონით „მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევაც მუშავდება ისინი.“<sup>10</sup> ცხადია, კანონის ამ ჩანაწერის მიხედვით დამკვიდრებული პროპორციულობისა და ადეკვატურობის პრინციპის რეალიზების გზები ყველა შემთხვევაში ვერ იქნება იდენტურად განმარტებული, ვინაიდან იგი უნდა დაექვემდებაროს ინდივიდუალური, კონტექსტუალური მოცემულობიდან გამომდინარე ანალიზს. ამ მხრივ, იგი შეგვიძლია მივიჩნიოთ რეგულირების აბსტრაქტულ დებულებად.

პირადი ცხოვრების უფლების ამომწურავი განმარტება არ იქმნება. პირადი ცხოვრების სხვადასხვა ასპექტის გათვალისწინებით, მისი ამომწურავი განმარტება სირთულეს წარმოადგენს როგორც ფილოსოფოსი, ისე წმინდად იურისტი მეცნიერების მიერ.<sup>11</sup> პირადი ცხოვრების უფლების შინაარსი განიცდის ცვალებადობას სოციალური და ისტორიული კონტექსტის გათვალისწინებით. ამ უფლების ფარგლების ცვალებადი ხასიათი, როგორც არამატერიალური კულტურის ნაწილი, რთულს ხდის მოხდეს მისი ერთიანი განმარტება.<sup>12</sup> პირადი ცხოვრების განმარტების უნიფიცირების შეუძლებლობას ადასტურებს საერთაშორისო სასამართლოებიც. მაგალითად, ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ პირადი ცხოვრება ფართო ცნებაა, იგი შეუძლებელია განიმარტოს ამომწურავად.<sup>13</sup> პირადი ცხოვრების ფართო ფარგლებზე უთითებს მართლმსაჯულების ევროპული კავშირის სასამართლოც, რომლის მიხედვითაც ცნება „პირადი ცხოვრება“ არ უნდა განიმარტოს ვიწროდ, ვინაიდან იგი მოიაზრებს პროფესიული

<sup>10</sup> იქვე, მ. 4, პ. „გ.“

<sup>11</sup> Solove, D. J., *Conceptualizing Privacy*, California Law Review (Vol. 90, Issue 4), 2002, p. 1088.

<sup>12</sup> Kasper, D.V.S., *The Evolution (Or Devolution) of Privacy*, Sociological Forum (Vol. 20, No. 1), Springer, 2005, p. 69-70.

<sup>13</sup> ECtHR, App. no. 13134/87, *Costello-Roberts v. The United Kingdom*, 25.03.1993.

საქმიანობის სფეროსაც და იგი ვერ იქნება განცალკევებული პირადი ცხოვრების ფარგლებისგან.<sup>14</sup> ნებისმიერ შემთხვევაში, უდავოა, რომ პირადი ცხოვრების უფლების ერთ-ერთ შემადგენელ ნაწილად პერსონალურ მონაცემთა დაცვის უფლება გვევლინება. პირადი ცხოვრების უფლების დოქტრინული ანალიზისას და დაცული სფეროს განხილვის დროს მასში პერსონალურ მონაცემთა დაცვის საკითხი ყოველთვის მოიაზრება.

პრივატულობას ახასიათებს დროსთან ერთად ცვალებადობა. ამის ნათელი დადასტურებაა 1890 წლის, სამუელ უორენისა და ლუი ბრანდისის პუბლიკაცია, სადაც საგაზეთო გამოცემებში ფოტოსურათების გამოქვეყნება და, ზოგადად, ფოტოგრაფიაში არსებული იმჟამინდელი ახალი ტექნოლოგიები საფრთხეს ქმნიდნენ რიგითი ინდივიდისთვის.<sup>15</sup> ამ მსჯელობის გამყარება სხვა მრავალი ფაქტობრივი მოვლენით შეიძლება, მაგალითად, ტექნოლოგიურ პროგრესთან ერთად, დროთა განმავლობაში სამართლებრივ რეგულირებას დაექვემდებარა პაკერული თავდასხმა ინტერნეტის მომხმარებელზე, რეგულირების ქვეშ მოექცა საგამოძიებო მოქმედების - ფარული მიყურადების ჩატარების წესი და ა.შ.

პირადი ცხოვრების უფლების შესახებ არაერთი თეორია არსებობს, ეს თეორიები განსხვავდება პირადი ცხოვრების დაცული სფეროს სხვადასხვა ასპექტის მიხედვით. დენიელ სოლოვის აზრით პრივატულობა შეიცავს ექვს ძირითად ნაწილს, ესენია:

1. უფლება იყო „დავინყებუდი“, რაც უორენისა და ბრანდისის ცნობილ პოსტულატს წარმოადგენს;
2. პირთან შეზღუდული წვდომა – პირის შესაძლებლობა მოახდინოს საკუთარი თავის დაცვა სხვათა არასასურველი წვდომისგან;
3. საიდუმლოება – გარკვეული საკითხების დამალვა სხვებისგან;
4. პერსონალურ მონაცემებზე კონტროლი;

14 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, *მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო*. – 2018 წლის გამოცემა, თბილისი, 2019, გვ. 100.

15 Warren, S. D., & Brandeis, L., *The Right to Privacy*. Harvard Law Review (Vol. 4, No. 5). 1890.

5. პიროვნულობის, ინდივიდუალურობისა და ღირსების დაცვა;

6. ინტიმურობა - პირის ცხოვრების ინტიმურ ასპექტებთან წვდომის შეზღუდვა.<sup>16</sup>

მეტი თვალსაჩინოებისთვის მნიშვნელოვანია მათი ცალ-ცალკე განხილვა.

პირადი ცხოვრების უფლება, როგორც უფლება იყო „დავიწყებული“ აქცენტს აკეთებს მისი სამართლებრივი მექანიზმებით დაცვაზე. უორენისა და ბრანდისის მიერ გამოყენებული ეს ფრაზა ემსახურებოდა მიზანს, რომელიც მათივე პუბლიკაციაშია მოცემული: დადგენილი ყოფილიყო პირადი ცხოვრების დამცავ ბერკეტთა რაოდენობა ანგლო-ამერიკული სამართლის სისტემაში.<sup>17</sup> მოგვიანებით, პირადი ცხოვრების უფლება გაიგივებულ იქნა უფლებასთან იყო „დავიწყებული“ და განიმარტა, როგორც პირის მიერ საკუთარი პირადი ცხოვრების წარმართვა ინდივიდუალური არჩევანის შესაბამისად, ყოველგვარი ჩარევის გარეშე, გარდა იმ შემთხვევებისა, როდესაც მეორე მხარეს დგას საზოგადოებრივი ან სხვა ინტერესი.<sup>18</sup> ეს უფლება გულისხმობს ინდივიდის პრივილეგიას დაგეგმოს საკუთარი საქმე დამოუკიდებლად.<sup>19</sup> უფლება იყო „დავიწყებული“ ძალზედ აქტუალურია პერსონალურ მონაცემებთან მიმართებით. იგი შესაძლებლობას აძლევს ინდივიდს მოითხოვოს ნებისმიერი დამშუშავებლისგან საკუთარი თავის შესახებ ინფორმაციის სრულად წაშლა და განადგურება.

პირთან შეზღუდული წვდომის თეორია აღიარებს ინდივიდის სურვილს იყოს სხვებისგან დაფარული და განცალკევებული. ამ კუთხით მას მჭიდრო კავშირი აქვს უფლებასთან იყო „დავიწყებული.“<sup>20</sup> აღსანიშნავია, რომ პირთან მიუწვდომლობის ხარისხის არსებობა პირადი ცხოვრების მნიშვნელოვან ნაწილს წარმოადგენს.<sup>21</sup> შეზღუდული წვდომის თეორია კავშირშია სა-

16 Solove.

17 იქვე, გვ. 1100.

18 Supreme Court of the United States, #385 U.S. 374, *Time, Inc. v. Hill*, 1967.

19 Supreme Court of the United States, #410 U.S. 179, *Doe v. Bolton*, 1973.

20 Solove, pp. 1102-1103.

21 Allen, A.L., *Uneasy Access: Privacy for Women in a Free Society*. Rowman & Littlefield Publishers, 1988, p. 10.

ზოგადოების დანარჩენ წევრებთან, ვინაიდან, მაგალითად, პირი, რომელიც იმყოფება კუნძულზე მარტო განიცდის პირადი სფეროს სრულ დაცვას, თუმცა აქ უფრო გამოდგება სიტყვა იზოლაცია, ვიდრე პირთან შეზღუდული წვდომა. ამიტომაც, ამ თეორიის მიხედვით ამ სფეროს დაცვა გულისხმობს დაცვას სხვა პირებისგან.<sup>22</sup>

პირადი ცხოვრების აღქმა, როგორც საიდუმლოებისა ერთ-ერთი გავრცელებულია. ამ მიდგომის თანახმად პირადი ცხოვრება დარღვეულია დახურული ინფორმაციის გამჟღავნების შედეგად, შესაბამისად, ინფორმაციის დასაიდუმლოების უფლება ირღვევა მაშინ, როდესაც ხდება პერსონალური ინფორმაციის მოპოვება კანონის დარღვევით ან იმ პირის ნების გარეშე, ვისაც ეკუთვნის ეს მონაცემი.<sup>23</sup> პირადი ცხოვრების ხედვა, როგორც ინფორმაციის დასაიდუმლოების შესაძლებლობა თვალნათლივ წარმოაჩენს ამ უფლებას, როგორც გარანტიას ინფორმაციული პრივატულობის უზრუნველყოფისთვის.<sup>24</sup> თუმცა, საიდუმლოების კონდიცია ვერ იქნება სრულფასოვნად რეალიზებული სახელმწიფოს მიმართ, როდესაც, მაგალითად, მოქალაქეთა სარეგისტრაციო მონაცემებში არსებული ინფორმაცია კანონის თანახმად არის შენახული.

პირადი ცხოვრების უფლების მორიგი თეორია ყურადღებას ამახვილებს მის აღქმაზე პერსონალური ინფორმაციის კონტროლის ჭრილში. ალან ვესტინის აზრით პრივატულობა ესაა ინდივიდების, ჯგუფების ან ინსტიტუციების მოთხოვნა, რომ განსაზღვრონ თუ როდის, როგორ და რა ოდენობით ინფორმაციაა მათ შესახებ სხვებისთვის მიწოდებული.<sup>25</sup> მეორე მხრივ, ინფორმაციაზე კონტროლის თეორია ვინრო სახის კონცეფციაა, იგი გამორიცხავს პრივატულობის იმ ნაწილს, რომელიც ინფორმაციული არაა, მაგალითად, უფლებას, მიიღო გარკვეული გადაწყვეტილებები სხეულის, რეპროდუქციისა და ბავშვის ჩასახვის შესახებ. გარდა ამისა, თუ ვიტყვი, რომ კონტროლის თეო-

22 Solove, p. 1104.

23 იქვე, გვ. 1105; Posner, R. A., *The Economics of Privacy*, Harvard University Press, 1981, pp. 272-273.

24 Solove, p. 1107.

25 Westin, A. F., *Privacy and Freedom*, Athentium, 1967, p. 7; Solove, p. 1110.

რია აქცენტს აკეთებს ინფორმაციაზე, რომლის მიხედვითაც ინდივიდი პირდაპირ ან არაპირდაპირ იდენტიფიცირებადია, ეს კიდევ უფრო ბუნდოვანს ხდის მისი ფარგლების დადგენას. მაგალითად, თუ პირი ცნობილი პოლიტიკოსია, მისი საჯარო სტატუსი პირდაპირ ახდენს მის იდენტიფიცირებას, თუმცა არ წარმოადგენს პრივატულ ინფორმაციას.<sup>26</sup> კონტროლის თეორიის სუსტ მხარედ შეიძლება ჩაითვალოს ისიც, რომ პიროვნებას საკუთარი პერსონალური მონაცემის მიმართ არ გააჩნია სრული კონტროლის შესაძლებლობა, კერძოდ, თუ სახელმწიფო მოისურვებს დააკანონოს გარკვეული ინფორმაციის სახელმწიფო ინსტიტუტებისთვის ფლობა, პირი იმთავითვე კარგავს უფლებას თავისუფლად განკარგოს საკუთარი პერსონალური მონაცემი, რამდენადაც ამგვარი ინფორმაცია საზოგადოებრივი საჭიროებების შესაბამისად, აუცილებელ დამუშავებას საჭიროებს.<sup>27</sup>

პირადი ცხოვრების მორიგი თეორია ერთმანეთთან აიგივებს პრივატულობისა და პიროვნულობის საკითხს. ამ მნიშვნელობით პრივატულობა გვევლინება ადამიანური ღირსებისა და თავისუფლების ანალოგად.<sup>28</sup> ამ მნიშვნელობით პრივატულობა წინაპირობაა ღირსებისა და თავისუფლების უზრუნველყოფისთვის, რაც საბოლოოდ ინდივიდის ნების თავისუფალი გამოვლენიდან მომდინარეობს.

პრივატულობა, როგორც ინტიმურობა აქცენტს აკეთებს ადამიანურ ურთიერთობებსა და ამ ურთიერთობების შესაძლებლობებზე. მეცნიერები პრივატული სფეროს მნიშვნელოვან მონაპოვრად მიიჩნევენ ინტიმური ურთიერთობების განვითარების შესაძლებლობას, ხოლო თუ რა არის ინტიმური, ამის პასუხად უთითებენ ფაქტობრივ ვითარებას, კერძოდ, ინტიმურია პირადი საკითხი მაშინ, როდესაც ის გაზიარებულია ძალზედ ვიწრო წრისთვის.<sup>29</sup> ამასთან, პირადი ცხოვრების ინტიმური მხარე არ არის შემოფარგლული მხოლოდ ამ მოცემულობით, მაგალითად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი პირის რელიგიური აღმსარებლობის შესახებ არსებულ

26 Solove, pp. 1110-1112.

27 იქვე, გვ. 1115.

28 იქვე, გვ. 1116-1117.

29 იქვე, გვ. 1121-1122.

პერსონალურ მონაცემებს განსაკუთრებული კატეგორიის მონაცემთა ჭრილში მოიხსენიებს და ამით ხაზს უსვამს ჩარევისგან მისი დაცვის აუცილებლობას.

თეორიების განხილვის შედეგად შესაძლებელია ჩამოვყალიბოთ შემდეგი დასკვნები:

1. პრივატულ სფეროს გააჩნია სხვადასხვაგვარი ალექმა, რაც დამოკიდებულია მასში შემავალი მრავალი საკითხის არსებობაზე;
2. თითოეული ჩამოთვლილი თეორია თუ კონცეფცია ყურადღებას ამახვილებს იმ ასპექტებზე, რის გამოც პირადი ცხოვრება ღირებულია ადამიანისთვის;
3. თითოეული კონცეფციის მიღმა, საზოგადოებრივი საჭიროებებიდან გამომდინარე, უმეტეს შემთხვევაში, დაცვადად უნდა მოვიაზროთ პერსონალური მონაცემებიც, როგორც პრივატულობის ინფორმაციული ნაწილი;
4. აუცილებელია სამართლებრივი მექანიზმების არსებობა, რათა ეს ასპექტები დაცვადად იყოს აღიარებული.

## 1.2. პირადი ცხოვრების უფლებით დაცული სფერო და ჩარევის ფარგლები

საერთაშორისო მასშტაბით პირადი ცხოვრების უფლება პირველად გაიწერა 1948 წლის 10 დეკემბრის ადამიანის უფლებათა საყოველთაო დეკლარაციაში, შემდეგი ფორმულირებით: „არავის მიმართ არ შეიძლება თვითნებური ჩარევა მის პირადსა და ოჯახურ ცხოვრებაში. თვითნებური ხელყოფა მისი საცხოვრებელი ბინის ხელშეუხებლობის, მისი კორესპოდენციის საიდუმლოების, ანდა მისი პატივისა და რეპუტაციისა, ყოველ ადამიანს აქვს უფლება დაცული იყოს ასეთი ჩარევისა და ხელყოფისგან.“<sup>30</sup>

მსგავსი შინაარსის შემცველია 1966 წლის 19 დეკემბრის საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ, სადაც მითითებულია: „1. არავინ არ უნდა განიცადოს თვითნებური ან უკანონო ჩარევა თავის პირად და ოჯახურ ცხოვრებაში, მისი საცხოვრებლის შეუვალობის ან მისი კორეს-

<sup>30</sup> გაერთიანებული ერების ორგანიზაციის ადამიანის უფლებათა საყოველთაო დეკლარაცია, მ. 12.

პოდეციის საიდუმლოების თვითნებური ან უკანონო ხელყოფა, ან მისი ღირსებისა და რეპუტაციის უკანონო ხელყოფა. 2. თითოეულ ადამიანს აქვს უფლება, რომ კანონმა დაიცვას ასეთი ჩარევისა თუ ხელყოფისგან.<sup>31</sup> პირადი ცხოვრების უფლება სამართლებრივად კიდევ სხვა არაერთ საერთაშორისო აქტშია განერილი. თუმცა, არ მაქვს მიზნად განვიხილო პირადი ცხოვრების უფლების სხვადასხვა აქტებში რეგლამენტირების საკითხი. ამდენად, უმჯობესია გადავინაცვლოთ საკითხზე, თუ როგორაა პირადი ცხოვრების უფლება დაცული ქართული, ევროპული და ამერიკული სამართლებრივი სტანდარტების მიხედვით.

### **1.2.1. პირადი ცხოვრების უფლების სამართლებრივი მოწესრიგება საქართველოში**

ტრადიციულად, უფლებათა კატალოგი სახელმწიფოს ძირითადი კანონით ან კონსტიტუციური მნიშვნელობის აქტითაა მოცემული. პირადი ცხოვრების უფლება ჯერ კიდევ საქართველოს 1921 წლის 21 თებერვლის კონსტიტუციით იყო განერილი, რომელიც ორი მუხლის შინაარსში ნაწილდებოდა, კერძოდ, „ყოველი მოქალაქის ბინა შეუვალია: მხოლოდ სასამართლოს დადგენილებით შეიძლება მისი გაჩხრეკა კანონით გათვალისწინებულ შემთხვევაში,<sup>32</sup> ამასთან, „კერძო მინერ-მოწერა ხელშეუხებელია: მისი ამოხმა და გადასინჯვა შეიძლება მხოლოდ სასამართლოს დადგენილებით.“<sup>33</sup>

დღეს, პირადი ცხოვრების დაცვის უფლებას საქართველოს 1995 წლის 24 აგვისტოს კონსტიტუციითაა გარანტირებული. დადგენილია, რომ „1. ადამიანის პირადი და ოჯახური ცხოვრება ხელშეუხებელია. ამ უფლების შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით. 2. ადამიანის პირადი სივრცე და კომუნიკაცია ხელშეუხებელია.

31 გაერთიანებული ერების ორგანიზაციის საერთაშორისო პაქტი სამოქალაქო და პოლიტიკური უფლებების შესახებ, მ. 17.

32 საქართველოს 1921 წლის 21 თებერვლის კონსტიტუცია, მ. 28.

33 იქვე, მ. 29.

არავის აქვს უფლება შევიდეს საცხოვრებელ ან სხვა მფლობელობაში მფლობელი პირის ნების სანაღმდეგოდ, აგრეთვე ჩაატაროს ჩხრეკა. ამ უფლებათა შეზღუდვა დასაშვებია მხოლოდ კანონის შესაბამისად, დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფის ან სხვათა უფლებების დაცვის მიზნით, სასამართლოს გადაწყვეტილებით ან მის გარეშეც, კანონით გათვალისწინებული გადაუდებელი აუცილებლობისას. გადაუდებელი აუცილებლობისას უფლების შეზღუდვის შესახებ არაუგვიანეს 24 საათისა უნდა ეცნობოს სასამართლოს, რომელიც შეზღუდვის კანონიერებას ადასტურებს მიმართვიდან არაუგვიანეს 24 საათისა.<sup>34</sup>

აქცენტები პირადი ცხოვრების, მათ შორის, პერსონალური მონაცემების დაცვაზე მოცემულია საქართველოს ზოგად ადმინისტრაციულ კოდექსშიც. მაგალითად, „ყველას აქვს უფლება, გაეცნოს ადმინისტრაციულ ორგანოში არსებულ საჯარო ინფორმაციას, აგრეთვე მიიღოს მისი ასლები, თუ ისინი არ შეიცავენ სახელმწიფო, პროფესიულ ან კომერციულ საიდუმლოებას ან პერსონალურ მონაცემებს.“<sup>35</sup> ამასთან, „საჯარო ინფორმაცია ღიაა, გარდა კანონით გათვალისწინებული შემთხვევებისა და დადგენილი წესით სახელმწიფო, კომერციული ან პროფესიული საიდუმლოებისთვის ან პერსონალური მონაცემებისთვის მიკუთვნებული ინფორმაციისა.“<sup>36</sup> კოდექსი უშუალოდ პერსონალურ მონაცემთა საიდუმლოების შესახებაც შეიცავს ჩანაწერს, სადაც აღნიშნულია, რომ „საჯარო დანესებულება ვალდებული არ გაახმაუროს პერსონალური მონაცემები თვით ამ პირის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად. თანამდებობის პირის, აგრეთვე თანამდებობაზე წარდგენილი კანდიდატის პერსონალური მონაცემები საჯაროა.“<sup>37</sup>

34 საქართველოს 1995 წლის 24 აგვისტოს კონსტიტუცია, მ. 15.

35 საქართველოს ზოგადი ადმინისტრაციული კოდექსი, მ. 10, ნან. 1.

36 იქვე, მ. 28, ნან. 1.

37 იქვე, მ. 44, ნან. 1.

დამატებით, კოდექსი უთითებს, რომ „განმცხადებელი უფლებამოსილია მოითხოვოს წარდგენილი, კომერციული საიდუმლოების ან პერსონალური მონაცემების შემცველი ინფორმაციის დაცვა, თუ სურს ამ ინფორმაციის საიდუმლოების უზრუნველყოფა.“<sup>38</sup> ეს ჩანაწერი ადმინისტრაციული წარმოების ზოგადი დებულებების თავშია მოცემული, რითაც განმცხადებელს ენიჭება შესაძლებლობა მოითხოვოს წარდგენილი ინფორმაციის დასაიდუმლოება. თუმცა, კოდექსის ეს ნორმა უსარგებლოა, ვინაიდან კოდექსით პერსონალური მონაცემების კონფიდენციალურად შენახვის ვალდებულება იმთავითვე დადგენილია, ხოლო საიდუმლო ინფორმაცია განიმარტება როგორც „[...] საჯარო დაწესებულებაში დაცული, აგრეთვე საჯარო დაწესებულების ან მოსამსახურის მიერ სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია, რომელიც შეიცავს პერსონალურ მონაცემებს, [...]“.<sup>39</sup>

პირადი ცხოვრების დაცვა კერძოსამართლებრივ ურთიერთობებშიც უზრუნველყოფილია. მხარეთა შორის თანასწორუფლებიან ურთიერთობაში არსებული დაცვის გარანტიების ორი მიმართულება შეიძლება გამოიყოს: პირველი, როდესაც პირადი ცხოვრების დაცვასა და მხარეთა შორის გაზიარებული ინფორმაციის კონფიდენციალურობაზე მითითება მოცემულია ამავე მხარეებს შორის დადებული ხელშეკრულებით და, მეორე, როდესაც მხარეებს არ დაუდიათ ხელშეკრულება, თუმცა მაინც მართებთ ერთმანეთის პირადი ცხოვრების პატივისცემა. ამ საკითხებზე ყურადღებას ამახვილებს სამოქალაქო კოდექსი,<sup>40</sup> რომლის მიხედვითაც დადგენილი უფლებები შემდეგ კატეგორიებად შეიძლება დავეყოთ: 1. პირის მიერ მისი სახელის უნებართვოდ გამოყენების წინააღმდეგ მიმართული ზომები; 2. სასამართლოს წესით პატივის, ღირსების, პირადი ცხოვრების საიდუმლოების, ხელშეუხებლობის ან რეპუტაციის დაცვა; 3. მასობრივი ინფორმაციის საშუალებებით ან სხვაგვარად დოკუმენტალურად მცდარი ინფორმაციის უარყოფის შესაძლებლო-

38 იქვე, მ. 82.

39 იქვე, მ. 2, პ. „ნ.“

40 საქართველოს სამოქალაქო კოდექსი, მ. 18.

ბა; 4. პირის უფლება საჯაროდ უარყოს მის წინააღმდეგ გამოქვეყნებული ინფორმაცია.

დამატებით, სამოქალაქო კოდექსის თანახმად, პირს საშუალება აქვს მიიღოს მის შესახებ არსებული ინფორმაცია სხვადასხვა პირისგან და, ასევე, მოიპოვოს სხვა პირის შესახებ ინფორმაცია მისი თანხმობისა და კონფიდენციალურობის დაცვის ვალდებულების გათვალისწინებით.<sup>41</sup>

პირადი ცხოვრების დაცვა სამოქალაქო და ადმინისტრაციული სამართლის გარდა, სისხლისსამართლებრივ ურთიერთობებშიც წარმოადგენს პასუხისმგებლობის საფუძველს. დასჯადია ქმედება, რომელიც მოიცავს პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ მოპოვებას, შენახვას, გამოყენებას, გავრცელებას ან ხელმისაწვდომობის სხვაგვარ უზრუნველყოფას, თუ იგი მნიშვნელოვანი ზიანის გამომწვევია, ასევე, უმართლოა ქმედება, რომელიც ეხება პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ გამოყენებას ან/და გავრცელებას ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით, თუ იგი მნიშვნელოვანი ზიანის გამომწვევია.<sup>42</sup> ორივე შემთხვევაში, ზემოხსენებული ქმედებების დანაშაულის კატეგორიაში მოსაქცევად აუცილებელია მნიშვნელოვანი ზიანის პირობის არსებობა, რითაც იგი ხარისხობრივად განსხვავდება, მაგალითად, კერძოსამართლებრივი დელიქტისგან.

გარდა ამისა, საქართველოს კანონმდებლობაში სხვა სამართლებრივი აქტებიც მოიპოვება, რომელიც შესაბამისი მოწესრიგების ფარგლებში ეხება პირადი ცხოვრების, საიდუმლოობის ან კონფიდენციალურობის დაცვას, მაგალითად, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, „პაციენტის უფლებების შესახებ“ საქართველოს კანონი, „კომერციული ბანკების საქმიანობის შესახებ“ საქართველოს კანონი და სხვა. მოცემული ნორმატიული აქტები, ძირითადად, წარმოადგენენ ე.წ. სექტორული კანონმდებლობის ნაწილს და, შესაბამის-

41 იქვე, მ. 18<sup>1</sup>.

42 საქართველოს სისხლის სამართლის კოდექსი, მ. 157, ნაწ. 1, 2.

სად, კონფიდენციალურობის დათქმის ნაწილში, რეგულირების ვინრო სფეროთი შემოიფარგლებიან.

გარდა ნორმატიული მონესრიგებისა, მიზანშეწონილია საკონსტიტუციო და საერთო სასამართლოების მიერ მიღებული ზოგიერთი გადაწყვეტილების ციტირება და განხილვა სამართლებრივი მიდგომების ზოგადი ანალიზის მიზნით.

პირადი ცხოვრების შესახებ საქართველოს საკონსტიტუციო სასამართლოს მიერ მიღებული გადაწყვეტილებები, ძირითადად, უფლებათა დაცვის ევროპულ მოდელში არსებული სტანდარტების შემცველია. სასამართლო მიიჩნევს, რომ „ზოგადად, პირადი ცხოვრება გულისხმობს ინდივიდის ცხოვრებისა და განვითარების კერძო სფეროს. უფლება პირად ცხოვრებაზე კი, ერთი მხრივ, ნიშნავს ინდივიდის შესაძლებლობას, პირადად, საკუთარი შეხედულებისამებრ, დამოუკიდებლად შექმნას და განვითაროს თავისი კერძო ცხოვრება, ხოლო, მეორე მხრივ იყოს დაცული და უზრუნველყოფილი მის კერძო სფეროში სახელმწიფოს, ისევე, როგორც ნებისმიერი სხვა პირების ჩარევისგან. [...] ნიშანდობლივია, რომ პირადი ცხოვრების ფართო და მრავალმხრივი შინაარსიდან გამომდინარე, შეუძლებელია მისი ზუსტი და ამომწურავი განმარტება.“<sup>43</sup> გარდა ამისა, სასამართლომ აღნიშნა, რომ „ეს უფლება სასიცოცხლოდ აუცილებელია ადამიანის თავისუფლების, თვითმყოფადობისა და თვითრეალიზაციისათვის, მისი სრულყოფილად გამოყენების ხელშეწყობა და დაცვა არსებითად განმსაზღვრელია დემოკრატიული საზოგადოების განვითარებისთვის.“<sup>44</sup>

გარდა პირადი ცხოვრების არსის განხილვისა, სასამართლო არაერთგზის უსვამს ხაზს პიროვნების თავისუფალი განვითარების უფლებასა და პირადი ცხოვრების უფლებას შორის არსებულ შინაარსობრივ კავშირს. სასამართლო მიიჩნევს, რომ, ფორმალური თვალსაზრისით, პირადი ცხოვრების უფლება შეიძლება ჩაითვალოს სპეციალურ ნორმად პიროვნების თავისუფალი განვითარების უფლებით დაცული სფეროსთვის, რამდე-

43 საქართველოს საკონსტიტუციო სასამართლო, საქმე 1/3/407, *ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ*, 26.12.2007.

44 საქართველოს საკონსტიტუციო სასამართლო, საქმე 31/2/519, *თამარ ჩუგოშვილი საქართველოს პარლამენტის წინააღმდეგ*, 24.10.2012.

ნადაც ის არეგულირებს პიროვნების განვითარების ერთ-ერთ მნიშვნელოვან სფეროს.<sup>45</sup>

ამა თუ იმ სადავო ნორმის პირადი ცხოვრების დაცვის უფლების კონსტიტუციურ ნორმასთან თავსებადობის ნაწილში, საკონსტიტუციო სასამართლო რიგ შემთხვევაში ყურადღებას ამახვილებს შემზღუდავი ნორმით პირადი ცხოვრების უფლებაში ჩარევის საფუძვლებთან (კონსტიტუციური ზღვარი) თავსებადობის საკითხზე, ხოლო სხვა შემთხვევაში ამ უფლებაში ჩარევის პროპორციებზე (ზღვრის ზღვარი). მაგალითად, საქმეში ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ მოსარჩელეთა მიერ სადავოდ იყო მიჩნეული ოპერატიულ-სამძებრო საქმიანობის შესახებ საქართველოს კანონის ჩანაწერი, რომლის თანახმადაც „ისეთი ოპერატიულ-სამძებრო ღონისძიების ჩატარება, რომელიც ზღუდავს კანონით გარანტირებული სატელეფონო და სხვა სახის ტექნიკური საშუალებებით წარმოებული შეტყობინებების საიდუმლოებას, დაიშვება მხოლოდ მოსამართლის ბრძანებით და პროკურორის დადგენილებით, ან იმ პირის წერილობითი განცხადების საფუძველზე, რომელიც არამართლზომიერ მოქმედებათა მსხვერპლია, ან თუ სახეზეა ისეთი მართლსაწინააღმდეგო ქმედების მონაცემები, რომლისთვისაც სისხლის სამართლის კანონით სასჯელის სახით გათვალისწინებულია თავისუფლების აღკვეთა 2 წელზე მეტი ვადით.“ მოსარჩელეთა აზრით, ინტერპრეტირების დროს ნორმაში გამოყენებული კავშირი „ან“ გაუმართლებელი იყო, იგი ეწინააღმდეგებოდა პირადი ცხოვრების უფლებაში ჩარევის კონსტიტუციურ საფუძვლებს. ნორმის ანალიზის შედეგად, საკონსტიტუციო სასამართლომ დაასკვნა, რომ სიტყვების - „მოსამართლის ბრძანებით და პროკურორის დადგენილებით“ - შემდეგი ნაწილი არაკონსტიტუციური იყო,<sup>46</sup> ხოლო 2014 წლის პირველი აგვისტოს საკანონმდებლო ცვლილების თანახმად ეს პუნქტი კანონიდან ამოიღეს და სხვაგვარ მოწესრიგებას დაუქვემდებარეს. მოცემულ გადაწყვეტილებაში თვალნათელია, რომ ნორმის

45 საქართველოს საკონსტიტუციო სასამართლო, საქმე 1/1/625, 640, საქართველოს სახალხო დამცველი და სხვები საქართველოს პარლამენტის წინააღმდეგ, 14.04.2016.

46 საქართველოს საკონსტიტუციო სასამართლო, საქმე 1/3/407, ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ, 26.12.2007.

ინტერპრეტირების შესახებ სასამართლოს მსჯელობა უფლება-ში ჩარევის საფუძვლების კონტექსტში განიხილებოდა.

ადამიანის უფლებების, მათ შორის, პირადი ცხოვრების უფლების, როგორც უშუალოდ მოქმედი სამართლის გამოყენების შემთხვევები ვლინდება საქართველოს საერთო სასამართლოების მიერ კერძო სამართლებრივ ურთიერთობებში არსებულ დავებზე გამოტანილ გადანყევტილებებშიც. მაგალითად, საქართველოს უზენაესი სასამართლოს თანახმად, საქართველოს კონსტიტუციით „აღიარებულია ადამიანის სულიერი ბუნების, მისი გრძნობებისა და ინტელექტის მნიშვნელობა;“ ამავდროულად პირი დაცულია რწმენაში, აზრებში, ინტიმურ გრძნობებში.<sup>47</sup> გარდა ამისა, საქართველოს უზენაესმა სასამართლომ განიხილა პირის მიერ კერძო საუბრის ფარული ჩანაწერის მტკიცებულებად გამოყენების დასაშვებობის საკითხი. გარემოებათა გათვალისწინებით სასამართლომ ეს უფლება განმარტა, როგორც კომუნიკაციის თავისუფლების გარანტი, სადაც იგი დაცულია გარეშე პირთა არასასურველი მონაწილეობისგან. შესაბამისად, კომუნიკაციის თავისუფლება ინდივიდს შესაძლებლობას აძლევს თავად განსაზღვროს კომუნიკაციის შინაარსი და პარტიონიორი. მოცემული ინტერპრეტირება თავსებადია პირადი ცხოვრების უფლების დაცვის თანამედროვე კონცეფციასთან. ამავდროულად, სასამართლოს აზრით, პირადი ცხოვრების სფეროში ჩარევა, განსხვავებულია დაცვის ხარისხის მიხედვით, კერძოდ, ინტიმური სფერო აბსოლუტური დაცვით სარგებლობს, რაც არ არის ანალოგიური კერძო სფეროსთან მიმართებით. შესაბამისად, კერძო სფეროში ჩარევა დასაშვებია დასაცავი ობიექტის ღირსი ინტერესისა და კანონიერი მიზნის არსებობის პირობებში. სასამართლომ აღნიშნა, რომ „სამოქალაქოსამართლებრივი გარიგების დადასტურების მიზნით მტკიცებულების შესაქმნელად პირად სფეროში ჩარევა და ამით პირადი ცხოვრებისა და პირადი კომუნიკაციის უფლების შეზღუდვა გამართლებული არ არის.“ სასამართლოს აზრით მსგავსი ფარული ჩანაწერი დასაშვები გახდებოდა თუ ეს ერთა-

47 ნაჭყებია ა., სამოქალაქოსამართლებრივი ნორმების განმარტებები უზენაესი სასამართლოს პრაქტიკაში – 2000-2013 წლები. GIZ, თბილისი, 2014, გვ. 24.

დერთი გზა იქნებოდა საკუთარი უფლების დასაცავად, „იმის გამო, რომ სხვაგვარად პირი საკუთარ უფლებას ვერ დაიცავს ან არსებობს რეალური საშიშროება ყველა სხვა მტკიცებულების განადგურების, ასეთ ვითარებაში ფარული ჩანანერის გზით მტკიცებულების შექმნა დასაშვებია.“<sup>48</sup>

მორიგი მნიშვნელოვანი განმარტება ეხება პირადი ხასიათის კომუნიკაციის სოციალური ქსელის მეშვეობით დამყარების საკითხს. სასამართლოს აზრით, ნებისმიერი პირადი სახის კომენტარი, თუ იგი განხორციელებულია სოციალური პლატფორმის მეშვეობით, უნდა შეფასდეს, როგორც საჯარო ადგილას აზრის გამოხატვად. უფრო კონკრეტულად, სასამართლოს აზრით „გამოხატვის თავისუფლების კონტექსტში, „საჯაროდ გავრცელება“ არ გულისხმობს ინფორმაციის მხოლოდ პრესასა თუ ტელევიზიაში გახმაურებას, მით უმეტეს იმ პირობებში, როდესაც სოციალური მედია, ბლოგინგი და მიკრობლოგინგი სულ უფრო დიდ როლს ასრულებს თანამედროვე საზოგადოების ცხოვრებაში. ნებისმიერი საშუალება, რომელიც ინფორმაციის პირთა განუსაზღვრელი წრისადმი მიწოდებისთვის გამოდგება, საჯაროდ გავრცელების წყაროდ უნდა შეფასდეს.“ მოცემულ საქმეში, გარემოებათა გათვალისწინებით, სასამართლომ სოციალური ქსელი Facebook საჯარო წყაროდ ცნო.<sup>49</sup> შესაბამისად, მიუხედავად პირადი კომუნიკაციების მიზნობრიობისა, კომენტარების ან საჯაროდ გამოცხადების სხვა ფორმები ვერ უზრუნველყოფს პირადი ცხოვრების დაცვას. ამ შემთხვევაში პიროვნება გაცნობიერებულად თუ გაუცნობიერებლად ახდენს პირადი შეხედულებების გასაჯაროვებას. აქვე, მნიშვნელოვანია იმის გააზრებაც, რომ მომხმარებლებს სრული თავისუფლება აქვთ მათ შესახებ არსებული ინფორმაციისა თუ ფოტოსურათების საკუთარ პირად გვერდზე განთავსებაში. თუმცა, მეტი სიფრთხილეა საჭირო, მაგალითად, პირად პროფილზე სხვა პირის გამოსახულების განთავსებისას. ამ ფაქტმა შესაძლოა გავლენა იქონიოს

48 საქართველოს უზენაესი სასამართლო, საქმე ას-1155-1101-2014, ნ.რ.-ე, ზ.მ.-ე და ე.ა.-ე-ს წინააღმდეგ, 04.05.2015.

49 საქართველოს უზენაესი სასამართლო, საქმე ას-1559-1462-2012, გ.კ.-ი, ნ.ა.-ი-ს წინააღმდეგ, 09.01.2014.

აღნიშნული პირის წარმოდგენაზე საზოგადოებაში.<sup>50</sup>

პერსონალური ხასიათის ინფორმაციის გასაჯაროვებას ეხება თბილისის სააპელაციო სასამართლოს გადაწყვეტილება, სადაც აპელანტი საჯარო დაწესებულებისგან ითხოვდა 2008 წლის განმავლობაში თანამშრომელთა ვინაობებისა და მათ მიერ დაკავებული თანამდებობების, ასევე, ბიუჯეტიდან თითოეულ თანამშრომელზე გაცემული ხელფასის, პრემიისა და ჯილდოს ოდენობის შესახებ ინფორმაციას, თითოეულ პირზე ინდივიდუალური მითითებით. გარდა ამისა, თითოეული თანამშრომლის სამივლინებო ხარჯებს 2008 წლის განმავლობაში, ასევე, ინდივიდუალური დიფერენციაციით. საჯარო რეესტრის სააგენტომ ინფორმაციის გაცემაზე უარი განაცხადა, ასევე, ვერ დაკმაყოფილდა სარჩელი პირველი ინსტანციის სასამართლოშიც, სადაც განიმარტა, რომ მოთხოვნილი ინფორმაცია წარმოადგენდა პირადი ხასიათის მონაცემებს, რაც ადმინისტრაციული ორგანოს მხრიდან ექვემდებარებოდა დაცვას. ამავდროულად, სუბიექტები ვის შესახებაც მოითხოვებოდა ინფორმაცია, არ იყვნენ თანამდებობის პირები, შესაბამისად, მათზე ვერ გავრცელდებოდა ის წესი, რომლის თანახმადაც საჯარო თანამდებობის პირების შესახებ ინფორმაცია უნდა იყოს ხელმისაწვდომი. სასამართლოს აზრით აპელანტის ლეგიტიმური მიზანი დაკმაყოფილდა, ვინაიდან მას მიენოდა ზოგადი სტატისტიკური ინფორმაცია 2008 წლის განმავლობაში გაწეული საბიუჯეტო ხარჯების შესახებ.<sup>51</sup>

პირადი ცხოვრების უფლების ქართული სტანდარტის განხილვისას, როგორც ნორმატიულ ისე სასამართლოს გადაწყვეტილებების ჭრილში, არაერთხელ შევეხეთ პერსონალური მონაცემების დაცვის საკითხს. შესაბამისად, პერსონალური მონაცემები პირადი ცხოვრების განუყოფელი ნაწილია.

50 Berg B.V., Potzsch S., Leenes R., Borcea-Pfitzmann K., Beato F., *Privacy in Social Software. Privacy and Identity Management for Life*, Springer, 2011, p. 41.

51 თბილისის სააპელაციო სასამართლო, საქმე 3/2909-09, ანა შალამბერიძე საჯარო რეესტრის ეროვნული სააგენტოს წინააღმდეგ, 28.12.2009, მითითებულია წყაროში: საქართველოს ახალგაზრდა იურისტთა ასოციაცია, *ინფორმაციის თავისუფლება საქართველოში*, თბილისი, 2010, გვ. 146-149.

### 1.2.2. პირადი ცხოვრების უფლების დაცვის ევროპული სტანდარტი

პოზიტიურ სამართალში დიდი მნიშვნელობის მქონეა კონსტიტუციები და ამ დოკუმენტით განერილი ძირითადი უფლებები. სახელმწიფოებში მათ შესაბამისად ხდება სხვა სამართლებრივი აქტების მიღება. ევროპული კონსტიტუციებიდან ერთ-ერთი ყველაზე ძველი, ნორვეგიის სამეფოს 1814 წლის კონსტიტუცია საკმაოდ ლაკონურ ჩანაწერებს შეიცავს პირად ცხოვრებასთან მიმართებით. პირველი მათგანი ეხება ინფორმაციის თავისუფლებისა და პირადი ცხოვრების დაცვას შორის ბალანსს, კონსტიტუციის თანახმად: „[...] ყველას აქვს სახელმწიფო და მუნიციპალიტეტის ადმინისტრაციის დოკუმენტებთან წვდომის უფლება [...]. ამ უფლების შეზღუდვა შესაძლებელია დანესდეს კანონით, რათა ინდივიდის პრივატულობა იყოს დაცული [...]“<sup>52</sup> ამასთან: „არ უნდა მოხდეს კერძო საცხოვრისის ჩხრეკა, გამოწვევა სისხლის სამართლის საქმეები.“<sup>53</sup> როგორც ვხედავთ ეს ჩანაწერი არ ავრცობს პირადი ცხოვრების უფლებას და შემოიფარგლება ვიწრო ფორმულირებით. ამგვარი მიდგომა, კონსტიტუციის შექმნის პერიოდში არსებული რეალობითაა გამოწვეული. XIX საუკუნის პირველ ნახევარში პირადი ცხოვრების უფლება არ წარმოადგენდა დიდი ყურადღების საგანს. გარდა ამ მექანიზმებისა, ნორვეგიულ კანონმდებლობაში გვხვდება პიროვნულობის ზოგადი დაცვა, რომელიც არსებობს დანერგილი სამართლისგან დამოუკიდებლად. იგი წარმოადგენს ნორმატიული ჩანაწერების შინაარსის განვრცობას და ვითარდება სასამართლო გადაწყვეტილებების მეშვეობით. საბოლოოდ, ამ გადაწყვეტილებათა მიზანია დაიცვას პირის ინტერესი პირადი ცხოვრების უფლების ჭრილში. მაგალითად, ნორვეგიის უზენაესი სასამართლოს მიერ განხილული ერთ-ერთი საქმე ეხებოდა ფილმის დაანონსებულ საჯარო ჩვენებას ორი პიროვნების შესახებ, რომლებმაც წლების წინ ჩაიდინეს სასტიკი დანაშაული. დადგინდა, რომ მიუხედავად გასული დროისა აღნიშნული ფილმის საჯაროდ გავრცელების შემთხვევაში დაირღვეოდა პირთა ზოგადი უფლება პიროვნულობაზე, რომელიც კანონმდებლო-

52 ნორვეგიის სამეფოს 1814 წლის კონსტიტუცია, მ. 100.

53 იქვე, მ. 102.

ბით პირდაპირ არ იყო განერილი.<sup>54</sup>

განსხვავებული სახის ფორმულირებას შეიცავს ნიდერლანდების სამეფოს 1815 წლის კონსტიტუცია, რომელიც ნორვეგიის უზენაეს კანონთან შედარებით, უფრო ფართოდ ახდენს ამ უფლების დეკლარირებას. მითითებულია, რომ „ყველას აქვს მისი პირადი ცხოვრების დაცვის უფლება, გარდა შეზღუდვებისა, რომელიც შეიძლება დანესდეს პარლამენტის აქტით.“<sup>55</sup> კონსტიტუციის მონაპოვარს წარმოადგენს ისიც, რომ დათქმა გაკეთებულია არა მხოლოდ პირადი ცხოვრების, არამედ პერსონალური მონაცემების დაცვაზეც, კერძოდ, „პირადი ცხოვრების დაცვის მიზნით პარლამენტის მიერ მიიღება წესები, რომელიც ეხება პერსონალური მონაცემების შენახვასა და გავრცელებას.“<sup>56</sup> ასევე, მითითებაა გაკეთებული მონაცემთა სუბიექტის უფლებებზეც, „წესები, რომელიც ეხება პირთა უფლებებს იყვნენ ინფორმირებული მათ შესახებ მონაცემთა ჩანერის, მათი გამოყენებისა ამ მონაცემთა შესწორების შესახებ განისაზღვრება პარლამენტის აქტით.“<sup>57</sup> მიუხედავად ამისა, პირადი ცხოვრების შესახებ პოლიტიკის ჩამოყალიბება XX საუკუნის 60-იან წლებში შეიმჩნევა, როდესაც დღის წესრიგში დადგა მოქალაქეთა მონიტორინგის საკითხი. გარდა ამისა, პერსონალურ მონაცემთა დაცვის უფლების კონსტიტუციური განმტკიცება თანდაპირველ ეტაპზე არ მომხდარა, ვინაიდან იგი 1983 წლის შესწორებით გაიწერა.<sup>58</sup>

პირადი ცხოვრების უფლებას შედარებით ვიწრო ფორმულირება გააჩნია გერმანიის ფედერაციული რესპუბლიკის 1949 წლის ძირითადი კანონის მიხედვით, სადაც მითითებულია, რომ „კორესპოდენციის, გზავნილებისა და ტელეკომუნიკაციის ხელშეუხებლობა დაცულია. შეზღუდვები შესაძლებელია დანესდეს

54 Personvern Pa Nettet. *Two Suspicious Individuals* [<http://personvern.info/rett-skilder/avgjorelser/to-mistenkelige-personer-rt-1952-s-1217/>]; Bygrave, L.A. & Aaro, H.A., *Privacy, Personality and Publicity – An Overview of Norwegian Law*; International Privacy, Publicity and Personality Laws, Butterworths, 2001, pp.340-341.

55 ნიდერლანდების სამეფოს 1815 წლის კონსტიტუცია, მ. 10, პ. 1.

56 იქვე, პ. 2.

57 იქვე, პ. 3.

58 Koops, B. J., *The Evolution of Privacy Law and Policy in the Netherlands*, Journal of Comparative Policy Analysis (Vol. 13, No. 2), 2011, pp. 166-167.

მხოლოდ კანონის თანახმად, თუ იგი მიზნად ისახავს დაიცვას თავისუფალი ძირითადი დემოკრატიული წყობილება ან ფედერაციის ან ლანდის არსებობა ან უსაფრთხოება, კანონი შეიძლება ადგენდეს, რომ პირი არ იქნეს ინფორმირებული შეზღუდვის შესახებ [...].<sup>59</sup> გერმანიაში დამკვიდრდა „პიროვნულობაზე უფლების“ კონცეფცია, რომელიც თავდაპირველ ეტაპზე არ გამოირჩეოდა წარმატებით.<sup>60</sup> დამატებით, პირადი ცხოვრების დაცვა სამოქალაქო სამართლით დაცვად საგანსაც წარმოადგენს. ერთ-ერთი საქმეში მოსარჩელე დააკავეს დანაშაულისთვის, რა ინფორმაციაც 20 წლის შემდეგ ხელმისაწვდომი გახდა საგამოძიებო სააგენტოს მხრიდან მისი კლიენტებისთვის. კანონმდებლობით, ამ შემთხვევაში, დარღვევა სახეზე იქნებოდა მაშინ თუ გაცემული ინფორმაცია იქნებოდა იმ აუცილებლობის მიღმა განხორციელებული, რასაც ადგილი ჰქონდა გაცემის მომენტში.<sup>61</sup> სასამართლოს აზრით, ამგვარი გაცემა ნებადართული იყო, რამდენადაც პირი თავისი ნებით ახორციელებდა არალეგიტიმურ ქმედებებს, ასევე, არ მოხდა დეტალების გაცემა მის დანაშაულთან მიმართებით.<sup>62</sup> მორიგი მნიშვნელოვანი გადაწყვეტილება მიიღო გერმანიის ფედერალურმა უზენაესმა სასამართლომ 1954 წელს. საქმეში მოცემული გარემოებების მიხედვით, მოსარჩელემ, რომელიც იყო ადვოკატი, თავისი კლიენტის დავალებით ყოველკვირეულ გამოცემას გაუგზავნა მოთხოვნა, რომლის თანახმადაც გამომცემლობისგან მოითხოვდა მისი კლიენტის შესახებ გამოქვეყნებული ინფორმაციის შესწორებას, რაც გამომცემლობამ ნაწილობრივ შეასრულა. მოსარჩელის აზრით კი, მისი კლიენტი, ამგვარი, ნაწილობრივი, შესწორებით საზოგადოების წინაშე მცდარი სახით წარდგა. ამის შემდეგ, გამომცემლობას დაევალა ინფორმაციის სრული სახით შესწორება.<sup>63</sup>

მოგვიანებით გერმანიის ფედერალურმა საკონსტიტუციო

59 გერმანიის ფედერაციული რესპუბლიკის 1949 წლის ძირითადი კანონი, §. 10.

60 Krause, H.D., *The Right to Privacy in Germany: Pointers for American Legislation?*, Duke Law Journal (No. 3), 1965, p. 485.

61 იქვე, გვ. 487-488.

62 იქვე, fn. 28.

63 იქვე, გვ. 488.

სასამართლომ 1983 წელს მოსახლეობის აღრიცხვასთან დაკავშირებულ გადანყვეტილებებში მიუთითა ინფორმაციული თვითგამორკვევის უფლებაზე. ამ გადანყვეტილებით სასამართლომ დაადგინა, რომ ზოგადი პიროვნული უფლებიდან გამომდინარე ყველას აქვს უფლება მოახდინოს საკუთარი თავის ინფორმაციული თვითგამორკვევა.<sup>64</sup> ზოგადად, პირადი ცხოვრების დაცვასთან დაკავშირებული კანონმდებლობის განვითარება გერმანიაში XX საუკუნის შუა პერიოდიდან შეინიშნება. მიიჩნევა, რომ პრივატულობის დაცვა მჭიდრო კავშირშია „პიროვნულობის“ კონცეფციასთან, იგი განიმარტება, როგორც „პირადი სივრცე, რომელშიც ადამიანები თავისუფლად და ინდივიდუალური პასუხისმგებლობით ახდენენ საკუთარი თავის განვითარებას.“ შესაბამისად, პრივატულობა თვითრეალიზაციის ნაწილს წარმოადგენს.<sup>65</sup>

პირადი ცხოვრების უფლებაზე უშუალო დათქმას არ აკეთებს საფრანგეთის რესპუბლიკის 1958 წლის კონსტიტუცია და არც 1789 წლის ადამიანისა და მოქალაქის უფლებათა დეკლარაცია. თუმცა, საფრანგეთში პირადი ცხოვრების უფლების საინტერესო ევოლუციას ჰქონდა ადგილი. პირველი კანონი, რომელიც პირადი ცხოვრების დაცვასთან დაკავშირებულ დებულებებს შეიცავდა იყო 1881 წლის 29 ივლისის კანონი პრესის თავისუფლების შესახებ. იგი პირს ანიჭებდა დაცვის სამუშალებას დეფამაციის წინააღმდეგ. მიიჩნევენ, რომ კანონის ამგვარი მიდგომა პირადი ცხოვრების დაცვას მხოლოდ ვიწრო შემთხვევებში, კერძოდ, დეფამაციის წინააღმდეგ უზრუნველყოფდა, ხოლო დროთა განმავლობაში, XX საუკუნის დასაწყისიდან სასამართლოებმა აღიარეს პიროვნების უფლება გამოსახულების დაცვაზე, რასაც მოჰყვა შესაბამისი გადანყვეტილებები. ამ პერიოდში სასამართლოები მორალური ზიანის არსებობაზე მიუთითებდნენ და არა ქონებრივზე.<sup>66</sup>

გარდა აღნიშნულისა, პირადი ცხოვრების უფლება შესაძლოა

64 *Freiheitsfoo. Volkszahlungsurteil in englischer Sprache: Census Act* [<https://freiheitsfoo.de/census-act/>].

65 Ramage, S. (ed.), *Privacy – Law of Civil Liberties*, iUniverse, 2007, p. 276.

66 Wagner, W.J., *The Development of the Theory of the Right to Privacy in France*, Washington University Law Review (Issue 1), 1971, pp. 49-50.

წინააღმდეგობაში იყოს სხვა უფლებებთანაც, მაგალითად, ხელოვნების თავისუფლებასთან, რასაც ადგილი ჰქონდა საქმეში *Allez v. Montpezat*. საფრანგეთში მოპასუხეების მიერ გამოქვეყნდა ნოველა, სადაც შვიდი მოსარჩელე მოთხრობის მოქმედი გმირი იყო. ამავდროულად, ნაწარმოებში გამოიყენეს ერთ-ერთი პირის ნამდვილი სახელი, ხოლო სხვების იდენტიფიცირება ირიბად, პიროვნებების ადგილმდებარეობის მიხედვით ხდებოდა. პერსონაჟები მოხსენიებულნი იყვნენ დამცინავი, ხოლო ზოგიერთი მათგანი - უღირსი ფორმით. სასამართლომ, ამ შემთხვევაშიც, მხარი დაუჭირა მორალური ზიანის იდეას და მოსარჩელების სასარგებლოდ გამოიტანა გადაწყვეტილება.<sup>67</sup>

პირადი ცხოვრების უფლება ევოლუციურ თავისებურებებს შეიცავს. სახელმწიფოთა კონსტიტუციებში ეს უფლება მეტნაკლები კონკრეტულობითაა განერილი, ხოლო ზოგ შემთხვევაში კი, სხვა უფლებების განმარტების შედეგად იქცა დეკლარირებულ უფლებათა ნაწილად. ამ უფლებით სარგებლობის თავდაპირველი შემთხვევები სამოქალაქო დავებს უკავშირდება, ამ დროს, ძირითადად, სხვა პიროვნების შესახებ არსებული სხვადასხვა პირადი ასპექტის უნებართვო გამოყენებას აქვს ადგილი. პიროვნების სახელმწიფოსგან დაცვის იდეა ადამიანის ძირითადი უფლებების განმტკიცების უპირველესი წინაპირობაა. მიუხედავად ამისა, თავდაპირველად ამ უფლების უზრუნველყოფასთან დაკავშირებული დავები, ძირითადად, პორიზონტალური ხასიათის იყო, რამდენადაც წარმოიშობოდა კერძო პირებს შორის.

### **1.2.3. პირადი ცხოვრების დაცული სფერო**

**ადამიანის უფლებათა ევროპული სასამართლოს  
გადაწყვეტილებათა მიხედვით**

ადამიანის უფლებათა დაცვის ერთ-ერთ ყველაზე გავლენიან დოკუმენტად გვევლინება ევროპის საბჭოს 1950 წლის 4 ნოემბრის ადამიანის უფლებათა და თავისუფლებათა დაცვის ევროპული კონვენციზ, რომელმაც მნიშვნელოვანი წვლილი შეიტანა ძირითად უფლებათა დაცვის გაძლიერებაში. ეს აქტი ქმედითია მის ფარგლებში შექმნილი სასამართლოს მეშვეობი, რომელიც

67 იქვე, გვ. 52-53.

ევროპის საბჭოს წევრ ქვეყნებში უზრუნველყოფს ადამიანის უფლებათა დაცვას, რაც მისი გადამწყვეტილებების სავალდებულო შესრულების პირობიდან გამომდინარეობს.

კონვენციის მე-8 მუხლი (პირადი და ოჯახური ცხოვრების პატივისცემის უფლება) ორი ნაწილისგან შედგება, კერძოდ, I ნაწილის თანახმად „ყველას აქვს უფლება, პატივი სცენ მის პირად და ოჯახურ ცხოვრებას, მის საცხოვრებელსა და მიმოწერას.“ II ნაწილის მიხედვით კი „დაუშვებელია ამ უფლების განხორციელებაში საჯარო ხელისუფლების ჩარევა, გარდა ისეთი შემთხვევებისა, როდესაც ასეთი ჩარევა ხორციელდება კანონის შესაბამისად და აუცილებელია დემოკრატიულ საზოგადოებაში ეროვნული უშიშროების, საზოგადოებრივი უსაფრთხოების ან ქვეყნის ეკონომიკური კეთილდღეობის ინტერესებისთვის, უნესრიგობის ან დანაშაულის თავიდან ასაცილებლად, ჯანმრთელობის ან მორალისა თუ სხვათა უფლებათა და თავისუფლებათა დასაცავად.“ როგორც სჩანს, უფლება კლასიკური სახით არის ფორმულირებული, კერძოდ, მითითებულია უფლებით დაცული სფერო და შემდგომ მასში ჩარევის საფუძვლები და ზღვრები.

გარდა ამისა, ეს ჩანაწერი სახელმწიფოს აკისრებს პოზიტირ და ნეგატიურ ვალდებულებებს. პირველი მათგანი ავალდებულებს სახელმწიფოს შექმნას ისეთი გარემო, რომელიც უზრუნველყოფს ადამიანის უფლებების, მათ შორის, პირადი ცხოვრების დაცვას, როგორც კანონის ფორმალური დანაწესით, ისე ქმედითი კუთხითაც, მისი ჯეროვანი რეალიზაციის მეშვეობით. სასამართლომ საქმეში Van Kuck v. Germany აღნიშნა, რომ ნეგატიურ მოვალეობებთან ერთად არსებობს პოზიტირი ვალდებულებები, რომელიც აუცილებელია პირადი და ოჯახური ცხოვრების პატივისცემისთვის. ეს ვალდებულებები შესაძლებელია მოიცავდეს პირადი ცხოვრების დაცვისკენ მიმართულ ზომებს, მაშინაც კი, როდესაც საქმე ეხება ინდივიდებს შორის არსებულ ურთიერთობებს. ნეგატიური ვალდებულების თანახმად კი, სახელმწიფო თავად არ უნდა იყოს ამ უფლების დარღვევის ინიციატორი და რეალიზატორი. პირველ რიგში, ჩარევა უნდა იყოს კანონთან შესაბამისი, ჩარევის წინაპირობა დადგენილი უნდა იყოს შიდასახელმწიფოებრივი კანონით და დაცული უნდა იყოს

კანონის უზენაესობა. გარდა ამისა, შეზღუდვისთვის გამოყენებული ზომა უნდა ემსახურებოდეს ლეგიტიმურ მიზანს, კერძოდ, ეხებოდეს ეროვნული და საჯარო უსაფრთხოების, ეკონომიკური კეთილდღეობის უზრუნველყოფას და არეულობის ან დანაშაულის აღკვეთას, ასევე, ჯანმრთელობის, მორალის ან სხვათა უფლებებისა და თავისუფლებების დაცვას. მესამე კრიტერიუმის თანახმად კი, გამოყენებული ზომა უნდა იყოს აუცილებელი დემოკრატიულ საზოგადოებაში, რაც გულისმობს მომეტებული საზოგადოებრივი საჭიროების არსებობას, ამის საფუძველზე კი, შემდგომ დგინდება იყო თუ არა შეზღუდვისთვის გამოყენებული ზომა პროპორციული. ნევრ სახელმწიფოებს, ასევე, გააჩნიათ ერთგვარი შეფასების თავისუფლება განსაზღვრონ თუ რა არის უფლების შეზღუდვისთვის აუცილებელი თავიანთ სახელმწიფოებში. ამის განსაზღვრა წინასწარ არ არის მარტივი.<sup>68</sup> შეფასების თავისუფლება განსხვავდება გარემოებების მიხედვით, განსახილველი საკითხისა და წინაპირობების გათვალისწინებით.

სასამართლომ დაადასტურა სახელმწიფოს უპირველესი ვალდებულება ჩარევისგან თავის შეკავების თაობაზე საქმეში *Airey v. Ireland*, სადაც აღნიშნა, რომ მე-8 მუხლის მიზანია არსებითად დაიცვას ინდივიდი საჯარო პირების მხრიდან უსაფუძვლო ჩარევის არსებობისას. მაგალითად, კერძო პირებს გააჩნიათ ზოგადი უფლება მიიღონ პირადი ფოსტა, დაამყარონ და განავითარონ ურთიერთობები სხვა პირებთან და ა.შ. ამ მუხლის საფუძველზე გამოტანილი გადაწყვეტილებები თავისებურებებით ხასიათდება ყოველ კონკრეტულ შემთხვევაში, ამიტომ მნიშვნელოვანია ის პრაქტიკა, რაც დამკვიდრებულია ადამიანის უფლებათა ევროპული სასამართლოს მიერ.<sup>69</sup>

თუმცა, არსებობს მოსაზრება, რომ პირადი ცხოვრების უფლება არ მოიცავს მხოლოდ პირადი ცხოვრების მკაცრად განსაზღვრულ სფეროს და იგი პირის სხვა აქტივობებზეც ვრ-

68 Moreham, N.A., *The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination*, European Human Rights Law Review, Sweet and Maxwell, 2008, p. 47.

69 Icelandic Human Rights Centre, *Interference with the Right to Privacy*, [<http://www.humanrights.is/en/human-rights-education-project/comparative-analysis-of-selected-case-law-achpr-iachr-echr-brc/the-right-to-respect-for-private-and-family-life/interference-with-the-right-to-privacy>].

ცელდება. ეს უფლება არ იცავს მხოლოდ პირის განმარტოებას, სადაც მას შეუძლია დამოუკიდებლად მოქმედება, არამედ, იგი იცავს ადამიანთა შორის ურთიერთობას, როგორც კერძო, ისე საჯარო გარემოში. ადამიანის უფლებათა ევროპულმა სასამართლომ აღნიშნა, რომ „პირადი ცხოვრების ცნების დაყვანა მხოლოდ „შიდა წრემდე“, სადაც ინდივიდი ცხოვრობს ისეთი პირადი ცხოვრებით, როგორსაც იგი ირჩევს და, დამატებით, გარესამყაროს სრულად გამორიცხვა, ამ ცნების ვიწრო განმარტება იქნება. არ არსებობს მართლზომიერი საფუძველი, რათა პირადი ცხოვრების ცნებიდან გამოვრიცხოთ ქმედებები, რომელიც ეხება საქმიანობას ან პროფესიას, ვინაიდან პირები სამუშაო ვითარებაში ამყარებენ ხელშესახებ კავშირს და გააჩნიათ გარესამყაროსთან ურთიერთობების განვითარების შესაძლებლობა.“ შესაბამისად, სამუშაო ადგილზე ჩატარებული ჩხრეკა, რომელიც არ იყო შემოფარგლული მოსაპოვებელი ინფორმაციის ლიმიტირების პრინციპით, ჩაითვალა მე-8 მუხლის დარღვევად.<sup>70</sup>

ადამიანის უფლებათა ევროპული სასამართლოს მიერ პირადი ცხოვრების თაობაზე განხილული საქმეები არაერთ სხვა უფლებასთან არის კავშირში. მაგალითად, როდესაც საქმე ეხება პირად ცხოვრებასთან, მათ შორის, პერსონალურ მონაცემებთან დაკავშირებულ დეტალებს და მათი გასაჯაროების საკითხს, მნიშვნელოვანია მოხდეს შეპირისპირებულ ინტერესთა შედარება სამი კრიტერიუმის მიხედვით, კერძოდ: 1. არის თუ არა სახეზე საზოგადოებრივი ინტერესი; 2. იყო თუ არა პირი საჯარო ფიგურა, რომლის მიმართაც საზოგადოებას მომეტებული ინტერესი გააჩნია; და 3. რა გზით იყო პირის შესახებ ინფორმაცია მოპოვებული.<sup>71</sup> სასამართლოს აზრით, როდესაც საუბარია ფიზიკურ და საზოგადო პირებს შორის პირადი ცხოვრების დაცვის უფლების რეალიზებაზე, მომეტებული საზოგადოებრივი ინტერესის გამო, საჯარო ფიგურები ვერ გაიზიარებენ უფლების დაცვის იმ დონეს, რითაც სარგებლობენ რიგითი ფიზიკური პირები.<sup>72</sup> მომეტებული საჯარო ინტერესის გამო პირადი ცხოვრე-

70 ECtHR, App. no. 13710/88, *Niemietz v. Germany*, 16.12.1992.

71 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 67-68.

72 ECtHR, App no. 39954/08, *Axel Springer AG v. Germany*, 07.02.2012.

ბის გარკვეულ დონეზე დათმობა გამართლებულია.<sup>73</sup> კერძო და საჯარო პირები არ სარგებლობენ პირადი ცხოვრების თანაბარი დაცვით, რის გამოც მათ მიმართ მოპყრობა სახელმწიფოსგან არ უნდა იყოს იდენტური.<sup>74</sup>

კონვენციით გარანტირებული პირადი ცხოვრების დაცვის უფლება, ასევე, მოიცავს სამუშაო ადგილსაც, თუმცა დაცვის დონე აქ უფრო დაბალია. მაგალითად, ადამიანის უფლებათა ევროპულმა სასამართლომ განმცხადებლის სარჩელი მის სამუშაო ადგილზე ფარული ვიდეოთვალთვალის გამო დასაშვებად არ ცნო, ვინაიდან სასამართლოს აზრით, ყველა წინაპირობა იყო გათვალისწინებული, რათა დაცული ყოფილიყო სწორი ბალანსი პირადი ცხოვრების დაცვის უფლებასა და საკუთრების უფლებას შორის.<sup>75</sup> სასამართლოს თანახმად, ფარული ვიდეოთვალთვალი სამუშაო ადგილზე განხორციელდა მხოლოდ მას შემდეგ, რაც დამსაქმებელმა განიცადა გარკვეული პროდუქციის დანაკლისი, გარდა ამისა, ვიდეოთვალთვალი მიმდინარეობდა მოკლე პერიოდში - ორი კვირის მანძილზე, დაკვირვება ხორციელდებოდა მხოლოდ იმ მონაკვეთზე, სადაც განმცხადებელი ასრულებდა თავის მოვალეობებს, მათ შორის, სალარო აპარატთან. შესაბამისად, ამგვარი თვალთვალი სასამართლომ პროპორციულად მიიჩნია.<sup>76</sup>

ზემოაღნიშნული სასამართლო გადაწყვეტილებებიდან გამომდინარე ნათელია ადამიანის უფლებათა ევროპული სასამართლოს მიდგომა პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებასთან მიმართებით. აღსანიშნავია, რომ კონვენციის მე-8 მუხლი და, ზოგადად, არც კონვენციის რომელიმე სხვა მუხლი, არ შეიცავს ფორმულირებას პერსონალურ მონაცემთა დაცვის შესახებ.

73 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 57.

74 ECtHR, App. no. 40660/08 and 60641/08, *Von Hannover v. Germany*, no. 2, 07.02.2012.

75 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 278.

76 ECtHR, App. no. 420/07, *Köpke v. Germany*, 05.10.2010.

#### 1.2.4. პირადი ცხოვრების უფლების დაცული სფერო ამერიკული პრეცედენტული სამართლის მიხედვით

პირადი ცხოვრების დაცვის შესახებ ერთ-ერთ პირველ სამართლებრივ და საკმაოდ გავლენიან სტატიაში ავტორებმა პრивატულობა განსაზღვრეს როგორც უფლება იყო „დავინყებულები“ (იყო „განმარტოებულები“).<sup>77</sup> თავისი შინაარსით ეს ფორმულირება ფართოა, ხოლო დროთა განმავლობაში შეიძინა განვითარების სხვადასხვა მიმართულებები. მოცემული სტატია ამერიკულ სამართლებრივ სივრცეში მონუმენტურ ნაშრომს წარმოადგენს და გარდამტეხი მნიშვნელობის მქონეა.<sup>78</sup> მთავარი საფრთხე, ავტორების აზრით, იმ პერიოდში არსებული საგაზეთო პუბლიკაციების სიხშირითა და ფოტოგადაღებებით იყო გამოწვეული, რაც პირადი და კერძო ცხოვრების „წმინდა“ საზღვრებს ლახავდა.<sup>79</sup> სირთულე მდგომარეობდა იმაში, რომ იმ მომენტისთვის ამერიკული კანონმდებლობა კონკრეტულად არ უზრუნველყოფდა უფლებას პირად ცხოვრებაზე. ცილისწამების წინააღმდეგ მიმართული კანონმდებლობა პირს იცავდა მასზე მცდარი ინფორმაციის გავრცელებისგან. სახელშეკრულებო სამართალი კი, პირს გარანტიებს ანიჭებდა მხოლოდ კონკრეტულ შემთხვევებში მხარესთან დადებული შეთანხმებიდან გამომდინარე.<sup>80</sup> მეტიც, პირის გამოსახულებით სარგებლობისას, ავტორები ვერც საკუთრების უფლებით სარგებლობაში ხედავდნენ გამოსავალს.<sup>81</sup> ამ პუბლიკაციამ მნიშვნელოვანი სათავე დაუდო აშშ-ში პირადი ცხოვრების უფლების კონსტიტუციურ აღიარებას.

ზოგადად, ნებისმიერი სამართლებრივი საკითხი, ამერიკის შეერთებული შტატების სამართლებრივი სისტემის განსხვავებულობიდან გამომდინარე, ექვემდებარება ევოლუციურ განვითარებას, რიგ შემთხვევაში სასამართლო პრეცედენტების, ხოლო სხვა შემთხვევაში ამერიკელი პრაქტიკოსი და თეორეტიკო-

77 Warren, S. D. & Brandeis, L.

78 Mathews, K.J. (ed.), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age: A Brief History of Information Privacy Law*, The Privacy and Data Security Practice Group at Proskauer Rose LLP, 2006, p. 10.

79 Warren, S. D. & Brandeis L., pp. 193, 195.

80 Mathews, (ed.), p. 11.

81 Warren, & Brandeis, p. 200.

სი მეცნიერების დოქტრინული შეხედულებების (Restatements) - შესაბამისად.

აშშ-ის კონსტიტუციის ტექსტი არ იცნობს სიტყვას „პრივატულობა“ (privacy), პირადი ცხოვრების დაცვის შინაარსთან ყველაზე ახლოს დგას აშშ-ის კონსტიტუციის IV შესწორება, რომლის ტექსტი შემდეგი ფორმულირებითაა მოცემული: „ადამიანების უფლება, რომ ისინი, მათი საცხოვრისები, ჩანაწერები და ქმედებები იქნეს დაცული დაუსაბუთებელი ჩარევისა და შეზღუდვისგან, არ უნდა იქნეს შელახული, გარდა იმ შემთხვევებისა თუ არსებობს გონივრული ეჭვი, რაც ნებადართულია სანქციით, და აღწერილია ის ადგილი, რომელიც უნდა იქნეს გამოკვლეული და ის პირები ან ნივთები, რომელიც უნდა იქნეს დაკავებული.“ მოცემული კონსტიტუციური დანაწესი არაერთხელ იქნა გამოყენებული აშშ-ის უზენაესი სასამართლოს მიერ. მაგალითად, სასამართლომ აღნიშნა, რომ „ადამიანთა უფლების კონსტიტუციური გარანტია მათი ჩანაწერების დაცვის შესახებ დაუსაბუთებელი ამოღებისა და ჩამორთმევისგან ვრცელდება იმ ჩანაწერებზეც, რომელიც დახურულია შემომწმებისთვის, სადაც არ უნდა ინახებოდეს იგი.“<sup>82</sup> გარდა ამისა, სასამართლომ, ასევე, აღნიშნა, რომ „უმართლო ქმედების არსი ვლინდება არა პირისთვის კარის შემტვრევასა და მისი ქვითრების ჩხრეკაში, არამედ იმაში, რომ მოხდა მისი ხელშეუვალი უფლების - პირადი უსაფრთხოების - შელახვა [...], დოკუმენტების ან პირადი ჩანაწერების ნებისმიერი იძულებითი და სავალდებულო გამოთხოვა, რომელიც დანაშაულისთვის გამოიყენება მტკიცებულებად, დაკავებისთვის ან ნივთების კონფისკაციისთვის, წარმოადგენს განაჩენის შემადგენელ ნაწილს.“<sup>83</sup>

პირადი ცხოვრების უფლების დარღვევასთან დაკავშირებული საკითხები აშშ-ის სასამართლო პრეცედენტების მიხედვით, მათ შორის, ჩამოყალიბდა დელიქტური სამართლის (Tort Law) რეგულირების საგნად. სასამართლოს განმარტების თანახმად, პირადი ცხოვრების აშკარად კერძო საკითხების დაცვის უფლება ბუნებითი სამართლის შემადგენელ ნაწილს წარმოადგენს. თუ პირი განიზრახავს, იცხოვროს ნაწილობრივ განმარტოებუ-

82 Supreme Court of the United States, 96 U.S. 727, *Ex Parte Jackson*, 1877.

83 Supreme Court of the United States, 116 U.S. 616, *Boyd v. United States*, 1886.

ლად, მას აქვს უფლება აირჩიოს დრო, ადგილი და პირობები რა დროსაც იგი იქნება საზოგადოებისთვის ხელმისაწვდომი. სხვა სიტყვებით, პირი არ უნდა იქნეს წარდგენილი საზოგადოებისთვის მისი თანხმობის გარეშე.<sup>84</sup>

XX საუკუნის მეორე ნახევარში ამერიკელმა მეცნიერმა უილიამ პროსერმა გააანალიზა იქამდე არსებული სასამართლო გადაწყვეტილებები და განაზოგადა დელიქტური სამართლის ის ნაწილი, რომელიც ეხება პირადი ცხოვრების უფლების დარღვევას, როგორც დელიქტს.<sup>85</sup> მისი დასკვნით, პირადი ცხოვრების უფლება მოიცავს ოთხი განსხვავებული სახის ჩარევას, რომელიც მოსარჩელის სხვადასხვა ინტერესს ეხება. მიუხედავად იმისა, რომ ისინი გაერთიანებულნი არიან ერთი, „ქოლგის“ ტიპის უფლების ქვეშ, მათ საერთო არაფერი გააჩნიათ გარდა იმისა, რომ ყოველი მათგანი ეხება მოსარჩელის უფლებას „განმარტოებული.“ მოცემული ოთხი დელიქტი შესაძლებელია შემდეგი სახით დაჯგუფდეს: 1. მოსარჩელის სიმარტოვის ხელყოფა ან მის პირად საქმეებში ჩარევა; 2. მოსარჩელის შესახებ შეურაცხყოფელი პირადი ფაქტების გამოქვეყნება; 3. მოსარჩელის შესახებ იმგვარი ინფორმაციის გამოქვეყნება, რომელიც მცდარია; 4. მოპასუხის მიერ მოსარჩელის სახელით ან გამოსახულებით სარგებლობა.<sup>86</sup>

Restatement (Second) of Tort-ის მიხედვით პირველი დელიქტის ფორმულირება შემდეგია: პირი, რომელიც ფიზიკურად ან სხვაგვარად განზრახ დაარღვევს მეორე პირის სიმარტოვს ან ჩაერევა მის პირადი საქმეებსა ან საკითხებში, პასუხისმგებელია ამ პირის პირადი ცხოვრების დარღვევისთვის, თუ ჩარევა აშკარად შეურაცხყოფელია რიგითი ადამიანისთვის.<sup>87</sup> თუმცა ეს განმარტება არ უნდა გავიგოთ ისე, თითქოს სამართლებრივი დაცვის გარანტიები მოსარჩელეს მხოლოდ კერძო საცხოვრისში გააჩნია, არამედ ეს უფლება მას გააჩნია ყველა იმ შემთხვევაში, სადაც არსებობს პირადი ცხოვრების დაცვის გონივრული მოლო-

84 Supreme Court of Georgia (state), 50 S.E. 68, *Pavesich v. New England Life Ins. Co.*, 1905.

85 Prosser, W., *Privacy*, California Law Review (Vol. 43, No. 3), 1960.

86 იქვე, გვ. 389.

87 The American Law Institute, *Restatement (Second) of the Law. Torts*, 1977.

დინი.<sup>88</sup>

მეორე დელიქტის დოქტრინული ფორმულირების მიხედვით თუ პირი გაასაჯაროებს მეორე პირის შესახებ არსებულ პირადი ცხოვრების საკითხებს, პასუხისმგებელია დარღვევისთვის თუ გასაჯაროება შეურაცხყოფელია რიგითი ადამიანისთვის და საზოგადოებას არ გააჩნია ლეგიტიმური ინტერესი ამ საკითხის მიმართ.<sup>89</sup> მოცემული განმარტება მედიისთვის ქმნის ერთგვარ გარანტიას იმისა, რომ მოპოვებული ინფორმაცია დაუბრკოლებლად გამოქვეყნდეს, მაგალითად, აშშ-ის უზენაესმა სასამართლომ აღნიშნა, რომ მას შემდეგ, რაც ინფორმაცია განთავსებულია სასამართლოს საჯარო დოკუმენტებში, რომელიც ხელმისაწვდომია საზოგადოებისთვის, პრესას არ უნდა დაეკისროს პასუხისმგებლობა მათი გამოქვეყნებისთვის,<sup>90</sup> ამასთანავე თუ გაზეთი კანონიერად მოიპოვებს სწორ ინფორმაციას საზოგადოებისთვის მნიშვნელოვან საკითხზე, მაშინ სახელმწიფოს კონსტიტუციურად არ აქვს უფლება დაანესოს პასუხისმგებლობა ინფორმაციის გამოქვეყნებისთვის.<sup>91</sup>

მცდარი ინფორმაციის გამოქვეყნებასთან დაკავშირებული მესამე სახის დელიქტის შინაარსი შემდეგი სახისაა: თუ პირი ასაჯაროებს მეორე პირის შესახებ ინფორმაციას, რომელიც მცდარია, ინვესტს პასუხისმგებლობას მის წინაშე პირადი ცხოვრების დარღვევისთვის, თუ ქმედება შეურაცხყოფელია რიგითი ადამიანისთვის და სინამდვილესთან შეუსაბამოა.<sup>92</sup> მაგალითად, საქმეები *Semler v. Ultem Publications* (1938), *Thompson v. Close-Up, Inc.* (1950); *Metzger v. Dell Pub. Co.* (1955); *Martin v. Johnson Pub. Co.* (1956) ხასიათდება იმით, რომ ყველა მათგანი ეხებოდა მოსარჩელის გამოსახულების გამოყენებას იმ სტატიების საილუსტრაციოდ, რომლებთანაც მას კავშირი არ ჰქონდა.<sup>93</sup>

პროსერის მიერ დასახელებული მეოთხე სახის დელიქტი შემდეგი ფორმულირების შემცველია: პირი, რომელიც გამოიყენებს

88 Mathews, (ed.), p. 14.

89 The American Law Institute.

90 Supreme Court of the United States, 420 U.S. 469, *Cox Broad. v. Cohn*, 1975.

91 Supreme Court of the United States, 443 U.S. 97, *Smith v. Daily Mail*, 1979.

92 The American Law Institute, 1977.

93 Prosser. p. 406.

მეორე პირის სახელს ან გამოსახულებას პირადი სარგებლობის მიზნით, პასუხისმგებელია ამ პირის პირადი ცხოვრების უფლების დარღვევისთვის.<sup>94</sup> პირი უფლებამოსილია სხვას მიაწოდოს მისი გამოსახულების გამოქვეყნების ექსკლუზიური უფლება.<sup>95</sup> გარდა ამისა, ბოლო სახის დელიქტთან მიმართებით საყურადღებოა, რომ ეს დელიქტი დაცვის გარანტიებს ქმნის მხოლოდ საზოგადოებისთვის კარგად ცნობილი ადამიანებისთვის.<sup>96</sup>

აშშ-ის კონსტიტუციის IV შესწორების მიხედვით განმტკიცებული პირადი ცხოვრების უფლების აღიარებაში დიდი წვლილი მიუძღვის აშშ-ის სასამართლოებს, რამდენადაც პრეცედენტული სამართალი დიდ როლს თამაშობს ამერიკული კანონმდებლობის განვითარებაში. მაგალითად, საქმეში *Olmstead v. United States* (277 U.S. 438, 1928) უზენაესმა სასამართლომ განიხილა საკითხი თუ რამდენად მოითხოვებოდა, კონსტიტუციის IV შესწორების თანახმად, ნებართვა სატელეფონო მიყურადების განხორციელებისთვის. სასამართლომ დაადგინა, რომ IV შესწორება არ ვრცელდებოდა მოსმენაზე, ვინაიდან ეს უკანასკნელი არ გულისხმობდა შეჭრას პირის საცხოვრისში.<sup>97</sup> ამ გადანყვეტილებაში განსხვავებული აზრი დააფიქსირა მოსამართლე ბრანდისმა. მან აღნიშნა, რომ ხელისუფლებისთვის ხელმისაწვდომი გახდა მეტად დახვეწილი და განვითარებული საშუალებები პირად ცხოვრებაში ჩარევისთვის. ამ მსჯელობის მთავარი არსი იყო ის, რომ კონსტიტუციის IV შესწორება არ უნდა ყოფილიყო განმარტებული ხისტად და უნდა მომხდარიყო მისი ადაპტირება თანამედროვე გამოწვევებზე ეფექტური რეაგირების მიზნით.<sup>98</sup> ეს მიდგომა სასამართლომ გაიზიარა საქმეში *Katz v. United States* (389 U.S. 347, 1967) და აღნიშნა, რომ რასაც პირი გააზრებულად ასაჯაროებს, თუნდაც მის სახლში ან სამსახურში, არ ექვემდებარება IV შესწორების ქვეშ დაცვას. თუმცა, რის შენარჩუნებასაც ცდილობს საიდუმლოდ, თუნდაც საჯაროდ ხელმისაწვდომ

94 The American Law Institute, 1977.

95 Court of Appeals of the Second Circuit of the United States, 202 F.2d 866, 2d Cir., *Haelan Labs. v. Topps Chewing Gum, Inc.*, 1953.

96 Solove, D., *Privacy Law in 60 Seconds*, You Tube [<https://www.youtube.com/watch?v=mlpZS5xjdk0>], 2013.

97 Mathews, (ed.), p. 18.

98 იქვე, გვ. 19.

ადგილას, შესაძლოა იქნეს კონსტიტუციურად დაცული. სასამართლოს მიერ გამოტანილი გადაწყვეტილება ეფუძნებოდა გონივრული მოლოდინის საკითხს, რაც პირს აქვს პირადი ცხოვრების მიმართ.<sup>99</sup>

XX საუკუნის მეორე ნახევარში, ტექნოლოგიური პროგრესის გათვალისწინებით, ამერიკულმა სასამართლოებმა IV შესწორება აღიარეს როგორც „ინფორმაციული პრივატულობის“ გარანტორი. მაგალითად, ფედერალურმა უზენაესმა სასამართლომ აღნიშნა, რომ „პრივატულობის“ ცნების ქვეშ დაცული ინტერესი მოიცავს შემთხვევებს, რომელიც დაკავშირებულია პერსონალურ საკითხებთან.<sup>100</sup>

მიუხედავად მზარდი საფრთხეებისა აშშ-ის კანონმდებლობით, ფედერალურ დონეზე, დღემდე არ არსებობს ერთიანი მარეგულირებელი ნორმატიული აქტი, რომელიც მოაწესრიგებს პერსონალურ მონაცემთა დაცვის საკითხებს როგორც კერძო, ისე საჯარო სექტორში. პერსონალურ მონაცემთა დაცვის უფლებასთან მიმართებით დაცვის განსაკუთრებული ხარისხი არც სასამართლო პრეცედენტებით არის დადგენილი. საქმეში *United States v. Miller* (#425 U.S. 435, 1976) აშშ-ის უზენაესმა სასამართლომ აღნიშნა, რომ ფინანსური ხასიათის ინფორმაცია, რომელსაც ფლობენ მესამე პირები, არ ექვემდებარება IV შესწორების საფუძველზე დაცვას. მოცემულ საქმეში ფედერალურმა სააგენტომ გამოსცა სავალდებულოდ შესასრულებელი ბრძანებები ბანკების მიმართ ფინანსური ჩანაწერების თაობაზე. მოპასუხის აზრით, მოცემული ბრძანება არ იყო საკმარისი და სააგენტოს ესაჭიროებოდა სასამართლოს ნებართვა ინფორმაციის მოპოვების მიზნით. თუმცა სასამართლოს მოსაზრებით მოპასუხეს არ გააჩნდა პირადი ცხოვრების დაცვის გონივრული მოლოდინი ამ ჩანაწერებთან მიმართებით, რამდენადაც IV შესწორება არ კრძალავს ინფორმაციის მოპოვებას, რომელიც გაცემულია მესამე პირისთვის, ამ უკანასკნელის მხრიდან სახელმწიფო ხელისუფლებისთვის გადაცემის მიზნით.<sup>101</sup> მსგავსი სახის ვიწრო განმარტებები გაკეთდა სხვა სასამართლო საქმეებზეც. საქმეში

99 იქვე, გვ. 22.

100 Supreme Court of the United States, 429 U.S. 589, *Whalen v. Roe*, 1977.

101 Mathews, (ed.), p. 29.

Smith v. Maryland (#422 U.S. 735, 1979) უზენაესმა სასამართლომ განმარტა, რომ IV შესწორება არ ვრცელდებოდა სატელეფონო ნომრების სიაზე, რომელიც აკრიფა პირმა და შემდგომ ჩაინერა რეესტრში. ეს მსჯელობა გამყარებული იყო იმ არგუმენტით, რომ ადამიანებს გაცნობიერებული აქვთ საკუთარი ვალდებულება მიაწოდონ ინფორმაცია სატელეფონო კომპანიას, ხოლო ეს უკანასკნელი აფიქსირებს ამ მონაცემს საგადახდო მიზნებისთვის, შესაბამისად ინდივიდებს ვერ ექნებათ რაიმე მოლოდინი იმისა, რომ მათ მიერ აკრეფილი ნომრები დარჩება საიდუმლო.<sup>102</sup>

IV შესწორებასთან დაკავშირებული ანალიზი სასამართლოს ფარგლებში განხილვის საგანი გახდა საჯარო ინფორმაციის მოპოვებასთან მიმართებით. მაგალითად, ერთ-ერთ საქმეში მსჯელობის საგანს წარმოადგენდა ერთგვარი „კონფლიქტი“ ინფორმაციის გასაჯაროვებასა და IV შესწორებით დაცული პირადი ცხოვრების უფლებას შორის. უზენაესი სასამართლოს აზრით, პოლიეთილენის ჩანთები, რომელიც დატოვებულია ქუჩაში, ხელმისაწვდომია ცხოველებისთვის, ბავშვებისთვის და საზოგადოების სხვა წევრებისთვის, მათ შორის, დასუფთავების სამსახურისთვის ან პოლიციისთვის. ამ გადაწყვეტილებიდან ნათელია, რომ აშშ-ის სასამართლო პრაქტიკა პერსონალურ მონაცემთა დაცვისა და ინფორმაციის საჯაროობას შორის კონფლიქტისას მხარს ამ უკანასკნელს უჭერს. ამ შემთხვევაშიც, მსჯელობის ამოსავალი წერტილი იყო პირადი ცხოვრების დაცვის გონივრული მოლოდინის საკითხი. შესაბამისად, ნებისმიერი ინფორმაცია, მათ შორის, პერსონალური, რომელიც „მდებარეობს,“ „განთავსებულია“ საჯარო სივრცეში ვერ სარგებლობს პირადი ცხოვრების დაცვის უფლებით, განსაკუთრებით იმ შემთხვევებში, თუ ამგვარი გასაჯაროვება მოხდა თავად იმ პირის მიერ ვისაც ეკუთვნის ინფორმაცია.<sup>103</sup>

აქვე, მცირე გადახვევის სახით აღვნიშნავ, რომ ამგვარი მიდგომა არაა უცხო პერსონალურ მონაცემთა დაცვის ევროპული მოდელისთვისაც. მიუხედავად იმისა, რომ მონაცემთა დაცვის ამერიკული და ევროპული მიდგომები რეგულირებისას რადიკალურად განსხვავებულია, არაერთი ევროპული ქვეყნის კანონ-

<sup>102</sup> იქვე, გვ. 31.

<sup>103</sup> Supreme Court of the United States, 486 U.S. 35, *California v. Greenwood*, 1988.

მდებლობა, მათ შორის, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ინფორმაციის გასაჯაროებისას უკანა პლანზე აყენებს პირადი ცხოვრების დაცვის მოლოდინს. მაგალითად, „პირდაპირი მარკეტინგის მიზნებისათვის შეიძლება დამუშავდეს საჯაროდ ხელმისაწვდომი წყაროებიდან მოპოვებული მონაცემები.“<sup>104</sup>

პირადი ცხოვრების დაცულ სფეროზე საუბრისას გარდაუვალია პერსონალურ მონაცემთა დაცვის საკითხებთან შემხებლობა. რიგ შემთხვევებში სასამართლო საქმეები, რომელიც განხილულია პირადი ცხოვრების უფლების დაცვის ჭრილში, ყურადღებას ამახვილებს პერსონალურ მონაცემებზე (მიუხედავად იმისა, სასამართლო უსვამს თუ არა ხაზს პერსონალური მონაცემის დაცვის საკითხს). ამდენად, პერსონალურ მონაცემთა დაცვის საკითხს პირადი ცხოვრების უფლების ანალიზისას განსაკუთრებული მნიშვნელობა ენიჭება და საჭიროებს შესაბამის დაცვას შესაბამის გამონწვევებზე საპასუხოდ.

## თავი II. პერსონალურ მონაცემთა დაცვის უზლეზა

პირადი ცხოვრების უფლების ანალიზის შედეგად გამოიკვეთა, რომ ხშირ შემთხვევაში საქმე გვაქვს პერსონალური მონაცემების დაცვის უფლებასთან. ცნება „პერსონალური მონაცემი,“ ტრადიციულად, წარმოადგენს პირადი ცხოვრების მეტად ვრცელი კონცეფციის ნაწილს.<sup>105</sup> ისტორიულად, პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საკითხები განიხილებოდა პირადი ცხოვრების უფლების დაცვის კონტექსტში, ვინაიდან მათ შორის შინაარსობრივი კავშირი ძალიან მჭიდროა.<sup>106</sup> მიუხედავად ამისა, პერსონალურ მონაცემთა უფლების დაცვის გარანტიები არ უნდა გაიგივდეს პირადი ცხოვრების უფლების დაცვის გარანტიებთან.<sup>107</sup>

არ იქნება გასაკვირი, თუ კიდევ ერთხელ ხაზს გავუსვამთ იმ გარემოებას, რომ თანამედროვე ტექნოლოგიური პროგრესი იწვევს პერსონალური ინფორმაციის გამუდმებულ გამოყენებას, განსაკუთრებით გამოკვეთს და განსხვავებულად არეგულირებს პირადი ცხოვრების უფლების ამ ნაწილს. სამართლებრივ მოწესრიგებაზე აქცენტირებისას, საყურადღებოა ის გარემოებაც, რომ პერსონალურ მონაცემთა დაცვა არამხოლოდ ცალკე საკანონმდებლო აქტით უნდა წესრიგდებოდეს, არამედ მხედველობაში მისაღები ამ უფლების კონსტიტუციური, სახელმწიფოს ძირითადი კანონის დონეზე დამოუკიდებელი დეკლარირების მიზანშეწონილობა. საქართველოს კონსტიტუციით პერსონალურ მონაცემთა დაცვის უფლება მოიაზრება პირადი ცხოვრების დაცვის უფლებაში, მაგრამ ეს საკმარისი არ არის. საქართველოში, პერსონალურ მონაცემთა დაცვის ძირითადი საკითხები სამართლებრივად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით წესრიგდება. პერსონალურ მონაცემთა დაცვის ქართული მოდელი ევროპული ანალოგის მსგავსია, სა-

105 კორკელია, კ. (რედ.), *ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო (სტატიათა კრებული)*, თბილისი, GIZ, 2011, გვ. 329.

106 კორკელია, კ. (რედ.), *ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე (სტატიათა კრებული)*, თბილისი, East-West Management Institute, 2015, გვ. 180.

107 კორკელია, (რედ.), 2011, გვ. 330.

დაც შიდასახელმწიფოებრივი და საერთაშორისო რეგულაციები ითვალისწინებენ ე.წ. „ქოლგის“ ტიპის, ყველა სექტორზე გავრცელებად კანონთა ფუნქციონირებას. სწორედ ამით განსხვავდება პერსონალურ მონაცემთა დაცვის ევროპული და ამერიკული მონესრიგება, სადაც ეს უკანასკნელი არ იცნობს ერთიან აქტს და აღნიშნული სფერო სხვადასხვა სექტორული კანონითაა რეგულირებული.

## 2.1. დაცული სფერო

რა არის პერსონალური მონაცემი? მისი ამომწურავი დეფინიცია ამ სფეროს მომწესრიგებელი ადგილობრივი და საერთაშორისო დოკუმენტებით არ არსებობს. მონაცემი „პერსონალური“ ხდება მაშინ, როდესაც იგი კავშირშია კონკრეტულ პიროვნებასთან, ინდივიდთან და გადმოსცემს რაიმეს მის შესახებ.

პერსონალური მონაცემის ცნებას მჭიდროდ უკავშირდება იდენტიფიცირების საკითხი. მონაცემთა დაცვის ევროპული კანონმდებლობის მიხედვით, მონაცემთა სუბიექტის იდენტიფიცირება მაღალი სიზუსტით აუცილებელი არაა. კანონის ნორმათა ამოქმედებისთვის საკმარისია პიროვნება იყოს იდენტიფიცირებადი, ხოლო ინდივიდის ვინაობის დადგენა შეიძლება მაშინ თუ ინფორმაცია შეიცავს პირის იდენტიფიცირების დამდგენ ელემენტებს.<sup>108</sup>

პერსონალურ მონაცემთა ცნება, საერთაშორისო სამართლებრივი რეგულირებით, პირველად გაიწერა ევროპის საბჭოს ფარგლებში, კერძოდ, „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციით.<sup>109</sup> დოკუმენტის თანახმად პერსონალური მონაცემი „აღნიშნავს ნებისმიერ ინფორმაციას, რომელიც შეეხება განსაზღვრულ ან განმსაზღვრელ პირს („ინფორმაციის სუბიექტს“).“<sup>110</sup> როგორც ვხედავთ კონვენციით პერსონალური მონაცემის განვრცობითი დეფინიცია არ არის მოცემული.

108 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 102-103.

109 აღნიშნულ კონვენციას, ასევე, მოიხსენიებენ, როგორც ევროპის საბჭოს 108-ე კონვენციას.

110 შ. 2, პ. „ა“.

მოგვიანებით, ევროპული კავშირის ფარგლებში დამკვიდრდა პერსონალური მონაცემის მეტად ფართო განმარტება, რომელიც მოცემული იყო ევროპული კავშირის 95/46/EC დირექტივით.<sup>111</sup> მის თანახმად, პერსონალური მონაცემის განმარტება შემდეგი სახით იყო მოცემული: „ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (მონაცემთა სუბიექტი); ინდივიდი იდენტიფიცირებადია, რომლის ვინაობის დადგენა შესაძლებელია პირდაპირ ან არაპირდაპირ, მათ შორის, საიდენტიფიკაციო ნომრით ან ერთდ ან მეტი ნიშნით, რომელიც ეხება მის ფიზიკურ, ფსიქოლოგიურ, მენტალურ, ეკონომიკურ, კულტურულ ან სოციალურ მახასიათებელს.“<sup>112</sup> ამავე დირექტივის პრეამბულის 26-ე ნაწილი კი ახდენდა ამ დეფინიციის შინაარსობრივ დაზუსტებას. მის თანახმად, „დაცვის პრინციპები უნდა გავრცელდეს ნებისმიერ ინფორმაციაზე, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ინდივიდს; იდენტიფიცირების განსაზღვრისთვის გასათვალისწინებელია ყველა ის საშუალება, რომელიც გონივრულობის ფარგლებში გამოიყენება დამმუშავებლის ან ნებისმიერი სხვა პირის მიერ ვინაობის დადგენისთვის; დაცვის პრინციპები არ გავრცელდება ანონიმურ მონაცემებზე, რომლის თანახმად მონაცემთა სუბიექტის იდენტიფიცირება ვერ ხდება; [...]“<sup>113</sup>

მას შემდეგ, რაც ევროპული კავშირის ფარგლებში ძალაში შევიდა მონაცემთა დაცვის ძირითადი რეგულაცია (2018 წლის 25 მაისი, რის შემდეგაც დირექტივა ძალადაკარგულად გამოცხადდა),<sup>114</sup> პერსონალურ მონაცემთა დეფინიციამ

111 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

112 იქვე, მ. 2, პ. „ა.“

113 Recital 10.

114 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). ზოგიერთ წყაროში, რეგულაციის სახელწოდების თარგმნისას, სიტყვა „ძირითადი“-ს ქართულენოვანი შესატყვისის სახით შესაძლებელია შეგვხვდეს სიტყვა „ზოგადი.“ მიუხედავად იმისა, რომ სიტყვა „general“ გრამატიკულად მეტად გამართლებულია,

გარკვეული ცვლილებები განიცადა და იგი შემდეგი სახითაა შემოთავაზებული: „პერსონალური მონაცემი ნიშნავს ნებისმიერ ინფორმაციას, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს („მონაცემთა სუბიექტი“); პირი იდენტიფიცირებადია თუ მისი ვინაობის დადგენა შეიძლება პირდაპირ ან არაპირდაპირ, კერძოდ, ისეთი იდენტიფიკატორებით, როგორიცაა სახელი, საიდენტიფიკაციო ნომერი, ადგილმდებარეობის მონაცემი, ონალინ იდენტიფიკატორი ან ერთი ან მეტი ფაქტორით, რომელიც უკავშირდება ფიზიკურ, ფიზიოლოგიურ, გენეტიკურ, ფსიქოლოგიურ, ეკონომიკურ, კულტურულ ან ფიზიკური პირის სოციალურ კუთვნილებას.“<sup>115</sup>

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი იზიარებს მონაცემთა დაცვის ევროპულ მოდელს, შესაბამისად, საკვანძო განმარტებები, პრინციპები და წესები მოცემულია ევროპული დოკუმენტების ანალოგიურად. კანონის თანახმად პერსონალური მონაცემია „ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.“<sup>116</sup> ამ განმარტებით დადგენილია, რომ პერსონალური მონაცემი ეხება ადამიანის პირადი ცხოვრების ინფორმაციულ ასპექტს, სხვა სიტყვებით, მის შესახებ არსებულ ნებისმიერ ინფორმაციას. ამდენად, პერსონალურია მონაცემი მაშინ, როდესაც იგი, სულ მცირე, იძლევა პი-

---

ითარგმნოს, როგორც სიტყვად „ზოგადი,“ მიმაჩნია, რომ ეს უკანასკნელი ვერ გამოხატავს რეგულაციის ქეშმარიტ ფუნქციასა და შინაარსს. რეგულაციაში მოცემულია საკმაოდ დეტალური წესები, რომელიც ეხება მონაცემთა დაცვასა და დამუშავებას, ამდენად იგი, თავისი შინაარსით, ვერ იქნება „ზოგადი.“ დამატებით, მისი მოქმედების სამართლებრივი ძალა და გავრცელების აერალი მოიცავს ევროპულ კავშირსა და ევროპულ ეკონომიკურ ზონაში შემავალ სახელმწიფოებს, ამდენად უმჯობესია გამოვიყენოთ სიტყვა „ძირითადი“ (ან „საერთო“), რომელიც, ასევე, თავსებადია ინგლისურენოვან შესატყვისთან.

115 იქვე, მ. 4, პ. 1.

116 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „ა.“

რის სხვებისგან გამორჩევის საშუალებას.<sup>117</sup> იმ განმასხვავებელი ნიშნების ჩამონათვალი, რის მიხედვითაც შესაძლებელია პირის გამორჩევა, ამოუნურავია. აქედან გამომდინარე, ნებისმიერი ინფორმაცია, მაგალითად ის, რომ კონკრეტული (იდენტიფიცირებული) ინდივიდი ფლობს ხუთ უცხო ენას, შესაძლებელია ჩაითვალოს პერსონალურ მონაცემად.

უნდა აღინიშნოს, რომ საქართველოს სასამართლოთა პრაქტიკაში გაზიარებულია პერსონალურ მონაცემთა განმარტების საყოველთაოდ აღიარებული მიდგომა. მაგალითად, თბილისის სააპელაციო სასამართლო მიუთითებს, რომ „პერსონალური მონაცემების დაცვის კანონმდებლობისათვის დამახასიათებელია მისი აგება იდენტიფიკაციის კრიტერიუმზე, რომლის თანახმად, პერსონალური მონაცემები იმთავითვე დახურულია, თუ კანონით სხვა რამ არ არის დადგენილი ან თუ პირი თავად არ ახდენს მონაცემის გახმაურებას. [...] პერსონალური მონაცემი არის პირადი ცხოვრების დაცვის ერთ-ერთი საშუალება, პერსონალური მონაცემის დაცვაში საბოლოოდ პრიორიტეტი ენიჭება არა მგრძნობიარობის, არამედ იდენტიფიკაციის კრიტერიუმს [...]“<sup>118</sup>

როგორც ვხედავთ, პერსონალურ მონაცემთა დაცვის ქართული მოდელი ევროპულ ანალოგზეა აგებული. ამას ადასტურებს ისიც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ამა თუ იმ ნორმის ფორმულირებისას, წყაროდ იყენებს ევროპული კავშირის 95/46/EC დირექტივას. ამ ორ დოკუმენტში მოცემული ნორმები, საკვანძო წესების დადგენის ნაწილში, მსგავსადაა განერილი.

ევროპული კავშირის საკონსულტაციო ორგანოს (WP 29)<sup>119</sup> დე-

117 Article 29 Data Protection Working Party (WP 29), *Opinion 4/2007 on the Concept of Personal Data*, 2007, p. 12 [[http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)].

118 თბილისის სააპელაციო სასამართლო, საქმე 33/1059-15, ნ.გ. და ა.კ., ო.ს. და ი.ბ.-ს წინააღმდეგ, 26.04.2016.

119 საყურადღებოა, რომ „მონაცემთა დაცვის საერთო რეგულაციის“ ამოქმედების შემდეგ (25.05.2018) მონაცემთა დაცვის სამუშაო ჯგუფმა (Article 29 Data Protection Working Party) შენიჭა ფუნქციონირება და მის უფლებამოსაცვლეს მონაცემთა დაცვის ევროპული ბორდი (European Data Protection Board) წარმოადგენს. მიუხედავად ამისა, სამუშაო ჯგუფს, არსებობის მანძილზე, გამოცემული აქვს არაერთი საკვანძო რეკომენდაცია, მოსაზრება

ტალურად და შესაბამისი შემადგენელი ელემენტების მიხედვით განიხილავს პერსონალური მონაცემის ცნებას:

1. „ნებისმიერი ინფორმაცია“ - იგი მოიცავს ნებისმიერი სახის ინფორმაციას პირის შესახებ, რომელიც რიგ შემთხვევაში წარმოადგენს ობიექტურად ცნობილ გარემოებას, მაგალითად, კონკრეტული პირის სისხლის ნიმუშის შემადგენლობა, ასევე, სუბიექტური შეხედულებები და მოსაზრებები;<sup>120</sup>
2. „რომელიც უკავშირდება“ - სხვა სიტყვებით, იგი უნდა იყოს ინდივიდის შესახებ. კავშირის დადგენა, რიგ შემთხვევაში, მარტივადაა შესაძლებელი, მაგალითად, მონაცემები დასაქმებული პირის შესახებ, რომელიც მოცემულია ორგანიზაციის საქალაქო წარმომადგენს მის შესახებ არსებულ ინფორმაციას. ამავე ლოგიკით, სამედიცინო ანალიზის შედეგად გამოვლენილი ინფორმაციაც პირთან დაკავშირებულ მონაცემს წარმოადგენს და ა.შ.;<sup>121</sup>
3. „იდენტიფიცირებული ან იდენტიფიცირებადი“ - ამ შემთხვევაში გადამწვეტია ის თუ, რამდენად არის პიროვნება სხვებისგან გამორჩეული ან რამდენად არის მისი გამორჩევა შესაძლებელი. იდენტიფიცირება (გამორჩევა) სხვადასხვა ინფორმაციაზე დაყრდნობითაა შესაძლებელი, როგორიცაა სიმაღლე, თმის ფერი, პროფესია, სახელი. აქვე, ერთმანეთისგან უნდა განვასხვავოთ პირდაპირი და არაპირდაპირი იდენტიფიცირების სახეები. ხშირ შემთხვევაში პირის სახელი და გვარი გამოიყენება, როგორც ყველაზე ტრადიციული იდენტიფიკატორი, ხოლო ისეთი ინფორმაციის დამატება, როგორიცაა სიმაღლე, სოციალური სტატუსი ან ასაკი, გვაძლევს პირის პირდაპირი იდენტიფიცირების საშუალებას მაღალი სიზუსტით. არაპირდაპირი იდენტიფიცირების შემთხვევაში კონკრეტული მონაცემის არსებობა საკმარისი აღარ არის, რის

---

თუ სხვა, რის გამოც მათ დიდი წვლილი შეიტანეს პერსონალურ მონაცემთა დაცვის სფეროს განვითარებაში. ამდენად, მათ მიერ საკვანძო საკითხების შესახებ გამოქვეყნებული პუბლიკაციები არ კარგავს აქტუალობას.

120 Article 29 Data Protection Working Party (WP 29), 2007. p. 6.

121 იქვე, გვ. 9.

გამოც ხდება დამატებითი, მცირე ან ვრცელი ინფორმაციის მოპოვება (მაგ. ფიზიკური, მენტალური, ეკონომიკური მდგომარეობის შესახებ), რათა მოხდეს პიროვნების გამორჩევა სხვებისგან;<sup>122</sup>

4. „ფიზიკური პირი“ - მონაცემთა დაცვის სამართალში, ამ უფლებით მოსარგებლე პირი, ძირითადად, მხოლოდ ფიზიკური პირია.<sup>123</sup>

ამ ოთხი ელემენტის გათვალისწინებით ნათელია თუ რა ტიპის ინფორმაცია შეგვიძლია მივიჩნიოთ პერსონალურად, მაგრამ, საინტერესოა, როგორ ნესრიგდება საკითხი მაშინ, როცა სახეზეა ინფორმაცია, თუმცა, ერთი შეხედვით, მისი მეშვეობით ვერ მოვახდენთ პირის იდენტიფიცირებას. ამ სახის ინფორმაციას განეკუთვნება პერსონალური მონაცემები, რომელიც გამოიყენება მარკეტინგული მიზნებისთვის. მიუხედავად იმისა, რომ, მაგალითად, მხოლოდ ტელეფონის ნომრით ვერ მოხერხდება პირის იდენტიფიცირება (სულ მცირე სანყის ეტაპზე), ამ სახის ინფორმაციის გამოყენება მაინც არის რეგულირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართვევის კანონით. რაში მდგომარეობს ამ მიდგომის თავისებურება? საკითხი ამ სახით მხოლოდ ქართული კანონმდებლობით არაა მოწესრიგებული. პირდაპირი მარკეტინგის შესახებ პრაქტიკული სახელმწიფოს კანონი აკეთებს აქცენტს და აწესრიგებს ამ საკითხს შესაბამისი ვალდებულებების თანხლებით. არც საქართველოს კანონმდებლობაა გამონაკლისი. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად პირდაპირი მარკეტინგი განიმარტება, როგორც „ფოსტის, სატელეფონო ზარების, ელექტრონული ფოსტის ან სხვა სატელეკომუნიკაციო საშუალებით საქონლის, მომსახურების, დასაქმების ან დროებითი სამუშაოს შეთავაზება.“<sup>124</sup> ნორმის შინაარსიდან გამომდინარე ცხადია, რომ მთავარი აქცენტი თუ რატომაც არის მარკეტინგული შეტყობინებები რეგულირებული კანონით, არის პირთან უშუალო კავშირის დამყარების შესაძლებლობა. პირდაპირი

122 იქვე, გვ. 12-13.

123 იქვე, გვ. 21-22.

124 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „უ.“

მარკეტინგი ის საშუალებაა, რომლითაც შესაძლებელია პირთან განხორციელდეს სარეკლამო სახის შეთავაზება უშუალოდ, რის შემდეგაც პირი იდენტიფიცირებაუნარიანი ხდება. ამდენად, ის ფაქტი, რომ სუბიექტთან მოხდა უშუალო კავშირზე გასვლა საკმარისია, რათა ამ ტიპის ურთიერთობები მოწესრიგდეს პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონით. აქედან გამომდინარე, იდენტიფიცირების ელემენტთან ერთად, კანონმდებლისთვის საყურადღებოა პირთან უშუალო კონტაქტის არსებობის საკითხიც.

საინტერესოა თუ რამდენად დაიყვანება სუბიექტის იდენტიფიცირების შესაძლებლობა მხოლოდ ისეთ კლასიკურ იდენტიფიკატორებზე, როგორიცაა სახელი, გვარი, პირადი ნომერი, დაბადების თარიღი და ა.შ.? თანამედროვე ტექნოლოგიები მრავალფეროვანი ინფორმაციის დამუშავების საშუალებას იძლევა უნიკალური კოდის, სპეციალური მაიდენტიფიცირებელი ნიშნის, ასევე, ინტერნეტში, ვებ-გვერდების დათვალიერებისას ფორმირებული ფაილების (cookies) გამოყენებით. ამრიგად, ელექტრონულ სივრცეში იდენტიფიკატორთა სახეობა განსხვავებულია. მაგალითად, პერსონალური კომპიუტერიდან განხორციელებული ინტერნეტ-საძიებო სისტემის ისტორია (browsing history) ებმის ამ კომპიუტერზე ინტერნეტით სარგებლობისთვის მინიჭებულ უნიკალურ IP (ინტერნეტ პროტოკოლი) მისამართს. ვებ-გვერდს, რომელზეც სუბიექტის მხრიდან ფიქსირდება ვიზიტები, შეუძლია დაიმახსოვროს მოცემულ IP მისამართი და თანმდევი cookies, რაც გენერირდება გვერდზე განხორციელებული აქტივობის შედეგად. მაგალითისთვის, თუ სუბიექტი ხშირად ეწვევა ონლაინ-მაღაზიას და იძენს ერთმანეთის მსგავს პროდუქციას, ეს აქტივობა ებმის პირის IP მისამართს და შემდგომი ვიზიტისას პირს ავტომატურ რეჟიმში სთავაზობს მისთვის საინტერესო პროდუქციას. ეს ყოველივე იმ უნიკალური მისამართის მიხედვით, რომელიც ენიჭება თითოეულ მომხმარებელს, რასაც თან ემატება ვებ-გვერდზე განხორციელებული აქტივობის ჩანაწერები; ამრიგად, თანამედროვე სამყაროში, სადაც განვითარებულია ციფრული ტექნოლოგიები, IP მისამართი, როგორც იდენტიფიცირების საშუალება, დიდ მნიშვნელობას იძენს. შესაბამისად, არ იქნება გადამეტებული თუ ვიტყვით, რომ ამ კონტე-

ქსტში იდენტიფიცირების მეთოდები მომხმარებლის IP მისამართის მისახვა პერსონალურ მონაცემებთან (რომელიც საჯარო ან არა) დაკავშირების გზით მრავალფეროვანია, განსაკუთრებით მაშინ, თუ დამუშავების საშუალებებად გამოყენებულია cookies.<sup>125</sup> ამდენად, თანამედროვე პირობებში იდენტიფიცირების არსსა, უფრო მეტად წარმოადგენს ის, რომ მოხდეს პირის მაიდენტიფიცირებელი მონაცემების სხვა უკვე არსებულ ინფორმაციასთან დაკავშირება, ვიდრე მხოლოდ პიროვნების ვინაობის დადგენა.<sup>126</sup>

როგორც ჩანს, პერსონალური მონაცემი, ან როგორც მას ზოგჯერ უწოდებენ - პერსონალურად მაიდენტიფიცირებელი ინფორმაცია - *PII*,<sup>127</sup> სხვადასხვა სახის მონაცემებს მოიცავს. ამავდროულად, პირის შესახებ არსებული მონაცემი ზოგ შემთხვევაში შეიძლება არ იყოს მისთვის დიდი მნიშვნელობის მქონე, ხოლო სხვა შემთხვევაში - მას არ სურდეს ამა თუ იმ ინფორმაციის ვინმესთვის გაზიარება. ამდენად, ცნება „პერსონალური მონაცემი“ მოიცავს ინფორმაციას, რომელიც ეხება ინდივიდის პირად და ოჯახურ ცხოვრებას და, ასევე, მათ, რომელიც უკავშირდება ინდივიდის ჩვეულ აქტივობებს ფიზიკურ და ციფრულ სივრცეში.<sup>128</sup>

ასეთი ვითარების გამო, პერსონალურ მონაცემთა დაცვის სამართალში საყოველთაოდ აღიარებულია მათი დაყოფა კატეგორიების მიხედვით. როგორც წესი, სამართლებრივ აქტებში მოცემულია მხოლოდ განსაკუთრებული (სენსიტიური) კატეგორიის პერსონალურ მონაცემთა ჩამონათვალი, ხოლო დანარჩენი ინფორმაცია, რაც ამ ჩამონათვალის მიღმა რჩება, მიიჩნევა ე.წ. „ჩვეულებრივი“ კატეგორიის პერსონალურ მონაცემებად, რისი ნუსხაც ამომწურავი, რა თქმა უნდა, ვერ იქნება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად განსაკუთრებული კატეგორიისა „მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან,

125 Article 29 Data Protection Working Party (WP 29), 2007, p. 17.

126 Supreme Court of the United States, 542, U.S. 177, *Hiibel v. Sixth Judicial District Court of Nevada*, 2004.

127 University of California - Santa Cruz, *Personal Identity Information*, 2015 [<https://its.ucsc.edu/security/pii.html>].

128 Article 29 Data Protection Working Party (WP 29), 2007, pp. 6-7.

პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში განევრიანებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის ალკეეთის 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.<sup>129</sup> ჩამონათვალი მკაფიოდ ფორმულირებულია. გარდა პერსონალური მონაცემების კატეგორიების მიხედვით დაყოფისა, კანონმდებლობით განსხვავებულადაა რეგულირებული სენსიტიური და ე.წ. „ჩვეულებრივი“ პერსონალური მონაცემების დამუშავების წესი. სენსიტიური პერსონალური მონაცემის დამუშავება მეტად მკაცრ წინაპირობებს ექვემდებარება.<sup>130</sup>

ამასთან, დადებით მხარეს წარმოადგენს ისიც, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით ცალკეა მოხსენიებული და განმარტებული ბიომეტრიული და გენეტიკური მონაცემები,<sup>131</sup> რაც განსაკუთრებული კატეგორიის პერსონალური მონაცემების ჭრილში ზრდის სუბიექტის უფლების დაცვის გარანტიებს. იდენტიფიცირების საკითხი, მაგალითად, ყველაზე დიდი სიხშირით, მათ შორის, ვლინდება ისეთ მონაცემებთან მიმართებით როგორიცაა ბიომეტრიული პერსონალური მონაცემი, კერძოდ, თითის ანაბეჭდი. თუმცა, უნდა გავითვალისწინოთ ისიც, რომ თუ ფიზიკური პირი გარკვეულ ნივთთან შეხების შემთხვევაში დატოვებს თითის ანაბეჭდს და სხვა პირი მოინდომებს მის მოპოვებას შესაბამისი საშუალებებით, ისე რომ არ იცოდეს თუ ვინ დატოვა კვალი, ეს არ ნიშნავს იმას, რომ აუცილებლად საქმე გვაქვს პერსონალურ მონაცემთან. თუ სხვა პირი ფლობს პერსონალურ მონაცემთა ბაზას, სადაც შედარების საფუძველზე არსებობს ბიომეტრიული მონაცემის

129 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „გ.“

130 თვალსაჩინოებისთვის ერთმანეთს შეად. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მ. 5 და მ. 6.

131 იქვე, მ. 2, პ. „გ“ და „გ1“.

მფლობელი პირის ვინაობის დადგენის შესაძლებლობა, მაშინ ეს ინფორმაცია ჩაითვლება პერსონალური მონაცემად, ვინაიდან სახეზეა იდენტიფიცირების კრიტერიუმი. ამის მსგავსად, თუ, მაგალითად, პირადი მობილური ტელეფონით სარგებლობისას შექმნილი გვაქვს შესაბამისი ანგარიში (Google Account ან Apple ID) და უსაფრთხოების უზრუნველსაყოფად ვიყენებთ თითის ანაბეჭდით ტელეფონის განბლოკვის შესაძლებლობას, მაშინ საქმე აუცილებლად პერსონალურ მონაცემებთან გვაქვს, რამდენადაც სერვისის მომწოდებლის (Google ან Apple) ხელში თავს იყრის სხვა მაიდენტიფიცირებელი ინფორმაცია (სახელი, გვარი, ელ-ფოსტის მისამართი და სხვ.).

გარდა ბიომეტრიული პერსონალური მონაცემისა საყურადღებოა გენეტიკური მონაცემის ცნება და მისი ინტერპრეტირების გზები. კანონის თანახმად გენეტიკური მონაცემი არის: „მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემი გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება;“<sup>132</sup> მოცემული დეფინიცია თანხვედრაშია ევროპის საბჭოს მინისტრთა კომიტეტის მიერ მიღებულ რეკომენდაციასთან ნევრ ქვეყნებში სამედიცინო მონაცემების დაცვის შესახებ.<sup>133</sup> გენეტიკური მონაცემის განმარტების თანახმად ასეთად მიიჩნევა ნებისმიერი მონაცემი, რომელიც ეხება ინივიდის მემკვიდრეობასთან დაკავშირებულ მახასიათებლებს ან ამგვარი მახასიათებლების ნაწილს ინდივიდთა მოცემულ გაერთიანებაში. არის მოსაზრება, რომ ეს რეკომენდაცია უნდა აღვიქვათ, როგორც პერსონალური გენეტიკური მონაცემის განმარტების გაფართოების მცდელობა. მეორე მხრივ, ევროპული კავშირის 95/46/EC დირექტივა არ შეიცავდა დამატებით მითითებას სამედიცინო მონაცემების განმარტების შესახებ, რის გამოც მისი ერთიანი დეფინიცია სამართლებრივი ნორმით არ იყო დადგენილი.<sup>134</sup> აღნიშნული ნაკლოვანება გამოსწორებულია მონაცემთა დაცვის ძირითადი

<sup>132</sup> „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „გ“.

<sup>133</sup> Council of Europe, *Recommendation No. R (97) 5 on the Protection of Medical Data*, 1997.

<sup>134</sup> Gertz, R., *Is it 'Me' or 'We'? Genetic relations and the Meaning of 'Personal Data' under the Data Protection Directive*, European Journal of Health Law, Martinus Nijhoff Publishers, 2004, p. 236.

რეგულაციის ფორმულირებით. დოკუმენტის პრეამბულაში ვკითხულობთ, რომ „გენეტიკური მონაცემი უნდა იქნეს მიჩნეული, როგორც პერსონალურ ინფორმაციად, რომელიც უკავშირდება ფიზიკური პირის მემკვიდრეობით გადაცემულ ან მიღებულ გენეტიკურ მახასიათებლებს, რაც დგინდება მოცემული ფიზიკური პირის ბიოლოგიური ნიმუშის ანალიზის შედეგად, კერძოდ, დეზოქსირიბონუკლეინის მუჟავის (დნმ) ან რიბონუკლეინის (რნმ) ანალიზით, ან სხვა ელემენტის ანალიზით, რომელიც ქმნის ექვივალენტური ინფორმაციის მოპოვების საშუალებას.“<sup>135</sup>

მიზანშეწონილია, ასევე, განვიხილოთ თუ ვინ შეიძლება იყოს პერსონალურ მონაცემთა დაცვის უფლებით მოსარგებლე სუბიექტი, სხვა სიტყვებით, ვის შეიძლება ეკუთვნოდეს პერსონალური მონაცემები. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად მონაცემთა სუბიექტია „ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემებიც მუშავდება.“<sup>136</sup> კანონის გავრცელების ფარგლები არ შემოისაზღვრება ისეთი ნიშნით, როგორიცაა მოქალაქეობა და ამიტომ სუბიექტად გვევლინება ნებისმიერი ფიზიკური პირი, რომელიც საქართველოს ტერიტორიაზე იმყოფება ან თუ კონკრეტულ ტერიტორიაზე ვრცელდება საქართველოს იურისდიქცია და ხდება მის შესახებ არსებული ინფორმაციის დამუშავება.<sup>137</sup> აქვე აღსანიშნავია, რომ ფიზიკური პირი მონაცემთა სუბიექტია მხოლოდ მაშინ, თუ მუშავდება მისი პერსონალური მონაცემი, ხოლო კანონით პერსონალურ მონაცემთა დამუშავება არის „ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება, კერძოდ, შეგროვება, ჩანერა, ფოტოზე აღბეჭდვა, აუდიოჩანერა, ვიდეოჩანერა, ორგანიზება, შენახვა, შეცვლა, აღდგენა, გამოთხოვა ან გამჟღავნება მონაცემთა გადაცემის, გავრცელების ან სხვაგვარად ხელმისაწვდომად გახდომის გზით, დაჯგუფება ან კომბინაცია, დაბლოკვა, ნაშლა ან

135 GDPR, Recital 34.

136 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „ვ.“

137 ამავე კანონის თანახმად, კანონის მოქმედება ვრცელდება საზღვარგარეთ საქართველოს დიპლომატიური წარმომადგენლობებისა და საკონსულო დაწესებულებების მიერ მონაცემთა დამუშავებაზე“ (მ. 3, პ. 2(ა)).

განადგურება.<sup>138</sup>

აქვე განვმარტოთ, არის თუ არა პერსონალურ მონაცემთა სუბიექტი მარტოოდენ ფიზიკური პირი. პერსონალურ მონაცემთა დაცვის მარეგულირებელი ძირითადი საერთაშორისო სამართლებრივი ინსტრუმენტები,<sup>139</sup> ასევე, რიგი სახელმწიფოების კანონმდებლობები, მათ შორის, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ მონაცემთა სუბიექტად მოიხსენიებს მხოლოდ ფიზიკურ პირს. თუმცა, არც პერსონალურ მონაცემთა დაცვის ძირითადი რეგულაციით და არც ევროპის საბჭოს 108-ე კონვენციით არ არის აკრძალული სუბიექტის უფლებების განვრცობა იურიდიულ პირებზე, მაგალითად, მაშინ, როდესაც იურიდიული პირის სახელწოდებით ხდება ფიზიკური პირის იდენტიფიცირება. შესაბამისად, ზოგიერთ შემთხვევაში იურიდიულ პირებზე პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობა ირიბი გზით მაინც შესაძლოა გავრცელდეს.<sup>140</sup>

სხვა საკვანძო ტერმინებიდან, უნდა აღინიშნოს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ცნებები. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად ისინი დამმუშავების პროცესის მთავარ მოქმედ პირებად გვევლინებიან. დამმუშავების კანონიერებასა და მთელი პროცესის მართვაზე, ძირითადად, პასუხისმგებელია პერსონალურ მონაცემთა დამმუშავებელი; კერძოდ, „[...] საჯარო დაწესებულება, ფიზიკური ან იურიდიული პირი, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამმუშავების მიზნებსა და საშუალებებს, უშუალოდ ან უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამმუშავებას,<sup>141</sup> ხოლო კანონის თანახმად უფლებამოსილი პირი გვევლინება დამმუშავებლის ერთგვარ დამხმარედ, რომელიც კანონით შემდეგი სახით განიმარტება „[...] ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც დამმუშავებს მონაცემებს მონაცემთა დამმუშავებლისთვის ან მისი სახელით.“<sup>142</sup> ამ

138 იქვე, მ. 2, პ. „დ.“

139 CoE Convention 108; EU GDPR.

140 Article 29 Data Protection Working Party (WP 29), 2007, p. 23.

141 მ. 2 პ. „ი.“

142 იქვე, პ. „კ.“

ორ პირს შორის ურთიერთობისას, უფლებამოსილი პირი ყოველთვის დამმუშავებლისადმი დაქვემდებარებულად გვევლინება, რამდენადაც მას დამუშავების დამოუკიდებელი მიზანი არ გააჩნია.<sup>143</sup> მიუხედავად ამისა, დაქვემდებარების საკითხი არ უნდა იქნეს გაგებული ისე, თითქოს დამმუშავებლის მხრიდან პერსონალურ მონაცემთა დაცვის წესების დარღვევაზე რეაგირება ღიად ტოვებს საკითხს უფლებამოსილი პირის პასუხისმგებლობის თაობაზე. შესაძლებელია უფლებამოსილი პირის მონაწილეობით პერსონალურ მონაცემთა დამუშავება ნარიმართოს ისე, რომ ეს უკანასკნელი პროცესში საკმაოდ დამოუკიდებლობით სარგებლობდეს. მაგალითად, როდესაც პერსონალურ მონაცემთა დამმუშავებლად გვევლინება უნივერსიტეტი, რომელიც საკუთარი სტუდენტების პერსონალური მონაცემების დამუშავებას (შეფასებას, დაგროვებული კრედიტების რაოდენობის აღრიცხვას, მათ მიერ დაწერილი განცხადებების ადრესატამდე გაგზავნას და სხვ.) უზრუნველყოფს დამოუკიდებელი კომპანიის მეშვეობით (ამგვარი პრაქტიკა საქართველოს უმაღლესი საგანმანათლებლო დაწესებულებების მიერ ფართოდაა აპრობირებული). ამ შემთხვევაში უფლებამოსილი პირი უნდა მოქმედებდეს დამმუშავებლის მიერ მინიჭებული მანდატის ფარგლებში და, მაგალითად, დაიცვას პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით დადგენილი უსაფრთხოების ტექნიკური და ორგანიზაციული ზომები, მათ შორის, კონფიდენციალურობა.<sup>144</sup>

პერსონალურ მონაცემთა დაცვის სფეროში დამკვიდრებული

143 გასათვალისწინებელია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დამკვიდრებული ტერმინი „უფლებამოსილი პირი“ არ უნდა იქნეს გაგებული სიტყვა „უფლებამოსილების“ ტრადიციული და ზოგადი მნიშვნელობით. მონაცემთა დაცვის სამართალში პირი „უფლებამოსილად“, გარდა კანონით დადგენილი პირობებისა, ჩაითვლება მაშინ, როდესაც იგი ორგანიზაციულად ან საქმიანობის შინაარსიდან გამომდინარე დისტანცირებულია დამმუშავებლისგან, ან მისი მხრიდან დამმუშავებლისთვის განეული საქმიანობა ერთჯერადი ხასიათისაა. ასევე, შესაძლო გაუგებრობის თავიდან აცილების მიზნით, აქვე ავლნიშნავ, რომ მაგალითად, ინგლისურენოვან წყაროებში „დამმუშავებელი“ მოხსენიებულია, როგორც „controller“ (მაკონტროლებელი), ხოლო „უფლებამოსილი პირი“ – „processor“ (დამმუშავებელი).

144 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, პ. 17, განსაკუთრებით პ. 4.

ლი საკვანძო ტერმინების განხილვის შემდეგად, ნათელია რომ ამ სფეროში მოცემული ცნებები, ინფორმაციის კატეგორიები, დამუშავების პროცესის მონაწილე პირები ერთიანობაში ინვესტს სამართლებრივი ურთიერთობების განსაკუთრებული მოწესრიგების აუცილებლობას შესაბამისი, სპეციალური, ნორმებით. ამ სფეროში სპეციალური კანონმდებლობის მიღება ადასტურებს იმ ფაქტს, რომ პერსონალურ მონაცემთა დაცვა განსაკუთრებულ ადგილს იკავებს ადამიანის ძირითად უფლებათა სისტემაში.

## **2.2. პერსონალურ მონაცემთა დაცვის მარეგულირებელი ძირითადი საერთაშორისო და შიდასახელმწიფოებრივი ინსტრუმენტები**

XX საუკუნის II ნახევრის შემდეგ, ტექნოლოგიური პროგრესის განვითარების პარალელურად, იზრდება პერსონალურ მონაცემთა გამოყენების შემთხვევები, რაც შედეგად ინვესტს მისი დაცვის ხარისხის გაზრდის აუცილებლობას. ითვლება, რომ გერმანიამ, საფრანგეთმა და შვედეთმა ევროპის ფარგლებში პირველებმა მიიღეს საკანონმდებლო აქტები, რომელიც ეხებოდა ინდივიდების შესახებ არსებული ინფორმაციის დაცვას. ეს აქტები პირველი თაობის მარეგულირებელ მექანიზმებად მიიჩნევა, მათი შემუშავება 1970-იან წლებში დაიწყო და დასრულდა 1981 წელს ევროპის საბჭოს 108-ე კონვენციის მიღებით.<sup>145</sup> მეცნიერებისა და ტექნოლოგიების განვითარების შედეგად შესაძლებელი გახდა პერსონალური მონაცემების ავტომატური დამუშავება, რაც გულისხმობს, მაგალითად, მათ გამარტივებულ ხელმისაწვდომობას, მონაცემთა ბანკების წარმოებას კერძო და საჯარო სექტორის მხრიდან.<sup>146</sup>

უშუალოდ პერსონალურ მონაცემთა დაცვაზე ორიენტირებული პირველი სამართლებრივი ინსტრუმენტი, 1970 წელს გერმანიის ფედერალურ ერთეულში - ჰესეში მიიღეს. მიზანი იყო საჯარო დაწესებულებებში ციფრული მასალის დაცვა საჯარო მოხელეების მხრიდან გამჟღავნების, უნებართვოდ გამოყენების, შეცვლის ან წაშლისგან, თუმცა იგი არ ეხებოდა პერსონა-

145 Fuster, G.G., *The Emergence of Personal Data Protection as a Fundamental Right of The EU*. Springer, 2014, p. 56.

146 კორკელია, (რედ.), 2015, გვ. 182.

ლურ მონაცემთა დაცვის ისეთ საკითხებს, როგორიცაა მათი მოპოვება და შენახვა. მიუხედავად ამისა, თუ პერსონალური მონაცემი ოფიციალური დოკუმენტის ნაწილი ხდებოდა, ის უნდა ყოფილიყო სწორი, წინააღმდეგ შემთხვევაში სუბიექტს ჰქონდა მისი შეცვლის მოთხოვნის უფლება. კანონის მთავარ მიღწევად ითვლებოდა დამოუკიდებელი პირის - პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშნვა, იგი პასუხისმგებელი იყო მოქალაქეთა პერსონალური მონაცემების კონფიდენციალურობის კონტროლზე. გერმანიაში ფედერალურ დონეზე, პირველი მსგავსი შინაარსის შემცველი კანონი 1977 წელს მიიღეს, შვედეთში - 1973 წელს, საფრანგეთში კი - 1978 წელს.<sup>147</sup>

საერთაშორისო დონეზე პერსონალურ მონაცემთა მიმართ ყურადღების გამოხატულების მაგალითია ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის (OECD) მიერ 1980 წელს შემუშავებული პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა საერთაშორისო გადაცემის თაობაზე მიღებული სარეკომენდაციო დებულებები.<sup>148</sup> მის უპირატეს მხარედ უნდა ჩაითვალოს ის, რომ დოკუმენტი წარმოადგენს ერთგვარ საერთაშორისო „კონსენსუსს“ იმის შესახებ, თუ როგორ უნდა დაბალანსდეს პირადი ცხოვრების დაცვა პერსონალური მონაცემების თავისუფალ გადაადგილებასთან მიმართებით. იგი, ასევე, გვთავაზობს რეგულირების მოქნილ მექანიზმს, რომელიც ერგება ყველა გარემოს, მათ შორის, გლობალურ ქსელებს და გამოიყენება არაერთ შიდასახელმწიფოებრივ რეგულაციურ მექანიზმში, საჯარო და კერძო სექტორის მიერ.

რეკომენდაცია ამკვიდრებს პერსონალურ მონაცემთა დაცვის 8 პრინციპს, ესენია:

1. სამართლიანობა, კანონიერება და პერსონალურ მონაცემთა მოპოვება სუბიექტის თანხმობის ან მისი ინფორმირების საფუძველზე;
2. მონაცემთა მიზნობრივი დამუშავების პრინციპი;
3. მონაცემთა მიზნის პროპორციული დამუშავების პრინციპი;

147 Rule, J.B. & Greenleaf G., *Global Privacy Protection*, Edward Elgar Publishing, 2010, p. 83.

148 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

4. თავდაპირველ მიზანთან შეუთავსებელი მიზნით დამუშავების დაუშვებლობა;
5. მონაცემთა უსაფრთხოდ შენახვა;
6. ინდივიდის მონაწილეობა პროცესში, რაც გულისხმობს მისი უფლებების რეალიზაციას დამმუშავებლის წინაშე;
7. წესების საჯაროობა, რაც ეხება ინფორმაციის ხელმისაწვდომობას მონაცემთა დამმუშავების წესების შესახებ;
8. ანგარიშვალდებულება, რომელიც უზრუნველყოფს დამმუშავებლის მიერ ზემოხსენებული პრინციპების დაცვას.<sup>149</sup>

პერსონალურ მონაცემთა დაცვის სფეროში მნიშვნელოვან მოვლენად ითვლება 1981 წლის 28 იანვარს ევროპის საბჭოს მიერ პერსონალურ მონაცემთა დაცვის თაობაზე საერთაშორისო აქტის მიღება. ევროპის საბჭოს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ წარმოადგენს პირველ საერთაშორისო სამართლებრივ დოკუმენტს, სადაც განერილია უზოგადესი პრინციპები და წესები, რომელიც შემდგომ სახელმძღვანელო დოკუმენტი გახდა სხვა უფრო დეტალური რეგულაციებისთვის. გარდა იმისა, რომ 108-ე კონვენციამ ამ სფეროში დაამკვიდრა დღესდღეობით საყოველთაოდ აღიარებული ტერმინოლოგია და განსაზღვრებები, მის ღირსებებს მიეკუთვნება ისიც, რომ დოკუმენტი სპეციალურ ვალდებულებას აწესებს მისი ხელმომწერი ქვეყნებისთვის - მიიღონ კანონმდებლობა, რომელიც მოახდენს კონვენციის ნორმების დანერგვას შიდასახელმწიფოებრივ დონეზე.<sup>150</sup> კონვენციის თანახმად „ყოველი მხარე იღებს ვალდებულებას განახორციელოს აუცილებელი ღონისძიებები შესაბამის კანონმდებლობაში იმ დებულებათა ჩართვისათვის, რომლებიც უზრუნველყოფენ ამ თავში წარმოდგენილი მონაცემების დაცვის ძირითადი პრინციპების რეალიზაციის შესაძლებლობებს.“<sup>151</sup>

149 იქვე, ნაწილი II.

150 კორკელია, (რედ.), 2011, გვ. 335.

151 ევროპის საბჭოს 108-ე კონვენცია, მ. 4, პ. 1. 2018 წლის 18 მაისს მიღებულ იქნა 108-ე კონვენციის მოდერნიზებული ვერსია, რომლის საფუძველზე შეცვლილ იქნა მთელი რიგი დებულებები, რითაც კონვენცია შესაბამისობაში მოვიდა მონაცემთა დაცვის თანამედროვე სტანდარტებთან. საყურადღებოა, რომ მოდერნიზებული ვერსია საქართველოს მხარის მიერ

ზემოაღნიშნული კონვენცია შეიცავს წესებს პერსონალურ მონაცემთა დამუშავებისთვის საჯარო და კერძო ორგანიზაციების ფარგლებში, ასევე, იცავს ფიზიკურ პირებს უფლების დარღვევისგან, მაგალითად, უნებართვო შეგროვებისა და შემდგომი დამუშავებისგან. გარდა ამისა, მოიცავს ნორმებს საერთაშორისო გადაცემის შესახებ. მნიშვნელოვანია, რომ მასში განმტკიცებულია პერსონალურ მონაცემთა დაცვის მთავარი პრინციპები, კერძოდ, სამართლიანობა, კანონიერება, მიზნობრიობა, პროპორციულობა და შესაბამისი ვადების დაცვა დამუშავებისას. 108-ე კონვენცია გამოირჩევა იმითაც, რომ იგი არის ერთადერთი საერთაშორისო სამართლებრივი ინსტრუმენტი პერსონალურ მონაცემთა დაცვის სფეროში, რომელიც ღიაა რატიფიცირებისთვის არაევროპული სახელმწიფოებისთვისაც.<sup>152</sup>

კონვენციის მნიშვნელობიდან გამომდინარე მიზანშეწონილია განვიხილოთ დოკუმენტით მოცემული საკვანძო დებულებები:<sup>153</sup>

კონვენციის თანახმად პერსონალური მონაცემი „აღნიშნავს ნებისმიერ ინფორმაციას, რომელიც შეეხება განსაზღვრულ ან განმსაზღვრელ პირს („ინფორმაციის სუბიექტს“).“<sup>154</sup> როგორც ჩანს კონვენცია აწესებს პერსონალური მონაცემის დეფინიციას მინიმალური ოდენობით, სხვა სიტყვებით, იგი არ აკონკრეტებს თუ რა მეთოდებით და გზებით ან ინფორმაციის რა სახეების გათვალისწინებით არის შესაძლებელი მოხდეს სუბიექტის იდენტიფიცირება, მათ შორის, როგორც პირდაპირ, ისე არაპირდაპირ;

კონვენციით, მონაცემთა ავტომატიზებული ფაილი „აღნიშნავს ინფორმაციის ნებისმიერ ნაკრებს, რომელიც ექვემდებარება ავტომატურ დამუშავებას.“<sup>155</sup> ამ ფორმულირებით კონვენცია საკმაოდ ავიწროვებს დამუშავების მეთოდებს და ადგენს,

---

არაა რატიფიცირებული, ამდენად, პუბლიკაციაში შემოვიფარგლები რატიფიცირებული ვერსიით.

152 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 29.

153 ნორმატიული ფორმულირებები ციტირებულია კონვენციის ქართულ-ნოვანი თარგმანიდან [<https://personaldata.ge/manage/res/docs/convention%20108.pdf>].

154 იქვე, მ. 2, პ. „ა.“

155 იქვე, პ. „ბ.“

რომ მისი გავრცელების ფარგლები ეხება მხოლოდ მონაცემთა ავტომატური დამუშავების შემთხვევებს, მაშინ როდესაც, პერსონალურ მონაცემთა დამუშავება არაავტომატური (სრულად მექანიკური) ან ნახევრად-ავტომატური (ნაწილობრივ მექანიკური) საშუალებებითაც დასაშვებია. პერსონალურ მონაცემთა დაცვასთან დაკავშირებული მოქმედი ნორმატიული აქტები მკაფიოდ ადგენენ დამუშავების მეთოდების სრულფასოვან ფორმულირებასა და მონესრიგებას;

კონვენციით მოცემულია ავტომატური დამუშავების განმარტება, იგი „აღნიშნავს შემდეგ ოპერაციებს, რომელიც სრულდება ინფორმაციის მთელ ნაკრებზე ან მის ნაწილზე ავტომატიზებული დამუშავების საშუალებებით, კერძოდ: მონაცემთა შენახვა, ამ მონაცემებზე ლოგიკური/მათემატიკური ოპერაციების შესრულება, მათი შეცვლა, წაშლა, ინფორმაციული მოძიება და გავრცელება.“<sup>156</sup> აქაც, კონვენცია შემოიფარგლება ვიწრო გავრცელების არეალით დამუშავების დეფინიციის ნაწილში. ამ ფორმულირებით მკაფიოდ იკვეთება კონვენციის მიღების მიზანი, კერძოდ; დოკუმენტის შემუშავებისა და მიღების პერიოდისთვის არსებულ განვითარებად ინფორმაციულ ტექნოლოგიებზე პერსონალურ მონაცემთა დამუშავების სამართლებრივი რეგულირების საჭიროება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი განმარტება არ შემოიფარგლება მხოლოდ ავტომატური დამუშავებით და იგი ეხება ნებისმიერ ოპერაციას, რაც შეიძლება განხორციელდეს ამ ტიპის ინფორმაციის მიმართ;

კონვენციით მოცემულია ფაილის ადმინისტრატორის დეფინიცია, იგი „აღნიშნავს ფიზიკურ ან იურიდიულ პირს, სახელმწიფო ხელისუფლების ორგანოს, დაწესებულებას ან სხვა ნებისმიერ ორგანიზაციას, რომელიც ადგილობრივი კანონმდებლობის შესაბამისად უფლებამოსილია გადაწყვიტოს, რა მიზნებისთვისაა გათვალისწინებული მოცემული ავტომატიზირებული ფაილი, პერსონალური მონაცემების რომელი კატეგორიები ექვემდებარება შენახვას და რა ოპერაციების ჩატარება შეიძლება მათთან მიმართებით.“<sup>157</sup> თანამედროვე ფორმულირებით, აქ

156 იქვე, პ. „გ.“

157 იქვე, პ. „დ.“

საუბარია პერსონალურ მონაცემთა დამმუშავებელზე, რომლის სტატუსის განსაზღვრა პირისთვის დამოკიდებულია ორი კრიტერიუმის კუმულაციურ შესრულებაზე, კერძოდ, იგი უნდა განსაზღვრავდეს დამმუშავების მიზნებს, ხოლო შემდგომ, ამ მიზნების მიღწევის საშუალებებსაც. თუ ეს ორივე პირობა სახეზეა, ნებისმიერი პირი ჩაითვლება დამმუშავებლად.

გარდა დამმუშავებლის დეფინიციისა, კონვენცია პირველი საერთაშორისო სამართლებრივი დოკუმენტია, სადაც მკაფიოდ განისაზღვრა თუ რა არის განსაკუთრებული, სენსიტიური კატეგორიის პერსონალური მონაცემი. ასეთ ინფორმაციად ჩაითვლება „პერსონალური მონაცემები, რომლებიც შეეხება რასობრივ წარმომავლობას, პოლიტიკურ, რელიგიურ ან სხვა მრწამსს, ისევე როგორც ჯანმრთელობის მდგომარეობასა თუ სექსუალურ ცხოვრებასთან დაკავშირებული პერსონალური მონაცემები [...]“<sup>158</sup> კონვენცია ამ კატეგორიის პერსონალურ მონაცემებთან მიმართებით მკაცრ წესებს ადგენს და მათი დამმუშავების მხოლოდ ძალზე განსაკუთრებულ შემთხვევებს ალიარებს კანონიერად. ამავე მუხლში ვკითხულობთ, რომ ამ კატეგორიის პერსონალური მონაცემები „[...] არ ექვემდებარება ავტომატიზებულ დამმუშავებას გარდა იმ შემთხვევისა, როცა ადგილობრივი კანონმდებლობა უზრუნველყოფს მათი დაცვის შესაბამის გარანტიებს. იგივე ეხება სისხლის სამართლებრივ პასუხისმგებლობასთან დაკავშირებულ მონაცემებსაც.“<sup>159</sup> პერსონალურ მონაცემთა გამიჯვნა ორი ძირითადი კატეგორიის მიხედვით დღესაც მოცემულია შიდასახელმწიფოებრივ თუ საერთაშორისო აქტებში.

კონვენციის მთავარ მიღწევად ითვლება დამმუშავების პრინციპების დადგენა. დოკუმენტი ამკვიდრებს შემდეგ ვალდებულებებს დამმუშავებლებისა და უფლებამოსილი პირებისთვის: „პერსონალური მონაცემები, რომლებიც ექვემდებარებიან ავტომატიზირებულ დამმუშავებას:

ა. მიღებული და დამმუშავებული უნდა იყოს პირდაპირი და კანონიერი გზით;

ბ. შენახული უნდა იქნას ზუსტად განსაზღვრული კანონიერი

158 იქვე, მ. 6, პ. 1.

159 იქვე.

მიზნებისათვის და არ უნდა იყოს გამოყენებული მათთან შეუთავსებელი გზით;

გ. უნდა იყოს ადეკვატური და არ უნდა აღემატებოდეს იმ მიზნებს, რომლებისთვისაც ისინი ინახებიან;

დ. უნდა იყოს ზუსტი და საჭიროებისამებრ განახლებადი;

ე. დაცული უნდა იყოს ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიკაციის საშუალებას მხოლოდ იმ დროში, რაც საჭიროა იმ მიზნებისათვის, რისთვისაც ინახება ეს მონაცემები.<sup>160</sup>

განვიხილოთ თითოეული მათგანი. ამასთან, მეტი სიცხადისთვის, მიზანშეწონილია<sup>161</sup> ეს პრინციპები შევადაროთ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ ანალოგებს:

1. დამუშავების პირველი პრინციპი ეხება ქმედებათა მთელი პროცესის კანონიერების უზრუნველყოფას. გარდა ამისა, მოითხოვება, რომ ინფორმაცია მოპოვებული იყოს პირველწყაროდან, სხვა სიტყვებით, პირდაპირი გზით შეგროვდეს. ამ დებულებით, კონვენცია ამკვიდრებს, რომ დამმუშავებელმა პერსონალურ მონაცემთა გამოყენებისას არათუ დამუშავების წესები უნდა დაიცვას, არამედ, თავად ინფორმაციის გამოყენების თითოეული ოპერაცია უნდა იყოს ზოგადი კანონიერების ჩარჩოში მოქცეული. საქართველოს კანონით, დამუშავების პირველი პრინციპი, განსხვავებულადაა ფორმულირებული, ვკითხულობთ, რომ „მონაცემები უნდა დამუშავდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად.“<sup>161</sup> კანონიერების მოთხოვნა აქაც გვხვდება, თუმცა საინტერესოა რა საკითხებს მოიცავს დამუშავების სამართლიანობისა და ღირსების შეულახაობის პირობები? სამართლიანობა სუბიექტური დატვირთვისა და ინდივიდუალური მნიშვნელობის მქონეა, მისი იდეალური, უნივერსალური განმარტება არ არსებობს. შესაბამისად, ჩვენს შემთხვევაში; ნაკლებად სავარაუდოა, რომ კანონმდებელმა სიტყვა „სამართლიანობა“ იგულისხმა, როგორც სუბიექტური და მეტად ინდივიდუალიზებული მოცემუ-

160 იქვე, მ. 5.

161 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 4, პ. „ა.“

ლობა. პერსონალურ მონაცემთა დაცვის არსიდან გამომდინარე საუბარია ადამიანის ძირითადი უფლების დაცვაზე, ამდენად სამართლიანობა უნდა აღვიქვათ თანასწორობის ანალოგად. შესაბამისად, სამართლიან პირობებში დამუშავების მოთხოვნა უზრუნველყოფს ინდივიდთა დიფერენცირების ისეთ პრევენციას, რომელიც დაუშვებელი და დისკრიმინაციულია. საქმეში Huber v. Germany (16.12.2008, C-524/06) მართლმსაჯულების ევროპული კავშირის სასამართლომ დაადგინა, რომ გერმანიაში დანაშაულის პრევენციის მიზნით შემუშავებული მონაცემთა ბაზა იყო დისკრიმინაციული იმ გაგებით, რომ იგი ეხებოდა მხოლოდ უცხოელ, გერმანიის მოქალაქეობის არმქონე პირებს. სასამართლოს აზრით ამგვარი ბაზის ფორმირება გულისხმობს ჩადენილი დანაშაულებებისა და მართლსაწინააღმდეგო ქმედებების პრევენციას, მისი ჩამდენი პირის ეროვნების მიუხედავად. ეს კი არღვევს ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების მე-18 მუხლს.<sup>162</sup>

გარდა ამისა, სამართლიანობის პრინციპის დანახვა სხვა პერსპექტივიდანაც შესაძლებელია. სამართლიანობის პირობა აერთიანებს პერსონალურ მონაცემთა დამუშავების პროცესისთვის დამახასიათებელ აუცილებელ პირობებს, ესენია: 1. დამუშავების გამჭვირვალობის უზრუნველყოფა ფიზიკური პირების წინაშე; 2. დამუშავების პროცესის დანყებამდე, დამუშავების მიზნის, დამუშავებლების ვინაობისა და მისამართის შესახებ ინფორმაციის ხელმისაწვდომობა; 3. ფარული და საიდუმლო დამუშავების შემთხვევათა მინიმალიზება; 4. ფიზიკური პირებისთვის მათ შესახებ დამუშავებული ინფორმაციის შესახებ შეტყობინების განხორციელებისთვის მუდმივი მზადყოფნა.<sup>163</sup>

რაც შეეხება ღირსების შელახვისგან თავის შეკავებას, აღსანიშნავია, რომ კანონი ამ გზით ცდილობს პერსონალურ მონაცემთა დაცვის პარალელურად უზრუნველყოს მეტად აღმატებული სიკეთის - ღირსების დაცვაც. ეს ყველაზე აშკარად ვლინდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს

162 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 174-175.

163 ჩაჩავა, ს., ზაალიშვილი, ვ. (რედ.), *შრომის სამართალი III – სტატიათა კრებული*, GLZ, 2014, გვ. 34.

კანონის დანაწესში, რომლის მიხედვითაც დაუშვებელია ჰიგიენისთვის განკუთვნილ ადგილებში და გამოსაცვლელ ოთახებში ვიდუოთვალთვალის სისტემის დამონტაჟება.<sup>164</sup> ამდენად, შეგვიძლია ვთქვათ, რომ კონვენციით მოცემული პირველი პრინციპი საქართველოს კანონმდებლობით არამარტო გაზიარებულია, არამედ შეიცავს უფლების დაცვის მეტ გარანტიებსაც;

2. მეორე პრინციპის თანახმად, პერსონალური მონაცემები უნდა ინახებოდეს მხოლოდ კანონიერი მიზნისთვის და თავი უნდა ავარიდოთ ნებისმიერ ისეთ გამოყენებას, რომელიც შეუთავსებელია თავდაპირველ მიზანთან. კონვენციის ეს ჩანაწერი საკმაოდ ვიწრო ფორმულირებას შეიცავს და ეხება მხოლოდ მონაცემთა შენახვას, მაშინ როდესაც, საქართველოს კანონით „მონაცემები შეიძლება დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან შეუთავსებელი მიზნით.“<sup>165</sup> შესაბამისად, კანონში საუბარია ცნება „დამუშავება“-ზე, რაც მოიცავს ნებისმიერ ოპერაციას პერსონალური მონაცემის მიმართ, მათ შორის, შენახვას (დაუშვებელია პერსონალურ მონაცემთა შენახვა იმ შემთხვევაში თუ აღარ არსებობს საამისო საფუძველი). ამ ფორმულირებით ცალსახაა, რომ დამუშავების მიზანი პროცესში მონაწილე პირებისთვის ნათელი უნდა იყოს, ასევე, დამუშავება კანონით ნებადართული საქმიანობის ნაწილს უნდა წარმოადგენდეს. პირობითად, თუ პერსონალურ მონაცემთა დამუშავების მიზანი კანონით აკრძალულ ქმედებას ეხება, თუმცა თავად დამუშავების პროცესი კანონიერია (დაცულია სხვა პრინციპები და წესები), ეს ოპერაციები ჩაითვლება არაკანონიერად, რამდენადაც თავად მიზანი ემსახურება კანონით აკრძალულ ქმედებას. ამასთან, მიზნის ფორმულირება რამდენიმე აუცილებელი პირობის ერთობლიობაა, კერძოდ: 1. მიზანი უნდა იყოს ნათლად ფორმულირებული დამუშავების პროცესის დაწყებამდე; 2. უნდა იყოს დასაბუთებული; 3. თავდაპირველ მიზანთან შეუთავსებლობის შემთხვევაში, დამუშავებისთვის საჭიროა დამატებითი არგუ-

164 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 12, პ. 4.

165 იქვე, მ. 4, „ბ.“

მენტირებული საფუძვლის არსებობა;<sup>166</sup>

3. პერსონალური მონაცემები უნდა იყოს ადეკვატური და იმ მიზნის შესაბამისი რისთვისაც მუშავდება იგი. პერსონალურ მონაცემთა დაცვის სამართალში მიზნობრიობის პრინციპთან მჭიდრო კავშირშია ადეკვატური ინფორმაციის დამუშავების პრინციპი, სხვა სიტყვებით, პერსონალურ მონაცემთა დამუშავების მართლზომიერების საკითხზე, სხვა პირობებთან ერთად, გავლენას ახდენს დამუშავების პროპორციულობის პირობაც. საქართველოს კანონით, ეს პრინციპი თითქმის იმავე ფორმულირებითაა მოცემული - „მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევაც მუშავდება ისინი.“<sup>167</sup> პერსონალურ მონაცემთა დამუშავების პროპორციულობის ტესტი განსაკუთრებულ ყურადღებას მოითხოვს. დამუშავების მიზანი შესაძლოა სხვადასხვა დაკავშირებული ქვე-მიზნების ერთობლიობა იყოს, სადაც, თითოეულ ეტაპზე დასამუშავებელი პერსონალური მონაცემების ოდენობა და სახე ჯეროვნად უნდა განისაზღვროს. შედეგად, პროპორციულობის პრინციპი მონაცემთა სუბიექტის შესახებ ნებისმიერი ინფორმაციის მოპოვების პრევენციისთვის საუკეთესო მექანიზმია;<sup>168</sup>

4. სიზუსტისა და საჭიროების შესაბამისად განახლების პრინციპი ეხება როგორც მონაცემთა შეგროვების, ისე მათი შემდგომი შენახვის პერიოდს. ამ დანაწესის მიზანია გამოირიცხოს ყოველი ისეთი შემთხვევა, სადაც ფიზიკური პირის შესახებ მიიღება გადაწყვეტილებები, რომელიც დაფუძნებულია მცდარ ინფორმაციაზე. საქართველოს კანონით ეს პრინციპი შემდეგი სახითაა ფორმულირებული: „მონაცემები ნამდვილი და ზუსტი უნდა იყოს და, საჭიროების შემთხვევაში, უნდა განახლდეს. კანონიერი საფუძვლის გარეშე შეგროვებული და დამუშავების მიზნის შეუსაბამო მონაცემები უნდა დაიბლოკოს, ნაიშალს ან

166 ჩაჩავა, ზაალიშვილი, (რედ.), 2014, გვ. 36.

167 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 4, „გ.“

168 ჩაჩავა, ზაალიშვილი, (რედ.), გვ. 37-38.

განადგურდეს.<sup>169</sup> კონვენციისგან განსხვავებით, საქართველოს კანონი დამატებით ადგენს თუ რა ვალდებულება ეკისრებათ დამმუშავებლებსა და უფლებამოსილ პირებს იმ შემთხვევაში თუ პერსონალური მონაცემები მიზნის გარეშე ან არაკანონიერად მუშავდება.

ამ პრინციპის პრაქტიკაში რეალიზება ორი მეთოდით არის შესაძლებელი, პირველი, იმ შემთხვევაში თუ მონაცემთა სუბიექტი ითხოვს დამმუშავებლისგან პერსონალური მონაცემების მოდიფიცირებას და, მეორე, თუ დამმუშავებელი თავად გადაწყვეტს, რომ ფიზიკური პირის შესახებ მის ხელთ არსებული ინფორმაცია საჭიროებს ცვლილებას.<sup>170</sup> ის ვალდებულება, რომ დამმუშავებელმა თავად, პროაქტიულად უზრუნველყოს პერსონალური მონაცემების მოდიფიცირება გამომდინარეობს შემდეგი დანაწესიდან „თუ მონაცემთა დამმუშავებელი მონაცემთა სუბიექტის მოთხოვნის გარეშე, თავად ჩათვლის, რომ მის ხელთ არსებული მონაცემები არასრულია, არაზუსტია ან არ არის განახლებული, მან შესაბამისად, უნდა გაასწოროს ან განაახლოს მონაცემები და ეს აცნობოს მონაცემთა სუბიექტს;“<sup>171</sup>

5. პერსონალურ მონაცემთა დაცვის V პრინციპი ვადების დაცვაზე აკეთებს აქცენტს. საქართველოს კანონი ვადიანობის პრინციპის ფორმულირებისას კონვენციით დადგენილ ფარგლებს არ სცდება, თუმცა კონვენციისგან განსხვავებით აზუსტებს იმ პერსონალური მონაცემების „ბედს,“ რომელიც აღარ არის საჭირო დამმუშავებლისთვის და ადგენს, რომ „მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, ნაიშალოს ან განადგურდეს ან შენახული უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით, თუ კანონით სხვა რამ არ არის დადგენილი.“<sup>172</sup> პერსონალურ მონაცემთა დამუშავების ნებისმიერ ოპერაციაზე პასუხისმგე-

169 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 4, პ. „დ.“

170 ჩაჩავა, ზაალიშვილი, (რედ.), გვ. 38-39.

171 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 23, პ. 3.

172 იქვე, მ. 4, პ. „ე.“

ბლობა და მტკიცების ტვირთი დამმუშავებელს ეკისრება, შესაბამისად, იგი ვალდებულია ასაბუთოს თუ რატომ არ დაბლოკა ან გაანადგურა ინფორმაცია, რომელიც მას ხელთ ჰქონდა ფიზიკური პირის შესახებ. მაგალითად, ინფორმაცია, რომელიც ეხება დანესებულებაში მომუშავეს ყოველწლიურ შრომით შეფასებას აღარ არის აქტუალური მაშინ, როდესაც გაივლის 15 წელი წელი ან ეს თანამშრომელი დატოვებს სამსახურს,<sup>173</sup> შესაბამისად, ეს ინფორმაცია ექვემდებარება კანონით გათვალისწინებულ რეაგირებას.

კონვენციის მორიგ მონაპოვარს წარმოადგენს პერსონალურ მონაცემთა სუბიექტის უფლებების დეკლარირება. ეს უფლებები შესაძლებელია სამ ჯგუფად დავყოთ: 1. უფლება, რომელიც უზრუნველყოფს ფიზიკური პირის მოთხოვნის შემთხვევაში ან დამმუშავებლის და უფლებამოსილი პირის მხრიდან პროაქტიულად ინფორმაციის მონოდებას დამმუშავების თაობაზე; 2. სუბიექტის უფლება მოხდეს მის შესახებ არსებული ინფორმაციის მოდიფიცირება (შეცვლა), თუ იგი არის არასწორი ან არაზუსტი; 3. ფიზიკურ პირთა უფლება, ნებისმიერ დროს მოითხოვოს მის შესახებ არსებული ინფორმაციის ნაშლა დამმუშავებლის ან უფლებამოსილი პირისგან, სხვა სიტყვებით, იყოს „დავინწყებული.“

პერსონალურ მონაცემთა სუბიექტს შეუძლია დაადგინოს მუშავდება თუ არა მის შესახებ ინფორმაცია, გაიგოს ამგვარი დამმუშავების მიზნები, ასევე, დამმუშავებლის ვინაობა და მისამართი. სუბიექტს, ასევე, ენიჭება უფლება გამოითხოვოს მის შესახებ დამმუშავებული ინფორმაციის ასლი და თავად აირჩიოს მიწოდების ფორმა. კონვენცია საშუალებას აძლევს სუბიექტს მოითხოვოს ინფორმაციის შეცვლა, გასწორება ან ნაშლა, იმ შემთხვევაში თუ მოხდა მათი დამმუშავება შიდასახელმწიფოებრივი კანონმდებლობის დარღვევით.<sup>174</sup>

კონვენციის მიღების პერიოდისთვის პერსონალურ მონაცემთა საერთაშორისო გადაცემა, ასევე, წარმოადგენდა გამოწვევას. ამ საკითხის სამართლებრივ ჩარჩოში მოსაქცევად, კონვენციით დადგინდა, რომ ხელმომწერ მხარეებს უფლება არ

173 ჩაჩავა, ზაალიშვილი, (რედ.), გვ. 39.

174 ევროპის საბჭოს 108-ე კონვენცია, მ. 8, პ. „ა“, „ბ“, „და“, „გ.“

აქვთ დაადგინონ პერსონალურ მონაცემთა გადაცემის ამკრძალავი ნორმები.<sup>175</sup> მიუხედავად ამისა, სახელმწიფოებს უფლება აქვთ დაადგინონ შემზღუდავი ნორმები გადაცემისთვის, იმ შემთხვევაში თუ: 1. წევრი ქვეყნის კანონმდებლობით დადგენილია სპეციალური წესები გარკვეული კატეგორიის ინფორმაციის გადაცემისთვის; 2. გადაცემა ხორციელდება იმ ქვეყნის ტერიტორიაზე, რომელიც არ არის კონვენციის ხელმომწერი მხარე.<sup>176</sup>

კონვენციის მიღებიდან 20 წლის შემდეგ, 2001 წლის 8 ნოემბერს, მიიღეს მისი დამატებითი ოქმი - ზედამხედველ ორგანოებთან და მონაცემთა ტრანსსასაზღვრო გადადინებასთან დაკავშირებით. იგი არეგულირებს ორ მნიშვნელოვან საკითხს: 1. პერსონალურ მონაცემთა გადაცემას იმ სახელმწიფოში, რომელიც არ ექვემდებარება კონვენციის სამართლებრივი მოქმედების იურისდიქციას და 2. საზედამხედველო ორგანოს ფუნქციონირების იმპერატიული მოთხოვნის დანესებას.

დამატებითი ოქმის მიხედვით თითოეულმა მხარემ უნდა უზრუნველყოს, სულ მცირე, ერთი საზედამხედველო ორგანოს შექმნა და ფუნქციონირება შიდასახელმწიფოებრივი კანონმდებლობის საფუძველზე.<sup>177</sup> რაც მთავარია, აღნიშნულ საზედამხედველო ორგანოს უნდა ჰქონდეს შემომწების, გამოძიების, სამართლებრივ პროცედურებში მხარედ გამოსვლის ან კომპეტენტური ადგილობრივი სამართალდამცავი ორგანოებისთვის კანონმდებლობის დარღვევებთან დაკავშირებული საკითხების განსახილველად გადაცემის უფლებამოსილება.<sup>178</sup> გარდა ამისა, ამგვარ უწყებებს უნდა გააჩნდეთ ფიზიკურ პირთა საჩივრების განხილვის უფლებამოსილება.<sup>179</sup> ამასთან, საზედამხედველო ორგანოები, უნდა ფუნქციონირებდნენ სრული დამოუკიდებლობით, ხოლო მათ მიერ გამოტანილი გადანყევითილების გასაჩივრების უფლება სასამართლოში უნდა იყოს უზრუნველყოფილი.<sup>180</sup>

175 იქვე, მ. 12, პ. 2.

176 იქვე, პ. 3.

177 ევროპის საბჭოს 108-ე კონვენციის დამატებითი ოქმი, მ. 1, პ. 1.

178 იქვე, მ. 1, პ. 2(ა).

179 იქვე, ქვეპ. „ბ.“

180 იქვე, მ. 1, პ. 3 და 4.

გარდა პერსონალურ მონაცემთა დაცვის საზედამხებდველო ორგანოს სავალდებულო ფუნქციონირების მოთხოვნისა, დამატებითი ოქმი, მხარეებს აკისრებს გარკვეულ ვალდებულებებს პერსონალურ მონაცემთა საერთაშორისო გადაცემის ნაწილში: თითოეულ მხარეს უფლება აქვს განახორციელოს საერთაშორისო გადაცემა კონვენციის არანეგირი მხარისთვის ან ორგანიზაციისთვის მხოლოდ იმ შემთხვევაში თუ მიმღები სახელმწიფო ან ორგანიზაცია უზრუნველყოფს მონაცემთა დაცვის ადეკვატურ დონეს.<sup>181</sup> გამონაკლისის სახით, დადგენილია შემთხვევები, როდესაც დასაშვებია პერსონალური ინფორმაციის ტრანსფერი არანეგირი მხარისთვის, ესენია: 1. პერსონალურ მონაცემთა სუბიექტის ინტერესების არსებობა; 2. აღმატებული ინტერესის გათვალისწინებით, მათ შორის, მნიშვნელოვანი საჯარო ინტერესის შემთხვევაში; 3. თუ მხარეთა შორის გაფორმებულია შეთანხმება, რომელიც ეხება პერსონალურ მონაცემთა ადეკვატურ დაცვას და ნებადართულია შესაბამისი შიდასახელმწიფოებრივი კომპეტენტური (საზედამხებდველო) ორგანოს მიერ.<sup>182</sup>

კონვენციისა და მისი დამატებითი ოქმის მთავარი დებულებების განხილვის შედეგად ცხადი გახდა, რომ მათი მნიშვნელობა, პერსონალურ მონაცემთა დაცვის სამართლის საკვანძო საკითხებთან მიმართებით, დიდია. იგი გვევლინება საწყის ეტაპად ამ სფეროს საერთაშორისო განვითარებისთვის. მიუხედავად იმისა, რომ კონვენცია არ შეიცავს მოცემულ დეტალურ რეგულირებებს, იგი მნიშვნელოვანი დოკუმენტია პერსონალურ მონაცემთა დაცვის, როგორც ძირითადი უფლების განსაზღვრისთვის საერთაშორისო დონეზე. აქვე, მსურს კვლავ ავლნიშნო, რომ კონვენციის რატიფიცირება საქართველოს პარლამენტმა 2005 წლის 28 ოქტომბერს მოახდინა, ხოლო დამატებითი ოქმი - 2013 წლის 27 ივლისს იქნა რატიფიცირებული. ამ პერიოდისთვის საქართველოს კანონმდებლობა შესაბამისობაშია კონვენციითა და მისი დამატებითი ოქმით დადგენილ ძირითად მოთხოვნებთან.

პერსონალურ მონაცემთა დაცვის შემდგომ განვითარებას ევროპული კავშირის ფარგლებში ჰქონდა ადგილი, როდესაც 1995 წლის 24 ოქტომბერს მიღებულ იქნა 95/46/EC დირექტივა

181 იქვე, მ. 2, პ. 1.

182 იქვე, პ. 2.

„პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადადინებისას ფიზიკურ პირთა დაცვის შესახებ.“<sup>183</sup> თავისი შინაარსით, დირექტივა ამყარებდა და განავრცობდა ევროპის საბჭოს 108-ე კონვენციით დადგენილ პრინციპებს. 108-ე კონვენციისგან განსხვავებით, იგი დეტალურად ეხებოდა პერსონალურ მონაცემთა დაცვის სფეროში არსებულ საკვანძო საკითხებს, როგორიცაა ტერმინები, დამუშავების საფუძველები, სუბიექტის უფლებები. ასე მაგალითად, დირექტივით დამატებით ჩამოყალიბდა უფლებამოსილი პირის, მესამე პირისა და მონაცემთა მიმღების განმარტებები. ამასთან, დირექტივამ შემოიღო დამუშავების საფუძველთა ჩამონათვალი, როგორც სენსიტიური ისე, არასენსიტიური კატეგორიის პერსონალური მონაცემებისთვის. გარდა ამისა, განსაზღვრული იყო იმ ინფორმაციის სახეობა, რაც უნდა ყოფილიყო მიწოდებული პერსონალურ მონაცემთა სუბიექტისთვის: თუ მუშავდებოდა მის შესახებ არსებული ინფორმაცია. ამ ყველაფერთან ერთად, დირექტივა ახდენდა მონაცემთა სუბიექტის უფლებათა დეკლარირებას და მისი რეალიზაციის საშუალებების განსაზღვრას. უსაფრთხოების ნაწილში, დოკუმენტი ავალდებულებდა დამუშავებლებს შესაბამისი ზომების მიღებას პერსონალური მონაცემების ტექნიკური და ორგანიზაციული უსაფრთხოებისთვის. სხვა მნიშვნელოვანი დებულებებიდან აღსანიშნავია ევროპული კავშირის არანერეკტეციუმი პერსონალურ მონაცემთა გადაცემის რეგულირება და შიდასახელმწიფოებრივი საზედამხებელო ორგანოს სავალდებულო შექმნის პირობა ხელმომწერ ქვეყნებში.

მნიშვნელოვანია იმის გააზრება, რომ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ წარმოადგენს ამ დირექტივის საფუძველზე შემუშავებულ დოკუმენტს. კანონში ისეთი საკითხები, როგორიცაა პერსონალურ მონაცემთა დაცვის სფეროში არსებული ტერმინები; დამუშავების პრინციპები და საფუძველები, მათ შორის, სენსიტიური და არასენსიტიური პერსონალური მონაცემებისთვის და სუბიექტის უფლებები, დი-

183 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

რექტივით მოცემული შინაარსის მიხედვითაა მოწესრიგებული.

მიუხედავად დირექტივის მნიშვნელობისა იგი უკვე მოძველებულ და ძალადაკარგულ სამართლებრივ ინსტრუმენტად გვევლინება. ამის ერთ-ერთი დამადასტურებელია ის ფაქტი, რომ 2018 წლის 25 მაისს ძალაში შევიდა მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR), რის შემდეგაც დირექტივის მოქმედება შეწყდა. პერსონალურ მონაცემთა დაცვის კუთხით ეს მოვლენა დიდ წინგადადგმულ ნაბიჯს წარმოადგენს სხვადასხვა მიზეზის გამო.

პირველ რიგში, ფორმალური თვალსაზრისით, რეგულაცია, დირექტივისგან განსხვავებით, ევროპული კავშირის წევრ სახელმწიფოებში უშუალოდ მოქმედ სამართლებრივ ინსტრუმენტს წარმოადგენს. შესაბამისად, თუ დირექტივაში მოცემული დებულებების შიდასახელმწიფოებრივი ამოქმედებისთვის ევროპული კავშირის წევრი სახელმწიფო ვალდებული იყო მიეღო შესაბამისი კანონმდებლობა, რეგულაციის ამოქმედებას მსგავსი მექანიზმი არ ესაჭიროება და იგი უშუალოდ მოქმედებს ევროპული კავშირის ყველა წევრ სახელმწიფოში. ამდენად, სახეზეა მეტად უნიფიცირებული მიდგომა და ყველა წევრ სახელმწიფოში მოქმედებს პერსონალურ მონაცემთა დაცვის ერთიანი სამართლებრივი რეჟიმი.

მეორე მხრივ, ყურადღებას იპყრობს რეგულაციის ზოგიერთი დებულება. კერძოდ, რეგულაცია ვრცელდება დამუშავებლის ან უფლებამოსილი პირის მიერ პერსონალურ მონაცემთა დამუშავებაზე, მიუხედავად იმისა აქვს თუ არა ადგილი დამუშავების პროცესს უშუალოდ ევროპული კავშირის ტერიტორიაზე.<sup>184</sup> გარდა ამისა, რეგულაცია ვრცელდება პერსონალურ მონაცემთა დამუშავების ისეთ შემთხვევებზე, როდესაც მუშავდება ევროპულ კავშირში მყოფი ფიზიკური პირების შესახებ ინფორმაცია და ეხება: 1. მათთვის საქონლის ან მომსახურების შეთავაზებას, მიუხედავად იმისა ხორციელდება თუ არა სუბიექტის მხრიდან ანგარიშსწორება ევროპული კავშირის ტერიტორიაზე; და 2. მათი ქცევის მონიტორინგს, თუ ამას ადგილი აქვს ევროპული კავშირის ტერიტორიაზე.<sup>185</sup>

<sup>184</sup> GDPR, Art. 3(1).

<sup>185</sup> იქვე, მ. 3(2).

რეგულაციაში განსაკუთრებული ყურადღება ეთმობა პერსონალურ მონაცემთა სუბიექტის თანხმობის შემთხვევაში მის შესახებ ინფორმაციის დამუშავების საკითხს. კერძოდ, დაკონკრეტებულია თუ რა პირობებს უნდა აკმაყოფილებდეს თანხმობა, რათა დამუშავება ჩაითვალოს მართლზომიერად. თუ მონაცემთა სუბიექტის თანხმობა გაცემულია წერილობითი ფორმით (დოკუმენტალურად, რომელიც სხვა პირობების შემცველიც არის), დამუშავების თაობაზე თანხმობის მისაღებად, ეს უკანასკნელი უნდა იქნეს მოთხოვნილი მკაფიოდ და სხვა საკითხებისგან განცალკევებულად, ცხადი და მარტივი ენის გამოყენებით.<sup>186</sup>

მნიშვნელოვანი ვალდებულებები დაწესდა პერსონალურ მონაცემთა დამუშავების მართლზომიერების კონტროლისთვის. დამმუშავებელი და უფლებამოსილი პირი ვალდებულია დანიშნოს მონაცემთა დაცვის ოფიცერი (შიდაორგანიზაციული მაკონტროლებელი) იმ შემთხვევაში თუ: 1. დამუშავება ხორციელდება საჯარო დაწესებულების ან პირის მიერ, გარდა სასამართლო ორგანოებისა; 2. თუ დამმუშავებლის და უფლებამოსილი პირის მიერ ხორციელდება პერსონალურ მონაცემთა სუბიექტების მოცულობითი მონიტორინგი; და 3. თუ დამმუშავებელი და უფლებამოსილი პირი ამუშავებენ პერსონალურ მონაცემთა განსაკუთრებულ კატეგორიებს.<sup>187</sup>

საქართველოში რეგულაციის დებულებებს არ აქვს პირდაპირი სამართლებრივი ეფექტი. თუმცა, 2014 წლის 27 ივნისს საქართველოსა და ევროპულ კავშირს შორის გაფორმებული ასოცირების შეთანხმებით<sup>188</sup> საქართველო ვალდებულია დაამკვიდროს მონაცემთა დაცვის ევროპულ კავშირში მოქმედი სტანდარტები. მხარედ წოდებული საქართველოს სახელმწიფო „უზრუნველყოფს მონაცემთა დაცვის სამართლებრივ დონეს, რომელიც მინიმუმ შეესაბამება ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის პერსონალურ მონაცემთა დაცვასა და

186 იქვე, მ. 7(2).

187 იქვე, მ. 37(1).

188 ასოცირების შესახებ შეთანხმება ერთი მხრივ, ევროკავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებსა და მეორეს მხრივ, საქართველოს შორის, მ. 14.

ასეთი ტიპის მონაცემთა თავისუფალ გადაადგილებასთან მიმართებით ინდივიდების დაცვის თაობაზე 95/46/EC დირექტივით გათვალისწინებულ დაცვის სტანდარტებს [...]. საჭიროებისამებრ, თითოეული მხარე გაითვალისწინებს 2008 წლის 27 ნოემბრის სისხლის სამართლებრივ საკითხებზე პოლიციასა და სასამართლოს შორის თანამშრომლობის ფარგლებში დამუშავებულ პერსონალურ მონაცემთა დაცვის შესახებ საბჭოს 2008/977/JHA, ჩარჩო გადანყვეტილებას ასევე 1987 წლის 17 სექტემბრის ევროპის საბჭოს მინისტრთა კომიტეტის R(87)15 რეკომენდაციას, რომელიც არეგულირებს პოლიციის სფეროში პერსონალურ მონაცემთა გამოყენებას.<sup>189</sup>

დამატებით, მნიშვნელოვანია, რომ მონაცემთა დაცვის ძირითადი რეგულაციის ძალაში შესვლის პარალელურად, გაუქმდა ზემოაღნიშნული ჩარჩო გადანყვეტილება 2008/977/JHA და ამოქმედდა ახალი დირექტივა EU 2016/680.<sup>190</sup> იგი არეგულირებს პერსონალურ მონაცემთა დაცვისა და დამუშავების საკითხებს შესაბამისი დანესებულებებისთვის, რომლებიც ახდენენ დანაშაულებათა პრევენციას, გამოძიებას, გამოვლენას, აღსრულებას და ზოგადად საჯარო უსაფრთხოების დაცვას.

აღსანიშნავია, როგორც რეგულაციის ისე ახალი დირექტივის გარდამავალ დებულებებში არის მითითება, რომ მითითებები 95/46/EC დირექტივასა და 2008/977/JHA ჩარჩო გადანყვეტილებაზე, უნდა იქნეს განმარტებული მითითებებად მონაცემთა დაცვის ძირითად რეგულაციასა და დირექტივაზე EU 2016/680.<sup>191</sup> ამდენად, ასოცირების შეთანხმებით მოცემული ფორმულირების გათვალისწინებით, საქართველო ვალდებულია უზრუნველყოს მონაცემთა დაცვის ის სტანდარტი, რომელიც მოცემულია რეგულაციით, ხოლო საჭიროების შემთხვევაში, ასევე, უზრუნველყოს დირექტივის დებულებათა იმპლემენტირება ეროვნულ

<sup>189</sup> იქვე, დანართი I.

<sup>190</sup> Directive (EU) 2016/680 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>191</sup> GDPR, Art. 94(2); Directive (EU) 2016/680, Art. 59(2).

კანონმდებლობაში.

საქართველოში პრაქტიკული ღონისძიებების გატარებისთვის ქმედითი ნაბიჯები გვიან გადაიდგა. ამის დამადასტურებელია ის, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, გარდა იმ მუხლებისა, რომელიც აწესებს პასუხისმგებლობას პერსონალურ მონაცემთა დაცვის წესების დარღვევისთვის, ამოქმედდა 2012 წლის 1 მაისს,<sup>192</sup> ხოლო 2013 წლის 1 იანვრიდან ამოქმედდა მუხლები, რომელიც სამართალდარღვევისთვის ითვალისწინებს დამმუშავებლის ან უფლებამოსილი პირის დაჯარიმებას.<sup>193</sup> რაც ყველაზე მთავარია, პერსონალურ მონაცემთა დაცვის ინსპექტორს 2014 წლის 1 ნოემბრამდე, კერძო სექტორის მიმართ არ შეეძლო გამოეყენებინა საზედამხედველო უფლებამოსილებები, კერძოდ, როგორიცაა ფიზიკური პირის საჩივრის განხილვა კერძო სექტორის დამმუშავებლის ან უფლებამოსილი პირის მიმართ. ასევე, ინსპექტორს არ ჰქონდა უფლებამოსილება საკუთარი ინიციატივით განეხორციელებინა შემოწმება კერძო სექტორში და დარღვევების გამოვლენის შემთხვევაში გაშოეყენებინა მის ხელთ არსებული მექანიზმები.<sup>194</sup>

გარდა ამისა, 2014 წლის 1 აგვისტოს ცვლილებების მიხედვით, კანონი გარკვეულ შესწორებებს დაექვემდებარა, კერძოდ, როგორიცაა მისი გავრცელება სამართალდამცავი ორგანოების საქმიანობაზე (გარკვეული გამოწვევების გარდა), დაზუსტდა მონაცემთა დამმუშავებლის ვალდებულებები, განისაზღვრა ფაილური სისტემის კატალოგის შექმნის ვალდებულება განუჩევლად დამმუშავებლის კატეგორიისა, ასევე, დაკორექტირდა ნორმები, რომელიც ეხება პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს არჩევასთან და მის ანგარიშვალდებულებასთან დაკავშირებულ საკითხებს, რითაც იგი მეტად მოვიდა შესაბამისობაში ევროპულ სტანდარტებთან.

მიღწევების მიუხედავად, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი გარკვეული ნორმების ფორმული-

192 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 56, პ. 1.

193 იქვე, პ. 2.

194 იქვე, პ. 3.

რებას ბუნდოვნად ახდენს. ეს, მაგალითად, ვიდეოთვალთვალის განხორციელების შესახებ წესებში ვლინდება. კანონის თანახმად „მონაცემთა დამმუშავებელი ვალდებულია შექმნას ვიდეოჩანაწერების შენახვისთვის განკუთვნილი ფაილური სისტემა. ჩანაწერების (სურათები/ხმა) გარდა, სისტემა უნდა შეიცავდეს ინფორმაციას მონაცემთა დამმუშავების თარიღის, ადგილისა და დროის შესახებ.“<sup>195</sup> ამ ნორმის მიხედვით ვიდეოთვალთვალის განხორციელების შემთხვევაში დამმუშავებელს ევალება შექმნას პერსონალურ მონაცემთა სტრუქტურებიზებული წყება (ფაილური სისტემა), რაც გულისხმობს მათ თავმოყრას კონკრეტული კრიტერიუმის მიხედვით (მაგ. თარიღი, ადგილი და ა.შ.). საყურადღებო ამ წესში არის ის, რომ კანონმდებელი დამმუშავებელს ანიჭებს შესაძლებლობას, გარდა გამოსახულებისა, ფაილურ სისტემაში შეინახოს აუდიო ჩანაწერებიც, რისი დასკვნის საშუალებას გვაძლევს ფრჩხილებში მოცემული სიტყვები „(სურათები/ხმა).“ აქ კი, ჩნდება კითხვა: ვიდეოთვალთვალის პარალელურად არის თუ არა კანონით რეგლამენტირებული აუდიო სიგნალის ჩანერა? კანონი ამის შესახებ ცალსახა განმარტებას არ გვაძლევს, მეტიც, კანონით არც ვიდეოთვალთვალის დეფინიციაა მოცემული. ამდენად, ვიდეოგამოსახულების ჩანერის პარალელურად აუდიოკონტროლის საკითხი სპეციალური რეგულირების მიღმა დარჩენილი. სხვა სიტყვებით, ვიდეოთვალთვალის განხორციელების წესების დადგენისას კანონი აუდიოკონტროლზე არ საუბრობს, თუმცა ვიდეოჩანაწერების შენახვისას ირიბად უშვებს იმის შესაძლებლობას, რომ პარალელურად შენახულ იქნეს აუდიოჩანაწერიც. ცალსახაა, რომ კანონი ამ საკითხის რეგულირებისას ხარვეზს შეიცავს. თუმცა, გასარკვევია ეს ხარვეზი არის ღია თუ ფარული? თუ ეს ხარვეზი ღიაა, მაშინ კანონმდებელს ამ საკითხის რეგულირება უბრალოდ „გამორჩა“, ან ვერ განჭვრიტა აქტის მიღების დროს კონკრეტული საკითხი, ხოლო თუ ეს ხარვეზი ფარულია მაშინ გამოდის, რომ კანონმდებელმა შეგნებულად არ მოაწესრიგა ეს საკითხი და რეგულირების სირთულიდან გამომდინარე ეს წინასწარ იყო გაშიზნული.<sup>196</sup>

პერსონალურ მონაცემთა დაცვის ინსპექტორი აუდიოკონ-

195 იქვე, მ. 12, პ. 6.

196 ხუბუა, გ., *სამართლის თეორია*, მერიდიანი, თბილისი, 2015, გვ. 217.

ტროლის განხორციელების კანონთან თავსებადობის საკითხს ვიდუოთვალთვალის შესახებ მომწესრიგებელი ნორმების ფარგლებში განიხილავს და მიიჩნევს, რომ „ისეთი ვიდუოთვალთვალის სისტემის გამოყენებისას, რომელიც ვიზუალური მონიტორინგის გარდა, იძლევა აუდიო მონიტორინგის შესაძლებლობას, პროპორციულობის პრინციპის დაცვა განსაკუთრებულ მნიშვნელობას იძენს და მონაცემთა დამუშავებელი ვალდებულია დაასაბუთოს აუდიო მონიტორინგის აუცილებლობა.“<sup>197</sup> მიუხედავად ამისა, რეკომენდაციაში დასაშვებობის დამატებით კრიტერიუმებზე საუბარი არაა.

აუდიოკონტროლთან დაკავშირებით გაერთიანებული სამეფოს ინფორმაციის კომისრის ანგარიშში მითითებულია რომ იგი ძალზედ შეზღუდულ შემთხვევებშია დასაშვები, მათ შორისაა: 1. ხმოვან სიგნალზე დაფუძნებული საგანგაშო სისტემები (როდესაც ხდება ხმოვანი სენსორის გააქტიურება მაღალი სიგნალის მიწოდების შემთხვევაში); 2. კლიენტსა და მომსახურების გამწვევს შორის განხორციელებული საუბრის ჩანერა, სადაც ეს აუცილებელია მომსახურების განწვევის მიზნით; 3. კონკრეტულ ადგილებში, საგანგაშო ლილაკის დაჭერისას ხმის ჩანერის ავტომატური დაწყების მიზნით.<sup>198</sup> ვიდუოკონტროლისას ხმოვანი სიგნალის ჩანერის საკითხი წარმოადგენს განსაკუთრებულ ჩარევას პირადი ცხოვრების, მათ შორის, პერსონალურ მონაცემთა დაცვის უფლებაში.

გარდა ზემოხსენებულისა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი დამუშავების საფუძველთა ფორმულირებისას, ასევე, შეიცავს ბუნდოვნებას. მონაცემთა დამუშავება დასაშვებია თუ „მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად.“<sup>199</sup> აქ ყურადღებას იპყრობს ფორმულირება „მნიშვნელოვანი საჯარო ინტერესი.“ ისმის კითხვა, როდესაც

197 საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაციები ვიდუოთვალთვალის განხორციელების შესახებ, გვ. 4 [<https://personaldata.ge>].

198 Information Commissioner's Office (ICO) of the United Kingdom, *CCTV Code of Practice*, 2008, p. 10 [<https://ico.org.uk>].

199 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 5, პ. „ზ.“

საუბარია საჯარო ინტერესზე, რამდენად არის გამართლებული სიტყვა „მნიშვნელოვანი“-ს გამოყენება, მაშინ როდესაც, ლოგიკურად, საჯარო ინტერესი საზოგადო ინტერესს ნიშნავს? აქვე, შეგვიძლია დავსვათ შეკითხვა სხვა კუთხით, კერძოდ, იძლევა თუ არა ეს ფორმულირება იმის თქმის საფუძველს, რომ საჯარო ინტერესი შეიძლება იყოს „უმნიშვნელო“ ან „ნაკლებად მნიშვნელოვანი“? „საჯარო ინტერესის“ ნორმატიული განმარტება არ მოიპოვება. არც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის განმარტებით ბარათშია მოცემული მსჯელობა ამ დანაწესთან მიმართებით.<sup>200</sup> ამდენად უცნობია თუ, რა იგულისხმა კანონმდებელმა ფორმულირებაში „მნიშვნელოვანი საჯარო ინტერესი.“ შესაბამისად, რთულია კანონმდებლის მიერ შემოთავაზებული ფორმულირების განმარტება იქამდე, ვიდრე სახეზე არ იქნება სასამართლოს მიერ დადგენილი განმარტებები.

გარდა ჩამოთვლილისა, კანონით არ არის რეგულირებული პერსონალურ მონაცემთა დაცვის ოფიცრის (DPO) ფუნქციონირების საკითხიც. ზოგადად, მონაცემთა დაცვის ოფიცერი არის თანამდებობის პირი, რომელიც შიდაორგანიზაციულად პასუხს აგებს დანესებულების მიერ პერსონალურ მონაცემთა მართვასთან დაკავშირებულ საკითხებზე. პერსონალურ მონაცემთა დაცვის ხარისხის ასამაღლებლად მიზანშეწონილია კანონმდებლობაში განხორციელდეს ცვლილებები და განისაზღვროს მონაცემთა დაცვის ოფიცრის ფუნქციონირების სავალდებულო პირობა.

ამასთან, ავლნიშნავ, რომ პუბლიკაციის მიზანს არ წარმოადგენს ყველა იმ ნაკლოვანების გამოვლენა, რომელიც გვხვდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედ რედაქციაში. ეს ნაწილი ემსახურება კანონის შესახებ ზოგადი წარმოდგენის შექმნას. ამდენად, მისი შემდგომი ანალიზისგან თავს შევიკავებ.

---

200 საქართველოს პარლამენტი, განმარტებითი ბარათი „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონპროექტის შესახებ, 2011, პუნქტი „ა.გ“ [<https://www.parliament.ge/>].

## 2.3. პერსონალურ მონაცემთა დაცვის უფლების სამართლებრივი და ინსტიტუციური გარანტიები

„მონაცემთა დაცვის უფლება წარმოშობილია პირადი ცხოვრების დაცვის უფლებიდან. პირადი ცხოვრების კონცეფცია უკავშირდება ადამიანებს. შესაბამისად, ფიზიკური პირები არიან მონაცემთა დაცვის უპირველესი ბენეფიციარები.“<sup>201</sup> თუმცა, ჯერ კიდევ რთულია შეთანხმება იმის შესახებ, თუ რა სახის ურთიერთდამოკიდებულებაა პერსონალურ მონაცემთა დაცვასა და პრივატულობას შორის. ევროპულ სამართლებრივ სისტემაში. მონაცემთა დაცვის ნიაღში აღმოცენებული ინტერესები პირადი ცხოვრების მეტად ფართო უფლების ნაწილად მოიხსენიება, ამასთან, პერსონალურ მონაცემთა დაცვის უფლება ცალსახად უნდა იზიარებდეს ძირითადი უფლების სრულფასოვან სტატუსს.<sup>202</sup>

ამ ვითარებაში, განსაკუთრებული როლი ენიჭება ცალკეული სამართლებრივი ნორმების სასამართლო გადანყვეტილებების მიხედვით ინტერპრეტირებასა და სუბიექტის უფლებების დაცვისკენ მიმართული პრაქტიკის ჩამოყალიბებას. მოცემული პრეცედენტების ფორმირება დიდწილადაა დამოკიდებული ნორმატიულ ჩანაწერებზე. ქვემოდმოყვანილი მსჯელობა ეხება, პირველ რიგში, იმ პრაქტიკას, რაც ჩამოყალიბებულია სასამართლო გადანყვეტილებების მეშვეობით. ამასთან, განხილულია საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ მიღებული გადანყვეტილებები.

### 2.3.1. საერთაშორისო სასამართლოების მიერ პერსონალურ მონაცემთა დაცვის უფლების თაობაზე მიღებული ზოგიერთი მნიშვნელოვანი გადანყვეტილება

201 ძირითად უფლებათა ევროპული კავშირის სააგენტო, ევროპის საბჭო, ადამიანის უფლებათა ევროპული სასამართლო, *მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო*, „იურისტების სამყარო“, თბილისი, 2015, გვ. 48.

202 Purtoṡ N., *Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights*, *Netherland Quarterly of Human Rights* (Vol. 28, No. 2), 2010, p. 3.

ევროპის ფარგლებში პერსონალურ მონაცემთა დამცავი ინსტრუმენტების განვითარებამ შედეგად გამოიწვია ის, რომ პირველად, საერთაშორისო დონეზე, ეს უფლება დამოუკიდებლად გაიწერა ევროპული კავშირის ძირითად უფლებათა ქარტიაში.<sup>203</sup> კერძოდ; „ყველას გააჩნია საკუთარი პერსონალური მონაცემების დაცვის უფლება;“ ასევე, „ამგვარი მონაცემი უნდა დამუშავდეს სამართლიანად კონკრეტული მიზნებისთვის და პირის თანხმობით ან სხვა კანონით დადგენილი საფუძვლით. ყველას გააჩნია საკუთარ მონაცემებზე წვდომის უფლება, ასევე, მათი შესწორების უფლება;“ გარდა ამისა, გათვალისწინებულია შესაბამისი მაკონტროლებელი დამოუკიდებელი ორგანოს შექმნის პირობაც და მითითებულია, რომ „ამ წესებთან შესაბამისობა ექვემდებარება დამოუკიდებელი საზედამხედველო ორგანოს ზედამხედველობას.“<sup>204</sup> ქარტია არ იზიარებს ადამიანის უფლებათა ევროპული კონვენციის მიდგომას უფლებათა დეკლარირებისას იმ გაგებით, რომ ცალკე მუხლად აყალიბებს პირობებს ძირითადი უფლებების შეზღუდვისთვის. დოკუმენტის თანახმად „ქარტიით აღიარებული უფლებებისა და თავისუფლებების ნებისმიერი შეზღუდვა უნდა იყოს დადგენილი კანონით და არ არღვევდეს ამ უფლებათა და თავისუფლებათა არსს. პროპორციულობის პრინციპის გათვალისწინებით, შეზღუდვა შეიძლება განხორციელდეს მხოლოდ მაშინ თუ იგი აუცილებელია და ემსახურება კავშირის მიერ აღიარებული საზოგადოებრივი ინტერესის მიზნებს ან საჭიროა სხვათა უფლებებისა და თავისუფლებების დასაცავად. [...]“<sup>205</sup>

ევროპული კავშირის კანონმდებლობა მეტად დახვეწილ დებულებებს შეიცავს პერსონალურ მონაცემთა დაცვასთან მიმართებით. ამდენად, არაა გასაკვირი, რომ მართლმსაჯულების ევროპული კავშირის სასამართლოს პრაქტიკა მრავალფეროვანია. სასამართლომ არაერთხელ მიუთითა ამ უფლების ფუნდამენტურ ხასიათზე. საყურადღებოა ისიც, რომ გადანყვეტილებებში პერსონალურ მონაცემთა დაცვის უფლების განხილვა ხდება დამოუკიდებელი სამართლებრივი სიკეთის ქრილში, მიუ-

203 Charter of Fundamental Rights of the European Union (2000/C 364/01), 2000.

204 იქვე, მ. 8.

205 იქვე, მ. 52(1).

ხედავად იმისა, რომ მას კავშირი აქვს ადამიანის პირადი ცხოვრების უფლებასთან. გარდა ამისა, სასამართლოს გადანყვეტილებები ახდენს მონაცემთა დაცვის სამართალში არსებული ამა თუ იმ ტერმინის, ასევე, პრინციპებისა და წესების განმარტებას. შესაბამისად, მიზანშეწონილია სასამართლოს რამდენიმე გადანყვეტილების განხილვა.

ევროპული კავშირის ფარგლებში მონაცემთა დაცვის კანონით დამკვიდრებული ერთ-ერთი საკვანძო ცნება - „პერსონალური მონაცემი“ - არაერთხელ გახდა განმარტების საგანი. მაგალითად, საქმეში *Vokler and Markus Scheke and Hartmut Eifert v. Land Hessen* სასამართლო დაეყრდნო ადამიანის უფლებათა ევროპული სასამართლოს მიდგომას და განმარტა, რომ პროფესიული სახის ქმედებათა შესახებ ინფორმაცია კი ექცევა პირადი ცხოვრების დაცული სფეროს ფარგლებში იმ შემთხვევაში, თუ ინფორმაცია იდენტიფიცირებული ფორმითაა მოცემული.<sup>206</sup> გარდა „პერსონალური მონაცემი“-ს დეფინიციისა, სასამართლომ ამ საქმეში განიხილა პერსონალურ მონაცემთა პროპორციული დამუშავების საკითხი. მან არამართლზომიერად მიიჩნია განმცხადებლების ვინაობის გამოქვეყნება საჯაროდ (ონლაინ) იმ პერსონალურ მონაცემებთან ერთად; რომელიც ეხებოდა მათ მიერ სახელმწიფოსგან მიღებულ აგრარულ სუბსიდიებს. სასამართლოს აზრით, ფიზიკური პირების სახელებისა და მათ მიერ მიღებული ზუსტი თანხობრივი ოდენობების შესახებ ინფორმაციის გამოქვეყნებით დაირღვა უფლებაში ჩარევის ის პროპორცია, რისი დაცვის ვალდებულებაზეც საუბარია ქარტიაში.<sup>207</sup> ამასთან, სასამართლომ აღნიშნა, რომ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული შეზღუდვები უნდა დაექვემდებაროს აუცილებლობის პირობას და ამდენად, მიზანშეწონილია მოვიძიოთ ისეთი გზები, რომელიც ნაკლებად იქონიებს გავლენას ფიზიკური პირების ძირითადი უფლების დაცვაზე.<sup>208</sup> ამ შემთხვევაში, ინფორმაციის მიღების მოტივით

206 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 99-100.

207 იქვე.

208 CJEU, C-92/09, C-93/09, *Vokler and Markus Scheke and Hartmut Eifert v. Land Hessen*, 09.11.2010, para. 83.

პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვა ვერ იქნებოდა მართლზომიერი. საინვესტიციო ფონდიდან თანხების გამოყოფის დროს საზოგადოების ინტერესს წარმოადგენს არა ის თუ ვინ არიან კონკრეტული ბენეფიციარები, არამედ ის თუ როგორ გადანაწილდა ფონდში აკუმულირებული თანხები. აღნიშნული საქმე ნათელი შემთხვევაა იმისა, თუ როგორ დგინდება ზღვარი ინფორმაციის თავისუფლებასა და პერსონალურ მონაცემთა დაცვას შორის.

პერსონალურ მონაცემთა დაცვის უფლება არ წარმოადგენს აბსოლუტურს, იგი შესაძლოა შეიზღუდოს სხვა ღირსი ინტერესისა თუ უფლების გათვალისწინებით, ხოლო რიგ შემთხვევებში იგი მეტ დაცვას საჭიროებს. გასათვალისწინებელია ისიც, რომ უფლებათა ბალანსის დროს არ შეიძლება მოვიძიოთ ყოველი შემთხვევისთვის შესაბამისი, ერთიანი მიდგომა. შეფასება უნდა მოხდეს ყოველ ჯერზე, პერსონალურ მონაცემთა დაცვის საკითხის კონტექსტუალური ანალიზის შესაბამისად. მაგალითად, საქმეში *European Commission v. Bavarian Lager* მართლმსაჯულების ევროპული კავშირის სასამართლომ ზუსტი გაუსვა პერსონალური მონაცემების გამჟღავნებისას თანხმობის მიღების აუცილებლობას, იმ შემთხვევაში თუ არ არსებობს სხვა ლეგიტიმური საფუძველი დამუშავებისთვის.<sup>209</sup> ამ გადაწყვეტილების გამოტანით სასამართლომ აქცენტი გააკეთა მონაცემთა სუბიექტის ერთ-ერთ უპირველეს უფლებაზე - გაცეს თანხმობა საკუთარი პერსონალური მონაცემების გამოყენებისთვის. სასამართლოს აზრით, დახურული პერსონალური მონაცემების მოთხოვნის შემთხვევაში აუცილებელია ცხადი და ლეგიტიმური საფუძვლის არსებობა, რათა ინფორმაციის მომთხოვნისთვის ინტერესთა ანონ-დანონვის საფუძველზე მოხდეს მათი გამჟღავნება.<sup>210</sup> ამასთან, თანხმობა ჯეროვნადაა გაცემული მაშინ თუ სუბიექტი იაზრებს, რომ თანხმობა არის არჩევანი და მასზე უარის თქმა არ იწვევს სანქციებს.<sup>211</sup>

209 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 75-77.

210 CJEU, C-28/08 P, *European Commission v. Bavarian Lager*, 29.06.2010. para. 78.

211 Gutwirth S., Pouillet Y., Hert, P.D., Terwangne C., Nouwt S., *Reinventing Data Protection?*, Springer, 2009, p. 101.

დამუშავების პროცესში პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვა არაერთხელ გახდა სასამართლოს მსჯელობის საგანი. მაგალითად, საქმეში *Huber v. Federal Republic of Germany* სასამართლომ პერსონალურ მონაცემთა დამუშავება განიხილა სამართლიანობის პრინციპის, კერძოდ, თანასწორი დამუშავების კონტექსტში. ფაქტობრივი გარემოებების მიხედვით, გერმანიაში მოქმედებდა ერთიანი რეესტრი, სადაც ფიქსირდებოდა ყველა იმ უცხოელი მოქალაქის შესახებ ინფორმაცია, რომელიც იმყოფებოდა გერმანიაში სამ თვეზე მეტი ვადით. მონაცემები, საბაზისო კატეგორიის გარდა, ეხებოდა უცხოელთა კანონსაწინააღმდეგო ქმედებების შესახებ ინფორმაციას. სასამართლომ აღნიშნა, რომ გარკვეული ღირსი მიზნებისთვის პერსონალურ მონაცემთა შეგროვება დასაშვებია იყო, თუმცა ის ფაქტი, რომ ამგვარი რეესტრი მხოლოდ გერმანული მოქალაქეობის არმქონე ფიზიკური პირებისთვის მოქმედებდა, ევროპული კავშირის ფუნქციონირების შესახებ ხელშეკრულების თანახმად, წარმოადგენდა უცხოელების მიმართ ეროვნების ნიადაგზე დისკრიმინაციულ მოპყრობას.<sup>212</sup> შესაბამისად, არათანაბარი მოპყრობა ეროვნების ნიადაგზე დასაშვებია მხოლოდ იმ შემთხვევაში, თუ პერსონალურ მონაცემთა ბაზა შეიცავს აუცილებელ ინფორმაციას და მისი ცენტრალიზებული ბუნება საშუალებას იძლევა გამოვიყენოთ იგი გაერთიანების იმ წევრების მიმართ, რომლებიც არ არიან წევრი ქვეყნის მოქალაქეობის მქონენი.<sup>213</sup> აღსანიშნავია ისიც, რომ ზოგადად სამართლიანობის პრინციპი ვერ იქნება განსაზღვრული კონკრეტულად. ამ პრინციპის იმპლემენტირებისას, აუცილებელია მოხდეს სხვა თანამდევი პრინციპების საფუძველზე პერსონალურ მონაცემთა სუბიექტის უფლებებისა და დამმუშავებლის ინტერესების ანონ-

ტერმინოლოგიური კუთხით, პერსონალურ მონაცემთა დაცვის კანონმდებლობა არაერთ საკვანძო ტერმინს ამკვიდრებს, მათ შორისაა - „დამუშავება.“ „პერსონალურ მონაცემთა დაცვის

212 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 174-175; European Commission, *Summaries of Important Judgements* [[http://ec.europa.eu/dgs/legal\\_service/arrets/listechrono\\_en.htm](http://ec.europa.eu/dgs/legal_service/arrets/listechrono_en.htm)].

213 CJEU, C-524/06, *Huber v. Federal Republic of Germany*, 06.12.2008, para. 82.

შესახებ“ საქართველოს კანონის თანახმად, დამუშავება არის ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით მონაცემთა მიმართ შესრულებული ნებისმიერი მოქმედება.<sup>214</sup> დამუშავებასთან დაკავშირებით, სასამართლომ მნიშვნელოვანი გადაწყვეტილება გამოიტანა საქმეზე Bodil Lindqvist სადაც აღნიშნა, რომ პიროვნების შესახებ მიიღენტიფიცირებელი ინფორმაციის ვებგვერდზე გამოქვეყნება წარმოადგენს სრულად ან ნაწილობრივ ავტომატური საშუალებებით დამუშავებას. საკითხზე, მიიჩნეოდა თუ არა ამგვარი გამოქვეყნება პერსონალური მონაცემების საერთაშორისო გადაცემად, სასამართლომ მიუთითა, რომ თუ ინფორმაციის ვებგვერდზე ჩატვირთვას მივიჩნევდით პერსონალურ მონაცემთა საერთაშორისო გადაცემად მაშინ ყველა იმ სახელმწიფოში, რომელიც ევროპული კომისიის მიერ აღიარებულია მონაცემთა დაცვის ადეკვატური დონის არმქონედ, ინფორმაციის გავრცელება უნდა იყოს შეზღუდული. შესაბამისად, მივიღებდით პირებისთვის ამკრძალავი მოთხოვნის შემცველ დანაწესს ინტერნეტში პერსონალურ მონაცემთა გამჟღავნებისთვის.<sup>215</sup> გარდა ამისა, სასამართლომ აქცენტი გააკეთა პერსონალურ მონაცემთა დაცვასა და ინფორმაციის თავისუფლებას შორის არსებულ ურთიერთდამოკიდებულებაზე 95/46/EC დირექტივის ჭრილში. სასამართლოს კზრით, დირექტივით მოცემული დებულებები არ არის წინააღმდეგობაში გამოხატვის თავისუფლების ძირითად პრინციპებთან. ამდენად, ევროპული კავშირის წევრი ქვეყნების მიერ პერსონალურ მონაცემთა დაცვასთან დაკავშირებით მიღებული ზომები უნდა იყოს დაბალანსებული ინფორმაციის თავისუფლებასთან მიმართებით.<sup>216</sup> ზოგადად, გამოხატვის თავისუფლების ჭრილში, პერსონალური მონაცემების ინტერნეტში გასაჯაროვების საკითხი სირთულეებთან არის დაკავშირებული. ნებისმიერი პირი, რომელიც დააპირებს დაამუშავოს პერსონალური მონაცემები საჯაროდ ხელმისაწვდომი წყაროდან, მოქმე-

214 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 2, პ. „დ.“

215 ძირითად უფლებათა ევროპული კავშირის სააგენტო, ევროპის საბჭო, ადამიანის უფლებათა ევროპული სასამართლო, გვ. 172-173.

216 CJEU, C-101/01, *Bodil Lindqvist*, 06.11.2003, para. 100.

დებს იმ პრეზუმფციის ფარგლებში, რომ ესა თუ ის ინფორმაცია კანონის მოთხოვნათა დაცვით არის გასაჯაროებული. თუმცა, სავსებით შესაძლებელია ეს ასე არც იყოს, ხოლო ფიზიკურმა პირმა ვერ უზრუნველყოს საჯაროდ ხელმისაწვდომი წყაროდან (ძირითადად ინტერნეტიდან) მის შესახებ არსებული ინფორმაციის სრული წაშლა.

მორიგი მნიშვნელოვანი გადაწყვეტილება ეხება დამმუშავებლის ცნებასა და სუბიექტის უფლებას მოითხოვოს დამმუშავებლისგან მის შესახებ არსებული პერსონალური მონაცემების წაშლა. საქმეში Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez სასამართლომ აღნიშნა, რომ Google-ის სუბსიდიარი კომპანია Google Spain, ევროპული კანონმდებლობის თანახმად, მიიჩნეოდა მონაცემთა დამმუშავებლად. საქმეში არსებული გარემოებების მიხედვით პიროვნების შესახებ საძიებო სისტემის მეშვეობით ხელმისაწვდომი იყო სხვადასხვა ინფორმაცია, ხოლო მონაცემთა სუბიექტს გააჩნდა ინფორმაციის წაშლის მოთხოვნის სრული ლეგიტიმური საფუძველი, ვინაიდან მონაცემები იყო მოძველებული და აღარ არსებობდა მონაცემთა დამმუშავების რაიმე საფუძველი. მოცემული გადაწყვეტილებით სასამართლომ ხაზი გაუსვა პერსონალურ მონაცემთა სუბიექტის უფლებას იყოს „დავიწყებული.“ სასამართლომ, აღნიშნა, რომ ქარტიით სუბიექტისთვის მინიჭებული უფლება საშუალებას აძლევს მას მოითხოვოს მის შესახებ არსებული ინფორმაციის წაშლა, რაც, რიგ შემთხვევაში, უპირატესია დამმუშავებლის ეკონომიკურ ინტერესებზე. ამავდროულად, სუბიექტის შესახებ ინფორმაციის მიღების საჯარო ინტერესი არსებობს ისეთ შემთხვევებში, როდესაც იგი საჯარო ფიგურაა. ამ დროს საზოგადოებას აქვს უფლება ჰქონდეს მეტი წვდომა მის პერსონალურ მონაცემებზე.<sup>217</sup> აქვე აღნიშნავ, რომ უფლება „იყო დავიწყებული,“ უმეტესწილად, არ წარმოადგენს აბსოლუტურად რეალიზებადს. მაგალითად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, ფიზიკური პირის უფლება მოითხოვოს მის შესახებ არსებული ინფორმაციის განადგურება შესაძლოა შეიზღუდოს იმ შემთხვევაში თუ

217 CJEU, C-131/12, *Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, 13.05.2014, para. 100.

საქმე ეხება ქვეყნის ეროვნული უსაფრთხოების ან თავდაცვის ინტერესებს, დანაშაულის გამოძიებას და სხვ.<sup>218</sup> აღმატებული მიზნის არსებობისას ფიზიკური პირი ვერ ახდენს ამ უფლების რეალიზებას. თუმცა, ერთ-ერთი მკაფიო მაგალითი თუ როდის არის ეს უფლება აბსოლუტურად განხორციელებადი უკავშირდება პირდაპირ მარკეტინგს. მაგალითად, თუ კომპანია მოკლეთესტური შეტყობინებების მეშვეობით აგზავნის სარეკლამო ხასიათის შეთავაზებას ფიზიკური პირის ტელეფონის ნომერზე, რომელიც საჯარო წყაროდან იქნა მოპოვებული, პერსონალურ მონაცემთა სუბიექტს მაინც აქვს უფლება მოითხოვოს, როგორც სარეკლამო მიზნებისთვის დამუშავების შეწყვეტა, ისე კომპანიის მონაცემთა ბაზიდან ტელეფონის ნომრის წაშლა. ეს მოთხოვნა სრულად უნდა რეალიზდეს დამმუშავებლის მიერ, ვინაიდან მარკეტინგული (სარეკლამო) მიზნები ვერ იქნება აღმატებული სუბიექტის უფლებაზე - მართოს საკუთარი პერსონალური ინფორმაცია.

პერსონალურ მონაცემთა დაცვის საკითხი არაერთხელ იყო განხილვის საგანი ადამიანის უფლებათა ევროპულ სასამართლოში. საყურადღებოა, რომ მართლმსაჯულების ევროპული კავშირის სასამართლოსგან განსხვავებით ადამიანის უფლებათა ევროპული სასამართლო პერსონალურ მონაცემთა დაცვასთან დაკავშირებით მიღებულ გადაწყვეტილებებს აფუძნებს ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლზე. მასში ფორმულირება „პერსონალური მონაცემი“ არაა მოცემული. აქვე უნდა აღინიშნოს მე-8 მუხლის ძირითადი ნაკლოვანებები: 1. მას უშუალო მოქმედების ძალა არ გააჩნია კერძო სექტორის მიმართ; 2. პირად ცხოვრებაზე უფლება არ მოიცავს ყველა პერსონალურ მონაცემს, არამედ მხოლოდ მათ, რომელიც მიიჩნევა პირადად; 3. იგი არ შეიცავს მითითებას სუბიექტისმხრიდან წვდომის უფლების შესახებ.<sup>219</sup>

მიუხედავად ამ ნაკლოვანებისა ადამიანის უფლებათა ევროპული სასამართლოს ერთ-ერთ მნიშვნელოვან პრინციპს წარმოადგენს კონვენციის დებულებათა ევოლუციური განმარტება.

218 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 24, პ. 1.

219 Purtova, p. 6.

სასამართლოს მიერ კონვენცია აღიარებულია როგორც „ცოცხალი“ დოკუმენტი, რის მიხედვითაც კონვენციის დებულებები უნდა განიმარტოს საზოგადოებაში დღეს არსებული განვითარების, ცნობიერებისა და კონკრეტული კონტექსტის მიხედვით და არა კონვენციის მიღების პერიოდისთვის არსებული რეალობიდან გამომდინარე. მეტიც, „კონვენციაში შეიძლება საერთოდ არ იყოს მოხსენიებული ის სამართლებრივი ურთიერთობა, რომელზეც ვრცელდება კონვენციით გათვალისწინებული უფლებები და თავისუფლებები.“<sup>220</sup> ამდენად, სასამართლოს მიერ ჩამოყალიბებული პრაქტიკით, პირადი ცხოვრების ის საკითხები, რომელიც პერსონალურ მონაცემთა მართლზომიერ დამუშავებას ეხება განხილულია მე-8 მუხლის ჭრილში.

საქმეში *Axel Springer AG v. Germany* ადამიანის უფლებათა ევროპულმა სასამართლომ გამოხატვის თავისუფლებისა და მონაცემთა დაცვის ინტერესებს შორის უპირატესობის მინიჭებისას ყურადღება მიაქცია იმ ფაქტს, რომ პერსონალური მონაცემების შემცველი საზოგადოებრივი მნიშვნელობის მქონე მოვლენა, შესაძლებელია მედიასაშუალების მიერ გაშუქდეს.<sup>221</sup> მსგავსი შინაარსის მქონეა გადანყვეტილება საქმეზე *Von Hannover v. Germany* (No. 2) რომლის თანახმად, საჯარო პირებთან მიმართებით პირადი ცხოვრების ის ნაწილი, რომელიც მოიცავს პირის შესახებ ინფორმაციის გავრცელებას ვერ იქნება დაცული იმგვარად, როგორც ეს ხდება რიგითი კერძო პირის მიმართ.<sup>222</sup>

კონვენციის დარღვევა დაადგინა სასამართლომ საქმეზე *Biriuk v. Lithuania*, რის მიხედვითაც პაციენტის შესახებ გამოქვეყნდა ცნობები მისი ჯანმრთელობის მდგომარეობის, კერძოდ, აივ ვირუსით ინფიცირების შესახებ. გადანყვეტილებაში სასამართლომ ხაზი გაუსვა ინდივიდისთვის პერსონალური მონაცემების, მათ შორის, განსაკუთრებული კატეგორიის მონაცემთა დაცვის აუცილებლობას.<sup>223</sup> სასამართლო არ დაეთანხმა ლიტვის უზე-

220 ბოხაშვილი, ბ., კორკელია, კ., *პირადი და ოჯახური ცხოვრების პატივისცემის უფლება და სახელმწიფოს ვალდებულებები*, IRZ, 2017, გვ. 20, 23.

221 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 67-68.

222 ECtHR, App. no. 59320/00, *Von Hannover v. Germany*, 2004.

223 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 70.

ნაეს სასამართლოს იმ საკითხში, რომ საზოგადოებრივ ჯანდაცვასა და უსაფრთხოებაზე ზრუნვის მიზნით მიზანშეწონილი იყო განმცხადებლის ჯანმრთელობის მდგომარეობისა და მისი ცხოვრების წესის გასაჯაროება. ამავდროულად, ევროპული სასამართლოს აზრით, სახელმწიფოში აუცილებელია არსებობდეს ეფექტური მექანიზმი ჯანმრთელობის მდგომარეობის პრესით გამოქვეყნების აღკვეთისთვის.<sup>224</sup> თითქმის იგივე შინაარსის საკითხი განიხილა სასამართლომ საქმეზე I. v. Finland. სასამართლომ ხაზი გაუსვა იმ მოთხოვნას, რომ პერსონალურ მონაცემთა უკანონო გამჟღავნების თავიდან აცილების მიზნით აუცილებელია დაინერგოს შესაბამისი ორგანიზაციული და ტექნიკური უსაფრთხოების ზომების დანერგვა.<sup>225</sup> პერსონალურ მონაცემთა ორგანიზაციული და ტექნიკური უსაფრთხოების ზომების უზრუნველყოფის საკითხი დამმუშავებლებისა და უფლებამოსილი პირების ერთ-ერთ ვალდებულებას წარმოადგენს. ეს მოთხოვნა დადგენილია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით,<sup>226</sup> რითაც იგი შესაბამისობაშია მონაცემთა დაცვის ევროპულ მოდელთან. მოცემული უსაფრთხოების ზომები აქცენტს აკეთებს დამმუშავებლის მხრიდან ისეთი მეთოდების დანერგვაზე, როგორიცაა პერსონალურ კომპიუტერებზე შესაბამისი პაროლების დაყენება, ანტივირუსული სისტემის ფუნქციონირება მთელს IT ინფრასტრუქტურაზე, დანესებულებაში მომუშავე პირთა რეგულარული გადამზადება პერსონალური მონაცემების დაცვის საკითხების შესახებ და სხვა. საყურადღებოა, რომ ინფორმაციული უსაფრთხოების ზომების უზრუნველყოფის ეფექტურ სახელმძღვანელო დებულებებს გვთავაზობს სტანდარტიზაციის საერთაშორისო ორგანიზაცია.<sup>227</sup> მათ მიერ შემუშავებული დოკუმენტი ISO 27001 განსაზღვრავს ინფორმაციული უსაფრთხოების მართვისთვის დადგენილ მოთხოვნებს, რომელიც გამოსადეგია ნებისმიერი სახის ორგანიზაციისთვის. გარდა ამისა, ის ადგენს წესებს თუ როგორ

224 ECtHR, App. no. 23373/03, *Biriuk v. Lithuania*, 2008, para. 43.

225 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 190-191.

226 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 17.

227 International Organization for Standardization.

უნდა მოხდეს ინფორმაციულ უსაფრთხოებასთან დაკავშირებული რისკების შეფასება და მათი მართვა. დოკუმენტი მნიშვნელოვანია იმითაც, რომ იგი არ ეხება მხოლოდ პერსონალურ მონაცემებს და შეიცავს წესებს ნებისმიერი სახის ინფორმაციის უსაფრთხოების უზრუნველსაყოფად.<sup>228</sup>

პერსონალურ მონაცემთა შენახვის შესაბამისი ვადის გასვლის შემდგომ განადგურების აუცილებლობაზე მიუთითა სასამართლომ საქმეში *Rotaru v. Romania*. სასამართლოს აზრით, იმ შემთხვევაში თუ კანონის ნორმა, რომელიც ეხება პერსონალური ინფორმაციის შენახვის წესებს, კერძოდ, შესანახი ინფორმაციის სახეობებს, კატეგორიებს, მიზნებსა და ვადებს, არ იქნება საკმარისად განჭვრეტადი, ეს პირადი ცხოვრების უფლების დარღვევების ტოლფასია. სასამართლოს აზრით, პერსონალური მონაცემების შენახვის შესახებ დაუზუსტებელი ან ბუნდოვანი ჩანაწერი წარმოადგენს პირადი ცხოვრების უფლების შეზღუდვის არალეგიტიმურ საფუძველს.<sup>229</sup> ამავე გადაწყვეტილებით სასამართლომ აღნიშნა, რომ ფარული თვალთვალის სისტემათა ფუნქციონირების კონვენციასთან თავსებადობის უზრუნველსაყოფად, უნდა არსებობდეს შესაბამისი დამცავი მექანიზმები, რომელიც გააკონტროლებს ამგვარი მეთოდების კანონიერებას. ეს მოთხოვნა კანონის უზენაესობის პრინციპიდან გამომდინარეობს, რა დროსაც ეფექტური კონტროლის ბერკეტები სასამართლოს ხელში უნდა იყოს.<sup>230</sup>

მსგავსი შინაარსის საკითხი განიხილეს საქმეში *Khelili v. Switzerland*, სადაც სასამართლომ ხაზი გაუსვა პერსონალურ მონაცემთა დაცვის სამართალში დამკვიდრებულ, შესაბამისი ვადების დაცვით შენახვის, პრინციპს და აღინიშნა, რომ არასათანადო დასაბუთების საფუძველზე პირის შესახებ ინფორმაციის მოპოვება და მისი შენახვა შესაბამის რეესტრში არღვევს პირადი ცხოვრების დაცვის უფლებას, განსაკუთრებით იმ შემთხვევაში, თუ ამგვარი (მცდარი) მონაცემის არსებობა ხელს უშლის პიროვნებას საკუთარი საქმიანობის რეალიზაციაში.<sup>231</sup>

228 <https://www.iso.org/iso/iec-27001-information-security.html>.

229 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 45-46.

230 ECtHR, App. no. 28341/95, *Rotaru v. Romania*, 04.05.2000, para. 59.

231 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 48-49.

მოცემულ საქმეში პოლიციამ დაუზუსტებელ ინფორმაციაზე დაყრდნობით მიიჩნია, რომ განმცხადებელი იყო სექს-მუშაკი. ეს ინფორმაცია მოგვიანებით, სუბიექტის მოთხოვნის საფუძველზე წაიშალა, თუმცა უწყების ბაზაში არ მომხდარა ამ ინფორმაციის სრული ამოშლა. ამდენად, სასამართლომ ჩათვალა, რომ ინფორმაციის შენახვა არ იყო აუცილებელი და გამართლებული დემოკრატიულ საზოგადოებაში.<sup>232</sup>

სახელმწიფო უწყების მიერ ვიდეოჩანანერების გამჟღავნების მართლზომიერების საკითხი დადგა დღის წესრიგში სასამართლოს გადანყევტილებაში საქმეზე *Peck v. United Kingdom*. სახელმწიფო ორგანოს მიერ ვიდეოჩანანერების გადაცემა სხვა ორგანიზაციისთვის, თუნდაც მედიასაშუალებებისთვის, იყო არამიზნობრივი. იქედან გამომდინარე, რომ ჩანანერებში პიროვნება იდენტიფიცირებადი იყო, სასამართლომ ამგვარი გადაცემა კონვენციის მე-8 მუხლის მოთხოვნების დარღვევად ჩათვალა.<sup>233</sup>

პერსონალურ მონაცემთა დაცვის სამართალში მნიშვნელოვანია სუბიექტის უფლებების რეალიზაციის საკითხიც. იმ შემთხვევაში, თუ მონაცემთა სუბიექტის კანონიერი ინტერესები პერსონალური მონაცემის მოდიფიცირების შესახებ აღემატება დამუშავებლის ინტერესს არ შეცვალოს მის შესახებ არსებული ინფორმაცია, სუბიექტის უფლება აუცილებელი ნესით უნდა რეალიზდეს. საქმეში *Ciubotaru v. Moldova* ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ კონვენციის მე-8 მუხლი მოიცავს პირის თვითგამორკვევის უფლებას. საქმის გარემოებათა მიხედვით, სახელმწიფომ არ უზრუნველყო პირის შესახებ სახელმწიფო მონაცემთა ბაზაში ეთნიკური წარმოშობის შესახებ ინფორმაციის შეცვლა და მისი რეგისტრაცია, როგორც რუმინული ეთნიკური წარმომავლობის მქონე პირად.<sup>234</sup> ეს საკითხი დაკავშირებულია ინფორმაციული თვითგამორკვევის კონცეფციასთან, რომლის შესახებაც გერმანიის საკონსტიტუციო სასამართლომ ჯერ კიდევ 1983 წელს გამოიტანა გადანყევტილე-

232 ECtHR Press Release (195), *A French Woman Classified as a "prostitute" for fifteen years in Geneva Police Database Violated Her Right to Respect for Private Life*, European Court on Human Rights Registrar, 2011.

233 ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 47.

234 ECtHR, App. no. 27138/04, *Ciubotaru v. Moldova*, 27.04. 2010, paras. 49, 59.

ბა.<sup>235</sup> ინფორმაციული თვითგამორკვევის უფლება პირს ანიჭებს შესაძლებლობას გადაწყვიტოს თუ როდის და რა ფარგლებში იქნება მისი პირადი ცხოვრება გაზიარებული სხვებისთვის. გარდა ამისა, ეს უფლება პიროვნების ღირსებას უკავშირდება და, ასევე, ზოგადი პიროვნული უფლების შემადგენელი ნაწილია.<sup>236</sup>

ადამიანის უფლებათა ევროპულმა სასამართლომ თვითგამორკვევის უფლების დარღვევის ქრილში განიხილა საქმე Van Kuck v. Germany, სადაც აღნიშნა, რომ პირადი ცხოვრების ცნება მოიცავს სქესის განსაზღვრის, ორიენტაციისა და სახელის არჩევის უფლებებს. გადაწყვეტილების თანახმად, სახელმწიფომ არ მისცა განმცხადებელს უფლება წარედგინა სამედიცინო დასკვნა სქესის შეცვლის ოპერაციის მიზნით, რითაც გაუმართლებლად ჩაერია მის თვითგამორკვევის უფლებაში, რომელიც უზრუნველყოფილია კონვენციის მე-8 მუხლით დაცული სფეროს ფარგლებით.<sup>237</sup>

მნიშვნელოვანია ხაზი გაესვას იმ გარემოებას, რომ ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაზე დაყრდნობით, მე-8 მუხლი არა მხოლოდ იცავს ინდივიდს პერსონალურ მონაცემთა არამართლზომიერი დამუშავებისგან, არამედ სახელმწიფოში ბიძგს აძლევს იმგვარი დამუშავების წესების განსაზღვრას, რომელიც ბოჭავს საჯარო და კერძო პირებს. შესაბამისად, სახელმწიფოს მხრიდან დარღვევა ვლინდება არა იქედან გამომდინარე, რომ სახელმწიფოში არსებულმა კერძო პირებმა დაარღვიეს კანონი, არამედ იმ მხრივ, რომ სახელმწიფომ ვერ უზრუნველყო კერძო პირებისთვის სამართლებრივი რეგულირებით შესაბამისი მიმართულების მიცემა.<sup>238</sup>

შეჯამების სახით, აღსანიშნავია ის სხვაობა, რომელიც ვლინდება მართლმსაჯულების ევროპული კავშირის სასამართლოსა და ადამიანის უფლებათა ევროპული სასამართლოს მიერ გადაწყვეტილებათა გამოტანისას პირადი ცხოვრების, მათ შორის, პერსონალური მონაცემების დაცვის მიმართ.

ევროპული კავშირის ფარგლებში პერსონალურ მონაცემთა დაცვის ინსტრუმენტთა სიმრავლე უზრუნველყოფს მეტ დამცავ

235 BverfGE, vol. 65, 15.12.1983.

236 Gurwirth. Pouillet, Hert, Terwangne, Nouwt, pp. 45-49.

237 ECtHR, App. no. 37968/97, *Van Kuck v. Germany*, 12.06.2003, para. 69, 73, 82.

238 Purtova, p. 14.

საშუალებებს სუბიექტის უფლებებისთვის. ამგვარ შესაძლებლობას მოკლებულია ადამიანის უფლებათა ევროპული სასამართლო. მისი გადანყვეტილებები ეყრდნობა მხოლოდ კონვენციის ჩანაწერს. ეს გამონეულია იმით, რომ მართლმსაჯულების ევროპული კავშირის სასამართლო, კლასიკური სახით, არ გვევლინება მხოლოდ უფლებათა დაცვაზე ორიენტირებულ ორგანოდ. ამავდროულად, გადანყვეტილების გამოტანისას შეუძლია დაეყრდნოს ყველა იმ სამართლებრივ აქტს, რომელიც ეხება კონკრეტულ ურთიერთობას და მოიცავს მონაცემთა დაცვასთან დაკავშირებულ საკითხებს.

თავის მხრივ, ადამიანის უფლებათა ევროპულ სასამართლოს, ინტერპრეტაციის მეშვეობით, უნეეს ყოველ კონკრეტულ შემთხვევაში იმსჯელოს პერსონალურ მონაცემთა დაცვის საკითხებზე. ეს ვითარება გართულებულია იმით, რომ ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპულ კონვენციაში მონაცემთა დაცვასთან მიმართებით ცალკე ჩანაწერი არ მოიპოვება.

### **2.3.2. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის<sup>239</sup> და თბილისის საქალაქო სასამართლოს მიერ პერსონალურ მონაცემთა დაცვის უფლების თაობაზე ჩამოყალიბებული პრაქტიკა<sup>240</sup>**

პირადი ცხოვრების უფლებაში პერსონალურ მონაცემთა განსაკუთრებული მნიშვნელობის დამადასტურებელია, დამატებით, ის ფაქტი, რომ ამ სფეროს მარეგულირებელი ევროპული კანონმდებლობა სავალდებულო წესით ითხოვს სპეციალური საზედამხებდებლო ორგანოს (თანამდებობის პირის) ფუნქციონირებას და მის აღჭურვას სამართლებრივი რეგულირების ბერ-

239 2018 წლის 21 ივლისს მიღებულ იქნა საქართველოს კანონი „სახელმწიფო ინსპექტორის სამსახურის შესახებ.“ კანონის მიხედვით (მ. 27, პ. 1; მ. 30, პ. 2) 2019 წლის 10 მაისს გაუქმდა პერსონალურ მონაცემთა დაცვის ინსპექტორის თანამდებობა, ხოლო სახელმწიფო ინსპექტორის სამსახური ჩაითვალა პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლედ.

240 საყურადღებოა, რომ ინსპექტორის სამსახურის მიერ გამოტანილი გადანყვეტილებები, რომელიც ეხება სუბიექტის დაჯარიმებას, არ საჩივრდება საკასაციო ინსტანციაში.

კეტიებით. იგი განიხილება როგორც ფუძემდებლური მნიშვნელობის ელემენტი პერსონალურ მონაცემთა დაცვის უფლებისთვის დემოკრატიულ საზოგადოებაში.<sup>241</sup>

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიღების<sup>242</sup> შემდეგ, 2013 წლის ივნისიდან საქართველოში შეიქმნა პერსონალურ მონაცემთა დაცვის ინსპექტორის თანამდებობა, რომელიც შემდგომ გაუქმდა, ხოლო მის უფლებამონაცვლედ განისაზღვრა საქართველოს სახელმწიფო ინსპექტორის სამსახური. მონაცემთა დაცვის მიმართულებით, იგი რამდენიმე უფლებამოსილებას ითავსებს, კერძოდ: ა) საჯარო და კერძო დაწესებულებებისთვის, აგრეთვე ფიზიკური პირებისთვის მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე კონსულტაციის გაწევა; ბ) მონაცემთა დაცვასთან დაკავშირებული განცხადებების განხილვა; გ) საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების კანონიერების შემოწმება (ინსპექტირება); დ) საქართველოში მონაცემთა დაცვის მდგომარეობისა და მასთან დაკავშირებული მნიშვნელოვანი მოვლენების შესახებ საზოგადოების ინფორმირება.<sup>243</sup> ამ დანაწესით კანონმდებელმა სახელმწიფო ინსპექტორის სამსახურს მიანიჭა ექსკლუზიური უფლებამოსილება განახორციელოს საზედამხედველო ღონისძიებები პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე. ამ უფლებამოსილებათა ფარგლებში დადგენილია ანგარიშვალდებულების პრინციპი წარმომადგენლობით ხელისუფლებასთან, კერძოდ: „სახელმწიფო ინსპექტორი საქართველოს პარლამენტს წელიწადში ერთხელ, არაუგვიანეს 31 მარტისა, წარუდგენს ანგარიშს საქართველოში პერსონალურ მონაცემთა დაცვის მდგომარეობის [...] შესახებ.“<sup>244</sup>

თავისი საქმიანობის ფარგლებში ინსპექტორის მიერ გამოქვეყნდა რამდენიმე ანგარიში, სადაც ასახულია მისი საქმიანობის მთავარი მიმართულებები და განხორციელებული აქტივობები. მიზანშეწონილია პერსონალურ მონაცემთა დაცვასთან

241 Gutwirth, Pouillet, Hert, Terwangne, Nouwt, p. 133.

242 28.12.2011.

243 „სახელმწიფო ინსპექტორის სამსახურის შესახებ“ საქართველოს კანონი, მ. 13, პ. 1.

244 იქვე, მ. 12, პ. 1.

დაკავშირებული საკითხების განხილვა ინსპექტორის საქმიანობის ქრილშიც.

ინსპექტორის 2015 წლის ანგარიშის მიხედვით იკვეთება ისეთი სირთულეები, როგორიცაა დიდი მოცულობით პერსონალური მონაცემების ფლობა, დისკრიმინაციული მოპყრობის შემთხვევები ნასამართლეობის ან ჯანმრთელობის მდგომარეობის გამო. ამავდროულად, სირთულეები იკვეთება საჯარო უწყებებში, სადაც ხდება პერსონალურ მონაცემთა შემცველი ბაზების მრავალჯერ კოპირება აუცილებლობის გარეშე.<sup>245</sup>

კანონსაწინააღმდეგო დამუშავების შემთხვევები კერძო სექტორშიც გამოვლინდა. მაგალითად, ინსპექტორის მიერ საკითხის შესწავლის შედეგად დადგინდა, რომ სს „კრედიტინფო საქართველო“-ს მონაცემთა ბაზაში (მოცემული ბაზა ახდენს საკრედიტო ისტორიის მქონე ფიზიკური პირების შესახებ მონაცემთა კონსოლიდირებას, ხოლო მასზე წვდომა ხორციელდება სუბიექტის წინასწარი ინფორმირებისა და თანხმობის საფუძველზე) ერთ-ერთი მიკროსაფინანსო ორგანიზაციის მიერ სუბიექტის პერსონალურ მონაცემებზე წვდომა განხორციელდა მისი თანხმობის გარეშე, თანაც მას შემდეგ, რაც საფინანსო ორგანიზაციასა და ფიზიკურ პირს შორის სასესხო ურთიერთობა დასრულებული იყო.<sup>246</sup>

მონაცემთა არამიზნობრივი გამოყენების ფაქტი გამოვლინდა საქართველოს შინაგან საქმეთა სამინისტროს საქმიანობის ფარგლებში. გარემოებათა მიხედვით, უწყებიდან გარეშე პირისთვის გამჟღავნდა კონკრეტული პირის ტელეფონის ნომერი, რომელიც ხელმისაწვდომი გახდა პირის ავტომობილის ნომრის მიხედვით. ამავდროულად, ვის მიმართაც მოხდა ტელეფონის ნომრის გამჟღავნება, იგი არ წარმოადგენდა უწყების თანამშრომელს. რეაგირების ფარგლებში სამინისტროს დაეკისრა ადმინისტრაციული ჯარიმა 2000 ლარის ოდენობით, ხოლო სამინისტროს თანამშრომელს დაეკისრა დისციპლინური პასუხის-

245 პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ, 2015, გვ. 9-10 [<https://www.personaldata.ge>].

246 იქვე, გვ. 12.

მგებლობა.<sup>247</sup> სამინისტრო 2014 წელსაც დაჯარიმდა პერსონალურ მონაცემთა უკანონო დამუშავების გამო. პერსონალური მონაცემების უკანონო გამჟღავნებას ადგილი ჰქონდა საპატრულო პოლიციის მიერ შედგენილი შიდაუწყებრივი ოქმიდან, რასაც წინ უძღოდა ფიზიკური პირის მიერ „112“-ის ცხელ ხაზზე შეტყობინების დატოვება. საქმის გარემოებათა გათვალისწინებით დადგინდა, რომ უწყების მიერ ინფორმაციის გამჟღავნება მოხდა კანონით გათვალისწინებული დამუშავების საფუძველების გარეშე, რის გამოც სამინისტროს დაეკისრა 500 ლარიანი ადმინისტრაციული ჯარიმა.<sup>248</sup>

პერსონალურ მონაცემთა დამუშავების IV პრინციპის დარღვევა (სისწორე, სიზუსტე) დაადგინა ინსპექტორმა, როდესაც საქმის გარემოებების მიხედვით გამოიკვეთა, რომ ფიზიკური პირი არასწორად იმყოფებოდა ნარკოლოგიურ აღრიცხვაზე სსიპ ლ. სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიუროს ბაზაში. მოცემულ ბაზაში პირის შესახებ ინფორმაცია შეიტანება მაშინ, თუ იგი ნარკომანიით დაავადებულია ან ნარკოტიკულ საშუალებებს უნებართვოდ მოიხმარს. ამ შემთხვევაში კი, მოცემულ პირს ექიმის დანიშნულების საფუძველზე ჰქონდა მიღებული ნარკოტიკული საშუალების შემცველი მედიკამენტი, რის გამოც მის შესახებ მონაცემთა ბაზაში ინფორმაციის შენახვა არ იყო თანხვედრაში მონაცემთა სიზუსტისა და სისწორის პრინციპთან. ამ საქმეში კიდევ ერთ დარღვევას ჰქონდა ადგილი, კერძოდ, საქართველოს შინაგან საქმეთა სამინისტროს მიერ ექსპერტიზის ბიუროსთვის ინფორმაციის გაგზავნა, რომელიც მიიღეს ნარკოტექსტის ჩატარების შემდეგ, განხორციელდა კანონიერი საფუძველის გარეშე.<sup>249</sup>

სასამართლოს მიერ გამოტანილი განაჩენის საჯარო ინფორმაციის სახით გაცემის საკითხი იქცა განხილვის საგანი ინსპექტორის მიერ. გარემოებათა მიხედვით ერთ-ერთმა არასამთავრობო ორგანიზაციამ პირის შესახებ სასამართლოდან გამოი-

247 იქვე, გვ. 16.

248 პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, *პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში*, 2014, გვ. 9-10 [<https://www.personaldata.ge>].

249 პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2015, გვ. 18-20.

თხოვა განაჩენის ასლი (სახელის და გვარის მითითებით), რაც დაშტრიხული ფორმით მიეწოდა განმცხადებელს. ინსპექტორის აზრით, მიუხედავად იმისა, რომ პიროვნების ვინაობა არ იყო განაჩენში სრულად მითითებული, მისი ამოცნობა ინიციალების მეშვეობით შესაძლებელი იყო, რის გამოც ადგილი ჰქონდა განსაკუთრებული კატეგორიის ინფორმაციის გამჟღავნებას კანონის წესების დარღვევით.<sup>250</sup> ამ შემთხვევაში, გამოდის, რომ ინფორმაციის გამოთხოვისას განცხადება არ უნდა შეიცავდეს კონკრეტულ იდენტიფიკატორებს - სახელი, გვარი და საქმის ნომერი, ვინაიდან, სასამართლო ამ ინფორმაციის გაცემის შემთხვევაში უკვე გვევლინება დამმუშავებლად, ახორციელებს რა საპასუხო ქმედებას ინფორმაციის მომთხოვნის მიმართ. ეს კი იწვევს პერსონალურ მონაცემთა დამუშავების პრინციპებისა და საფუძვლების დარღვევას იქედან გამომდინარე, რომ მას შემდეგ, რაც სასამართლოს გამოაქვს გადაწყვეტილება, მართლმსაჯულების პროცესი სრულდება, ხოლო ამ მომენტიდან კი გადაწყვეტილებების (განაჩენების) გაცემაზე (დამუშავებაზე) ვრცელდება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი.<sup>251</sup>

ცალკე განხილვის საგანია ინსპექტორის მიერ ჩატარებული შემოწმება სახელმწიფო სერვისების განვითარების სააგენტოში. როგორც ცნობილი გახდა სააგენტოს მონაცემთა ბაზაზე წვდომა 73 სხვადასხვა საჯარო და კერძო ორგანოს გააჩნდა, თუმცა მათ შორის გაფორმებული ხელშეკრულებების თანახმად, ბუნდოვანი იყო ის თუ რა მოვალეობების შესასრულებლად იყო გათვალისწინებული ამგვარი წვდომა. რეაგირების შედეგად არსებული ხელშეკრულებები შესწორებას დაექვემდებარა, ხოლო საქართველოს მთავრობის ადმინისტრაციას, ეკონომიკისა და მდგრადი განვითარების სამინისტროს, სსიპ ფინანსთა სამინისტროს აკადემიას და რეგიონული მართვის-საკითხებში აფხაზეთის ავტონომიური რესპუბლიკის მინისტრის აპარატს მოცემულ ბაზასთან წვდომა შეუწყდათ.<sup>252</sup>

250 იქვე, გვ. 26-27.

251 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 3, პ. 3(„გ“).

252 პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2014, გვ. 16.

საქართველოში აქტუალურია ვიდეოთვალთვალის სისტემის მეშვეობით მონაცემთა დამუშავების საკითხიც. ინსპექტორმა რამდენიმე სააფთიაქო ქსელში არსებული ვიდეოკონტროლისა და აუდიოკონტროლის ერთობლივი სისტემა მომსახურების ხარისხის გაუფობესების მიზნით, უკანონოდ მიიჩნია, ვინაიდან კომუნიკაციის დროს ადგილი ჰქონდა ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გავრცელებას, ეს კი პირად ცხოვრებაში არაპროპორციული ჩარევის სახეობას წარმოადგენს. საკითხის შესწავლის შემდგომ ვიდეო და აუდიოთვალთვალის განმახორციელებელი სააფთიაქო დაწესებულებები დაჯარიმდნენ, ამასთან, მათ დაევალით მოპოვებული მასალის სრულად განადგურება.<sup>253</sup> გარდა ამისა, ვიდეოთვალთვალის სისტემა კანონთან შეუთავსებლად შეფასდა თბილისის მეტროსადგურებშიც, რამდენადაც მათი ვესტიბიულის, ბაქანისა და მიმდებარე ქუჩის ვიდეოტრანსილების ხილვა ვებ-გვერდის საშუალებით ხდებოდა, ზოლო გამოსახულება ხელმისაწვდომი იყო ნებისმიერი დაინტერესებული პირისთვის. საკითხის შესწავლის შედეგად ინსპექტორმა დაადგინა მათი კანონსაწინააღმდეგო ხასიათი, რის გამოც მიმართა ვიდეოტრანსილების განმახორციელებელ კომპანიებს რეკომენდაციით ამგვარი დამუშავების შეწყვეტის მიზნით.<sup>254</sup>

ინსპექტორის მიერ 2016 წელს გამოქვეყნებული ანგარიშის მიხედვით მონაცემთა დაცვის მიმართულებით ტენდენციები კვლავ ყურადღების გამახვილებას საჭიროებს. ანგარიშის მიხედვით, 2015 წელს, პერსონალურ მონაცემთა დაცვის მიმართულებით ერთ-ერთ პრობლემატურ საკითხად მონაცემთა დაცვის პრინციპების დარღვევა სახელდება.<sup>255</sup> მაგალითად, პერსონალურ მონაცემთა დაცვის წესების დარღვევა გამოვლინდა სს „კრედიტინფო საქართველო“-სთან მიმართებით. საყურადღებოა, რომ საკრედიტო მონაცემების ბაზასთან წვდომის რიგი საკითხები, როგორიცაა პირთა/ორგანიზაციათა წრის დადგენა, რომელთაც მხოლოდ შესაბამისი საჭიროების შემთხვევაში შეიძლება ჰქონდეთ მონაცემთა ბაზაზე წვდომის უფლება, განსა-

253 იქვე, გვ. 22.

254 იქვე, გვ. 25.

255 იქვე, გვ. 11.

ზღვრული არაა. ასევე, პრობლემატურ საკითხს წარმოადგენს თავად სს „კრედიტინფო საქართველო“-ს მიერ პერსონალურ მონაცემთა გადაცემამდე, თითოეული მონაცემის დამუშავების (გადაცემის) მართლზომიერების დადგენა.<sup>256</sup> ინსპექტორის მითითებით, საკრედიტო ორგანიზაციებისთვის მნიშვნელოვანია, რომ: 1. პერსონალურ მონაცემთა ბაზაზე წვდომა განხორციელდეს შესაბამისი მიზნისა და სამართლებრივი საფუძვლის არსებობისას; 2. შესაბამისი ორგანიზაციული და ტექნიკური უსაფრთხოების ზომები აუცილებელ პირობას წარმოადგენს არასანქცირებული წვდომის მინიმიზაციისთვის; 3. ამგვარ ბაზებით პერსონალურ მონაცემთა სარგებლობის საკითხი უნდა გაიწეროს ნორმატიულად, შესაბამისი კანონმდებლობით.<sup>257</sup>

ინსპექტორის ყურადღების ქვეშ მოექცა შრომითი ბაზარიც. ანგარიშის თანახმად, კერძო ორგანიზაციების შემოწმებისას გამოიკვეთა, რომ დანესებულებები განუსაზღვრელი ვადით ინახავდნენ იმგვარ ინფორმაციას, რომლის დამუშავების მიზანიც აღარ არსებობდა, მაგალითისთვის, ესენია კანდიდატთა რეზუმეები, მათი ოჯახის წევრების შესახებ არსებული ინფორმაცია, ტესტირების შედეგები. ასევე, სუბიექტის მიმართვის საფუძველზე გამოიკვეთა, რომ მის დამსაქმებელს (კომპანიას) არ ჰქონდა განსაზღვრული დასაქმებულთა სარგებლობაში არსებული კომუნიკაციის საშუალებების მონიტორინგის პირობები, რაც იწვევდა არამართლზომიერი (პროპორციულობის პრინციპთან შეუთავსებელი) დამუშავების რისკებს. ამ მიმართულებით მნიშვნელოვანია, რომ დადგინდეს მკაფიო ინსტრუქციები კომუნიკაციის საშუალებების გამოყენებისთვის, მონიტორინგის შესახებ მოხდეს მომუშავეთა წინასწარი გაფრთხილება და ამგვარი პროცედურა (მონიტორინგი) განხორციელდეს მხოლოდ უკიდურესი აუცილებლობისას.<sup>258</sup>

საქართველოში, ისევე, როგორც სხვა ქვეყნებში, სადაც აქტიურად ხდება ინტერნეტსა და ვებ-ზე დაფუძნებული სისტემების გამოყენება, აქტუალურია ციფრულ სივრცეში პერსონალურ მონაცემთა დაცვის საკითხი. ადგილი ჰქონდა საქართვე-

256 იქვე, გვ. 15.

257 იქვე, გვ. 16-17.

258 იქვე, გვ. 30-32.

ლოს ადვოკატთა ასოციაციის მიერ პერსონალურ მონაცემთა განთავსების (დამუშავების) წესების დარღვევას, კერძოდ, ორგანიზაციის ვებ-გვერდზე ადვოკატთა დისციპლინური პასუხისმგებლობის დაკისრების შესახებ გადანყვეტილებები არ ნაიშალა მაშინაც კი, როდესაც აღნიშნული სახდელები უკვე გაქარწყლებული იყო. შესაბამისად, ინსპექტორის გადანყვეტილებით ადგილი პქონდა კანონით დადგენილ მოთხოვნებთან შეუთავსებლობას, კერძოდ, შესაბამისი ვადით დამუშავების პრინციპის დარღვევას, რის შედეგადაც ასოციაციას დაევალა დეტალურად დაედგინა ვებ-გვერდზე აღნიშნული მონაცემების განთავსების წესები.<sup>259</sup>

პერსონალური მონაცემებისა და საზოგადოებრივ უსაფრთხოებას შორის ბალანსს ეხება ინსპექტორის ერთ-ერთი გადანყვეტილება, რომლითაც ამ უკანასკნელმა საქართველოს შინაგან საქმეთა სამინისტრო ცნო სამართალდამრღვევად. საქმის გარემოებების მიხედვით, სამინისტრომ საკუთარ ოფიციალურ ვებ-გვერდზე განათავსა დაკავებული პირის ვიდეოკადრები, რის მიხედვითაც შესაძლებელი იყო მისი პირდაპირი იდენტიფიცირება. სამინისტროს მტკიცების თანახმად, ამგვარი მიდგომა ემსახურებოდა საზოგადოებრივი უსაფრთხოების დაცვის ინტერესებს, ასევე, მოსალოდნელი უარყოფითი შედეგების პრევენციას. ინსპექტორის აზრით, მოცემულ შემთხვევაში პირის დაკავებით უკვე მოხდა სავარაუდო, შესაძლო უარყოფითი შედეგების განეიტრალება, რის გამოც აღარ არსებობდა საზოგადოებრივი უსაფრთხოების ან სხვა აღმატებული სიკეთეების დაცვის აუცილებლობა. ამ მიდგომის გათვალისწინებით, სამინისტრო ცნობილ იქნა სამართალდამრღვევად კანონით დადგენილი პრინციპებისა და საფუძვლების გარეშე პერსონალურ მონაცემთა დამუშავებისთვის.<sup>260</sup>

პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშში, ასევე, აქტუალურია სენსიტიური (განსაკუთრებული) კატეგორიის პერსონალურ მონაცემთა დამუშავების საკითხიც. ერთ-ერთი საჯარო სკოლის დირექტორმა, საკუთარი სკოლის მოსწავლეების ჯანმრთელობის დაცვისა და დამატებითი ინფორმაციის მიღების მიზნით, სკოლაში მობილობით გადმოსული მოსწავლეების ჯანმრთელობის მდგომარეობის შესახებ

259 იქვე, გვ. 42-43.

260 იქვე, გვ. 44-45.

ცნობები გადაამოწმებინა ერთ-ერთი საავადმყოფოს მკურნალ ექიმს, ასევე, საკითხი განიხილა მშობელთა კრებაზე. განხილვის შემდგომ დადგინდა, რომ ამ მოსწავლეების დაშვება სასწავლო პროცესში შესაძლებელი იყო, რამდენადაც ისინი არ უქმნიდნენ საფრთხეს სხვა მოსწავლეთა ჯანმრთელობას. ინსპექტორმა დაადგინა, რომ პირველ შემთხვევაში, სკოლის დირექტორი მოქმედებდა შესაბამისი ლეგიტიმური მიზნის ფარგლებში, კერძოდ, როდესაც სხვა მოსწავლეთა ჯანმრთელობის დაცვის მიზნით გადაწყვიტა შესაბამისი ინფორმაციის მიღება. თუმცა, ის ფაქტი, რომ ეს ინფორმაცია გამჟღავნებული იყო მესამე პირთათვის, უკვე აღარ იყო თავსებადი პერსონალურ მონაცემთა დაცვის შესახებ კანონით დადგენილ მოთხოვნასთან, რის მიხედვითაც პერსონალურ მონაცემთა სუბიექტის თანხმობის გარეშე დაუშვებელია განსაკუთრებული კატეგორიის პერსონალური მონაცემის გადაცემა მესამე პირისთვის.<sup>261</sup>

პერსონალურ მონაცემთა დაცვის კუთხით, ასევე, აქტუალური იყო ვიდეოთვალთვალის მართლზომიერი განხორციელების საკითხიც. ერთ-ერთი შემთხვევის შედეგად დადგინდა, რომ ავტოგასამართ სადგურებზე, გარდა კანონით ნებადართული მიზნებისა, ვიდეოთვალთვალის მეშვეობით ხორციელდებოდა მომსახურების სერვისის კონტროლიც. მონიტორინგის ამგვარი პროცედურა ჩაითვალა კანონთან შეუთავსებლად, ვინაიდან, ამ გზით დამმუშავებელი გასცდა კანონით მინიჭებულ უფლებამოსილებას - ეწარმოებინა ვიდეოთვალთვალის მხოლოდ კანონით ნებადართული წინაპირობების არსებობისას.<sup>262</sup> აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის შესახებ კანონის თანახმად „საჯარო და კერძო დაწესებულებებს შესაბამისი მონიტორინგის განხორციელების მიზნით შეუძლიათ განახორციელონ თავიანთი შენობების ვიდეოთვალთვალის, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვნის მავნე ზეგავლენისგან დაცვისა და საიდუმლო ინფორმაციის დაცვის მიზნებისთვის.“<sup>263</sup> ამდენად, ნებისმიერი სხვა მიზნით ვიდეოთვალთვალის განხორციელება უნდა ჩაითვალოს კანონით

261 იქვე, გვ. 52-54; ასევე, იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 6, პ. 3.

262 იქვე, გვ. 84-85.

263 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 12, პ. 1.

დადგენილი მოთხოვნების დარღვევად.<sup>264</sup> პერსონალურ მონაცემთა დაცვის ინსპექტორი ამ მიდგომას, ასევე, განამტკიცებს შესაბამის დოკუმენტში - რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ.

აღსანიშნავია, რომ არამიზნობრივ მონაცემთა დამუშავებას 2018 წელსაც ჰქონდა ადგილი საჯარო უწყებებში, სადაც ხდებოდა არასამსახურებრივი მიზნით მონაცემთა წვდომისა და, ზოგადად, კონფიდენციალობის ხელყოფა. ამ მიმართულებით, დისციპლინური რეაგირებების მიუხედავად, სახელმწიფო ინსპექტორი აღნიშნავს, რომ მნიშვნელოვანია შიდა კონტროლის სათანადო მექანიზმების დანერგვა.<sup>265</sup> ასევე, ადგილი ჰქონდა არასრულწლოვანთა პერსონალური მონაცემების უკანონო დამუშავებას, რაც შესწავლილ იქნა ინსპექტორის მიერ და გამოვლინდა არაერთი დარღვევა.<sup>266</sup> საკითხის აქტუალობიდან გამომდინარე, ამავე ანგარიშში ინსპექტორი განიხილავს ამომრჩეველთა პერსონალური მონაცემების დამუშავების საკითხს საარჩევნო პროცესის მიმდინარეობისას და უთითებს, რომ მონაცემთა დაცვის სტანდარტებისა და უსაფრთხოების ზომების მიღება მნიშვნელოვანია სუბიექტის უფლებათა დაცულობისთვის,<sup>267</sup> თუმცა ღიად არის დატოვებული ამომრჩეველთა ერთიანი სიის საჯარო ხელმისაწვდომობის საკითხი პროპორციული დამუშავების ჭრილში და არაა მოცემული მსჯელობა არსებული პრაქტიკის კანონთან თავსებადობის მხრივ. ანგარიშში, დამატებით, ყურადღება არის გამახვილებული პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავების კანონიერებაზე, კერძოდ, სისტემური დარღვევები გამოვლინდა მონაცემთა დამუშავებელსა და უფლებამოსილ პირს შორის დადებულ ხელშეკრულებებში, სადაც არ იყო გათვალისწინებული მონაცემთა სუბიექტისთვის უარის თქმის მექანიზმები, დამუშავების შეწყვეტის მოთხოვნის შემთხვევაში შესაბამისი რეაგირების მეთოდები, ხელშეკრულე-

264 პერსონალურ მონაცემთა დაცვის ინსპექტორი, *რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ*, გვ. 4.

265 პერსონალურ მონაცემთა დაცვის ინსპექტორი, *ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ (2018)*, 2019, გვ. 27.

266 იქვე, გვ. 37.

267 იქვე, გვ. 52.

ბით გათვალისწინებული პირობების შესრულების შემდეგ უფლებამოსილი პირის მიერ მონაცემთა დამუშავებისთვის გადაცემის ვალდებულება და ა.შ.<sup>268</sup> მთლიანობაში, ანგარიშის მიხედვით შეინიშნება მონაცემთა დაცვის მიმართ საზოგადოების ცნობიერების მატება, მათ შორის, ინსპექტორისთვის მიმართვიანობის რაოდენობა, მიუხედავად ამისა, წინა წლებში არსებული გამოწვევები კვლავ არ არის ბოლომდე აღმოფხვრილი.

პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ თავისი უფლებამოსილებების განხორციელების პარალელურად რიგი საკითხები კვლავ გამოწვევად რჩება, რაც ამ სფეროში ქმნის სირთულეებს და უფლების დაცვას ნაკლებად გარანტირებულს ხდის. მაგალითად, 2016 წლის მინურულს, ევროპის საბჭოს წინაშე წარდგენილ ანგარიშში საქართველოში პერსონალურ მონაცემთა დაცვის სისტემის შესახებ, ინსპექტორის აპარატი მთავარ გამოწვევებათა შორის უთითებს საზოგადოებაში ცნობიერების ნაკლებობას, ადამიანური რესურსების სიმცირესა და სასამართლო გადანყვეტილებების ნაკლებობას.<sup>269</sup>

ყველაზე მეტად, საყურადღებოა სასამართლო გადანყვეტილებებთან დაკავშირებული გამოწვევა. ამ შემთხვევაში, ყურადღებას იპყრობს წესი, რომლის მიხედვითაც სახელმწიფო ინსპექტორის სამსახურის მიერ ადმინისტრაციული სახდელის (ჯარიმის) დაკისრების შესახებ გადანყვეტილება არ საჩივრდება საკასაციო ინსტანციის სასამართლოში. აღნიშნული პერსონალურ მონაცემთა დაცვის სფეროს განვითარებისთვის შემაფერხებელ ფაქტორს წარმოადგენს. მონაცემთა დამუშავებასთან დაკავშირებული სამართლებრივი ურთიერთობების ნორმატიული მოწესრიგება საქართველოში სიახლეა. ამდენად, აუცილებელია რაც შეიძლება მოკლე ვადებში ჩამოყალიბდეს პრაქტიკა. ერთი მხრივ, პრაქტიკის ჩამოყალიბებაში აქტიურ როლს თამაშობს სახელმწიფო ინსპექტორის სამსახური, თუმცა, გამომდინარე იქედან, რომ სასამართლო გადანყვეტილებებით ხდება ნორმათა ანალიზი და ვითარდება სამართალი, აუცილებელია არსე-

268 იქვე, გვ. 101.

269 პერსონალურ მონაცემთა დაცვის ინსპექტორი, *პერსონალურ მონაცემთა დაცვის სისტემა საქართველოში*, 2016, გვ. 26 [<https://rm.coe.int/16806cead9>].

ბობდეს საკასაციო ინსტანციის სასამართლოს პრაქტიკა პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საქმეებზე.

საყურადღებოა, რომ ქვემოდმოყვანილი გადანყვეტილებებიდან საქალაქო სასამართლომ არც ერთ შემთხვევაში არ დააკმაყოფილა მოსარჩელის მოთხოვნა ჯარიმის შესახებ პერსონალურ მონაცემთა დაცვის ინსპექტორის გადანყვეტილების გაუქმების თაობაზე. ამდენად, სასამართლომ გაიზიარა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ ჩამოყალიბებული სამართლებრივი არგუმენტაცია.

გადანყვეტილებებიდან აღსანიშნავია თბილისის საქალაქო სასამართლოს მიერ გამოტანილი დადგენილება საქმეზე საქართველოს მთავარი პროკურატურა პერსონალურ მონაცემთა დაცვის ინსპექტორის წინააღმდეგ,<sup>270</sup> სადაც პროკურატურის საჩივარი არ დაკმაყოფილდა. საქმის გარემოებათა მიხედვით 2014 წლის 13 აგვისტოს პროკურატურის ოფიციალურ ვებგვერდზე გამოქვეყნდა პიროვნების ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია. უნების განმარტებით ამგვარი ინფორმაციის გამოქვეყნების მიზანი იყო კონკრეტული დანაშაულის შესახებ საზოგადოების ინფორმირება ამ უკანასკნელის ინტერესებიდან გამომდინარე. თუმცა, სასამართლომ არ გაიზიარა ეს არგუმენტი იმ საფუძველით, რომ ინფორმაციის ვებგვერდზე გამოქვეყნება სცდება დანაშაულის გამოძიების მიზნებს, ხოლო ჯანმრთელობის მდგომარეობა განეკუთვნება განსაკუთრებული კატეგორიის მონაცემებს, რომელთა დამუშავება შესაძლებელია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-6 მუხლით დადგენილ შემთხვევებში და ამავე კანონის მე-4 მუხლით განსაზღვრული პრინციპების დაცვით. კანონის მე-6 მუხლში კი, განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავების საფუძველად საზოგადოებრივი ინტერესის მიზნები არ არის მითითებული. ამდენად, სასამართლომ არ დააკმაყოფილა საქართველოს მთავარი პროკურატურის საჩივარი გადანყვეტილების (ჯარიმის) გაუქმების შესახებ

კერძო პირის საჩივარი განიხილა სასამართლომ საქმეში შპს „X“ პერსონალურ მონაცემთა დაცვის ინსპექტორის წინააღმ-

<sup>270</sup> საქმე 4/6516-14, 27.10.2014.

დეგ.<sup>271</sup> საქმის გარემოებათა მიხედვით შპს-მ განმცხადებლის სასესხო დავალიანების შესახებ ინფორმაცია გასცა მესამე პირებზე, ისე, რომ ამის სამართლებრივი საფუძველი არ გააჩნდა. ამავდროულად შპს-მ (გამსესხებელმა) ვერ დაასაბუთა თუ რისთვის სჭირდებოდა და რატომ იყო აუცილებელი მესამე პირებთან დაკავშირება იმ პირობებში, როდესაც იგი სისტემატურად უკავშირდებოდა თავად განმცხადებელს და მის მიერ სესხის ხელშეკრულებაში მითითებულ საკონტაქტო პირს. ამდენად, სასამართლომ დაადგინა, რომ დამმუშავებელი (შპს) ინფორმაციის გასაჯაროებისას არ მოქმედებდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი დამუშავების რომელიმე საფუძველით.

პერსონალურ მონაცემთა არასამართლობრივი დამუშავების ფაქტი დადგინდა საქმეში შპს „Y“ პერსონალურ მონაცემთა დაცვის ინსპექტორის წინააღმდეგ.<sup>272</sup> შპს, რომელიც წარმოადგენდა პრობლემური აქტივების მართვის კომპანიას, სესხის ამოღების მიზნით დაუკავშირდა მოვალის ძმას, თუმცა ამ უკანასკნელის შესახებ ინფორმაცია სესხის ხელშეკრულების გაფორმების დროს მსესხებლის მიერ არ ყოფილა მიწოდებული იქედან გამომდინარე, რომ სესხის განაცხადის შევსებისას ასეთი ველი არ ივსებოდა. მოცემულ საქმეზე სასამართლომ გაიზიარა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიდგომა შპს-ს მიერ მთელი რიგი სამართლებრივი ნორმების უგულვებელყოფის თაობაზე და მიუთითა, რომ დარღვეულ იქნა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4, მე-5, ასევე, მე-16 მუხლი (უფლებამოსილი პირის ვალდებულება იმოქმედოს დამმუშავებლის მიერ მისთვის დადგენილ ფარგლებში), უფრო კონკრეტულად, კომპანიამ ვერ უზრუნველყო პერსონალურ მონაცემთა დამუშავება პროპორციულობის პრინციპის დაცვით, გარდა ამისა, მას არ ჰქონდა საფუძველი დამუშავებისთვის, მთლიანობაში კი, მან არ იმოქმედა დამმუშავებელთან დადებული ხელშეკრულების ფარგლებში.

პერსონალურ მონაცემთა დამუშავება კანონით გათვალისწინებული საფუძვლის გარეშე დაადგინა სასამართლომ საქმეში

271 საქმე 4/-----17, 10.07.2017.

272 საქმე 4/-----16, 30.10.2017.

შპს „Z“ პერსონალურ მონაცემთა დაცვის ინსპექტორის წინააღმდეგ.<sup>273</sup> საქმის გარემოებათა მიხედვით, შპს-ს, რომელიც იყო პრობლემური აქტივების მართვის კომპანია, გაფორმებული ჰქონდა ხელშეკრულებები სხვადასხვა ორგანიზაციებთან, რის საფუძველზეც იგი ახდენდა სასესიო დავალიანების ამოღებას იმ შემთხვევაში, თუ სესხის გამცემი კომპანია მიიღებდა შესაბამის დავალებას. მას შემდეგ, რაც პრობლემური აქტივების მართვის კომპანია ვერ დაუკავშირდა ერთ-ერთ მსესხებელს, დაამყარა კომუნიკაცია მესამე პირთან იმ მიზნით, რომ ამ უკანასკნელს გადაეცა ინფორმაცია მსესხებლისთვის, რათა, თავის მხრივ, მსესხებელი დაკავშირებოდა კომპანიას. სასამართლოს აზრით პერსონალურ მონაცემთა გადაცემა მესამე პირისთვის არ იყო გამართლებული, ვინაიდან სახეზე არ იყო დამმუშავებლის ან უფლებამოსილი პირის აღმატებული ინტერესის დაკმაყოფილების საფუძველი. გადაწყვეტილების უცვლელად დატოვების ძირითადი არგუმენტი იყო ის, რომ პრობლემური აქტივების მართვის კომპანიამ არ გამოიყენა ყველა საშუალება სუბიექტთან (მსესხებელთან) დაკავშირებისთვის. ამდენად, პერსონალურ მონაცემთა გასაჯაროება (დამუშავება) ჩაითვალა არაპროპორციულად, რასაც შედეგად მოჰყვა ის, რომ შპს-მ იმოქმედა მასსა და სასესიო კომპანიას შორის დადებული ხელშეკრულების დებულებათა დარღვევით.

### **2.3.3. 2017 წლის 13 ოქტომბრის კონსტიტუციური ცვლილებები - გარანტია პერსონალურ მონაცემთა დაცვისთვის?**

პირველ რიგში, ზოგადად კონსტიტუციური კანონის არსებული რედაქციით, მნიშვნელოვნად იცვლება სხვადასხვა სამართლებრივი საკითხის ფორმულირება, მათ შორის, ის თავიც, რომელიც ეხება ადამიანის ძირითად უფლებებს.

საყურადღებოა, რომ ახალი კანონპროექტით გაჩნდა „პირადი სივრცის“ ცნება და კანონის მე-15 მუხლი დასათაურებულია როგორც „პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობისა და ინფორმაციული თვითგამორკვევის უფლებები.“ ახლებური მონესრიგება არსე-

273 საქმე 4/45-----, 06.10.2017.

ბულისგან განსხვავდება ცნებათა ფორმულირებითა და სტრუქტურით. თვალსაჩინოა, რომ კანონმდებელმა ამჯერადაც უარი თქვა პერსონალურ მონაცემთა დაცვის უფლების დამოუკიდებელ რეგულირებაზე.

კონსტიტუციური კანონის ინიცირებული ვერსიის მე-15 მუხლი განსხვავებულია იმ ვერსიისგან, რომელიც არის მიღებული. თავდაპირველად ცნებები „პირადი და ოჯახური ცხოვრება“ არ ფიგურირებდა კანონპროექტში. ნახსენები იყო მხოლოდ „პირადი სივრცე.“ კონსტიტუციური კანონპროექტის ინიცირებული ვერსიის განმარტებით ბარათში კანონმდებელი მიუთითებდა, რომ მთავარი მიზეზი თუ რატომაც ფორმულირება „პირადი ცხოვრების უფლება“ ამოიღეს იყო ის, რომ პირადი ცხოვრება დაცული იქნებოდა პიროვნების თავისუფალი განვითარების უფლებით, რაც პროექტის თანახმად მე-12 მუხლით არის დადგენილი. ამასთან, განმარტებითი ბარათი უთითებდა, რომ „პირადი სივრცე და კომუნიკაცია სრულად მოიცავს ადამიანის თავისუფლების იმ ასპექტებს, რომელიც საჭიროებს დაცვას კონსტიტუციის მოცემული მუხლით.“<sup>274</sup> ამ მოცემულობით, კანონმდებელმა, ერთი შეხედვით, გამიჯნა პირადი ცხოვრების, პირადი სივრცისა და კომუნიკაციის უფლებები ერთმანეთისგან.

პირადი სივრცის ცალსახა განმარტება არ არსებობს. შესაბამისად, არც ის შეგვიძლია ვთქვათ თუ რა განმასხვავებელი ნიშნები ახასიათებს მას „პირადი ცხოვრების“ ფორმულირებით მოცემული შინაარსისგან. ადამიანის უფლებათა ევროპული კონვენციის მიხედვით, პირადი სფერო შედგება ოთხი ძირითადი ელემენტისგან: ადამიანის პირადი ცხოვრება, ოჯახური ცხოვრება, საცხოვრისი და კორესპოდენცია, ამასთან, ეს სფეროები არ არიან ურთიერთგამომრიცხავნი. ადამიანის უფლებათა ევროპული სასამართლო არ აკეთებს რომელიმე მათგანის ფარგლების ამომწურავ ინტერპრეტაციას და მოქნილია თავის მიდგომაში. ეს საშუალებას იძლევა ეს ელემენტები განიმარტოს ისე, რომ გათვალისწინებულ იქნეს სოციოლოგიური, სამართლებრივი და ტექნოლოგიური პროგნოზით გამოწვეული საკითხე-

274 საქართველოს პარლამენტი, განმარტებითი ბარათი საქართველოს კონსტიტუციური კანონზე „საქართველოს კონსტიტუციაში ცვლილებების შეტანის შესახებ“, პ. „ა.გ.“ (მე-15 მუხლი) [<https://www.parliament.ge/>].

პირად სფეროსთან დაკავშირებული საკითხები ფართო დიაპაზონის შემცველია, მასში მოიაზრება უკიდურესად პირადი საკითხები, ასევე, საზოგადო მოვლენებიც. საქმეში *Bruggemann and Scheuten v. Federal Republic of Germany* (1981) აღინიშნა, რომ პირადი სფეროს დაცვის უფლება უზრუნველყოფს ინდივიდისთვის შესაძლებლობას, რითაც მას თავისუფლად შეუძლია საკუთარი თავის თავისუფალი განვითარება და მოიცავს სქესობრივ (ინტიმურ) ცხოვრებასთან დაკავშირებულ საკითხებსაც.<sup>275</sup> მეორე მხრივ, პირადი სფეროს განვრცობილი ინტერპრეტაცია სასამართლომ ჩამოაყალიბა საქმეში *Moreno Gomez v. Spain* (2005). გარემოებათა მიხედვით განმცხადებლის საცხოვრისთან არსებული ხმაური მას არ აძლევდა მშვიდი ძილის საშუალებას. სასამართლომ დაადგინა, რომ შესაბამისმა მუნიციპალიტეტმა არ აღკვეთა აღნიშნული ვითარება და, ამდენად, სახელმწიფომ ვერ უზრუნველყო განმცხადებლის პირადი სფეროს დაცვა. ამით სახელმწიფომ არ შეასრულა პოზიტიური ვალდებულება. აღსანიშნავია, რომ ასეთ შემთხვევებში, პირის პირად სფეროზე გავლენას ნეგატიური ხასიათი ექნება მაშინ თუ, მაგალითად, განმცხადებლს საკუთარი საცხოვრებელი მიდამოს ფარგლებში მიაღება სერიოზული ზიანი.<sup>277</sup>

გამომდინარე იქედან, რომ პირადი სივრცე ფართო ცნებაა, მასში ჩარევის საფუძვლები აუცილებლად უნდა პასუხობდეს ადამიანის უფლებათა ევროპული კონვენციით დადგენილ მოთხოვნებს, კერძოდ, ამ უფლების შეზღუდვისთვის უნდა არსებობდეს მართლზომიერი საფუძველი, შეზღუდვას უნდა ჰქონდეს კანონიერი მიზანი და უფლების შეზღუდვა აუცილებელი უნდა იყოს დემოკრატიულ საზოგადოებაში. გარდა ამისა, თითოეული საფუძველი უნდა აკმაყოფილებდეს კონკრეტულ მოთხოვნებსაც. მართლზომიერ საფუძველში უნდა მოვიზროთ კანონი (ნორმატიული აქტი), რომელიც არის ყველასათვის ხელ-

275 Roagna I., *Protecting the right to respect for private and family life under the European Convention on Human Rights*. Strasbourg: Council of Europe Human Rights Handbooks, Council of Europe, 2012, p. 10.

276 იქვე, გვ. 16.

277 იქვე, გვ. 79-80.

მისანვდომი და განჭვრეტადი.<sup>278</sup> მიზანს უნდა წარმოადგენდეს ჩამოთვლილთაგან ერთ-ერთი მაინც: ეროვნული უშიშროება, საზოგადოებრივი უსაფრთხოება, ქვეყნის ეკონომიკური ინტერესები, უნესრიგობის ან დანაშაულის თავიდან აცილება, ჯანმრთელობის, მორალის ან სხვათა უფლებებისა და თავისუფლებების დაცვა. უფლების შეზღუდვის აუცილებლობა დემოკრატიულ საზოგადოებაში უნდა იყოს გამოწვეული მწვავე საზოგადოებრივი საჭიროებით, რაც თანაზომიერების პრინციპის საფუძველზე უნდა გადაწყდეს. ამდენად, სახელმწიფოს მიერ გატარებული ღონისძიება ძირითადი უფლების შეზღუდვის ნაწილში უნდა გამომდინარეობდეს მომეტებული საზოგადოებრივი საჭიროებიდან.<sup>279</sup> ამდენად, საინტერესო იქნება ის განმარტებები, რასაც შემოგვთავაზებენ საერთო სასამართლოები და საკონსტიტუციო სასამართლო. სასურველია, პირადი სივრცის ფორმულირებას ისეთივე განმარტება მიეცეს, როგორიც დადგენილია ადამიანის უფლებათა ევროპული სასამართლოს მიერ პირად სფეროსთან დაკავშირებით.

ამდენად, ახლებური რედაქციით პერსონალური მონაცემების დაცვის უფლება ინდივიდს გარანტირებული აქვს, როგორც პიროვნების თავისუფალი განვითარების უფლებით, ისე პირადი და ოჯახური ცხოვრების ხელშეუხებლობის, ასევე, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებით. თუმცა, ეს არ გამოირიცხავს პერსონალურ მონაცემთა დაცვისთვის განსაკუთრებული სამართლებრივი რეჟიმის დანესების აუცილებლობას, რამდენადაც კონსტიტუციის ახალი რედაქციით კანონმდებელი მხოლოდ აფართოებს პირადი ცხოვრების ცნებას, ზრდის დაცული სფეროს ფარგლებს, სადაც, რა თქმა უნდა, მოიაზრება უფლება პერსონალურ მონაცემთა დაცვაზე, თუმცა მას განსაკუთრებული ადგილი მაინც არ ეთმობა.

278 ბოხაშვილი, კორკელია, გვ. 27-28.

279 იქვე, გვ. 31-33.

# თავი III. პერსონალურ მონაცემთა დაცვის, როგორც ძირითადი უფლების კონსტიტუციით დამოუკიდებლად მონესრიგების მიზანშეწონილობა

## 3.1. ტექნოლოგიური პროგრესის გავლენის ზოგადი თავისებურებები პერსონალურ მონაცემთა დაცვაზე

შინაარსობრივად პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებები ერთმანეთთან დაკავშირებულია. თუმცა, თუ ამ საკითხს მიუვდგებით ინდივიდის დაცვის პერსპექტივიდან, მიიჩნევა, რომ ის ინტერესები, რაც გვევლინება პერსონალურ მონაცემთა დაცვის უფლების ქვეშ არ უნდა განიხილებოდეს პირადი ცხოვრების უფლების ნაწილად. სხვა სიტყვებით, პრივატულობა (privacy) არის წმინდად „დაცვითი“ უფლება, რომელიც იცავს პირის პირად სფეროს ინტერვენციისგან. შესაბამისად, პირადი ცხოვრების დამცავი ბერკეტები ვერ გვთავაზობენ ბერკეტებს პერსონალურ მონაცემთა დაცვისთვის, ვინაიდან ამ უკანასკნელს უფრო „ღია“ ხასიათი აქვს. ნაცვლად აკრძალვისა, იგი აწესებს გარკვეულ პირობებს პერსონალური მონაცემების გამოყენებისთვის.<sup>280</sup> აქედან გამომდინარე, არ არსებობს შეჯერებული აზრი იმის შესახებ, თუ რა სახის ურთიერთმიმართება არსებობს პერსონალურ მონაცემთა დაცვასა და პრივატულობას შორის.<sup>281</sup>

ზოგადად, პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებას დაცვის განსხვავებული წინაპირობები და ტრადიციები გააჩნიათ. უფლება პერსონალურ მონაცემთა დაცვაზე მეტად ახალია და დაკავშირებულია ტექნოლოგიურ განვითარებასთან, რომლის შედეგადაც მათი შეგროვება, შენახვა და დამუშავება უფრო და უფრო მარტივი ხდება. გარდა ამისა, არსებობს მოსაზრება, რომ უფლება პერსონალურ მონაცემთა დაცვაზე უმეტესად ორიენტირებულია პორიზონტალური ტიპის ურთიერთობებზე და სუბიექტს იცავს ისეთი დამმუშავებლებისგან, როგორიცაა მაგალითად Google და Facebook. საყურადღებოა თავად ცნებაც, „პერსონალური მონაცემი“ არ

280 Purtova, p. 2.

281 იქვე, გვ. 3.

არის პირადი ან სენსიტიური ინფორმაციის ანალოგი, არამედ ძალზედ ფართოა. იგი მოიცავს, მათ შორის, საჯაროდ ცნობილ ინფორმაციას, რომლის მიხედვითაც შესაძლებელია პირის იდენტიფიცირება.<sup>282</sup> გარდა კერძო დაწესებულებებისა, პერსონალურ მონაცემთა საკმაოდ მსხვილ დამმუშავებლებად სახელმწიფო ორგანოები გვევლინებიან. სახელმწიფოს მიერ იდენტიფიცირების მექანიზმების გამოყენება ნახალისებულია საჯარო დაწესებულებების საქმიანობის კონტექსტში. ამ მიზნით, ხელისუფლებისთვის ხელსაყრელია განვითარებული ტექნოლოგიების დანერგვა, ხოლო ამ განვითარების პარალელურად ჩნდება ციფრული იდენტიფიცირების მართვის მოთხოვნა, რომელიც უნდა დაექვემდებაროს სამართლებრივ ჩარჩოებს და მომხმარებლის უფლებებზე იყოს ორიენტირებული.<sup>283</sup>

თანამედროვე საზოგადოებრივი ურთიერთობების გათვალისწინებით, პერსონალური მონაცემი არა მხოლოდ ინფორმაციული კატეგორიის ჭრილში არსებულ საგნად გვევლინება, არამედ იგი სავაჭრო გარიგების ობიექტსაც კი წარმოადგენს. პერსონალური ინფორმაცია, როგორც ადამიანური არსების გარდაუვალი „პროდუქტი“ გამუდმებული დაკვირვების პირობებში ქმნის ინფორმაციის დიდ ერთობას, რომელიც შემდგომ ხელმისაწვდომია შეგროვებისთვის, შენახვისთვის, გამოყენებისა და გავრცელებისთვის, როგორც ღირებული საქონელი.<sup>284</sup> პერსონალური მონაცემებით ვაჭრობა მრავალი კორპორაციისა და კომპანიის საქმიანობის ნაწილს წარმოადგენს. მას შემდეგ, რაც პერსონალური მონაცემი ხდება ვაჭრობის საგანი, თავს იჩენს ისეთი საკითხი, როგორიცაა ამ ვაჭრობის შეზღუდვა. აქ შემთხვევაში მეცნიერთა აზრი ორად იყოფა, რომელთაგან ზოგიერთი მსგავსი პრაქტიკის ჩამოყალიბების მომხრეა, ხოლო ზოგი, მიიჩნევს, რომ აუცილებელია დანესდეს მკაცრი შეზღუდვები.<sup>285</sup> საქართველოში პერსონალური მონაცემებით ვაჭრობა საკმაოდ აქტიურ ფაზაშია. ამასთან, პერსონალურ მონაცემთა

282 Sloot B.V.D., *Privacy as Personality Right: Why the ECtHR's Focus on Ultimate Interests Might Prove Indispensable in the Age of "Big Data"*. *Utrecht Journal of International and European Law*, 31 (80), 2015, p. 40.

283 Hert, 2008, p. 72.

284 Holland, p. 895.

285 Schwartz, p. 2057.

დაცვის ქართული სტანდარტი არ უშვებს იმის შესაძლებლობას, რომ პერსონალური ინფორმაცია დაექვემდებაროს „ყიდვა-გაყიდვას.“ მაგალითად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს „ჯანონის თანახმად,<sup>286</sup> პირდაპირი მარკეტინგული შეტყობინებების<sup>287</sup> განხორციელებისთვის, ტელეფონის ნომრის გამოყენებამდე; აუცილებელია დავრწმუნდეთ, რომ ეს ნომერი საჯარო წყაროდან იქნა მოპოვებული ან სუბიექტმა (ფიზიკურმა პირმა) განაცხადა თანხმობა მის გამოყენებაზე. არაა გამორიცხული, რომ ფიზიკურმა პირმა თანხმობა გასცეს მისი ტელეფონის ნომრის გასხვისების თაობაზე. თუმცა, სირთულე იჩენს თავს მაშინ, როდესაც ფიზიკური პირი გადაწყვეტს მისი პერსონალური მონაცემის გამოთხოვას ყველა იმ დამმუშავებლისგან, რომელიც იყენებს ამ ინფორმაციას.<sup>287</sup>

დამუშავების პროცესის პრობლემატურ მხარეს წარმოადგენს პერსონალური მონაცემების შეგროვება ქსელური მეთოდების გამოყენებით, როგორიცაა “spyware” და “adware.” ქსელში ჩართული კომპიუტერული კომუნიკაციის ფარგლებში, პროგრამებს მრავალ სხვა კომპიუტერთან შეუძლიათ დაკავშირება. მაგალითად “spyware” განმარტებულია, როგორც პროგრამა, რომელიც ინსტალირდება მომხმარებლის ნების გარეშე და უნებართვოდ ერთება მოქმედებაში. მისი ერთ-ერთი ფუნქციაა კომპიუტერული რესურსების გამოყენება სხვადასხვა მიზნებისთვის, მათ შორის, პერსონალური ინფორმაციის შეგროვებისთვის (ინტერნეტში მომხმარებლის პრეფერენციებისა და ინტერესთა სფეროს მიხედვით) და მის საფუძველზე მომხმარებლისთვის სარეკლამო შეტყობინებების გაგზავნისა და მიწოდებისთვის.<sup>288</sup> “Spyware” ტექნოლოგიას შეუძლია მომხმარებლის ინფორმაციის მითვისება სისტემური და მომხმარებლის პირადი ფაილებიდან. მრავალი კომპანიის პირადი ცხოვრების დაცვის პოლიტიკა იუნწყება, რომ მათ მიერ არ ხდება სენსიტიური ინფორმაციის შეგროვება, თუმცა სრულებით იმის დადგენა, აქვს თუ არა ადგილი მსგავს პრაქტიკას, შეუძლებელია.<sup>289</sup>

286 მ. 8, პ. 1, 3.

287 შეად., Purtova, 2010.

288 Schwartz, p. 2064-2065.

289 <http://www.pctools.com/security-news/what-is-adware-and-spyware/>.

განხილული პროცესის გათვალისწინებით, მაგალითად, პერსონალურ მონაცემთა სავაჭრო საქონლის კატეგორიაში მოქცევა რამდენიმე ეტაპისგან შედგება: 1. პირთა სიის ფორმირება, რომლებიც თანხმობას გამოთქვამენ პერსონალური მონაცემების სავაჭრო საგნად ქცევაზე; 2. პირთა სიის ფორმირება, რომელთაც სურთ მიიღონ თავიანთი ინტერესის შესაბამისი სარეკლამო შეტყობინებები; 3. ონლაინ ტრანზაქციების ჩამონათვალი, როგორიცაა შესყიდვები, რასაც შემდგომ თან მოსდევს ამ ინფორმაციის შენახვა სავაჭრო მიზნებისთვის; 4. მეტამონაცემთა (metadata - ინფორმაცია ინფორმაციის შესახებ) ფორმირება, რომელიც მოიცავს ინფორმაციას ინდივიდის ინტერესების შესახებ.

ჩამოთვლილთაგან მეტად საყურადღებოა მეტამონაცემი. იგი შეიცავს კომპიუტერული ფაილის ავტორის სახელსა და ინიციალებს, კომპანიისა და ორგანიზაციის დასახელებას, კომპიუტერის ან ქსელური სერვერის, ასევე, მყარი დისკის დასახელებებს, რომელიც შემდგომ გამოიყენება ვაჭრობის საგნად და წარმოშობს პირად ცხოვრებაში ჩარევის რისკებს.<sup>290</sup> ცხადია, თუ პერსონალურ მონაცემთა დამუშავების სცენარი ზემოხსენებული პუნქტების შესაბამისად განვითარდა, რაც ნებისმიერ შემთხვევაში მონაცემთა სუბიექტის მაქსიმალური ინფორმირების ვალდებულებას გულისხმობს, პროცესი კანონიერებას დაექვემდებარება. თუმცა ამ დროს, მონაცემთა სიმრავლის გათვალისწინებით, სულ უფრო მეტად საყურადღებოა ამ პროცესის კანონიერების ზედმიწევნითი უზრუნველყოფა.

გასათვალისწინებელია ისიც, რომ ინფორმაციული პრივატულობა წარმოშობს განსხვავებულ გამოწვევებს ფიზიკურ პრივატულობასთან შედარებით. ინფორმაციული პრივატულობის მთავარ საკითხებს შორისაა პერსონალურ მონაცემთა გამოყენება მესამე პირების მიერ და ამგვარი გამოყენების თანმდევი შედეგები, მაგალითად, ინდივიდთა კატეგორიზაცია მათი პერსონალური ინფორმაციის მიხედვით.<sup>291</sup> ამ პროცესმა შესაძლოა ბიძგი მისცეს მაიდენტიფიცირებელ ინფორმაციაში საკუთრების უფლების გაჩენას, რაც ზრდის ვაჭრობის ხარისხს და აქვეი-

290 Schwartz, p. 2070.

291 იქვე, გვ. 2075.

თებს პირადი ცხოვრების დაცვის დონეს.<sup>292</sup> საყურადღებოა, რომ ხელშეკრულების კლასიკური გაგების თანახმად, იგი მოიცავს ინდივიდუალურ შეთანხმებებს, რომელზეც მომხმარებელი გაცნობიერებულად და საკუთარი ნებით გასცემს თანხმობას. სირთულე მდგომარეობს იმაში, რომ პერსონალური მონაცემებით ონლაინ ვაჭრობისას, პირობები უკიდურესად სტანდარტიზებული და არამოლაპარაკებადი იქნება, გაცემული თანხმობა ვერ იქნება. სათანადო.<sup>293</sup> მართლაც, გაცნობიერებული თანხმობის, როგორც ნების თავისუფალი გამოვლენის მაგალითი მნიშვნელოვნად წყვეტს სამართლებრივი ურთიერთობის კანონიერების საკითხს. ევროპული კანონმდებლობის მიხედვით არსებობს კანონიერი თანხმობის სამი ელემენტი, რომელიც კუმულაციურ დაცვას საჭიროებს პროცესის ლეგიტიმურობისთვის, კერძოდ, აუცილებელია, რომ: 1. პირი არ იმყოფებოდეს ზენოლის ქვეშ; 2. იგი უნდა იყოს ჯეროვნად ინფორმირებული მიზნისა და შედეგების თაობაზე; 3. რაც შეიძლება კონკრეტული იყოს იმ ურთიერთობის ფარგლები, რაზეც გაიცემა თანხმობა.<sup>294</sup>

არსებობს მოსაზრებაც, რომ თუ სუბიექტებს პერსონალურ მონაცემებთან მიმართებით საკუთრების უფლების გარკვეული ელემენტებით ავლჭურავთ, შესაძლოა სახეზე იყოს რამდენიმე უპირატესობა, კერძოდ: 1. მონაცემთა სუბიექტები მეტად დაინტერესდებიან თავიანთი ინფორმაციით ვაჭრობის შესახებ; 2. მათ მეტად მიეცემათ შესაძლებლობა გააკონტროლონ თავიანთი პერსონალური ინფორმაცია; 3. მათ მიეცემათ საშუალება მეტად უზრუნველყონ საკუთარი პირადი ცხოვრების დაცვა, სარგებლის მიღების პარალელურად.<sup>295</sup>

მიუხედავად ამისა, პერსონალურ მონაცემებზე საკუთრების უფლების გარკვეული თავისებურებების გავრცელება არ უნდა აღიქმებოდეს ისე, თითქოს იგი კარგავს ყველა იმ მახასიათებელს, რითაც იგი გვევლინება პირადი ცხოვრების ნაწილად. მისი ბუნებიდან გამომდინარე საკუთრების უფლების გავრცე-

<sup>292</sup> იქვე, გვ. 2077.

<sup>293</sup> Holland, p. 908.

<sup>294</sup> ევროკავშირის ფუნდამენტურ უფლებათა სააგენტო, ევროპის საბჭო, ევროკავშირის მონაცემთა დაცვის ზედამხედველი, გვ. 128-129.

<sup>295</sup> Holland, p. 910-911.

ლების პარალელურად სრულებით არ უნდა შეიზღუდოს ის შესაძლებლობები, რაც ინდივიდს ანიჭებს უნარს მართოს საკუთარი პერსონალური მონაცემი.<sup>296</sup>

მიუხედავად იმისა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მთელ რიგ წინაპირობებს შეიცავს მარკეტინგული მიზნებისთვის მონაცემთა გამოყენების თაობაზე, დამუშავების გაძლიერებული სისტემებისა და საზოგადოებაში ინფორმირებულობის სათანადო დონის არარსებობის გათვალისწინებით ეს პროცესი კანონიერი ჩარჩოებიდან მარტივად ექვემდებარება გამოსვლას. თუ საკითხს მივუდგებით ეკონომიკური გადმოსახედიდან, ნათელი გახდება, რომ მონაცემთა დამუშავებას ამ მიზნებისთვის დიდი მნიშვნელობა აქვს. თავის მხრივ, ამას გავლენა აქვს პერსონალურ მონაცემთა დაცვის უფლებასა და შესაბამის მარეგულირებელ კანონმდებლობაზე. აქვე უნდა ავღნიშნოთ, რომ დამუშავებლის მიერ პრივატულობის პოლიტიკის (privacy policy) დეკლარირება ინფორმაციის გამჟღავნების დონის გაზრდას იწვევს, მიუხედავად იმისა კითხულობს ან იგებს თუ არა ამ პოლიტიკის შინაარსს მომხმარებელი.<sup>297</sup> თუმცა, პრივატულობის პოლიტიკის შემუშავება და მისი საჯარო განთავსება არ არის მეორეხარისხოვანი დანიშნულების მქონე. საზოგადოების წევრებისთვის ამ დოკუმენტის მეშვეობით ხდება იმ მიდგომებისა და წესების გაცნობა, რასაც ესა თუ ის დამუშავებელი იყენებს საქმიანობის ფარგლებში. აქ საუბარია იმ პროცედურის აღწერაზე, რომელსაც ადგილი აქვს დამუშავებისას. სასურველია, იგი მაქსიმალურად ინფორმაციული იყოს დაინტერესებული პირებისთვის. ამასთან, პრივატულობის პოლიტიკა უნდა ახორციელებდეს საკანონმდებლო მოთხოვნათა ფორმულირების ადაპტაციას და საზოგადოებისთვის მიწოდებას ყველასთვის გასაგები ენით.

არსებობს სხვა სირთულეც, რაც უკავშირდება პრივატულობის „სავაჭრო ბაზარს.“ შესაძლოა წარმოიშვას ე.წ. „ინფორმაციული ასიმეტრია“ მონაცემთა შემგროვებლებსა და ინდივიდებს შორის. მონაცემთა შემგროვებლები რთული ტერმინოლოგიით ახდენენ იმ საკითხების ფორმულირებას, რომელიც

296 Purtova, p. 16.

297 Holland, p. 899.

მონაცემთა მოპოვებასა და გამოყენებას ეხება. მაგალითად, შეტყობინებები პირადი ცხოვრების დაცვის შესახებ, ნოდებუ-  
ლი როგორც კონფიდენციალურობის პოლიტიკა (მონაცემთა  
დაცვის პოლიტიკა), ხშირად ვერ ახდენს ვებგვერდის მიერ და-  
მუშავების არსებულ შესაძლებლობათა დემონსტრირებას. ამა-  
ვდროულად, ვებგვერდები იტოვებენ უფლებას შეცვალონ მათი  
პირადი ცხოვრების პოლიტიკა, რაც ვიზიტორთათვის გულისხ-  
მობს ცვლილებათა მუდმივი შემოწმების აუცილებლობას.<sup>298</sup> ეს  
მეტად თვალნათელია ონლაინ ტრანზაქციების კონტექსტში,  
როდესაც მონაცემთა სუბიექტს შესაძლოა არასრული ინფორ-  
მაცია გააჩნდეს გარკვეულ საკითხებზე, მაგალითად, პირად  
ცხოვრებაში ჩარევის ხარისხზე, რაც მეტადაა სახეზე იქ, სადაც  
შემგროვებელს სუბიექტის შესახებ არსებულ ინფორმაციას  
ანვდის მესამე მხარე. მრავალი მსგავსი რისკი მატერიალიზე-  
ბის შემდგომ იჩენს თავს. შესაბამისად, მონაცემთა სუბიექტს არ  
აქვს სრული ინფორმაცია დამცავი ტექნოლოგიებისა და მათი  
ხელმისაწვდომობის თაობაზე.<sup>299</sup>

პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონე-  
ბი ცდილობენ სამართლიანი ბალანსის მოძიებას ფუნდამენტურ  
უფლებებსა და ინფორმაციის თავისუფალ მიმოსვლას შორის.  
ამა თუ იმ საზოგადოებაში, წესები, რომელიც განსაზღვრავს  
პერსონალური მონაცემების გამოყენების შესაძლებლობას სა-  
ჯარო და კერძო პირებისთვის, განსხვავებულია.<sup>300</sup> მიუხედავად  
ამისა, რისკები რაც გამოწვეულია ტექნოლოგიური საშუალებე-  
ბის გამოყენების სიმარტივეთა და მოხერხებულობით, უკავშირ-  
დება პერსონალურ მონაცემთა დამუშავების კანონიერების  
უზრუნველყოფასაც. მას შემდეგ, რაც განვითარდა ინფორმა-  
ციული ტექნოლოგიები, განვითარდა ე.წ. ინფორმაციული პრი-  
ვატულობის კონცეფცია. მის ძირითად დანიშნულებად გვევლი-  
ნება პერსონალურ მონაცემთა დაცვა.<sup>301</sup>

298 Schwartz, p. 2080.

299 Hoiland, p. 903.

300 Reidenberg, pp. 1341-1342.

301 Vedder A., *Medical Data, New Information Technologies and the Need  
for Normative Principles other than Privacy Rules*, Law and Medicine (vol.  
3), 2000, pp. 444-445.

პერსონალურ მონაცემთა გამოყენებისა და გავრცელების მრავალფეროვნებაზე მეტყველებს მათი მართვის ისეთი მოქნილი მეთოდი, როგორიცაა Cloud. მისი მეშვეობით პერსონალურ მონაცემთა დამუშავების აღწერამდე, მიზანშეწონილია განვიხილოთ თავად Cloud-ის ფუნქციონირებისთვის დამახასიათებელი ნიშნები. Cloud ესაა ტექნოლოგიური საშუალებებისა და მომსახურების ნაკრები, რომელიც აქცენტირებულია მომხმარებლისთვის IT აპლიკაციების, დამუშავების შესაძლებლობების, შენახვისა და მეხსიერების ადგილის ინტერნეტის მეშვეობით მინოდებაზე. შესაბამისად, ვირტუალური სისტემა პერსონალურ კომპიუტერებზე ინსტალირების გზით უზრუნველყოფს მომხმარებლისთვის პროგრამების ხელმისაწვდომობას. მაგალითად, კალენდრების, ტექსტის რედაქტორებისა და სხვა ფაილების შენახვისთვის შეიძლება გამოიყენებოდეს ვირტუალური სივრცე.<sup>302</sup> იგი ხასიათდება სამი სახეობით, რომელთაგან თითოეული განსხვავდება ფუნქციონალური მახასიათებლების მიხედვით. ესენია:

1. IAAS (Cloud Infrastructure as a Service) – Cloud ინფრასტრუქტურა, როგორც მომსახურება. ამ შემთხვევაში სახეზე გვაქვს ვირტუალური ინფრასტრუქტურა, რომელიც მომხმარებლისთვის ხელმისაწვდომს ხდის სხვადასხვა სერვისებს, რითაც კორპორატიული IT სისტემები მარტივად ჩანაცვლებადია;

2. SAAS (Cloud Software as a Service) – Cloud პროგრამული უზრუნველყოფა, როგორც მომსახურება. ამ სერვისის შინაარსი გულისხმობს სხვადასხვა პროგრამული უზრუნველყოფის ინტერნეტის მეშვეობით მომხმარებლისთვის მინოდებას. საუბარია საშუალებებზე, როგორიცაა ტექსტისა და ცხრილების დამუშავების საშუალებები, საზიარო კალენდრები და ა.შ.;

3. PAAS (Cloud Platform as a Service) – Cloud პლატფორმა, როგორც მომსახურება. ამ დროს სისტემა გამოიყენება სხვადასხვა აპლიკაციების შექმნისა და პოსტინგისთვის. მის ძირითად დანიშნულებას წარმოადგენს დეველოპერული შესაძლებლობების (პროგრამების შექმნის) რეალიზაცია.<sup>303</sup>

ზემოაღნიშნული მსჯელობის გათვალისწინებით, ნათელია

302 WP 29, 2012, p. 4.

303 იქვე, გვ. 26.

თუ რა შინაარსის შემცველია თანამედროვე IT სისტემები და შესაძლებლობათა რა არეალია სახეზე მონაცემთა დამუშავებისთვის. გარდა პერსონალური მონაცემების დამუშავების მრავალფეროვნებისა, Cloud შეიცავს რისკებს, რომელიც დაკავშირებულია დამუშავების ექსტრატერიტორიულობასთანაც. Cloud-ის მომწოდებელი (პროვაიდერი) შესაძლოა არ იყოს დაფუძნებული იმ სახელმწიფოში, სადაც დაფუძნებულია მისი მომხმარებელი. მაგალითად წარმოვიდგინოთ, რომ საქართველოში დარეგისტრირებული იურიდიული პირი საკუთარი თანამშრომლების შესახებ არსებული ინფორმაციის მართვისთვის იყენებს Google-ის მიერ მოწოდებულ PAAS ტიპის Cloud-ს (Google Drive). მისი მეშვეობით კომპანია, პერსონალური მონაცემების მართვისთვის, ელექტრონულად, ინტერნეტის მეშვეობით იყენებს ტექსტის რედაქტორს. თუ ამ საკითხს განვიხილავთ სამართლებრივ ჭრილში, კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის გადმოსახედიდან, იგი ბადებს კითხვებს მის მართლზომიერებასთან დაკავშირებით. პერსონალურ მონაცემთა გადაცემა სხვა სახელმწიფოსთვის დასაშვებია მხოლოდ შემდეგ შემთხვევებში: 1. თუ არსებობს საერთაშორისო შეთანხმება, რომელიც ითვალისწინებს პერსონალურ მონაცემთა გადაცემის პირობას; 2. თუ სხვა სახელმწიფოში არსებობს პერსონალურ მონაცემთა დაცვის ადეკვატური გარანტიები.<sup>304</sup> სხვა ნებისმიერი გადაცემა (თუ გადაცემის საფუძველი არაა საერთაშორისო ხელშეკრულება ან თუ გადაცემა არ ხორციელდება იმ სახელმწიფოში, რომელიც სახელმწიფო ინსპექტორის მიერ აღიარებულია მონაცემთა დაცვის ადეკვატურობის მქონე სახელმწიფოდ) საჭიროებს ინსპექტორის წინასწარ თანხმობას. სხვა სახელმწიფოში მონაცემთა დაცვის ადეკვატურობის გარანტიების ერთადერთი უფლებამოსილი შემფასებელი პირი სახელმწიფო ინსპექტორია.<sup>305</sup> მაგალითად, ამერიკის შეერთებული შტატები ვერ უზრუნველყოფს პერსონალურ მონაცემთა დაცვის ადეკვატურობას.<sup>306</sup> ჩვენს მიერ მოყვანილ მაგალითში კი Google-ის მიერ მოწოდებული აპლიკაციის გამოყენება და

304 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 41.

305 იქვე, მ. 42.

306 პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის 16 სექტემბრის ბრძანება №1.

მისი მეშვეობით პერსონალურ მონაცემთა დამუშავება შეიძლება შეფასდეს მონაცემთა სხვა სახელმწიფოსთვის გადაცემად, ვინაიდან ამ დროს გამოიყენება Google-ის სერვერული სისტემა. დროის სხვადასხვა მონაკვეთში პერსონალური მონაცემები (სერვერის მდებარეობის მიხედვით) შეიძლება განთავსებული იყოს აშშ-ში ან სხვა ისეთ სახელმწიფოში, რომელიც კანონმდებლობის თანახმად არ არის შეყვანილი მონაცემთა დაცვის ადეკვატურობის გარანტიების მქონე სახელმწიფოთა სიაში. საქართველოში დამუშავებული ბოლომდე ვერ იქნება დარწმუნებული თუ რამდენად ამუშავებს Google კანონის ნესების დაცვით პერსონალურ მონაცემებს. შედეგად, სახეზეა დამუშავებელსა და უფლებამოსილ პირს (Google) შორის უფლებრივი დისბალანსი, რომელიც ვლინდება (უფლებრივად) ძლიერ უფლებამოსილ პირისა და (უფლებრივად) სუსტ დამუშავებელს შორის.<sup>307</sup> მთავარი ხარვეზი მდგომარეობს იმაში, რომ საერთაშორისო გადაცემისას დამუშავებას (გადაცემას) არ გააჩნია ლეგიტიმური საფუძველი.

პერსონალურ მონაცემთა ელექტრონული საშუალებებით დამუშავების მეთოდების განვითარების პარალელურად იზრდება დამუშავებასთან დაკავშირებული უსაფრთხოების რისკები. მონაცემთა დამუშავება ინტერნეტის გამოყენებით აკისრებს მთელ რიგ ვალდებულებებს დამუშავებლებს. ამ ვალდებულებათა ხასიათი, მაგალითად, აღწერილია ელექტრონული კომუნიკაციების სექტორში პერსონალურ მონაცემთა დამუშავებისა და პირადი ცხოვრების დაცვის შესახებ 2002/58/EC დირექტივაში, კერძოდ, კერძოდ, სერვისის მომწოდებლები (პროვაიდერები) ოპერირებისას ვალდებული არიან მიიღონ შესაბამისი უსაფრთხოების ზომები, საჭიროების შემთხვევაში, ინტერნეტის მომწოდებელთან (პროვაიდერთან) შეთანხმებით. ამავდროულად, ანგარიშვალდებულების პრინციპის გათვალისწინებით, ქსელის უსაფრთხოების დარღვევის შემთხვევაში, ამის შესახებ ვალდებული არიან შეატყობინონ სერვისით მოსარგებლებებს. დირექტივა უთითებს, რომ დამუშავებისთვის მომეტებული რისკის შემცველ საშუალებებად გვევლინება ინტერნეტსა და მობილურ ტელეფონზე დამყარებული ელექტრონული კომუნიკაცი-

ზოგადად, 2002/58/EC დირექტივა არ შეიცავს თანამედროვე ტექნოლოგიური საშუალებების ყოველდღიურ ცხოვრებაში დანერგვისთვის ხელისშემშლელ დებულებებს. მისი მთავარი მიზანია ამ საშუალებათა ფუნქციონირება მოაქციოს სამართლებრივი რეგულირების ფარგლებში. საშუალებები, როგორიცაა cookie, პროდუქტიულია ვებ-გვერდზე რეკლამების განთავსებისთვის, მისი მუშაობის ეფექტურობის განსაზღვრის მიზნით, ასევე, ონლაინ ტრანზაქციებში მონაწილე მომხმარებელთა ვინაობის განსაზღვრისთვის. ამგვარი მეთოდების გამოყენება გამართლებული იქნება მხოლოდ მაშინ, თუ იგი კანონიერ მიზანს ემსახურება და მომხმარებლები მკაფიოდ და ნათლად არიან ინფორმირებული ამგვარი საშუალებების გამოყენების მიზანთა შესახებ. ამავდროულად, მომხმარებლებს უნდა ჰქონდეთ საშუალება უარი განაცხადონ ამგვარი მეთოდების გამოყენებაზე.<sup>309</sup>

პერსონალური მონაცემების დაცვის მიმართულებით ელექტრონული უსაფრთხოების საკითხები მეტ ყურადღებას საჭიროებს. იმის გათვალისწინებით, რომ, მაგალითად, სრულად შეესებული Facebook-ის მომხმარებლის ანგარიში შეიცავს დაახლოებით ორმოცამდე სახეობის პერსონალურ მონაცემს, მათ შორის, სახელს, დაბადების თარიღს, პოლიტიკურ და რელიგიურ შეხედულებებს, ონლაინ და ქსელს გარეთ არსებული კონტაქტების შესახებ ინფორმაციას, სქესსა და პირადი ურთიერთობის სტატუსს - მას მოქმედებაში მოყავს სხვადასხვა საშუალებები პოტენციური კონტაქტების მოძებნისა და დამატებისთვის. ამის გარდა, ხდება მომხმარებლის აქტივობის კონტროლი, შენახვა და ანალიზი. პერსონალურ მონაცემთა დაცვის ევროპული კანონმდებლობის გათვალისწინებით, ამგვარი ინფორმაცია დამუშავების სპეციალურ, სენსიტიური მონაცემების დამუშავებისთვის დადგენილ წესებს უნდა ექვემდებარებოდეს.<sup>310</sup>

308 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recital 20.

309 იქვე, 25.

310 Berg B.V., Potzsch S., Leenes R., Borçea-Pfitzmann K., Beato F., *Privacy in Social Software, Privacy and Identity Management for Life*, Springer, 2011, p. 38.

ტექნოლოგიურ გამოწვევათა გათვალისწინებით, გამოსავალი უსაფრთხოების შესაბამის ორგანიზაციულ და ტექნიკურ ზომებშიც უნდა ვეძიოთ. საინტერესოა, მოითხოვს თუ არა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი უსაფრთხოების სტანდარტების დანესებას ინფორმაციის დამუშავების კანონიერების უზრუნველყოფისთვის. დადგენილია, რომ „მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისგან, შეცვლისგან, გამჟღავნებისგან, მოპოვებისგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისგან.“<sup>311</sup> ამასთან, „მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.“<sup>312</sup> ამ ჩანაწერით კანონმდებელი აწალდებულებს ყველა დამმუშავებელს შესაბამისი უსაფრთხოების ზომების მიღებას, თუმცა აქ რაიმე კონკრეტულ მეთოდსა და საშუალებაზე მითითება არ არის გაკეთებული. მიუხედავად ამისა, კანონი აკეთებს დათქმას, რომ „მონაცემთა უსაფრთხოების დაცვის ზომები განისაზღვრება საქართველოს კანონმდებლობით.“<sup>313</sup>

საინტერესოა, არის თუ არა განსაზღვრული ამგვარი ზომები ყველა ტიპის დამმუშავებლისთვის, სხვა სიტყვებით; როგორც საჯარო, ისე კერძო სექტორის წარმომადგენელთათვის? მაგალითად „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი განსაზღვრავს უსაფრთხოების მეტნაკლებად კონკრეტულ ზომებს დანესებულებებში. მისი მიზანია „ხელი შეუწყოს ინფორმაციული უსაფრთხოების დაცვის ქმედით და ეფექტიან განხორციელებას, დაანესოს საჯარო და კერძო სექტორების უფლება-მოვალეობები ინფორმაციული უსაფრთხოების დაცვის სფეროში, აგრეთვე განსაზღვროს ინფორმაციულ უსაფრთხოების პოლიტიკის განხორციელების

311 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 17, პ. 1.

312 იქვე, პ. 3.

313 იქვე, პ. 5.

სახელმწიფო კონტროლის მექანიზმები.<sup>314</sup> კანონი არ ადგენს კონკრეტულ ჩამონათვალს იმ დაწესებულებებისა, რომელზეც ვრცელდება კანონის დებულებები. იგი ზოგადად განსაზღვრავს, კრიტიკული ინფორმაციული სისტემის სუბიექტს, რომელიც არის „სახელმწიფო, ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.“<sup>315</sup> უშუალოდ კრიტიკული ინფორმაციული სისტემა კი განმარტებულია, როგორც „ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისთვის.“<sup>316</sup> კანონი ვრცელდება, ძირითადად, საჯარო დაწესებულებებზე ან კერძო ორგანიზაციებზე, რომლებიც ითავსებენ საჯარო უფლებამოსილებებს. ნაკლებად სავარაუდოა, რომ კრიტიკული ინფორმაციული სისტემის სუბიექტი იყოს ყოველი კერძო დაწესებულება, რომელიც ამუშავებს პერსონალურ ინფორმაციას (მაგალითად, სარეკლამო კომპანიები, სავაჭრო მაღაზიათა ქსელი და ა.შ.). რა თქმა უნდა, უნიფიცირებული რეგულირების არარსებობა იწვევს უსაფრთხოების სტანდარტებისადმი ძალზედ სუბიექტურ მიდგომას. სხვა სიტყვებით, კერძო სექტორის იმ დამმუშავებლებს, რომლებიც არ არიან კრიტიკული ინფორმაციული სისტემის სუბიექტები, შეუძლიათ დანერგონ უსაფრთხოების ზომები, რომელიც მათი შეხედულებით იქნება ადეკვატური, თუმცა, რეალურად, იგი არ პასუხობდეს უსაფრთხოების წინაშე არსებულ გამოწვევებს.

ტექნოლოგიური შესაძლებლობების რეალიზაციიდან გამომწვეული რისკები შესაძლებელია თავიდან იქნეს აცილებული იმ შემთხვევაში თუ დამმუშავებლები მიმართავენ პერსონალური მონაცემების დამუშავების დამცავი მექანიზმების პროაქტიულ მეთოდებს. არსებობს მცდარი მოსაზრება, რომ პერსო-

314 „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, მ. 1.

315 იქვე, მ. 2, პ. „ზ.“

316 იქვე, მ. 2, პ. „ვ.“

ნალურ მონაცემთა დაცვის მარეგულირებელი ნორმების ზედმინევნითი შესრულება დააქვეითებს ამა თუ იმ ორგანიზაციის საქმიანობის ხარისხს, რაც გამოიხატება ნაკლები მოგების მიღებაში, მომსახურების განვითარების გახანგრძლივებულ ვადებში და ა.შ.<sup>317</sup> თუ პერსონალურ მონაცემთა დამუშავების წესებთან შესაბამისობის უზრუნველყოფას შევხედავთ, როგორც კომპანიის მონაპოვარს და საზოგადო იმიჯზე დადებითი გავლენის მომტან ბერკეტს, იგი სასურველ მექანიზმად მოგვევლინება პერსონალურ მონაცემთა დამუშავებლებისთვის.

იმისთვის, რათა დამუშავების პროცესში, საწყის ეტაპზე დაინერგოს პერსონალურ მონაცემთა დამცავი მიდგომები აუცილებელია მომდევნო 7 ძირითადი პრინციპის დაცვა, კერძოდ:

1. ნებისმიერი დამუშავებელი უნდა იყოს ორიენტირებული პერსონალურ მონაცემთა დამუშავების წესების დარღვევის თავიდან აცილებაზე. აქ ძირითადი აქცენტი კეთდება პროაქტიული დაცვის აუცილებლობაზე, რაც იწვევს შესაძლო რისკების მინიმუმამდე დაყვანას;
2. სისტემურ დონეზე პერსონალურ მონაცემთა დაცვა ყურადღებას ამახვილებს დამცავი მექანიზმების თანდაყოლილ ბუნებაზე. როგორც ავტომატური, ისე არაავტომატური (ან ნახევრადავტომატური) დამუშავების პროცესი უნდა დაექვემდებაროს პერსონალურ მონაცემთა დაცვის თანდაყოლილ პირობებს;
3. დამუშავების წესების დაცვა უნდა განვიხილოთ ნებისმიერი საქმიანობის კონცეფციისა და თავისებურებების შემადგენელ ნაწილად;
4. პერსონალურ მონაცემთა დაცვის წესების პრაქტიკული დანერგვა უნდა ქმნიდეს მომხმარებლისა და კომპანიის მიზნების მიღწევის შესაძლებლობას ისე, რომ არ დაზიანდეს, რომელიმე მათგანის ინტერესი;
5. დამუშავების პროცესის კანონიერება და წესებთან თავსებადობა უნდა მოიცავდეს მის სრულ ციკლს, დაწყებული პერსონალური მონაცემების მოპოვებიდან - დამთა-

317 კავუკიანი, ა., *Privacy by Design კონცეფცია სამართალში, რეგულირებასა და პრაქტიკაში (თარგმანი)*, თბილისი, „იურისტების სამყარო“, 2016, გვ. 59.

ვრებული მისი საბოლოო განადგურებით;

6. თუ ორგანიზაციის შიგნით მიმდინარე დამუშავების პროცესი არ იქნება გამჭვირვალე, ვერც მისი სათანადო ანალიზი მოხდება მომხმარებლის ან სხვა დაინტერესებული პირის მიერ. შესაბამისად, იგი გამოიწვევს გამჭვირვალობის არარსებობას, რაც, ანგარიშვალდებულების პრინციპის გათვალისწინებით, დაუშვებელია. ამდენად, სუბიექტის მიმართ დამუშავების წესებზე სრული წვდომა ამ პროცესის გამჭვირვალობასა და ანგარიშვალდებულებას უზრუნველყოფს;
7. ორგანიზაციულად, პერსონალურ მონაცემთა დამუშავების ცალკეული შემთხვევები პერიოდულად ცვლილებებს ექვემდებარება. დამუშავების წესები იმ შემთხვევაში დარჩება სუბიექტების ინტერესებზე მორგებული, თუ მოხდება ამ უკანასკნელთა შეხედულებებისა და მოლოდინების გათვალისწინება ნებისმიერი ახალი წესის შემუშავებისას.<sup>318</sup>

### 3.2. პერსონალურ მონაცემთა დაცვა, როგორც ძირითადი უფლება

ძირითადი უფლებების დახასიათებისას, ზოგადი მსჯელობის მიხედვით, აუცილებელია ვისაუბროთ მათ უნივერსალურ ხასიათზე, მათ საყოველთაო ბუნებაზე. ადამიანური საჭიროებები ნებისმიერ საზოგადოებაში და კულტურაში მსგავსია, შესაბამისად, გარკვეული ადამიანური მოთხოვნები იწვევს მათთვის უფლებების ფორმირებას, რომელიც ანიჭებს მათ ამ მოთხოვნების უზრუნველყოფის გარანტიებს. ამდენად, ეს უფლებები მატერიალურად ძირითად ხასიათს ატარებს, ხოლო გავრცელების მხრივ – უნივერსალურს.<sup>319</sup> მართლაც, მეცნიერთა აზრით, ძირითადი უფლების არსებობისთვის აუცილებელია „მოთხოვნის“ ელემენტის არსებობა. ადამიანის მხრიდან გარკვეული სიკეთის ან ღირებულების მოთხოვნის არსებობა გარდაუვალი და აუცილებელი წინაპირობაა ძირითადი უფლების ფორმირებისთვის.

318 იქვე, გვ. 86-89.

319 Phillips, D.L, *Fundamental Rights and the Supportive State - Theory and Society*, Kluwer Academic Publisher, 1988, pp. 574, 577.

ეს უფლებები საყოველთაოა და ფუნდამენტური იმ გაგებით, რომ იცავს ადამიანის არსებით ინტერესებს, ხოლო კონსტიტუციონალიზმის ისტორიული განვითარების მიხედვით უფლებები ემთხვევა ისეთ საყოველთაო ღირებულებებს, როგორიცაა, მაგალითად, სიცოცხლე, თანასწორობა, ადამიანური ღირსება და ა.შ.<sup>320</sup>

ძირითადი უფლებებისთვის, ასევე, დამახასიათებელია ის, რომ ისინი გვევლინება ევოლუციის შედეგად წარმოშობილ ღირებულებებად. ისტორიულად, უფლებების წარმოშობის პროცესი, მათ შორის, პოლიტიკური რეპრესიების გამოძახილს წარმოადგენს და არა წინასწარ გეგმით განერილი მიდგომის შედეგად ჩამოყალიბებულ ღირებულებებს. ადამიანური არსება ეფუძნება პიროვნული განვითარების, ჯანმრთელობის, განათლების, შრომის და სხვა უფლებებს. ისინი საშუალებას აძლევს ინდივიდს განავითაროს პიროვნება დამოუკიდებლად, რის გამოც, ეს უფლებები თავისი ბუნებით ძირითადია, იმის და მიუხედავად, არის თუ არა საზოგადოებაში მზაობა მათი პრაქტიკული რეალიზაციისთვის. აქვე უნდა ავლიწნოთ, რომ ძირითადი უფლებები ნებისმიერი პოლიტიკური ხელისუფლებისთვის წინმსწრებია, ამიტომაც არის ფუნდამენტური, უნივერსალური და წარუვალი.<sup>321</sup>

მოცემული მსჯელობიდან იკვეთება, რომ ამა თუ იმ უფლებისთვის „ძირითადი“ სტატუსის მინიჭებისთვის აუცილებელია შემდეგი პირობების არსებობა:

1. უფლება უნდა ანიჭებდეს პირს იმ შესაძლებლობათა რეალიზაციის საშუალებას, რომელიც ინდივიდისთვის არის აუცილებელი;
2. უფლებას წინაპირობად უნდა ჰქონდეს „მოთხოვნის“ ელემენტი, ანუ, უფლება უნდა ვალიაროთ ძირითადად იმ საზოგადოება ითხოვს ამა თუ იმ ადამიანური ღირებულების უზრუნველყოფას სახელმწიფოსგან;
3. უფლება უნდა ქმნიდეს პიროვნების თავისუფალი განვითარების შესაძლებლობას საზოგადოებაში;

320 Baccelli, L., *The Logical Foundation of Fundamental Rights and their Universality*, Res Publica, Springer, 2011, pp. 372, 374.

321 Narain, J., *Human and Fundamental Rights: What are they About*. The Liverpool Law Review, vol. XV (2), 1993, pp. 164, 168-169; 175.

4. უფლება უნდა იცავდეს ადამიანური ღირებულების რომელიმე, მეტ-ნაკლებად, კონკრეტულ სეგმენტს, კატეგორიას.

ახლა კი, უნდა დავადგინოთ, აკმაყოფილებს თუ არა პერსონალურ მონაცემთა დაცვის უფლება ყველა იმ პირობას, რის გამოც შევძლებთ მის აღიარებას ძირითად უფლებად. ამ მიზნით, უნდა გავარკვიოთ თუ რა ბუნებისაა უფლება პერსონალურ მონაცემთა დაცვაზე და რა თავისებურებებით გამოირჩევა იგი. ეს უფლება გვევლინება, როგორც პირადი ცხოვრების უფლების პირმო და ყველაზე კარგად იგი შეიძლება განიმარტოს, როგორც ინფორმაციული თვითგამორკვევის უფლება. ეს უკანასკნელი წარმოადგენს თავისუფალი, დემოკრატიული საზოგადოების ფუნქციონალურ ნაწილს.<sup>322</sup>

დამატებით, მიზანშეწონილია მოკლედ შევადაროთ ერთმანეთს პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებები. მიიჩნევა, რომ პრივატულობა სუბიექტებს ანიჭებს პრეროგატივას – თავად განახორციელონ პირადი ცხოვრების მენეჯმენტი, მაშინ როდესაც, პერსონალურ მონაცემთა დაცვის უფლების უმთავრესი აქცენტი ინდივიდების შესახებ არსებული ინფორმაციის გამოყენების მართლზომიერების უზრუნველყოფაა. შესაბამისად, მთავარი მახასიათებელი პერსონალურ მონაცემთა დაცვის უფლებისა არის ის, რომ ამგვარი ინფორმაციის დამუშავება თანამედროვე საზოგადოებაში გარდაუვლად მიმდინარეობს. ეს უფლება არასდროს კრძალავს დამუშავებას, იგი მხოლოდ განსაზღვრავს პერსონალური მონაცემების დამუშავების გზებსა და მიმართულებებს.<sup>323</sup> გარდა ამისა, პირადი ცხოვრების უფლება გაცილებით უფრო ფართო ფარგლების მქონეა და მოიცავს სხვადასხვა უფლებებსა და ღირებულებებს, როგორიცაა უფლება იყოს „დავინწყებული“, ასევე, განმარტოვებისა და საიდუმლოების შენარჩუნების უფლებები და ა.შ. პირადი ცხო-

322 Tzanou, M., *Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a not so new Right*, International Data Privacy Law, vol. 3, no. 2. Oxford University Press, 2013, pp. 88-90.

323 Fuster, G.G. & Gellert R., *The Fundamental Right of Data Protection in The European Union: In Search of an Uncharted Right*, International Review of Law, Computers & Technology, Issue 1, Volume 26, 2012, p. 80.

ვრების უფლების დაცული სფერო არ დაიყვანება პერსონალური მონაცემების დაცვამდე.<sup>324</sup>

პირადი ცხოვრებისა და პერსონალურ მონაცემთა დაცვის უფლებები ერთმანეთისგან უნდა გაიმიჯნოს ისე, რომ ამ უკანასკნელი უფლების შეზღუდვის ან ხელყოფის დროს, აუცილებელი არ იყოს პირადი ცხოვრების უფლებაზე დაყრდნობა.<sup>325</sup> მართლაც, ევროპული კავშირის ძირითად უფლებათა ქარტიაში პერსონალურ მონაცემთა დაცვის უფლების განმტკიცებით, მიიჩნევა, რომ საუბარია პრივატულობის მიღმა არსებულ დამატებით ღირებულებებზე.<sup>326</sup> მიუხედავად ამ ორი უფლების არაერთი საერთო მახასიათებლისა, პერსონალურ მონაცემთა დაცვის უფლებით განსაზღვრული დაცული სფერო სცდება პრივატულობის ფარგლებს და ეხება, მაგალითად, საკითხებს, როგორიცაა პერსონალურ მონაცემთა უსაფრთხოება, მათი ხარისხი, რაც დღეს კანონმდებლობით ნორმატიულად წესრიგდება.<sup>327</sup> სხვა ღირებულებითი კატეგორიებიდან აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის მარეგულირებელი აქტები, ასევე, შეიცავენ დისკრიმინაციის ამკრძალავ ნორმებს, რომელიც, ირიბად, თუმცა ემსახურება ნებისმიერი გაუმართლებელი დიფერენცირების თავიდან აცილებას. მეტწილად, დისკრიმინაციის ამკრძალვა აქტუალურია. პროფილირების (profiling) ক্ষრილში, კერძოდ, იმ მიზნით, რომ არ მოხდეს პერსონალურ მონაცემთა სუბიექტების დიფერენცირება ეთნიკური, რელიგიური ან სხვა სენსიტიური ინფორმაციის დამუშავების გზით. სწორედ ამიტომ, პერსონალურ მონაცემთა დაცვის მარეგულირებელი აქტები ადგენენ მკაცრ წესებს ამ ტიპის ინფორმაციის დამუშავებისთვის.<sup>328</sup> გარდა ამისა, შეიძლება სხვა ღირებულების გამოყოფა, რომელსაც, მაგალითად, იცავს საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.“ კერძოდ, „ვიდეოთვალთვალის განხორციელება დაუშვებელია გამოსა-

324 Tzanou, p. 90.

325 იქვე, გვ. 98-99.

326 იქვე, გვ. 90.

327 იქვე, გვ. 91.

328 იქვე, გვ. 92.

ცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში.<sup>329</sup> ცხადია, ამ ნორმით აკრძალულია ვიდეოგამოსახულების, როგორც პერსონალური ინფორმაციის დამუშავება, თუმცა, შინაარსის მიხედვით, იგი უფრო მეტად გავლენას ახდენს პირადი ცხოვრების ინტიმური ასპექტის დაცვაზე, ვიდრე პერსონალურ მონაცემთა დაცვის მართლზომიერების საკითხზე.

განსხვავების ნაწილში, სასურველია ჩამოვთვალოთ ის რისკებიც, რაც სპეციფიკურია პერსონალურ მონაცემთა დაცვის უფლებისთვის. უნდა გავითვალისწინოთ, რომ:

1. არ არსებობს ზღვარი იმისა, თუ რა ოდენობის ინფორმაცია შეიძლება იქნეს შენახული სუბიექტის შესახებ. აქ საუბარია ელექტრონული საშუალებებით პერსონალურ მონაცემთა შენახვაზე;

2. არ არსებობს ზღვარი იმისა, თუ რა ტიპის ანალიზი შეიძლება განხორციელდეს პერსონალური მონაცემების მიმართ. აქაც, ანალიზი ტექნოლოგიურ საშუალებების გამოყენებით დამუშავებას უკავშირდება. ამის მკაფიო მაგალითი მეტამონაცემთა (metadata) ფორმირება და სუბიექტთა პროფილირებაა (profiling);

3. ინფორმაცია შეიძლება შენახულ იქნეს სამუდამოდ, რაც პერსონალურ მონაცემთა ელექტრონული ბაზების გამოყენებით შეიძლება მოხდეს. ამ რისკების შესამცირებლად კი, სუბიექტს საშუალება ეძლევა ჩაერთოს პროცესში და თვალი ადევნოს მის კანონიერებას.

სწორედ ამიტომ, პირადი ცხოვრების უფლება გვევლინება დამცავ ბერკეტად, მაშინ როდესაც უფლება პერსონალურ მონაცემთა დაცვაზე დამუშავების პროცესის გამჭვირვალობასა და მის კანონის შესაბამისად წარმართვას უზრუნველყოფს.<sup>330</sup>

### 3.3. პერსონალურ მონაცემთა დაცვის ძირითადი

უფლების კონსტიტუციურად დამოუკიდებელი

მონესრიგების თეორიული და პრაქტიკული ასპექტები

ზოგადად, პერსონალურ მონაცემთა დაცვის უფლების ფუნდამენტურ ხასიათს არაერთხელ გაეცვა ხაზი საქართველოში-

329 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 12, პ. 4.

330 Tzanou, pp. 91-92.

სო სასამართლოების მიერ, მეორე მხრივ, მონაცემთა დაცვის უფლება მოიაზრება, როგორც პირადი ცხოვრების უფლების ერთ-ერთი შემადგენელი ნაწილი. ამ გარემოებათა გათვალისწინებით, შესაძლებელია განვავითაროთ მსჯელობა იმის შესახებ თუ რა დანიშნულება და მიზნები გააჩნია პერსონალურ მონაცემთა დაცვის უფლების კონსტიტუციურად ცალკე განერას, მაშინ როდესაც პირადი ცხოვრების ქვეშ ეს უფლება დაცვადად ისედაც არის აღიარებული.

პერსონალურ მონაცემთა დაცვის კანონმდებლობა გამოირჩევა მისთვის ფუძემდებლური მნიშვნელობის მქონე პრინციპებით, რომელზეც აგებულია დამუშავების მთელი პროცესი. ეს პრინციპებია: 1. სამართლიანობა, კანონიერება, ღირსების შეუღახაობა; 2. მიზნობრიობა; 3. პროპორციულობა; 4. სიზუსტე და ნამდვილობა; 5. შესაბამისი ვადით დამუშავება. როგორც ცნობილია უფლება პერსონალურ მონაცემთა დაცვაზე არ არის აბსოლუტური და იგი ექვემდებარება შეზღუდვას. ამ შეზღუდვის წინაპირობები გარდაუვლად გულისხმობს დამუშავების (შეზღუდვის) პროცესის დაქვემდებარებას პრინციპებისადმი.

ზოგადად, ადამიანის ძირითადი უფლების შეზღუდვის საფუძველი სახელმწიფოს დამფუძნებელ აქტებშია მოცემული. ამ მხრივ, არც საქართველოს კონსტიტუციაა, რომელიც ანესებს პირადი ცხოვრებისა და პირადი სივრცის შეზღუდვის წინაპირობებს, კერძოდ, ჩარევა უნდა ეფუძნებოდეს დემოკრატიულ საზოგადოებაში სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველყოფას ან სხვათა უფლებების დაცვას, რაც, თავის მხრივ, კანონის შესაბამისად უნდა განხორციელდეს.<sup>331</sup> დამატებით, კონსტიტუციით გარანტირებულია საცოვრებელ ან სხვა სახის მფლობელობაში შესვლა ან ჩხრეკის ჩატარება მხოლოდ სასამართლოს წინასწარი გადანყევტილებით ან ქმედების პოსტ-ფაქტუმ ლეგიტიმაციის საფუძველზე.<sup>332</sup>

საინტერესოა, რამდენად გამოსადეგია ჩარევის ეს საფუძველები პერსონალურ მონაცემთა დაცვის უფლებისთვის? მნიშვნელოვანია გავიაზროთ, რომ პირადი ცხოვრების უფლებას გააჩნია მეტად „დახურული“ ხასიათი, სხვა სიტყვებით, მისი

<sup>331</sup> საქართველოს კონსტიტუცია, მ. 15, პ. 1.

<sup>332</sup> იქვე, მ. 15, პ. 2.

მნიშვნელობა ინდივიდისთვის გამოიტახება იმ საკითხში, რომ მეტად იზრუნოს ფიზიკური პირის ხელშეუხებლობაზე, მაშინ როდესაც პერსონალურ მონაცემთა დაცვის უფლება ხასიათდება უფრო „ღია“ მიდგომით. მისი „ღია“ გამოვლინებაა ის, რომ ინდივიდი საკუთარი თავის ინტეგრაციას საზოგადოებაში ახდენს პერსონალური მონაცემების გაცემის მეშვეობით, შესაბამისად, ამ უფლებაზე ვერ გავრცელდება დაცვის იგივე სტანდარტები, როგორცაა დადგენილი პირადი ცხოვრების უფლებისთვის. სხვა სიტყვებით, პერსონალურ მონაცემთა დაცვის ინტერესის საფუძველი არ უნდა ვეძიოთ პირადი ცხოვრების უფლებაში, რამდენადაც უფლება პირად ცხოვრებაზე წმინდად დამცავ მექანიზმად გვევლინება მასში გარეშე პირის ინტერვენციის სანაღმდეგოდ. აქედან გამომდინარე, პირადი ცხოვრების დამცავ მექანიზმებს არ ძალუძთ „იზრუნონ“ პერსონალურ მონაცემთა დაცვაზე, რომელიც მოითხოვს მეტად „გახსნილ“ მიდგომას დამუშავების გზების დანესების მიმართულებით და არა მათი აკრძალვის მხრივ.<sup>333</sup>

თუ ეს ორი უფლება სხვადასხვა შინაარსის მქონეა და სხვადასხვა დანიშნულება გააჩნიათ, ე.ი. მიზანშეწონილია მათი ცალკე განერა. ეს არ გულისხმობს იმას, რომ პერსონალურ მონაცემთა დაცვის უფლება პირადი ცხოვრების უფლებისგან არ გამომდინარეობს. აქ საუბარია იმის შესახებ, რომ პერსონალურ მონაცემთა დაცვის სპეციალური ხასიათიდან და საზოგადოებისთვის მათი მნიშვნელობიდან გამომდინარე უნდა მოხდეს ამ უფლებაზე ცალკე მითითება და, ასევე, იმ საფუძვლების ცალკე განერა, რომლის თანახმად ხდება ამ უფლების შეზღუდვა. მნიშვნელოვანია იმის გააზრება, რომ პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დაცვის უფლებათა დამოუკიდებელი განერა არ გამორიცხავს ამ უკანასკნელის განმარტებას, როგორც პირადი ცხოვრების უფლების ნაწილად, თუმცა მთელი რიგი თავისებურებების გათვალისწინებით.<sup>334</sup>

საქართველოს კონსტიტუციით დადგენილი პირადი ცხოვრე-

333 Purtova, N., *Private Law Solutions in-European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights* Netherland Quarterly of Human Rights, Vol. 28, No. 2, 2012, p. 2.

334 იქვე, გვ. 6.

ბის უფლების შეზღუდვის საფუძვლები არ არის მორგებული პერსონალურ მონაცემთა დაცვის უფლებაზე. ამის დასადასტურებლად, საკმარისია იმის აღნიშვნა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით მონაცემთა დამუშავება (ამ უფლებაში ჩარევა) სპეციფიკურ პრინციპებს ექვემდებარება; რაც მის კომპლექსურ ბუნებას განაპირობებს. კერძოდ, ზემოხსენებული კანონი ადგენს ამ სფეროში მოქმედ ხუთ ძირითად პრინციპს, ხოლო დამატებით დადგენილია დამუშავების ცალკეული საფუძვლები. გარდა ამისა, უნდა გავიაზროთ, რომ დამუშავების პრინციპების დაცვას უპირატესი მნიშვნელობა ენიჭება დამუშავების საფუძვლებთან მიმართებით დამუშავების პროცესის ლეგიტიმურობის უზრუნველსაყოფად. სხვა სიტყვებით, პირველ რიგში უნდა იყოს დაცული დამუშავების პრინციპები, ხოლო შემდგომ, დაკმაყოფილდეს შესაბამისი საფუძვლით დამუშავების პირობა. ეს მსჯელობა გამომდინარეობს იმ მარტივი რეალობით, რომ სამართლის ნებისმიერ დარგში პრინციპები ფუძემდებლური მნიშვნელობის დანაწესებია, ხოლო კონკრეტული კანონები და ქვეყნის წესები უნდა გამომდინარეობდეს და არ ეწინააღმდეგებოდეს უზენაეს პრინციპებს.

ამდენად, კონსტიტუციით მიზანშეწონილია კონკრეტული, სპეციალური მარეგულირებელი ნორმის განერა, რომელიც შეეხება უშუალოდ პერსონალურ მონაცემთა დაცვას. პერსონალურ მონაცემთა დაცვის უფლებასთან მიმართებით, პირადი ცხოვრების უფლება და მისი ფორმულირება, რომელიც კონსტიტუციითაა დადგენილი ნარმოადგენს ზოგადი ხასიათის რეგულაციას. პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებები კავშირში მყოფი კატეგორიებია, თუმცა განსხვავება მათ შინაარსობრივ მონესრიგებაშია.

საინტერესოა, თუ როგორ არის რეგულირებული პერსონალურ მონაცემთა დაცვის საკითხი სხვა ქვეყნების კონსტიტუციებით. მაგალითად, ნიდერლანდების სამეფოს კონსტიტუციის მე-10 მუხლი პირადი ცხოვრების უფლებისა და პერსონალურ მონაცემთა დაცვის უფლების განერას ერთად ახდენს შემდეგი ფორმულირების სახით:

1. ყველას გააჩნია პირადი ცხოვრების დაცვის უფლება, გარდა იმ შეზღუდვებისა, რაც დადგენილია ან მიღებული

ლია პარლამენტის აქტით.

2. პირადი ცხოვრების დაცვის წესები დგინდება პარლამენტის აქტით, რომელიც შეეხება პერსონალური მონაცემების შენახვასა და ჩანერას.
3. წესები, რომელიც შეეხება პირთა უფლებებს შენახული მონაცემების ინფორმირების, მათი გამოყენების და ამ მონაცემთა შესწორების შესახებ, დგინდება პარლამენტის აქტით."

მოცემულ ჩანაწერში ნიდერლანდების სამეფოს კონსტიტუცია არ ახდენს პერსონალურ მონაცემთა დამუშავების საფუძვლებისა და პირობების ცალკე განერას. მისი ფორმულირების გათვალისწინებით ნათელია, რომ, პირველ რიგში, უზრუნველყოფილია პერსონალური მონაცემების დაცვა, ხოლო მეორე მხრივ, ამ საკითხების მონესრიგება დელეგირებულია წარმომადგენლობითი ხელისუფლებისთვის. ამრიგად, მოცემული კონსტიტუცია ეხება, თუმცა სიღრმისეული ფორმით არ ახდენს, პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვის შესაძლებლობათა დეკლარირებას.

საინტერესო მიდგომით გამოირჩევა პორტუგალიის კონსტიტუცია, რომელიც პირადი ცხოვრების, პერსონალური მონაცემებისა და გენეტიკური მონაცემების დაცვას ეხება. მისი 26-ე მუხლის თანახმად:

1. ყველას გააჩნია [...] პირადი და ოჯახური ცხოვრების დაცვის და დისკრიმინაციის ნებისმიერი ფორმის წინააღმდეგ დაცვის უფლება [...].
2. კანონით დადგენილია ეფექტური გარანტიები პირადი და ოჯახური პერსონალური ინფორმაციის მითვისებისა და უკანონო გამოყენების წინააღმდეგ, რომელიც წინააღმდეგობაშია ადამიანურ ღირსებასთან.
3. კანონით უზრუნველყოფილია პიროვნული ღირსება და გენეტიკური იდენტურობა, მათ შორის, ტექნოლოგიების შექმნისგან, განვითარების, გამოყენებისგან და სამეცნიერო ექსპერიმენტებისგან. [...]."

ამ ფორმით, პორტუგალიის კონსტიტუცია აქცენტირებულია გარკვეული სახის პერსონალური ინფორმაციისთვის კონსტიტუციური დაცვის მინიჭებისკენ. მიუხედავად ამისა, გენეტიკუ-

რი პერსონალური მონაცემი წარმოადგენს განსაკუთრებული კატეგორიის, თუმცა მონაცემთა მხოლოდ ერთ სახეობას. შესაბამისად, კონსტიტუცია ერთიანი სახის მითითებას აკეთებს ზოგადად პერსონალური მონაცემების მიმართ, მეორე მხრივ გენეტიკური კატეგორიის მონაცემს განსაკუთრებულად უსვამს ხაზს.

პერსონალურ მონაცემთა დაცვაზე აკეთებს დათქმას შვედეთის 1974 წლის კონსტიტუციური კანონი, რომლის მეორე თავის მე-3 მუხლით მოცემულია შემდეგი ჩანაწერი:

„მოქალაქის პოლიტიკური შეხედულებების შესახებ არსებული ჩანაწერები არ უნდა ინახებოდეს საჯარო რეესტრში მისი თანხმობის გარეშე. ყველა მოქალაქე დაცულია იმ ფარგლებში, პიროვნულობის ნებისმიერი დარღვევის წინააღმდეგ, [...] რაც გამოიხატება პერსონალური ინფორმაციის რეგისტრაციით მონაცემთა დამუშავების ავტომატურისაშუალებების გამოყენების მეშვეობით.“

თვალნათელია, რომ კონსტიტუციური ჩანაწერი ყურადღებას ამახვილებს პერსონალურ მონაცემთა დამუშავების მეთოდებზე. თუმცა, რთულია საუბარი იმის შესახებ დადგენილია თუ არა კონკრეტული შეზღუდვები ინფორმაციის შესაბამისი ნესების დაცვით გამოყენებისთვის.

მონაცემთა დაცვის შესახებ ფორმალურ მითითებას შეიცავს ფინეთის კონსტიტუციაც, რომლის მე-10 მუხლის თანახმად:

„ყველას აქვს უზრუნველყოფილი პირადი ცხოვრების, პატივისცემისა და საცხოვრებლის ხელშეუვალობა. პერსონალურ მონაცემთა დაცვის შესახებ მეტად დეტალური დებულებები დადგენილია კანონით.“

არც ამ შემთხვევაში ვხვდებით პერსონალურ მონაცემთა დაცვის უფლების სიღრმისეულ დეკლარირებას. მითითება იმის შესახებ, რომ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები ნესრიგდება კანონით ახდენს ამ უფლების კონსტიტუციურ აღიარებას, თუმცა მისი შეზღუდვის საფუძვლების განერას არ ახდენს.

საკმაოდ დახვეწილი მიდგომებით გამოირჩევა პოლონეთის კონსტიტუცია, მასში განერილია პერსონალური მონაცემების დაცვასთან დაკავშირებული საკვანძო დებულებები. ამ დოკუ-

მენტით აღიარებულია მონაცემთა დაცვის ფუნდამენტური ხასიათი და მისი შეზღუდვის უზოგადესი საფუძვლები. კონსტიტუციის 51-ე მუხლის თანახმად:

1. „არავინ არაა ვალდებული მოახდინოს პირის შესახებ არსებული ინფორმაციის გამჟღავნება, გარდა კანონით გათვალისწინებული საფუძვლისა.
2. საჯარო პირები არ უნდა მოიპოვებდნენ, აგროვებდნენ ან ახორციელებდნენ წვდომას მოქალაქეთა ინფორმაციაზე, გარდა დემოკრატიულ სახელმწიფოში არსებული აუცილებლობისა, რაც დადგენილია კანონით.
3. ყველას გააჩნია საკუთარი თავის შესახებ არსებულ ოფიციალურ დოკუმენტებთან და მონაცემთა ბაზებთან წვდომის უფლება. შეზღუდვები ამ უფლებაზე შეიძლება დაწესდეს კანონით.
4. ყველას აქვს უფლება მოითხოვოს არასწორი, არასრული ან კანონის საწინააღმდეგო საშუალებებით მოპოვებული ინფორმაციის შესწორება ან წაშლა.
5. პრინციპები ინფორმაციის შეგროვებისა და წვდომისთვის განისაზღვრება კანონით.“

ტექსტის მიხედვით დადგენილია პერსონალური მონაცემის გამოყენების აუცილებლობის პირობა და სუბიექტის უფლება პქონდეს წვდომა საკუთარ პერსონალურ მონაცემზე. მიუხედავად ამისა, დამატებითი პირობები მონაცემთა გამოყენებისთვის, როგორცაა პერსონალურ მონაცემთა დამუშავების პრინციპები, კონსტიტუციით არაა მოცემული.

როგორც ჩანს ევროპული სახელმწიფოების კონსტიტუციები მეტ-ნაკლებად ახდენენ პერსონალურ მონაცემთა დაცვის უფლების დეკლარირებას. ზოგიერთ შემთხვევაში, ეს უფლება პირადი ცხოვრების უფლების ფარგლებშია მოხსენიებული, რაც მეტყველებს ამ ორი უფლების შინაარსობრივ ბმაზე. ამრიგად, ეს მოცემულობა მხოლოდ სამართლებრივი ტექნიკის გამოქაჩილს არ წარმოადგენს.

ნიშნავს თუ არა ეს იმას, რომ იმ ქვეყნებში, რომელთა კონსტიტუციებშიც პერსონალურ მონაცემთა დაცვის უფლებას ცალკე ჩანაწერი არ ეთმობა, უფლება არ არის სათანადოდ დაცული? რა თქმა უნდა პრა. ზოგადი მსჯელობის მიხედვით, არ

იქნება მართებული თუ ვიტყვით, რომ თუ რომელიმე უფლება სახელმწიფოს ძირითად კანონში განმტკიცებული არაა, იგი სათანადოდ არაა დაცული. ამ კონკრეტულ უფლებასთან დაკავშირებით, მაგალითისთვის განვიხილოთ რამდენიმე ევროპული სახელმწიფოს ძირითადი კანონი, სადაც ამ უფლებას არ ეთმობა ცალკე ნორმა და ვნახოთ სხვა რა ალტერნატიული მექანიზმებია გამოყენებული უფლების უზრუნველსაყოფად.

გერმანიის 1949 წლის ძირითადი კანონის მე-2 მუხლი ეხება ინფორმაციული თვითგამორკვევის უფლებას, ხოლო მე-10 მუხლი კორესპოდენციის, ფოსტისა და ტელეკომუნიკაციის ხელშეუხებლობას. არც ერთ მუხლში არაა ნახსენები პერსონალურ მონაცემთა დაცვის უფლება. მიუხედავად ამისა, მონაცემთა დაცვის მიმართულებით გერმანია ერთ-ერთ მონინავე სახელმწიფოდ მიიჩნევა. ამის განმაპირობებელი ფაქტორი, უპირველესად, გერმანიის საკონსტიტუციო სასამართლოს მიერ ჩამოყალიბებული პრაქტიკა და სახელმწიფოში ამ სფეროს მომწესრიგებელი კანონების მოქმედების ხანგრძლივი გამოცდილება უნდა იყოს. როგორც ცნობილია, გერმანიაში პირველი ფედერალური აქტი უშუალოდ მონაცემთა დაცვის შესახებ 1977 წელს იქნა მიღებული, ხოლო 1983 წელს გერმანიის ფედერალურმა საკონსტიტუციო სასამართლომ მნიშვნელოვანი გადანყვეტილება გამოიტანა ე.წ. „მოსახლეობის აღწერის“ საქმეზე, სადაც მოახდინა „ინფორმაციული თვითგამორკვევის“ უფლების ფორმულირება, როგორც ზოგადი პიროვნული უფლების ნაწილად. ამდენად, გერმანიაში პერსონალურ მონაცემთა დაცვას დიდი მნიშვნელობა ენიჭება.<sup>335</sup> შეიძლება ითქვას, რომ დამკვიდრებული ნორმატიული გამოცდილებისა და პრაქტიკის შესაბამისად გერმანიაში პერსონალურ მონაცემთა დაცვის უფლების კონსტიტუციური გაწერის აუცილებლობა არ დგას დღის წესრიგში.

გერმანიის მსგავსად, დამოუკიდებლად არც საფრანგეთის კონსტიტუცია განსაზღვრავს პერსონალურ მონაცემთა დაცვის უფლებას. თუმცა, საყურადღებოა, რომ ჯერ კიდევ 1978 წელს საფრანგეთში მიღებული იყო კანონი ინფორმაციული ტექნო-

335 Koroff, D. (ed.), *Comparative Study on Different Approaches to New Privacy Challenges in Particular in The light of Technological Developments*. A.4., 2010, p. 2.

ლოგიების, ფაილებისა და თავისუფლებების შესახებ, რომლის პირველი მუხლი ადგენს შემდეგს: „ინფორმაციული ტექნოლოგიები თითოეულ მოქალაქეს უნდა ემსახურებოდეს. [...] იგი არ უნდა ლახავდეს ადამიანის იდენტურობას, უფლებებს, პირად ცხოვრებას, ინდივიდუალურ ან საჯარო თავისუფლებებს.“ აღნიშნული კანონი დეტალური და მძლავრი რეგულირების მქონეა, ხოლო ევროპული კავშირის 95/46/EC დირექტივა მისი დებულებებით არის შთაგონებული.<sup>336</sup> ამდენად, საფრანგეთში შესაბამისი საკანონმდებლო და ინსტიტუციური გარანტიები პერსონალურ მონაცემთა დაცვის უფლების უზრუნველყოფის მყარი გარანტიაა, რის გამოც, დიდი ალბათობით, ამ უფლების კონსტიტუციური განერის აუცილებლობა არ დგას დღის წესრიგში.

პერსონალურ მონაცემთა დაცვის უფლების შესახებ ჩანაწერს არც ღანის 1953 წლის კონსტიტუცია შეიცავს, თუმცა ევროკომისიის ექსპერტთა შეფასებით პერსონალურ მონაცემთა დაცვის რეჟიმი კარგად ორგანიზებულია და ეფექტურად მუშაობს.<sup>337</sup>

განხილული მაგალითებიდან ჩანს, რომ იმ სახელმწიფოებში სადაც პერსონალურ მონაცემთა დაცვის უფლება კონსტიტუციურად არ არის განერილი, უფლების დაცვა სხვა ისეთი მექანიზმებით არის უზრუნველყოფილი, რომელიც ქმნის მისი დაცვის ეფექტურ გარანტიებს. გამომდინარე იქედან, რომ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ურთიერთობების სამართლებრივი რეგულირება ქართულ სინამდვილეში გამოწვევებითა და სირთულეებით ხასიათდება, მისი სათანადო დაცვის უზრუნველყოფის მიზნით, მიზანშეწონილია ამ უფლების კონსტიტუციით დამოუკიდებლად განერა და, ამ გზით, უფლების დაცვის გაძლიერება.

უფლების კონსტიტუციურ ხაზგასმას შესაძლებელია სხვა კუთხითაც მოეძებნოს არგუმენტი. კერძოდ, უნდა განისაზღვროს თუ რამდენად „ღირსია“ პერსონალურ მონაცემთა დაცვის უფლება იმისა, რომ გაინეროს კონსტიტუციის ტექტში დამოუკიდებელ უფლებად და, ასევე, განისაზღვროს თუ რა პრაქტიკული შედეგების მომტანი იქნება ეს მოვლენა. კონსტიტუციის

<sup>336</sup> იქვე, გვ. 1, 54.

<sup>337</sup> იქვე, გვ. 7.

ტექსტში ამა თუ იმ ფუნდამენტური უფლების განერა განპირობებულია იმით, რომ ადამიანური შესაძლებლობების რეალიზებისთვის უფლება სარგებლობს განსაკუთრებული დაცვით. გარდა ამისა, სახელმწიფოს აკისრია პასუხისმგებლობა კონკრეტული უფლების უზრუნველყოფის მხრივ, რაც ვლინდება პოზიტიური და ნეგატიური ვალდებულებების შესრულების აუცილებლობაში. აქედან გამომდინარე, პერსონალური მონაცემების მზარდი მნიშვნელობის გამო სახეზეა მისი ცალკე დეკლარირების აუცილებლობა.

მიიჩნევა, რომ პერსონალურ მონაცემთა დაცვის უფლება ევროპული კონსტიტუციის (ევროპული კავშირის დამფუძნებელი აქტების) ნაწილია და მან დამოუკიდებელი ფუნდამენტური უფლების სტატუსი მოიპოვა პირადი ცხოვრების უფლების გვერდით.<sup>338</sup> პირადი ცხოვრების უფლება მეტად გამოკვეთს ინდივიდუალურ კომპონენტს და პირს ანიჭებს შესაძლებლობას აღკვეთოს სხვა პირთა ჩარევა პირად და ოჯახურ ცხოვრებაში, შესაბამისად, იგი ნეგატიური კატეგორიის უფლებად გვევლინება. ამის საპირისპიროდ, პერსონალურ მონაცემთა დაცვის უფლება განსაზღვრავს ნესებს, მეთოდებს მათი დამუშავებისთვის და ადგენს დინამიურ დაცვას სხვადასხვა პირობების გათვალისწინებით.<sup>339</sup> საყურადღებოა ისიც, რომ პერსონალურ მონაცემთა დაცვა არეგულირებს ინფორმაციული დისტრიბუციის საკითხებს ფიზიკურ პირებსა და სახელმწიფოს შორის, მომხმარებლებსა და სერვისის/პროდუქციის მომწოდებლებს შორის. შესაბამისად, პერსონალურ მონაცემთა დაცვა შესაძლებელია აღვიქვათ, როგორც ინფორმაციული დისტრიბუციის დაცვა.<sup>340</sup>

ახლა კი, დავუბრუნდეთ პერსონალურ მონაცემთა დაცვის უფლების უშუალოდ კონსტიტუციის ტექსტში განმტკიცების საკითხს. აქ შეგვიძლია დავსვათ შემდეგი შეკითხვა: რა ხელშესახები და პრაქტიკული შედეგი ექნება ამ უფლების კონსტი-

338 Hert, P. D. & Gutwirth, S., *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*. Springer Science, 2009, p. 7.

339 Gutwirth, S., Pouillet, Y., Hert, P.D., Terwangne, C., Nouwt, S. *Reinventing Data Protection?*, Springer, 2009, p. 79-80.

340 იქვე, გვ. 340.

ტუციურ დეკლარირებას? ამ შეკითხვაზე პასუხი მსჯელობას საჭიროებს, ხოლო უშუალოდ პასუხის გაცემამდე, მიზანშეწონილია პუნქტობრივად მივყვეთ საყურადღებო პირობებს, რომლებსაც გააჩნიათ გავლენა ზემოაღნიშნულ საკითხზე:

1. საქართველოს კონსტიტუცია არ შეიცავს ჩანაწერს პერსონალურ მონაცემთა დაცვის უფლების შესახებ;
2. შესაბამისად, როდესაც საუბარია მონაცემთა დაცვის უფლებაში ჩარევაზე, იგი ყოველთვის უნდა განვიხილოთ პირადი ცხოვრების უფლების დაცვის ან, მეტად ზოგადი, პიროვნების თავისუფალი განვითარების უფლების ფარგლებში;
3. თუ პერსონალურ მონაცემთა დაცვის უფლებას მოვიაზრებთ პირადი ცხოვრების უფლების დაცვის ფარგლებში, მაშინ, ამ უფლების შეზღუდვისთვის უნდა გამოვიყენოთ ის საფუძვლები (ზღვრები), რომელიც დადგენილია პირადი ცხოვრების უფლებაში ჩარევისთვის;
4. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, განსხვავებით საქართველოს კონსტიტუციისგან, იცნობს ამ უფლებაში ჩარევის სხვა საფუძვლებსაც. ისინი დიფერენცირებულია დასამუშავებელ მონაცემთა კატეგორიების მიხედვით. კანონი განასხვავებს დამუშავების საფუძვლებს არასენსიტიური და განსაკუთრებული კატეგორიის ინფორმაციისთვის. საყურადღებოა ისიც, რომ განსაკუთრებული პერსონალური მონაცემების დამუშავების შემთხვევაში, ზემოაღნიშნული საფუძვლებით დამუშავებისას, მათი გასაჯაროება და მესამე პირებისთვის გადაცემა დაუშვებელია მონაცემთა სუბიექტის თანხმობის გარეშე. ამდენად, პერსონალურ მონაცემთა დაცვის სამართალში განსაკუთრებული ყურადღება ეთმობა პირის შესახებ არსებული ინფორმაციის გამოყენების წესებს. ამით, იგი დეტალიზებულ რეგულირებას გვთავაზობს.
5. შეიძლება ითქვას, რომ კანონი აკონკრეტებს კონსტიტუციით დადგენილ საფუძვლებს პირადი ცხოვრების ამ სფეროში ჩარევისთვის, თუმცა, საქართველო, უფლების შეზღუდვის კონსტიტუციით დადგენილი

საფუძვლები არაა სრულყოფილი. სხვა სიტყვებით, როდესაც დამუშავების საფუძვლად გათვალისწინებულია დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების, დანაშაულის თავიდან აცილების პირობა, ან თუნდაც სხვთა უფლებების დაცვის ზოგადი დანაწესი, დამუშავების შემთხვევაში პროცესი უნდა ექმნება რეზოლუციის პერსონალურ მონაცემთა დაცვის სამართალში აღიარებულ პრინციპებს, მაგალითად სისწორესა და ვადიანობას. ამ სფეროში მოქმედი ძირითადი პრინციპები დამუშავებელს წინასწარ ავალდებულებს იზრუნოს დასამუშავებელი პერსონალური მონაცემების კანონიერებაზე, მიზანზე, პროპორციებზე, სისწორეზე და მათი ნაშლის დროისა და პირობის წინასწარ განსაზღვრაზე, იქედან გამომდინარე, რომ გარკვეული სამართლებრივი ურთიერთობისთვის საჭირო პერსონალური მონაცემების რაოდენობა, კატეგორიები და სახეები წინასწარ დადგენილია. ამიტომ, პერსონალურ მონაცემთა დამუშავების პრინციპები პრევენციული ღონისძიებებია და პოსტ-ფაქტუმ ასამოქმედებელი რეპრესიული მექანიზმი.

6. ამ არგუმენტაციით, კონსტიტუციის როგორც მოქმედი, ისე ახალი რედაქციის ტექსტი, ჩარევის საფუძვლების ნაწილში მოკლებულია პერსონალურ მონაცემთა დამუშავებისთვის დადგენილ საფუძვლებთან ფორმალურ და მატერიალურ კავშირს. ამდენად, კონსტიტუციური ნორმა ადეკვატურად ვერ პასუხობს პერსონალურ მონაცემთა დამუშავებისთვის დადგენილ მოთხოვნებს.

პერსონალურ მონაცემთა დაცვის სამართლის მთელი არსი ვლინდება იმაში, რომ დამუშავების პროცესის კანონიერების გარდა, გადამწყვეტი მნიშვნელობა აქვს მიზნის არსებობას. იქედან გამომდინარე, რომ დამუშავებელმა წინასწარ უნდა განსაზღვროს მიზნები, მან ასევე, წინასწარ უნდა იცოდეს რა სახისა და კატეგორიის პერსონალურ მონაცემთა დამუშავება მოუწევს. სხვა სიტყვებით, რამდენადაც მონაცემები ინფორმაციის ძალზედ კონკრეტული სახეობებია, დამუშავებელი წინასწარ არის ვალდებული დაადგინოს შეზღუდვის ფარგლები (პრინციპების

მეშვეობით), რათა მისი საქმიანობა რაც შეიძლება მეტად გან-  
ჭვრეტადი იყოს.

ახლა კი, განვიხილოთ თუ როგორ ვლინდება პერსონალურ  
მონაცემთა დამუშავებასთან დაკავშირებული პრობლემური სა-  
კითხები პრაქტიკაში. ყველაზე მკაფიოდ, პერსონალურ მონაცე-  
მთა დამუშავების პრობლემატიკა ვლინდება ისეთ შემთხვევებ-  
ში, როგორიცაა მათი დამუშავება კანონის თანახმად. როგორც  
აღინიშნა, კანონის საფუძველზე არასენსიტიურ პერსონალურ  
მონაცემთა დამუშავება დასაშვებია „პერსონალურ მონაცემთა  
დაცვის შესახებ“ საქართველოს კანონით შესაბამისად, საკმარი-  
სია სამართლებრივად განისაზღვროს ნორმა, რაც საშუალებას  
მოგვცემს დავინყოთ დამუშავების პროცესი. პრაქტიკაში არ-  
სებული მიდგომის თანახმად, მონაცემთა კანონისმიერი დამუ-  
შავების საფუძვლის ინტერპრეტირება ძალზედ ფართოდ ხდება.  
დემონსტრირებისთვის მიზანშეწონილია განვიხილოთ შემდეგი  
მაგალითები:

### მაგალითი №1

„საჯარო რეესტრის შესახებ“ საქართველოს კანონის თა-  
ნახმად „საჯარო რეესტრში რეგისტრირებული მონაცემები და  
მარეგისტრირებელ ორგანოში დაცული დოკუმენტაცია არის  
საჯარო და ხელმისაწვდომია გასაცნობად ნებისმიერი პირი-  
სათვის, გარდა საქართველოს კანონმდებლობით დადგენილი  
შემთხვევებისა.“<sup>341</sup> ეს ჩანაწერი წარმოადგენს დამუშავების კა-  
ნონით გათვალისწინებულ საფუძველს. საჯარო რეესტრის საქ-  
მიანობის ფარგლებში დამუშავების ამგვარი საფუძვლის ინერ-  
პრეტირებას ფართო ხასიათი გააჩნია. მაგალითად, საჯარო რე-  
ესტრში იურიდიული პირის (შპს, ა(ა)იპ და სხვა) რეგისტრაციი-  
სას ხდება ისეთი სარეგისტრაციო დოკუმენტების გასაჯარო-  
ვება, როგორიცაა იურიდიული პირის დამფუძნებლის ვინაობა  
(სახელი, გვარი), პირადი ნომერი, პირადობის მონმობის ელექ-  
ტრონული ასლი, იურიდიული პირის წესდება და დამფუძნებლის  
წესდებაზე თანდართული ხელმოწერა. ერთი შეხედვით, ამკარაა  
საზოგადოებრივი ინტერესის საკითხი, უფრო კონკრეტულად,  
მონაცემთა ამგვარი გასაჯაროვება ხელს უწყობს უძრავი ქო-

341 „საჯარო რეესტრის შესახებ“ საქართველოს კანონი, მ. 6, პ. 1.

ნების მესაკუთრის მოძიებას, ასევე, იურიდიული პირის დამფუძნებლის ვინაობის გაგებას, რათა მიღებული ინფორმაციის მეშვეობით სამართლებრივი ურთიერთობების დამყარება რისკ-ფაქტორების არსებობის გარეშე განხორციელდეს.

მეორე მხრივ, მიუხედავად მოცემული მიზნებისა, ბალანსი ინფორმაციის ხელმისაწვდომობასა და მონაცემთა დაცვას შორის აშკარად არაა პროპორციული. მაგალითად, უძრავი ქონების საკუთრების დამადასტურებელი დოკუმენტის (ამონაწერის) შემთხვევაში, კითხვას ბაღებს ფიზიკური პირის პირადი, უნიკალური ნომრის მითითების საკითხი. დამუშავების მიერ არ არის გათვალისწინებული ის გარემოება, რომ უნიკალური იდენტიფიკატორის საჯაროდ მითითება საშუალებას იძლევა მოხდეს მისი მოძიება სხვა საინფორმაციო, საჯარო წყაროებშიც. ამასთან, ამონაწერში პირადი ნომერი მითითებულია სხვა ინფორმაციასთან ერთად, როგორიცაა სახელი, გვარი, უძრავი ქონების ზუსტი მისამართი, რაც პიროვნების იდენტიფიცირებას ხდის ძალიან მარტივს.

იურიდიული პირის რეგისტრაციის შემდგომ განთავსებული მონაცემები განსხვავებით უძრავი ქონების ამონაწერისა, მეტად თვალსაჩინოდ წარმოაჩენს არაპროპორციულობის პრინციპს. როგორც აღინიშნა, იურიდიული პირის რეგისტრაციისას, სხვა მონაცემებთან ერთად, საჯარო ხდება დამფუძნებლის პირადობის მოწმობის ელექტრონული ასლი და მისი ხელმოწერა, რომელიც ახლავს წესდებას. პერსონალური მონაცემების გადამეტებით დამუშავება სახეზეა, რამდენადაც არ არსებობს რაიმე საფუძველი (აქ არ უნდა ვიგულისხმოთ კანონით დადგენილი დამუშავების ზოგადი საფუძველი), რომელიც აუცილებელს ხდის მონაცემთა ამგვარი მოცულობით გასაჯაროვებას. იურიდიული პირის ავთენტურობის დასადასტურებლად, არაა საჭირო ამგვარი ინფორმაციის საჯარო განთავსება, რადგან საჯარო რეესტრში არსებული ამონაწესების მიმართ მოქმედებს პრეზუმფცია, რის მიხედვითაც გარკვეული ქონების ან იურიდიული პირის რეგისტრაციისას მოქმედებს მისი ნამდვილობის პირობა. უფრო კონკრეტულად, „საჯარო რეესტრში რეგისტრირებულ მონაცემთა მიმართ მოქმედებს უტყუარობის

პრეზუმფცია [...]."<sup>342</sup> შესაბამისად, პერსონალურ მონაცემთა დამუშავება საჯარო რეესტრის მიერ ამ და დამუშავების სხვა ნაწილში არღვევს პროპორციულობის პრინციპს, რომლის მიხედვითაც „მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევაც მუშავდება ისინი.“<sup>343</sup> გასათვალისწინებელია ისიც, რომ პერსონალურ მონაცემთა დამუშავებისთვის დადგენილი პრინციპები ერთობლიობაში უნდა განვიხილოთ, კერძოდ, დამუშავების პირველი პრინციპის მიხედვით პერსონალური მონაცემები უნდა დამუშავდეს „სამართლიანად და კანონიერად, მონაცემთა ღირსების შეუღახავად.“<sup>344</sup> ნორმის გრამატიკული განმარტების თანახმად, სამართლიანობის, კანონიერებისა და ღირსების შეუღახაობის კრიტერიუმები კუმულაციურად უნდა დაკმაყოფილდეს. საჯარო რეესტრის მიერ დანერგილი პრაქტიკა კი, წინააღმდეგობაშია, სულ მცირე, სამართლიანობის პრინციპთან მიმართებით, რის გამოც სახეზეა პერსონალურ მონაცემთა დამუშავების ფუნდამენტური პრინციპების დარღვევა.

დამატებით, კანონის მოცემულ დანაწესში, ფართო გაგებით, დარღვეულია ნორმის განსაზღვრულობის პრინციპიც. როდესაც ნორმატიულ აქტებში დაშვებულია პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვა (იმ გაგებით, რომ მათი დამუშავება ამ უფლების შეზღუდვას ნიშნავს), არაა დადგენილი თუ რა ოდენობით, რა პროპორციების დაცვითაა იგი დასაშვები. შესაბამისად, კანონმდებელი ვალდებულია, მიიღოს განჭვრეტადი და მკაფიო მარეგულირებელი აქტები, რომელიც კანონის განსაზღვრულობის კრიტერიუმს დააკმაყოფილებს.

## მაგალითი №2

დამუშავების პროპორციულობის პრინციპთან შეუთავსებლობის პრობლემატიკა მეტად აშკარადაა სახეზე საარჩევნო

342 იქვე, მ. 5.

343 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მ. 4, პ. „გ“.

344 იქვე, პ. „ა“.

სიების საჯაროდ გამოქვეყნების ნაწილში. ამომრჩეველთა სიაში საკუთარი თავის გადამწმენის მიზნით საქართველოს საარჩევნო კოდექსის საფუძველზე შექმნილია პერსონალურ მონაცემთა საჯარო ელექტრონული ბაზა (voters.cec.gov.ge), სადაც სუბიექტებს გვარისა და პირადი ნომრის ჩანერის მეშვეობით შეუძლიათ შეიტყონ არიან თუ არა შეყვანილნი ამომრჩეველთა ერთიან სიაში და გაიგონ თუ რომელ საარჩევნო უბანზე არიან რეგისტრირებულები. ამ ინფორმაციის საჯაროობას უზრუნველყოფს საქართველოს ცენტრალური საარჩევნო კომისია, რომელიც მოქმედებს საქართველოს საარჩევნო კოდექსის მიხედვით, კერძოდ, „ცესკო პასუხისმგებელია ამომრჩეველთა ერთიანი სიის ფორმირებისათვის, მისი კომპიუტერული დამუშავებისა და საჯარო ინფორმაციისთვის მიკუთვნებული ნაწილის (გვარი, სახელი; ფოტოსურათი; დაბადების თარიღი; მისამართი საქართველოს მოქალაქის პირადობის მონმობის ან სააგენტოს მონაცემთა ბაზის მიხედვით, აგრეთვე ფაქტობრივი საცხოვრებელი ადგილის მისამართი – საქართველოს ოკუპირებული ტერიტორიებიდან იძულებით გადაადგილებული პირისთვის, მისამართის მითითების გარეშე რეგისტრირებული პირისთვის, საცხოვრებელი ადგილის მიხედვით რეგისტრაციიდან მოხსნილი პირისთვის და პირისთვის, რომლის რეგისტრაციაც ძალადაკარგულად გამოცხადდა სააგენტოს გადანაცვებით; ამომრჩეველთა ერთიან სიაში ამომრჩევლის რეგისტრაციის თარიღი) ცესკოს ოფიციალურ ვებგვერდზე განთავსებისთვის.“<sup>345</sup>

თუ გავითვალისწინებთ იმ გარემოებას, რომ პიროვნების სახელისა და გვარის, ასევე, მისი პირადი ნომრის მოპოვება სხვა საჯარო ბაზების მეშვეობითაც შესაძლებელია, მაგალითად, როგორცაა საჯარო რეესტრის ბაზა, სავსებით დასაშვებია, რომ ამ წყაროს გამოყენებით მოპოვებული ინფორმაციის მეშვეობით ამომრჩეველთა ვებ-გვერდზე მოხდეს პიროვნების შესახებ დამატებითი ინფორმაციის მოპოვება. ეს მონაცემები საჯარო რეესტრის ვებ-გვერდზე არაა მოცემული. შედეგად, ვიღებთ მოცემულობას, რომლის თანახმად ორი სხვადასხვა წყაროს გამოყენებით ერთი და იმავე პირის შესახებ სხვადასხვა სახის ინფორმაცია ხდება ხელმისაწვდომი.

345 საქართველოს საარჩევნო კოდექსი, მ. 31, ნაწ. 4.

აქვე, საარჩევნო სიებთან მიმართებით გასათვალისწინებელია ერთი მნიშვნელოვანი საკითხი: საქართველოში საარჩევნო კანონმდებლობის მთავარ მოქმედ სამართლებრივ აქტად საარჩევნო კოდექსი გვევლინება, რომელიც ორგანული კანონის სახითაა მიღებული. ეს კი იმას ნიშნავს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმები ვერ იქნება ქმედუნარიანი ვებ-გვერდზე მონაცემთა გამოქვეყნების პროპორციების უზრუნველსაყოფად, ვინაიდან საარჩევნო კოდექსი იერარქიულად მაღლა მდგომ სამართლებრივ აქტს წარმოადგენს. შესაბამისად, ორგანულ კანონში მოცემული ზოგადი ჩანაწერი პერსონალურ მონაცემთა გამოქვეყნების შესახებ დამმუშავებელს საშუალებას აძლევს გამოაქვეყნოს ინფორმაცია ამ აქტით დადგენილი წესის თანახმად, ისე, რომ არ გაითვალისწინოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილი პრინციპები.

უნდა ავლნიშნოთ, ასევე, პერსონალურ მონაცემთა დაცვის ინსპექტორის (ამჟამად, სახელმწიფო ინსპექტორი) პოზიცია საჯარო რეესტრის ეროვნულ სააგენტოსა და ცესკო-ში პერსონალურ მონაცემთა დამუშავების (ხელმისაწვდომობის) მართლზომიერებასთან დაკავშირებით. ორივე დამმუშავებელთან მიმართებით ინსპექტორმა აღნიშნა, რომ პერსონალურ მონაცემთა დამუშავება არ სცდება კანონიერების ფარგლებს და არსებობს შესაბამისი მიზნები და საფუძვლები. მისი აზრით, საჯარო რეესტრის ეროვნული სააგენტოს მიერ ბიზნესისა და უძრავი ქონების რეგისტრაციასთან დაკავშირებული მონაცემების საჯაროობა ემსახურება შესაბამის მიზანს, კერძოდ, სააგენტოსთვის კანონით დაკისრებული მოვალეობების შესრულებას. ასევე, რამდენადაც გასაჯაროება დადგენილია შესაბამისი ნორმატიული აქტით (კანონით) არც ამ მიმართულებით არსებობს ხარვეზები და პროცესი სავსებით თავსებადია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან. ინსპექტორის პოზიცია ცესკო-ს მიერ პერსონალურ მონაცემთა გამოქვეყნებასთან დაკავშირებით ანალოგიური არგუმენტებით არის გამყარებული, კერძოდ, მიზანს წარმოადგენს ამომრჩეველთა ერთიანი სიის ფორმირება და შესაძლო უზუსტობების აღმოფხვრა, ხოლო საფუძვლად გვევლინება საარჩევნო კოდექსის შესაბამისი ნორ-

მა. ამრიგად, ინსპექტორის აზრით, ეს პროცესიც არ ეწინააღმდეგება კანონის მოთხოვნებს.<sup>346</sup>

თუ ამ არგუმენტებს მივიღებთ და ხელს შევეწყობთ ამგვარი პრაქტიკის განვითარებას, სახეზე გვექნება მოცემულობა, სადაც პერსონალურ მონაცემთა დამუშავებისთვის (გასაჯაროებისთვის) საკმარისი იქნება მარტოდენ შესაბამისი პროცედურების დაცვით მიღებული ნორმატიული აქტი. სხვა სიტყვებით, მთავარია გასაჯაროების პირობა კანონით იყოს დადგენილი, ხოლო შემდგომ ნორმის პრაქტიკაში გამოყენებისას აღარ იქნება საჭირო შესაბამისი პროპორციების დაცვა. ამ ლოგიკით, საჭირო აღარ იქნება ნორმის შემდგომი გამოყენების მართლზომიერების, გამოყენების პროპორციებისა და ნორმის კონკრეტულ სიტუაციაში მორგების (თანაზომიერების) წინასწარი გათვალისწინება. დღეს არსებული პრობლემა, რომელიც ამ ტიპის ქმედებებს (გასაჯაროებას კანონის საფუძველზე) თან ერთვის არის სწორედაც ნორმის ზედაპირული გააზრება, მისი ხისტი და ყოვლისმომცველი განმარტება. იქამდე, სანამ პერსონალურ მონაცემთა დამუშავების პროცესი, რომელიც კანონით იქნება ნებადართული, არ შემოწმდება პროპორციულობისა და ზოგადი კონსტიტუციურობის ჭრილში, რთული იქნება პერსონალურ მონაცემთა სუბიექტების უფლების დაცვა მათ შესახებ არსებული მონაცემების დამუშავებისას პროპორციულობის უზრუნველყოფა. დავამატოთ ისიც, რომ ნებისმიერი კანონი, რომელიც არის ძირითადი უფლების შემზღუდავი, სხვა პირობებთან ერთად, უნდა აკმაყოფილებდეს სიცხადის კრედიტერიუმს, ხოლო სადაც ძირითად უფლებაში ჩარევა ინტენსიურ ხასიათს იძენს, კანონი, ამავდროულად, უნდა შეიცავდეს დეტალურ მონსრიგებას და შეზღუდვის გასაგებ წესებს.<sup>347</sup>

ამ სიტუაციიდან გამოსავალი შესაძლოა საერთაშორისო აქტმა მოგვცეს. როგორც ცნობილია საქართველოს რატიფიცირებული აქვს ევროპის საბჭოს 108-ე კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ.“ საქართველოს კონსტიტუციის თანახმად „[...]“

346 საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიში, 2014, გვ. 10-11.

347 ბოხაშვილი, კორკელია, გვ. 28-31.

საქართველოს საერთაშორისო ხელშეკრულებას ან შეთანხმებას, თუ იგი არ ეწინააღმდეგება საქართველოს კონსტიტუციას ან კონსტიტუციურ შეთანხმებას, აქვს უპირატესი იურიდიული ძალა. შიდასახელმწიფოებრივი ნორმატიული აქტების მიმართ.<sup>348</sup> „საქართველოს საერთაშორისო ხელშეკრულებების შესახებ“ საქართველოს კანონის თანახმად „ოფიციალურად გამოქვეყნებული საქართველოს საერთაშორისო ხელშეკრულების დებულებები, რომლებიც ადგენენ კონკრეტული ხასიათის უფლებებსა და მოვალეობებს და არ საჭიროებენ დამაზუსტებელი შიდასახელმწიფოებრივი ნორმატიული აქტის მიღებას, საქართველოში მოქმედებენ უშუალოდ.“<sup>349</sup> 108-ე კონვენცია შეიცავს ნორმებს, რომელიც შინაარსობრივად უნარიანია იმოქმედოს უშუალოდ და დაარეგულიროს პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული ფუნდამენტური საკითხები. დამუშავების პროპორციულობის პრინციპი ამ დოკუმენტიდან განერილია, კერძოდ, ავტომატურ დამუშავებას დაქვემდებარებული პერსონალური მონაცემები „უნდა იყოს ადეკვატური და არ უნდა აღემატებოდეს იმ მიზნებს, რომლებისთვისაც ისინი ინახება.“<sup>350</sup>

გარდა ამისა, ცესკო-ს მიერ ამომრჩეველთა სიების ხელმისაწვდომობის საკითხში დამუშავების პროპორციულობის პირობა ირღვევა იმითაც, რომ ფიზიკური პირების შესახებ ინფორმაცია ხელმისაწვდომია არამარტო წინასაარჩევნო ან საარჩევნო პერიოდში, არამედ მუდმივად. კონვენციის მიხედვით პერსონალური მონაცემები „დაცული უნდა იყოს იმ ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიკაციის საშუალებას მხოლოდ იმ დროში, რაც საჭიროა იმ მიზნებისთვის, რისთვისაც ინახება ეს მონაცემები.“<sup>351</sup> ცესკო-ს შემთხვევაში კი, პერსონალური მონაცემების საჯაროდ განთავსება (დამუშავება) ხორციელდება არასაარჩევნო პერიოდშიც, რითაც იგი არღვევს შესაბამის ვადებით დამუშავებისა და პროპორციულობის პრინციპს. სამწუხაროა ის ფაქტი, რომ ასეთ შემთხვევაში დამ-

348 საქართველოს კონსტიტუცია, მ. 4, პ. 5.

349 „საქართველოს საერთაშორისო ხელშეკრულებების შესახებ“ საქართველოს კანონი, მ. 6, პ. 3.

350 ევროპის საბჭოს 108-ე კონვენცია, მ. 5, პ. „გ.“

351 იქვე, მ. 5, პ. „ე.“

მუშავებელი ინფორმაციის გამოქვეყნებისას არ იყენებს 108-ე კონვენციით დადგენილ დამუშავების პრინციპებს. მათი დაცვის ვალდებულება მას ზემდგომი აქტით - საერთაშორისო ხელშეკრულებით აკისრია.

მოცემული მაგალითები ცხადყოფს, რომ პერსონალურ მონაცემთა ორი უდიდესი დამუშავებლის მიერ არ ხდება კანონით დადგენილი პრინციპების დაცვა მათი საქმიანობის პროცესში. უგულებელყოფილია პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის ნორმები. მოცემულობას ამწვავებს ის, რომ პრაქტიკაში არსებული მიდგომის თანახმად, თუ დამუშავების საფუძველს წარმოადგენს კანონით გათვალისწინებული საფუძველი, თავად დამუშავების მართლზომიერების შემოწმება პროპორციების ჭრილში აღარ ხდება. მიუხედავად იმისა, რომ საერთაშორისო აქტი იერარქიულად ზემდგომ აქტს წარმოადგენს ორგანულ კანონთან მიმართებით, ყურადღება მაინც არ ექცევა მასში მოცემულ უშუალოდ მოქმედ ნორმებს.

ამ გარემოებათა გათვალისწინებით პერსონალურ მონაცემთა დაცვის უფლების კონსტიტუციური განმტკიცების ერთ-ერთი მიზანია აღმოიფხვრას ბუნდოვანება, ნებისმიერი საფუძვლით დამუშავებისას, პრინციპების აპრიორი მოქმედების/უმოქმედობის თაობაზე. პრინციპების კონსტიტუციური განმტკიცებით ცალსახად დადგინდება, რომ რა საფუძველიც არ უნდა გვექონდეს პერსონალურ მონაცემთა დამუშავებისთვის, იგი აუცილებლად უნდა გამომდინარეობდეს კონსტიტუციაში მოცემული დანაწესიდან. სხვა სიტყვებით, დამუშავების საფუძვლები არ უნდა განიმარტოს კონსტიტუციურ დებულებებთან წინააღმდეგობრივად.

ამდენად, სიტუაციიდან ქმედით გამოსავალს წარმოადგენს პერსონალურ მონაცემთა დაცვის უფლებისა და მისი შეზღუდვის საფუძვლების კონსტიტუციური დეკლარირება. ამასთან, კანონმდებელი არ უნდა შემოიფარგლოს მხოლოდ უფლების დეკლარირებით, არამედ აუცილებელია გაინეროს მონაცემთა დამუშავების ფარგლები, პრინციპები და უფლების შეზღუდვის საფუძვლებიც. საორიენტაციოდ შესაძლებელია აღებულ იქნეს ევროპული კავშირის ძირითად უფლებათა ქარტიის მე-8 მუხლი, რომელიც ეხება პერსონალურ მონაცემთა დაცვის უფლებას.

მასში მოცემული პრინციპები და შეზღუდვის გზები ის მინიმალური ფორმაა, რის მიხედვითაც უნდა მოხდეს ამ უფლების დეკლარირება.

შეჯამებისას, აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის უფლება პირადი ცხოვრების უფლებასთან მიმართებით წარმოადგენს სპეციალურ ნორმას. არ იქნება გასაკვირი თუ ვიტყვით, რომ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები აქტუალობით დღეს - ტექნოლოგიური პროგრესის ფონზე გამოირჩევა. პერსონალური მონაცემების, როგორც თანამედროვეობის მატერიალური და არამატერიალური ღირებულებების შესახებ ნაშრომში არაერთხელ გაკეთდა მითითება. ეს მოცემულობა პერსონალური მონაცემების ახლებურ აღქმის განმსაზღვრებელია, თანამედროვე ციფრულ სამყაროში პირის შესახებ არსებული მონაცემების გახშირებული გამოყენების გამო დამკვიდრდა ინფორმაციული პრიატულობის ცნება. ამრიგად, მისი ადგილი პირადი ცხოვრების უფლების ფარგლებში მეტად თვალსაჩინოა და განსაკუთრებული.

ეჭვგარეშეა, რომ პირის პერსონალური მონაცემების ფლობით შესაძლებელია მის პირად ცხოვრებაში შეჭრა იმგვარად, რომ მან ამის შესახებ ვერ გაიგოს. შესაბამისად, პერსონალურ მონაცემთა ბაზების ფორმირება და მათი შენახვა თანამედროვე იურისპრუდენციის უდიდეს გამოწვევას წარმოადგენს.

თანამედროვე სამყაროში პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობა მეტ და მეტ დატვირთვას იძენს. გარდა კანონის მოქმედებისა, აუცილებელია მისი ნორმები მკაფიოდ განსაზღვრავდეს პერსონალურ მონაცემთა მართვასთან დაკავშირებულ საკითხებს. მიუხედავად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დადებითი მხარეებისა, მისი ზოგიერთი დებულება საჭიროებს დახვეწასა და დაზუსტებას. ნორმის განჭვრეტადობის პირობის დაკმაყოფილებისა და, საბოლოოდ, უფლების დაცვის მკაფიო დანაწესების ფორმირების მიზნით.

გარდა ბუნდოვანი დებულებებისა, კანონში არაა გაკეთებული რაიმე მითითება უსაფრთხოების ერთიან სტანდარტზე; რომელიც გავრცელდება თითოეულ დამმუშავებელსა და უფლებამოსილ პირზე. პერსონალურ მონაცემთა დამმუშავებისას ტე-

ქნიკური და ორგანიზაციული უსაფრთხოების უზრუნველყოფა ისეთივე მნიშვნელობის მქონეა, როგორც დამუშავების პრინციპების გარანტირება. ამდენად, კანონის ეს ნაკლოვანი მხარე საჭიროებს დროის მოკლე ვადებში რეაგირებას.

ერთ-ერთი მთავარი დაბრკოლება, რაც ხელს უშლის პერსონალურ მონაცემთა დაცვის სფეროს განვითარებას სახელმწიფოში, არის პერსონალურ მონაცემთა დაცვის ინსპექტორის გადანყვეტილებათა სასამართლოში გასაჩივრების შეზღუდული ფარგლები. დაჯარიმების თაობაზე ინსპექტორის გადანყვეტილებების გადასინჯვა არ ხდება საკასაციო ინსტანციაში, რაც აფერხებს ამ მიმართულებით სასამართლოს მრავალფეროვანი პრაქტიკის ჩამოყალიბებას.

პერსონალურ მონაცემთა დაცვის უფლება აკმაყოფილებს ძირითადი უფლებისთვის დამახასიათებელ აუცილებელ თვისებებს. ეს კი ერთ-ერთი საფუძველია მისი დამოუკიდებელი რეგულირებისთვის. ამავდროულად, ცალკე მონესრიგება ხაზს გაუსვამს მის მნიშვნელობას სახელმწიფოში და შექმნის დაცვის მეტ გარანტიებს.

სახეზეა სხვა გამონკვევებიც, კერძოდ, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი საკანონმდებლო აქტების იერარქიაში ყველაზე დაბალ საფეხურზეა, რის გამოც თუ მასზე იერარქიულად მაღლა მდგომი ნორმატიული აქტით დადგინდა პერსონალურ მონაცემთა დამუშავების მოთხოვნა, პერსონალურ მონაცემთა დაცვის შესახებ კანონს არ ექნება სამართლებრივი მოქმედების ძალა ზემდგომი აქტის მიმართ. საკითხს ართულებს ის ფაქტორიც, რომ პრაქტიკაში არ ხდება საერთაშორისო აქტების დებულებათა გათვალისწინება, მაშინაც კი, თუ მათნორმებს შესწევთ უნარი პირდაპირ და უშუალოდ დაარეგულიროს საკითხი. არც დამუშავების პროცესის ფარგლებთან, პროპორციებთან დაკავშირებული სირთულეები არის უმნიშვნელო. პრაქტიკის მიხედვით, თუ პერსონალურ მონაცემთა დამუშავება ხდება კანონის საფუძველზე, დამუშავების პროპორციებს ნაკლებად ექცევა ყურადღება.

სწორედ ამ გამონკვევებზე საპასუხოდ მიზანშეწონილია პერსონალურ მონაცემთა დაცვის უფლების კონსტიტუციის ტექსტში ასახვა, რასაც არ გააჩნია მხოლოდ ფორმალური დატვირთვა.

სახელმწიფოს უზენაეს კანონში მისი ფორმულირება სხვადასხვა სახითაა შესაძლებელი, თუმცა ნებისმიერ შემთხვევაში უნდა გაინეროს პრაქტიკული შედეგის მომტანი დებულებები. მთავარი გასათვალისწინებელი საკითხები შესაძლებელია შემდეგი სახით დაჯგუფდეს:

1. განისაზღვროს, რომ პერსონალურ მონაცემთა დაცვის უფლება არის ერთ-ერთი ფუნდამენტური უფლებათაგანი. თავდაპირველად მიზანშეწონილია დადგინდეს მისი დაცვის ზოგადი არსი და დაცული სფერო;
2. შემდგომ, სასურველია მოხდეს პერსონალურ მონაცემთა დამუშავების პრინციპების ფორმულირება. მთავარია, კონსტიტუციის ტექსტში ნათლად ჩამოყალიბდეს პერსონალურ მონაცემთა დამუშავების პრინციპები, რომლებიც წარმოადგენენ სახელმძღვანელო დებულებებს დამუშავებლებისა და უფლებამოსილი პირების მიერ მონაცემთა გამოყენებისთვის;
3. უნდა განისაზღვროს სუბიექტის უფლებები პერსონალურ მონაცემთა დამუშავებისას და მათი შეზღუდვის საფუძვლებიც, რომელიც უკავშირდება აღმატებული საზოგადო ინტერესის და მესამე პირთა კანონიერი უფლებების დაცვას;
4. ხაზი უნდა გაესვას პერსონალურ მონაცემთა დამუშავების საკითხებზე მაკონტროლებელი ორგანოს/თანამდებობის პირის სტატუსსა და უფლებამოსილებებს.



**გამომცემლობა „იურისტების სამყარო“**

**თბილისი, მ. კოსტავას ქ. №75**

**ტელ: (+995 032)238 35 99; (+995)557 51 51 34**

**ვებ-გვერდი: [www.law.ge](http://www.law.ge)**

**ელ-ფოსტა: [Info@law.ge](mailto:Info@law.ge)**

**[www.facebook.com/PublishingWorldofLawyers](https://www.facebook.com/PublishingWorldofLawyers)**