

პერსონალურ მონაცემთა დამუშავებისა და საჯაროობის სამართლებრივი მოწესრიგება

შესავალი

ჯერემი ბენტამი, როდესაც ციხის ახალი მოდელის – პანოპტიკონის – შექმნაზე ფიქრობდა, ალბათ, ვერც კი წარმოიდგენდა, რომ სამი საუკუნის შემდეგ არამატერიალური სამყაროს, ინტერნეტის, მეშვეობით ადამიანზე მუდმივი ზედამხედველობის განხორციელება შესაძლებელი გახდებოდა. პანოპტიკონის პროექტის კონცეფცია იმაში მდგომარეობს, რომ ციხის ზედამხედველი ყველა ბინადარს ისე აკვირდება, რომ მათ ამის შესახებ არ იციან. ახალ ციფრულ ეპოქაში ინტერნეტი მასობრივი დაკვირვების იარაღად იქცა, ელექტრონულ პანოპტიკონად, როგორც სახელმწიფოს, ისე კომპანიების ხელში.¹

როგორც ლიტერატურაში აღნიშნავენ, 21-ე საუკუნეში ინფორმაციული თვითგამორკვევა იგივეა, რაც თავისუფლება ჯონ სტიუარტ მილის დროს². თანამედროვე ტექნოლოგიების განვითარებამ მონაცემები ფართო საზოგადოებისთვის უფრო ადვილად ხელმისაწვდომი გახადა, ვიდრე ეს ტრადიციული ფორმებით დამუშავების დროს იყო³. ელექტრონულმა ეპოქამ ადამიანის პირადი ცხოვრების ხელშეუხებლობა, მისი რეპუტაცია, ინფორმაციული თვითგამორკვევა საფრთხის ქვეშ დააყენა. აღსანიშნავია, რომ ინდივიდის პირად

¹ EU data protection reform: A pandora's box or a new dawn for personal data? იხ., <<http://thenextweb.com/insider/2013/06/01/eu-data-protection-reform-a-pandoras-box-or-a-new-dawn-for-personal-data/>>[2.06.2013].

² Anonymity, Privacy and Identity in a Networked Society, edited by Ian Kerr, Valerie Steeves, Carole Luckock, Oxford, 2009, 8, იხ., <<http://www.idtrail.org/content/view/799>>[2.06.2013].

³ Opinion 4/2007 on the Concept of Personal Data, Article 29 Data Protection Working Party, adopted on the 20th June, 5, იხ., <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>[2.06.2013].

ცხოვრებას, როგორც ადამიანის ერთ-ერთ ძირითად უფლებას, კონსტიტუცია იცავს. სახელმწიფო ისევეა ვალდებული, არ ხელყოს ადამიანის პირადი ცხოვრება, როგორც უფლება არ აქვს, აწამოს, ცემოს ან მოკლას ადამიანი. ამასთან, პიროვნების პირადი ცხოვრების ხელყოფისგან დაცვა არა მხოლოდ სახელმწიფოსგან გახდა საჭირო, არამედ სხვა კერძო, ფიზიკური ან იურიდიული პირებისგანაც. შესაბამისად, კანონმა ინდივიდი უნდა დაიცვას, როგორც სახელმწიფოს, ისე მესამე პირთა უკანონო ჩარევისგან.

საქართველოში პერსონალური მონაცემების დაცვის სტანდარტის ამღლევისა და საქართველოს კანონმდებლობის საერთაშორისო აქტებთან ჰარმონიზაციის მიზნით 2012 წელს მიღებული იქნა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი. მიუხედავად იმისა, რომ ამ საკითხებს საქართველოს კონსტიტუცია და ზოგადი ადამინისტრაციული კოდექსი აწესრიგებდა, საჭირო იყო თანამედროვე რეალობისა და გამოწვევების გათვალისწინება, მეტი დეტალიზაცია პერსონალური მონაცემების დამუშავების, გადაცემის, შენახვის ვადების კუთხით. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის პირველ მუხლში აღნიშნულია, რომ კანონის მიზანია, პერსონალური მონაცემების დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა. წინამდებარე სტატიის განხილვის ძირითად საგანს სწორედ ეს საკითხი წარმოადგენს – კანონის მიღების შედეგად მიღწეულია თუ არა პირის პირადი ცხოვრების დაცვის მიზანი. სტატიაში ასევე განხილულია პერსონალური ინფორმაციის ცნება და „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის სხვა საკანონმდებლო აქტებთან მიმართების საკითხი.

1. პირადი ცხოვრების კონსტიტუციური გარანტიები

საქართველოს კონსტიტუციის მე-20 მუხლი ადამიანის პირადი ცხოვრების ხელშეუხებლობის უფლებას განამტკიცებს. პიროვნების პირადი ცხოვრების ხელშეუხებლობა ფართო ცნებაა და იგი განიმარ-

ტება არა მხოლოდ პირადი კორესპონდენციისა და საცხოვრებლის გარეშე პირთა ჩარევისგან დაცვის უფლებით, არამედ ის მოიცავს: ა) პირის ფიზიკურ და მორალურ ხელშეუხებლობას; ბ) სახელმწიფოს მიერ პირადი მონაცემების შეგროვებასა და შენახვას და პირადი ინფორმაციის ხელმისაწვდომობას; გ) სქესობრივი ცხოვრების საიდუმლოებას; დ) სახელებს.⁴ ეს იმდენად ყოვლისმომცველი უფლებაა, რომ შეიძლება ითქვას, ესაა უფლება მთელი დანარჩენი სამყაროს წინააღმდეგ.⁵ სახელმწიფოს ან მესამე პირის მიერ პირადი ინფორმაციის შეგროვება პირადი ცხოვრების არეალში შეჭრად ითვლება. ევროსამართლოს მართლმსაჯულებამ ადამიანის სახელი და გვარი, ასევე სხვა სახის მაიდენტიფიცირებელი ინფორმაცია პირადი ცხოვრების სფეროში მოაქცია.⁶

სახელმწიფოს მიერ პირადი მონაცემების შეგროვებისა და შენახვის და პირადი ინფორმაციის ხელმისაწვდომობის უფლებას საქართველოს კონსტიტუციის ცალკე მუხლი ეთმობა. კონსტიტუციის 41-ე მუხლის თანახმად „1. საქართველოს ყოველ მოქალაქეს უფლება აქვს კანონით დადგენილი წესით გაეცნოს სახელმწიფო დაწესებულებებში მასზე არსებულ ინფორმაციას, აგრეთვე იქ არსებულ ოფიციალურ დოკუმენტებს, თუ ისინი არ შეიცავენ სახელმწიფო, პროფესიულ ან კომერციულ საიდუმლოებას. 2. ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, მის ფინანსებთან ან სხვა კერძო საკითხებთან, არავისთვის არ უნდა იყოს ხელმისაწვდომი თვით ამ ადამიანის თანხმობის გარეშე, გარდა კანონით დადგენილი შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, ჯანმრთელობის, სხვათა უფლებებისა და თავისუფლებების დასაცავად“. ამ უფლებას ინფორმაციულ თვითგამორკვევას უწოდებენ. ინდივიდი

⁴ იზორია ლ., კორკელია კ., კუბლაშვილი კ., ზუბუა გ., საქართველოს კონსტიტუციის კომენტარები, თბილისი, 2005, 123.

⁵ იქვე, 17.

⁶ ოქრუაშვილი მ., პირადი ცხოვრების ხელშეუხებლობა, თბილისი, 2012, 48, იხ. <<http://liberty.ge/wp-content/uploads/2012/10/Piradi-zxovrebi-xelsheuxebloba.pdf>> [2.06.2013].

უფლებამოსილია თავად გააკონტროლოს მის შესახებ არსებული ინფორმაცია.⁷ კონსტიტუციის 41-ე მუხლი მიმართულია სახელმწიფოს წინააღმდეგ. სახელმწიფო დაწესებულებებში არსებული ინფორმაცია არ შეიძლება ყოვლისმომცველი იყოს, რამდენადაც ამ შემთხვევაში სახელმწიფოსთვისაც და მესამე პირებისთვისაც ადვილია ადამიანით მანიპულაცია და მისი მართვა.⁸ ამიტომ პიროვნებამ უნდა იცოდეს თუ რა ინფორმაციის მოპოვება შეუძლია სახელმწიფოს მის შესახებ და რა ინფორმაციას ფლობს იგი.

2. რა არის პერსონალური მონაცემები?

2.1. კანონის მოქმედების სფერო

პერსონალური მონაცემების შეგროვების, შენახვისა და გადაცემის საკითხებს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი აწესრიგებს. იმისთვის, რომ აღნიშნული კანონით დაცვის სფერო დადგინდეს, უპირველესად, აუცილებელია გაანალიზდეს, თუ რას გულისხმობს პერსონალური ინფორმაცია. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, პერსონალური მონაცემი ნებისმიერი ინფორმაციაა, რომელიც იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს უკავშირდება. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი პირდაპირ ან არაპირდაპირ იდენტიფიცირება, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.

კანონმდებელმა პერსონალური მონაცემების ცნებისთვის ძალზე ფართო მნიშვნელობის მინიჭება განიზრახა. პერსონალური მონაცემების ცნება იმდენად ზოგადია, რომ ის მოიცავს ყველა ინფორმაციას, რომელიც იდენტიფიცირებად პირს უკავშირდება. მიუხედავად „პერსონალური მონაცემების“ ფართო ცნებისა, იდენტიფიცირებად

⁷ ბიჭია მ., პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით, თბილისი, 2012, 48.

⁸ იზორია ლ., კორკელია კ., კუბლაშვილი კ., ხუბუა გ., საქართველოს კონსტიტუციის კომენტარები, თბილისი, 2005, 352.

პირთან დაკავშირებული ყველა სახის ინფორმაცია პერსონალურ მონაცემებად არ უნდა ჩაითვალოს. კანონის მოქმედება არასტრუქტურული ფორმით, ხელით დამუშავებაზე არ ვრცელდება. იგი ვრცელდება მხოლოდ „საქართველოს ტერიტორიაზე ავტომატური ან ნახევრად ავტომატური საშუალებებით მონაცემთა დამუშავებაზე, აგრეთვე არაავტომატური საშუალებებით იმ მონაცემთა დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შეტანის მიზნით მუშავდება“.⁹ კანონი ასევე არ ვრცელდება ფიზიკური პირის მიერ აშკარად პირადი ან საოჯახო მიზნებისთვის მონაცემების დამუშავებაზე, სასამართლო სამართალწარმოებაზე, სახელმწიფო საიდუმლოებაზე, მონაცემთა საზოგადოებრივი და სახელმწიფო უსაფრთხოების (მათ შორის ეკონომიკური უსაფრთხოების), თავდაცვის, ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნებისათვის დამუშავებაზე.¹⁰ მართლაც, არასასურველი შედეგი ექნება ამ წესების იმ საკითხებზე გავრცელებას, რომელთათვისაც ის კანონმდებელს არ შეუქმნია.¹¹ კანონი გამონაკლისების ჩამონათვალში ნოტარიუსებს, ადვოკატებს, დეტექტივებს არ გამოყოფს, რაც მოცემული კანონის მათზე ჩვეულებრივ გავრცელებას გულისხმობს.

2.2. პერსონალური მონაცემების ლეგალური დეფინიცია

პერსონალური მონაცემების ლეგალური დეფინიცია, რომელიც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-2 მუხლის „ა“ ქვეპუნქტითაა გათვალისწინებული, შეიძლება ოთხ ძირითად ელემენტად დაიყოს: ა) „ნებისმიერი ინფორმაცია“; ბ) „რომელიც

⁹ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის 1-ლი პუნქტი.

¹⁰ იქვე, მე-3 პუნქტი.

¹¹ Opinion 4/2007 on the Concept of Personal Data, Article 29 Data Protection Working Party, adopted on the 20th June, 4,

ბზ. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> [2.06.2013].

უკავშირდება“; გ) „იდენტიფიცირებული ან იდენტიფიცირებადი“; დ) „ფიზიკური პირი“. ¹²

2.2.1. პირველი ელემენტი – „ნებისმიერი ინფორმაცია“

ფრაზა „ნებისმიერი ინფორმაცია“ უკვე მიუთითებს მის ფართო მნიშვნელობაზე. ინფორმაციის ბუნების გათვალისწინებით იგი შეიძლება იყოს ობიექტური, მაგალითად, პიროვნების სისხლის ჯგუფი, ან სუბიექტური, როგორიცაა, მისი შეხედულებები და შეფასებები. ამასთან, „პერსონალურ მონაცემთა“ ცნებისთვის მნიშვნელობა არ უნდა ჰქონდეს, ის სიმართლეა თუ საეჭვო ინფორმაციას წარმოადგენს. ეს იმთავითვე გათვალისწინებულია კანონით, რადგან პერსონალურ მონაცემთა დაცვის ნორმები არასწორი ინფორმაციის წაშლას ითვალისწინებს. „პერსონალური მონაცემების“ ცნება მოიცავს, როგორც პირის პირად და საოჯახო ცხოვრებას („stricto sensu“), რომელიც განსაკუთრებით მგრძნობიარე მონაცემთა კატეგორიას მიეკუთვნება, ისე პირის ყველა სახის აქტივობას, მის სამსახურებრივ, ეკონომიკურ თუ სოციალურ ქცევას. იგი მოიცავს პირის, როგორც მომხმარებლის, პაციენტის, დასაქმებულის, კლიენტის შესახებ ინფორმაციას.¹³

2.2.2. მეორე ელემენტი – „რომელიც დაკავშირებულია“

ერთი შეხედვით, ნებისმიერი ინფორმაცია, რომელიც ინდივიდს უკავშირდება, მის პერსონალურ მონაცემებს წარმოადგენს. თუმცა, ზოგჯერ ინფორმაცია ობიექტს და არა პირს უკავშირდება, მაგალითად, უძრავი ქონების ფასი. ეს არაა პერსონალური ინფორმაცია, მაგრამ ობიექტი მესაკუთრეს ეკუთვნის, რომლის მიმართაც ამ მონაცემის მიხედვით საგადასახადო ვალდებულებები წარმოიშობა. ამ კონტექსტში ეს ინფორმაციაც პერსონალურ მონაცემებს წარმოადგენს.¹⁴

¹² იქვე, 6.

¹³ იქვე, 6-7.

¹⁴ იქვე, 11.

2.2.3. მესამე ელემენტი „იდენტიფიცირებული ან იდენტიფიცირებადი“

პირი შეიძლება იდენტიფიცირებულად ჩაითვალოს, როდესაც მისი ჯგუფის სხვა წევრებისგან „გამორჩევა“ შესაძლებელია. ლეგალური დეფინიციის მე-3 ელემენტი განსაკუთრებით მნიშვნელოვანია ვიდეო თვალთვალის განხორციელებისას, რადგან მაკონტროლებლები ხშირად აცხადებენ, რომ შეგროვებული მასალიდან მხოლოდ მცირე ნაწილის იდენტიფიცირებას ახერხებენ, ამიტომ პირის იდენტიფიცირებამდე ეს მონაცემები პერსონალურ მონაცემებად არ უნდა ჩაითვალოს. თუმცა, ვიდეო თვალთვალის მიზანი სწორედ ფირზე გამოსახულ პირთა ამოცნობაა. შესაბამისად, ვიდეო თვალთვალის მონაცემები პერსონალურ მონაცემებად იმ შემთხვევაშიც უნდა ჩაითვალოს, როდესაც ჩანაწერში ასახული პირის იდენტიფიცირება ვერ ხერხდება.¹⁵

პერსონალურ მონაცემებზე საკითხის განხილვისას ასევე მნიშვნელოვანია ფსევდონიმები და ანონიმური მონაცემები. ფსევდონიმი პერსონალურ მონაცემად ჩაითვალება თუ არა, დამოკიდებულია იმაზე, რამდენად დაცულია იგი. თუ ფსევდონიმის კონკრეტულ პიროვნებასთან დაკავშირება შეუძლებელია, მაშინ ის ასეთად ვერ ჩაითვლება, მაგრამ თუ პირის დადგენა ფსევდონიმით შესაძლებელია, პერსონალურ მონაცემთა დამუშავების წესები შედარებით დაბალი ხარისხით მასზეც უნდა გავრცელდეს.¹⁶

ანონიმური მონაცემები პერსონალურ მონაცემებად არ უნდა ჩაითვალოს, რამდენადაც მათი იდენტიფიცირება შეუძლებელია. თუმცა, თუ ანონიმური ინფორმაცია მოცემულია ძალზე მადისკრიმინირებელი კრიტერიუმით, შეიძლება, ანონიმურობა მოიხსნას და პირი სხვებისთვის იდენტიფიცირებადი გახდეს. მაგალითად, ქალაქის 6000 მოსახლეს მხოლოდ ერთი ექიმი ემსახურება.¹⁷

¹⁵ იქვე, 16.

¹⁶ იქვე, 20.

¹⁷ იქვე, 21.

2.2.4. მეოთხე ელემენტი - „ფიზიკური პირი“

კანონი პირდაპირ აღნიშნავს, რომ მონაცემები ფიზიკურ პირს უნდა უკავშირდებოდეს. აქ წარმოიშობა საკითხი იმის შესახებ ვრცელდება თუ არა პერსონალურ მონაცემთა დაცვა გარდაცვლილ და იურიდიულ პირებზე.

2.2.4.1. გარდაცვლილი პირი და საკანონმდებლო მოწესრიგებები

გარდაცვლილ პირებთან დაკავშირებით კანონმა გადაწყვეტილება ცალსახად მიიღო. მე-7 მუხლში აღნიშნულია, რომ მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება დასაშვებია მონაცემთა სუბიექტის შმობლის, შვილის, შვილიშვილის ან მეუღლის თანხმობით ან თუ მონაცემთა სუბიექტის გარდაცვალებიდან გასულია 30 წელი. თუმცა, ეს ჩანაწერი წინააღმდეგობაში მოდის „ეროვნული საარქივო ფონდისა და არქივის შესახებ“ კანონთან, რომლის 22-ე მუხლის მე-4 პუნქტის „ბ“ ქვეპუნქტში აღნიშნულია, რომ მოქალაქეთა დაშვება შეზღუდულია პერსონალური მონაცემების შემცველ დოკუმენტებთან, გარდა მოქალაქეთა საკუთრების უფლების შემცველი დოკუმენტებისა, მათი შექმნიდან 75 წლის განმავლობაში, თუ ეროვნულ არქივს და იმ პირებს შორის, რომლებსაც უშუალოდ ეხებათ ეს მასალები, უფრო მცირე ვადა არაა დადგენილი. ასევე 23-ე მუხლში აღნიშნულია, რომ „პირს უფლება აქვს, ეროვნულ არქივს მოსთხოვოს არ დაუშვას თავისი კუთვნილი დოკუმენტის გამოყენება ან საჯაროდ ჩვენება თავის მიერ განსაზღვრული ვადით, რომელიც არ უნდა აღემატებოდეს 75 წელს“. აქედან გამომდინარე, პერსონალური მონაცემების შექმნიდან 75 წლის განმავლობაში დასაშვებია მათი გასაიდუმლოება. შესაძლოა, პერსონალური მონაცემები პირის გარდაცვალებამდე 10 წლით ადრე შეიქმნას, ისე რომ ეროვნულ არქივსა და ამ პირს შორის რაიმე შეთანხმება არ იყოს. მაშინ, ამ კანონის თანახმად, ეს მონაცემები არა 30 წლის, არამედ კიდევ 65

წლის განმავლობაში პირად საიდუმლოებას უნდა წარმოადგენდეს. ნორმათა კოლიზიის გადასაჭრელად სპეციალური ნორმის პრინციპის გამოყენებაც რთულია, რადგან ძნელია განისაზღვროს ამ ორ კანონს შორის რომელია სპეციალური. ასეთ შემთხვევაში „ნორმატიული აქტების შესახებ“ კანონი საკითხს იმის მიხედვით წყვეტს, თუ რომელი ნორმატიული აქტია უფრო გვიან მიღებული¹⁸, რაც არცთუ ისე კარგი გამოსავალია. მით უმეტეს იმ პრაქტიკის გათვალისწინებით, რომ მუხლის რედაქციაში ცვლილებები ძალზე ხშირად შედის, ყველაზე ახალი კანონის პრინციპის მიხედვით, შესაძლოა არაერთგვაროვანი პრაქტიკა ჩამოყალიბდეს. ამიტომ უმჯობესია, ამ ორი კანონის კოლიზიური ნორმები ერთმანეთთან შესაბამისობაში მოვიდეს.

გარდაცვლილ პირთან დაკავშირებით „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-7 მუხლთან მიმართებაში ასევე კოლიზიურ ნორმად მიიჩნევა „პაციენტის უფლებების შესახებ“ კანონის 27-ე მუხლი, რომელშიც აღნიშნულია, რომ სამედიცინო მომსახურების გამწევი ვალდებულია პაციენტის შესახებ მის ხელთ არსებული ინფორმაციის კონფიდენციალობა დაიცვას, როგორც პაციენტის სიცოცხლეში, ისე მისი სიკვდილის შემდეგ. ამ შემთხვევაში ინფორმაციის, მათ შორის, ავადმოყოფობის ისტორიების, შენახვის ვადები დაწესებული არაა, რაც ამ ინფორმაციის საიდუმლოებაზე მიუთითებს მთელი მისი არსებობის მანძილზე და არა მხოლოდ 30 წლის განმავლობაში. ამიტომ უმჯობესი იქნება, თუ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-7 მუხლის პირველ პუნქტს დაემატება ფრაზა „თუ კანონით სხვა რამ არ არის განსაზღვრული“.

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-7 მუხლი გარდაცვლილი პირის შესახებ მონაცემების დამუშავების წრეს მეტისმეტად აფართოებს. გარდა ამ ორი საფუძვლისა, როგორცაა, მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის თანხმობა ან მონაცემთა სუბიექტის

¹⁸ „ნორმატიული აქტების შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-7 პუნქტი.

გარდაცვალებიდან 30 წლის გასვლა, მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ მონაცემების შეგროვება დასაშვებია ყველა იმ შემთხვევაში, რომელსაც კანონი ჩვეულებრივი და განსაკუთრებული კატეგორიის მონაცემების შეგროვებისთვის განსაზღვრავს.

გარდაცვლილ პირთან მიმართებაში, ასევე, საინტერესოა ის საკითხი, როდესაც გარდაცვლილი პირის შესახებ ინფორმაციით ცოცხალი ფიზიკური პირის შესახებ ინფორმაციის გაგებაა შესაძლებელი. მაგალითად, თუ გაიას ჰქონდა ჰემოფილია, ეს ნიშნავს, რომ მისი ვაჟი ტიტიუსიც იტანჯება ჰემოფილიით.¹⁹ ვფიქრობ, რომ ასეთ შემთხვევაში პერსონალურ მონაცემთა დაცვის ჩვეულებრივ დადგენილი წესები უნდა გავრცელდეს და არა გარდაცვლილ პირებზე მოცემული მოწესრიგებები.

2.2.4.2. იურიდიული პირი

როგორც პერსონალური ინფორმაციის ცნება განმარტავს, იგი ფიზიკურ პირებს შეეხება. თუმცა, ირიბად დასაშვებია, იგი ასევე იურიდიულ პირებზე გავრცელდეს, რადგან ინფორმაცია იურიდიულ პირებზე ამავე დროს შეიძლება ფიზიკურ პირებზე ინფორმაციას მოიცავდეს. თუ იგი რაღაც ფორმით მაინც ფიზიკურ პირს უკავშირდება, მაშინ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი იურიდიულ პირებზეც უნდა გავრცელდეს.

3 მონაცემთა დამუშავება

3.1. მონაცემთა დამუშავების დასაშვები შემთხვევები

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, მონაცემთა დამუშავება დასაშვებია, თუ: „ა) არსებობს მონაცემთა

¹⁹ Opinion 4/2007 on the Concept of Personal Data, Article 29 Data Protection Working Party, adopted on the 20th June, 22, იხ., <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> [2.06.2013].

სუბიექტის თანხმობა; ბ) მონაცემთა დამუშავება გათვალისწინებულია კანონით; გ) მონაცემთა დამუშავება საჭიროა მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად; დ) მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად; ე) მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესი; ვ) კანონის თანახმად, მონაცემები საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა; ზ) მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად; თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად)“.²⁰

კანონში მონაცემთა დამუშავების საკმაოდ ფართო წრეა ჩამოთვლილი. მონაცემთა დამუშავება შესაძლებელია მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად, ამავე დროს, ცალკეა აღნიშნული, რომ მონაცემთა დამუშავება შესაძლებელია, თუ ეს აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად. საჯარო ინტერესი იმდენად ფართო ცნებაა, რომ პრაქტიკულად ყველა შემთხვევაშია ინფორმაციის შეგროვება შესაძლებელი. ეს ნიშნავს, რომ პერსონალური მონაცემების შეგროვება შესაძლებელია იმ საჯარო ინტერესების დასაცავად, რომელიც კანონში მითითებული არაა, რის შედეგადაც არაგონივრულადაა გაზრდილი მონაცემთა დამუშავების შესაძლებლობა.

²⁰ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლი.

3.2. პირის უფლებები მონაცემთა დამუშავების პროცესში

თუ მონაცემთა შეგროვება უშუალოდ მონაცემთა სუბიექტისაგან ხორციელდება, მონაცემთა დამუშავებელი ან უფლებამოსილი პირი ვალდებულია მონაცემთა სუბიექტს მიაწოდოს შემდეგი ინფორმაცია: მონაცემთა დამუშავებლისა და უფლებამოსილი პირის ვინაობა და რეგისტრირებული მისამართი, მონაცემთა დამუშავების მიზანი, სავალდებულოა თუ ნებაყოფლობითი მონაცემთა მიწოდება. თუ სავალდებულოა მასზე უარის თქმის სამართლებრივი შედეგები, მონაცემთა სუბიექტის უფლება, მიიღოს ინფორმაცია მის შესახებ დამუშავებულ მონაცემთა თაობაზე, მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა და განადგურება. კანონის თანახმად, თუ მონაცემთა შეგროვება უშუალოდ მონაცემთა სუბიექტისაგან არ ხორციელდება, მონაცემთა დამუშავებელი ან უფლებამოსილი პირი ვალდებულია მოთხოვნის შემთხვევაში მონაცემთა სუბიექტს მიაწოდოს ამ მუხლის პირველ პუნქტში აღნიშნული ინფორმაცია. თუმცა, ევროსაბჭოს 1995 წლის 24 ოქტომბრის „პირთა დაცვის შესახებ მათი პირადი მონაცემების გადამუშავების პროცესში და ასეთი მონაცემების თავისუფალი მიმოქცევის შესახებ“ დირექტივის თანახმად აუცილებელია, რომ ზემოაღნიშნული ინფორმაცია, პირის მოთხოვნისგან დამოუკიდებლად, ყველა შემთხვევაში პირისთვის მიწოდებული უნდა იქნას²¹. მართლაც, გაუგებარია, როგორ უნდა მოითხოვოს თავად პირმა ინფორმაციის მიწოდება, თუ არ ეცოდინება, ვინ აგროვებს მის შესახებ ინფორმაციას. ზოგადი ადმინისტრაციული კოდექსით გათვალისწინებული იყო საჯარო დაწესებულების ვალდებულება – „დაუყოვნებლივ აცნობოს შესაბამის პირს მის უკანასკნელ ცნობილ მისამართზე მესამე პირის ან საჯარო დაწესებულების მიერ მისი პერსონალური მონაცემების მოთხოვნის

²¹ 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 movemonet of such data, article 11. ახ, <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf>

შესახებ“. როგორც ვხედავთ, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი პერსონალურ მონაცემთა დამუშავების უფრო დაბალ სტანდარტს აწესებს, ვიდრე ეს ზოგადი ადმინისტრაციული კოდექსით იყო გათვალისწინებული.

კანონში მოცემული არაა პერსონალურ მონაცემთა შენახვის ვადები. ყოველ ადამიანს აქვს უფლება, რომ დავიწყებული იქნას. მის შესახებ ერთხელ მოპოვებული ინფორმაცია, სამუდამოდ შენახული არ უნდა იყოს. ამიტომ კანონი შენახვის ვადას უნდა აწესებდეს.

4. განსაკუთრებული კატეგორიის მონაცემები

4.1. განსაკუთრებული კატეგორიის მონაცემების ცნება

პერსონალური მონაცემების მნიშვნელობის მიხედვით კანონი განსაკუთრებული კატეგორიის მონაცემებს გამოყოფს. განსაკუთრებული კატეგორიის მონაცემებს წარმოადგენს: „მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული ორგანიზაციის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან ან ნასამართლობასთან, ასევე, ბიომეტრული მონაცემი, რომლითაც შესაძლებელია პირის იდენტიფიცირება ზემოაღნიშნული ნიშნებით“. ²² ცხადია, „მგრძნობიარობის“ კრიტერიუმი სუბიექტივიზმს უკავშირდება, მაგრამ განსაკუთრებულად სენსიტიურად უნდა მივიჩნიოთ ისეთი ინფორმაცია, რომლის გამოქვეყნებას საჩოთიროდ მიიჩნედა ყველა ჩვეულებრივი მგრძნობიარე ადამიანი. ²³ როგორც ვხედავთ, კანონში სხვადასხვა კატეგორიის მონაცემები ერთადაა დაჯგუფებული. მაგალითად, ჯანმრთელობის შესახებ მონაცემებს წარმოადგენს ის, რომ პირს ფეხი აქვს მოტეხილი და ასევე ისიც, რომ ფსიქიკური პრობლემები აქვს. ამათგან, განსაკუთრებული სენსიტიურობით მეორე

²² „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ბ“ ქვეპუნქტი.

²³ ბიჭია მ., პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით, თბილისი, 2012, 76.

მათგანი გამოირჩევა, თუმცა, კანონი ორივეს ერთ კატეგორიაში აერთიანებს. იგივე შეიძლება ითქვას ნასამართლეობაზე, რომელიც სხვა მონაცემებთან შედარებით ნაკლები სენსიტიურობით გამოირჩევა.

4.2. განსაკუთრებული კატეგორიის მონაცემების დამუშავება

აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვაზე ზოგადი ადმინისტრაციული კოდექსის მოწესრიგება, რომელიც 2012 წელს გაუქმდა, კრძალავდა საჯარო დაწესებულების მიერ იმგვარი პერსონალური მონაცემების დამუშავებას, რომელიც დაკავშირებულია პირის რელიგიურ, სექსუალურ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ ან მსოფლმხედველობრივ შეხედულებებთან. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია. თუმცა, იქვე გამონაკლისი შემთხვევების ვრცელი ჩამონათვალია მოცემული, რაც გულისხმობს იმას, რომ კანონმა განსაკუთრებული კატეგორიის მონაცემების დამუშავების შესაძლებლობა დაუშვა. ეს შემთხვევებია: „ა) მონაცემთა სუბიექტმა გამოხატა წერილობითი თანხმობა განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე; ბ) მონაცემთა სუბიექტმა საჯარო გახადა მის შესახებ მონაცემები მათი გამოყენების აშკარა აკრძალვის გარეშე; გ) მონაცემთა დამუშავება აუცილებელია მონაცემთა დამუშავებლის მიერ შრომითი ვალდებულების შესრულებისათვის ან მასთან დაკავშირებული უფლების განხორციელებისათვის; დ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად უნარი არა აქვს, განაცხადოს თანხმობა მონაცემთა დამუშავებაზე; ე) მონაცემთა დამუშავება ზორციელდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნებისათვის, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის; ვ) მონაცემთა დამუშავება ზორციელდება ლეგიტიმური საქმიანობის განხორციელებისას პოლიტიკური,

ფილოსოფიური, რელიგიური ან სავაჭრო გაერთიანების, ასოციაციის ან სხვა არაკომერციული ორგანიზაციის მიერ. ასეთ შემთხვევაში მონაცემთა დამუშავება შეიძლება დაკავშირებული იყოს მხოლოდ ამ ორგანიზაციის წევრებთან ან პირებთან, რომლებსაც მუდმივი კავშირი აქვთ ამ ორგანიზაციასთან“.²⁴

4.3. განსაკუთრებული კატეგორიის მონაცემების დაცვის ხარისხი

პერსონალური მონაცემებიდან განსაკუთრებული კატეგორიის მონაცემების ცალკე გამოყოფა ამ კატეგორიის მონაცემების უფრო მაღალი ინტენსივობით დაცვის მოლოდინს აჩენს. განსაკუთრებული კატეგორიის მონაცემების დაცვა მინიმუმ უნდა გულისხმობდეს მონაცემთა სუბიექტის მიერ ამ ინფორმაციის კონტროლის საშუალებას. პირის ექსკლუზიურ ნებაზე, მის არჩევანზე უნდა იყოს დამოკიდებული, მონაცემთა დამუშავებელის მიერ მონაცემთა დამუშავების შესაძლებლობა. მე-6 მუხლის მე-2 პუნქტში მოცემული საფუძვლები ითვალისწინებს იმგვარ გარემოებებს, როდესაც პირის თანხმობის გარეშე შეიძლება განსაკუთრებული კატეგორიის მონაცემების დამუშავება მოხდეს („დ“ და „ვ“ ქვეპუნქტები). მე-6 მუხლის მე-3 პუნქტში კი აღნიშნულია, რომ ამ მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტის საფუძველზე მონაცემთა დამუშავების შემთხვევაში დაუშვებელია მონაცემთა მესამე პირისათვის გამჟღავნება მონაცემთა სუბიექტის თანხმობის გარეშე. რაც გულისხმობს იმას, რომ სხვა შემთხვევაში დასაშვებია მონაცემთა სუბიექტის თანხმობის გარეშე მესამე პირისთვის განსაკუთრებული კატეგორიის მონაცემების გადაცემა. უფრო მეტიც, კანონი ზოგადად უშვებს მესამე პირისგან მონაცემების დამუშავებას, რომლის შესახებაც მონაცემთა სუბიექტს ინფორმაციას არ აწვდიან, გარდა იმ შემთხვევისა თუ პირი თვითონ არ მოითხოვს ინფორმაციის გაცნობას. ზოგადად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება ან აკრძალულია ან

²⁴ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტი.

განსაკუთრებული დაცვის ღონისძიებების მეშვეობითაა დასაშვები²⁵. საბოლოოდ კი გაუგებარი ხდება განსაკუთრებული კატეგორიის მონაცემების ცალკე გამოყოფა და მასთან დაკავშირებით სპეციალური ნორმების არსებობა, თუ ეს ვერ უზრუნველყოფს მის განსაკუთრებულ დაცვას.

განსაკუთრებული კატეგორიის მონაცემების დამუშავების წრე უნდა შემცირდეს. უმჯობესია, დიფერენცირებულად იქნას განხილული თითოეული განსაკუთრებული კატეგორიის მონაცემის დამუშავების საკითხი. მაგალითად, რელიგიური და ფილოსოფიური შეხედულებების შესახებ მონაცემების დამუშავების უფლება მიენიჭოს მხოლოდ რელიგიურ და ფილოსოფიურ ორგანიზაციებს. ეთნიკური წარმომადგენლობის შესახებ მონაცემების დამუშავება დასაშვები იყოს მხოლოდ მაშინ, როდესაც ეს მონაცემთა სუბიექტის იდენტიფიკაციის ერთადერთი საშუალებაა ან ეს აუცილებელია იმ პირის იდენტიფიკაციისთვის, რომელიც მიეკუთვნება იშვიათი კატეგორიის ეთნიკურ ან კულტურულ უმცირესობას. პოლიტიკური შეხედულებების შესახებ მონაცემების დამუშავების უფლება მხოლოდ პოლიტიკურ ინსტიტუტებსა და გაერთიანებებს მიენიჭოს, სავაჭრო კავშირისადმი კუთვნილება – სავაჭრო კავშირებს, პირის ჯანმრთელობის მდგომარეობის შესახებ – სამედიცინო და სადაზღვევო კომპანიებს.²⁶ რაც შეეხება, მონაცემებს სქესობრივ ცხოვრებაზე, მისი განსაკუთრებული სენსიტიურობიდან გამომდინარე, უმჯობესია, განსაკუთრებული კატეგორიის მონაცემთა ჩამონათვალიდან ამოღებული იქნას, რაც მისი დამუშავების შესაძლებლობას აკრძალავს.

4.4. ბიომეტრიული მონაცემები

განსაკუთრებული კატეგორიის მონაცემებს წარმოადგენს ასევე ბიომეტრიული მონაცემები. ასეთი მონაცემები შეიძლება იყოს პირის

²⁵ ბიჭია მ., პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით, თბილისი, 2012, 76.

²⁶ მსგავს მდგომარეობას ავითარებს ჰოლანდიის კანონმდებლობა, იხ: პერსონალური მონაცემების დაცვა საზღვარგარეთის ქვეყნების კანონმდებლობის ანალიზი, საქართველოს ახალგაზრდა იურისტთა ასოციაცია, თბილისი, 2007, <<http://gyla.ge/geo/news>> [2.06.2013].

ბიოლოგიური პროპორციები, ფსიქოლოგიური ხასიათი, ცხოვრებისეული თვისებები ან განმეორებადი ქცევები, რომელიც ყველა პიროვნებისთვის უნიკალური და განუმეორებელია. ბიომეტრიული მონაცემია თითის ანაბეჭდი, სახის სტრუქტურა, ხმა, ხელმოწერა. ამასთან, პერსონალური მონაცემია თითის ანაბეჭდი, მაგრამ არა თითი.²⁷

მე-9 მუხლის თანხმად, რომელიც შეეხება საჯარო დაწესებულების მიერ ბიომეტრიული მონაცემების დამუშავებას, აღნიშნულია, რომ „1. საჯარო დაწესებულების მიერ ბიომეტრულ მონაცემთა დამუშავება შეიძლება მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნებისათვის, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით, თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. 2. ამ მუხლის პირველი პუნქტით გათვალისწინებული პირობების მიუხედავად, ბიომეტრულ მონაცემთა დამუშავება შეიძლება კანონით დადგენილი წესით პირადობის დამადასტურებელი დოკუმენტის გაცემის ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიკაციის მიზნებისათვის“. კანონის მოცემული ჩანაწერი ასევე არ იძლევა მონაცემთა სუბიექტის მიერ ბიომეტრიული მონაცემების დამუშავებაზე უარის თქმის შესაძლებლობას. ბიომეტრიული მონაცემების შეგროვება, როდესაც ის დაკავშირებული არაა, სახელმწიფო ან საზოგადოებრივ უსაფრთხოებასთან, გამოძიების ინტერესებთან, ყოველთვის უნდა იყოს ნებაყოფლობითი. ამიტომ პირადობის დამადასტურებელი დოკუმენტის გაცემისას ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიკაციისას ბიომეტრიული მონაცემების შეგროვება პირის ნებიდან უნდა გამოდინარეობდეს, ხოლო თუ პირი წინააღმდეგია, მაშინ მას ალტერნატიული არაბიომეტრიული პირადობის დამადასტურებელი მოწმობის მიღების შესაძლებლობა უნდა ჰქონდეს. თუმცა, თუ საკითხს სხვაგვარად

²⁷ Opinion 4/2007 on the Concept of Personal Data, Article 29 Data Protection Working Party, adopted on the 20th June, 8-9. იხ. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> [2.06.2013].

შეგზედავთ, პირი არ იქნება ვალდებული, გასცეს თავისი ბიომეტრიული მონაცემები, თუ იგი უარს იტყვის პირადობის მოწმობის აღებაზე ან სახელმწიფო საზღვრის გადაკვეთაზე. ეს ძალიან ჰგავს კანადის აეროპორტის გაფრთხილებას: „უსაფრთხოების ზომებიდან გამომდინარე მგზავრებს აკვირდებიან და ამოწმებენ. არც ერთი მგზავრი არ გაიჩხრიკება, თუ ის გადაწყვეტს, რომ ჩვენი თვითმფრინავით არ იმგზავროს“. თვითგამორკვევის უფლებით აღჭურვილი მგზავრები უფლებამოსილნი არიან აირჩიონ, ან უარი თქვან ჩხრეკაზე და არ გაფრინდნენ ან გასცენ ინფორმაცია მათ სახელზე, მისმართზე, ტელეფონის ნომერზე, იმეილსა და საფოსტო კოდზე (თუმცა, ბიომეტრიული მონაცემები არ გროვდება). როცა არჩევანი „ყველაფერსა და არაფერს შორისაა“, ეს, ძირითადად, არჩევანი არაა. ²⁸

მე-9 მუხლში ასევე არაფერია ნათქვამი ამ მონაცემების შენახვის კადებზე.

5. პერსონალურ მონაცემთა დაცვის ინსპექტორი

კანონი ითვალისწინებს პერსონალურ მონაცემთა დაცვის ინსპექტორის თანამდებობის შემოღებას, რომელიც თავისი ბუნებით სახალხო დამცველის ინსტიტუტთან ძალიან ახლოსაა. საზღვარგარეთის ქვეყნებში მსგავსი პრაქტიკა აპრობირებულია და მას ხშირად არა მხოლოდ პერსონალურ მონაცემებზე, არამედ მთლიანად ინფორმაციის თავისუფლების დაცვაზე კონტროლი აკისრია. საქართველოში ჯერჯერობით ეს ინსტიტუტი არ ამოქმედებულა, თუმცა საკითხავია, რამდენად ეფექტური იქნება ინსპექტორის მოღვაწეობა, როდესაც მისი დამოუკიდებლობის გარანტიები კანონმდებლობით ნაკლებადაა გათვალისწინებული.

უპირველეს ყოვლისა, ეს მისი არჩევის წესით გამოიხატება. პერსონალურ მონაცემთა დაცვის ინსპექტორი თანამდებობაზე ღია

²⁸ Anonymity, Privacy and Identity in a Networked Society, edited by Ian Kerr, Valerie Steeves, Carole Luckock, Oxford, 2009, 9, იხ., <<http://www.idtrail.org/content/view/799>> [2/06.2013].

კონკურსის წესით ინიშნება. საკონკურსო კომისიას პრემიერ-მინისტრი ამტკიცებს. საკონკურსო კომისია არჩევს კანდიდატს, ხოლო შერჩეულ პირს პრემიერი 10 დღის ვადაში ნიშნავს ან აცხადებს ხელახალ კონკურსს²⁹. მსოფლიო პრაქტიკა ინსპექტორის თანამდებობაზე გამწესების ორ ძირითად ფორმას იცნობს - აღმასრულებელი ხელისუფლების მიერ დანიშვნასა და საკანონმდებლო ხელისუფლების მიერ არჩევას. პირველ შემთხვევაშიც, აღმასრულებელი ხელისუფლების მიერ დანიშვნის საფუძველს პარლამენტის სარეკომენდაციო რეზოლუცია წარმოადგენს. საკანონმდებლო ორგანოს მიერ არჩევის შემთხვევაში კი პარლამენტი ან პირდაპირ ირჩევს ან მთავრობის მიერ კანდიდატურის დასახელების შემდეგ ირჩევს, მაგალითად, როგორც ეს გერმანიაშია. ყველა შემთხვევაში პარლამენტს აქვს დომინანტური როლი.³⁰ საქართველოში კი პარლამენტის წევრები მხოლოდ საკონკურსო კომისიის წევრებად არიან წარმოდგენილნი. აღმასრულებელი ხელისუფლების მიერ დანიშნული პირისაგან აღმასრულებელი ხელისუფლების გაკონტროლებისას ობიექტურობა ნაკლებად მოსალოდნელია. ამიტომ უმჯობესია, თუ ინსპექტორის დანიშვნაში პარლამენტს წამყვანი როლი მიენიჭება.

კანონის თანახმად, ინსპექტორი ნებისმიერი პროფესიის პირი შეიძლება იყოს, აუცილებელი არაა იურიდიული განათლების ქონა. თუმცა, მიზანშეწონილია, კანონით დაკისრებული ამოცანების ჯეროვნად შესასრულებლად ინსპექტორს იურიდიული განათლება ჰქონდეს მიღებული. ინსპექტორი 3 წლის ვადით ინიშნება. დანიშნული ვადის ხანგრძლივობა დამოუკიდებლობის ერთ-ერთი გარანტია. იგი არ უნდა იყოს ძალიან ხანმოკლე, რათა ვადის გაგრძელებით, ხელმეორედ დანიშვნის სურვილით, მასზე მანიპულაცია არ მოხდეს. როგორც წესი, ინსპექტორის უფლებამოსილების ვადა ხუთიდან შვიდ წლამდე მერყეობს³¹. საქართველოშიც უმჯობესი იქნება, თუ ინსპექტორის ვადა

²⁹ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 28-ე მუხ-ლი.

³⁰ ჯანჯღავა კ., კომისიონერი და საჯარო ინფორმაციის ღიაობა (მსოფლიო პრაქტიკის მიმოხილვა), თბილისი, 2013, 27, იხ. <<http://www.idfi.ge>> [2.06.2013].

³¹ იქვე, 29.

ოთხი ან ხუთი წელი იქნება და ასევე თუ იმუნიტეტით ისარგებლებს. აღსანიშნავია, რომ ინსპექტორი, როგორც წესი, ანგარიშვალდებულია საკანონმდებლო ორგანოს მიმართ, თუმცა, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით ინსპექტორი ანგარიშს მთავრობას წარუდგენს.

უნდა აღინიშნოს, რომ კანონი ინსპექტორს მონაცემთა დამმუშავებლის შემოწმების უფლებას ანიჭებს. ინსპექტორი უფლებამოსილია ნებისმიერ დაწესებულებასა და ორგანიზაციაში შევიდეს და გაეცნოს ნებისმიერ დოკუმენტსა და ინფორმაციას, მიუხედავად მათი შინაარსისა და შენახვის ფორმისა. ინსპექტორი ვალდებულია დაგეგმილი შემოწმებისა და მისი ფარგლების შესახებ არანაკლებ 3 დღით ადრე აცნობოს იმ დაწესებულებას, რომლის საქმიანობაც დაკავშირებულია სახელმწიფო უსაფრთხოებასა და თავდაცვასთან ან რომელიც ოპერატიულ-სამძებრო საქმიანობას ახორციელებს. საჯარო სექტორთან მიმართებით, აღსანიშნავია, რომ ძალოვანი სტრუქტურები პრივილეგირებულ მდგომარეობაში არიან. კერძო სექტორთან მიმართებით კი, შემოწმების პროცედურა კონსტიტუციის მე-20 მუხლით დადგენილ მოთხოვნებს არ ითვალისწინებს. მე-20 მუხლში აღნიშნულია, რომ არავის არა აქვს უფლება შევიდეს საცხოვრებელ ბინაში და სხვა მფლობელობაში მფლობელ პირთა საწინააღმდეგოდ, აგრეთვე, ჩაატაროს ჩხრეკა, თუ არ არის სასამართლოს გადაწყვეტილება ან კანონით გათვალისწინებული გადაუდებელი აუცილებლობა. „სხვა მფლობელობაში“ იგულისხმება ნებისმიერი სახის კერძო საკუთრება. შესაბამისად, ინსპექტორის მიერ შემოწმების ჩატარება, მფლობელ პირთა ნების საწინააღმდეგოდ, მოსამართლის ბრძანების გარეშე, არაკონსტიტუციური დებულებაა. კერძო კომპანიების შემოწმების მექანიზმში მოსამართლის ჩართვა აუცილებელია.

6. პასუხისმგებლობა – ადმინისტრაციული თუ სისხლისსამართლებრივი?

კანონში მოცემულია ადმინისტრაციული სამართალდარვევებიც, რომლებიც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოთ-

ხოვნების დარღვევას უკავშირდება. ამავე დროს სისხლის სამართლის კოდექსი ითვალისწინებს პასუხისმგებლობას პირადი ან ოჯახური საიდუმლოს უკანონოდ მოპოვების, შენახვის ან გავრცელებისთვის, რაც მნიშვნელოვან ზიანს იწვევს. პირადი ან ოჯახური საიდუმლო პერსონალურ მონაცემებს წარმოადგენს. მათი უკანონო მოპოვება, შენახვის ან გავრცელების შემთხვევაში რომელი კანონი უნდა იქნას გამოყენებული? სისხლის სამართლის კოდექსში განსაზღვრული არაა ადმინისტრაციულსაზღვრულშეფარდებული პირის მიმართ გამოყენების საკითხი, შესაბამისად, საკითხავია, ეს სისხლის სამართლის პასუხისმგებლობას იწვევს თუ ადმინისტრაციულს, თუ ორივეს ერთად? თუმცა, თუ კონსტიტუციით განმტკიცებულ ორჯერ დასჯის დაუშვებლობის პრინციპს გავითვალისწინებთ, მაშინ ადმინისტრაციული პასუხისმგებლობა დადგება, როცა ქმდება მნიშვნელოვან ზიანს არ იწვევს, ხოლო თუ იწვევს, მაშინ - სისხლისსამართლებრივი.

7. საკითხები, რომლებზეც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი არ ვრცელდება

საკითხებს, რომლებზეც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი არ ვრცელდება, აწესრიგებს სამოქალაქო ან სისხლის სამართალი, ასევე, ცალკეული კანონები, რომლებიც ამ სფეროს შეეხება. თუმცა, არსებობს სფეროები, რომელსაც არცერთი საკანონმდებლო აქტი არ აწესრიგებს, მაგალითად, საზოგადოებრივი მართლწესრიგის დაცვა და საზოგადოებრივი უსაფრთხოება. არადა, ყველაზე მეტად პოლიციის საქმიანობაში ხდება ადამიანთა თვალთვალი, ფარული მოსმენა, კომპიუტერების კონტროლი და ამის შედეგად პერსონალური მონაცემების შეგროვება. კანონი „პოლიციის შესახებ“ და „საზოგადოებრივი უსაფრთხოების სამსახურის შესახებ“ პერსონალურ მონაცემებთან დაკავშირებით რაიმე სპეციალურ მოწესრიგებას არ მოიცავს, ამავე დროს არც „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი ვრცელდება. საქართველოს კანონმდებლობა პოლიციის უფლებამოსილების ფარგლებს ინფორმაციის მოპოვებისა და

დამუშავების პროცესში არ ადგენს. არაა განსაზღვრული იმ ინფორმაციის სახეები, რომელთა მოპოვება და შენახვა დასაშვებია, ასევე რა ვადით ინახება და რა გარანტიები არსებობს პირის უფლებების დასაცავად. ადამიანის უფლებათა ევროპულმა სასამართლომ რუმინეთის მოქალაქის საჩივარზე დაადგინა, რომ ირღვეოდა ინფორმაციული თვითგამორკვევის უფლება და პირის ინდივიდუალური ავტონომია, როდესაც ქვეყნის კანონმდებლობით დადგენილი არ იყო საიდუმლო პოლიციის უფლებამოსილებები პერსონალური მონაცემების დამუშავების პროცესში³². საქართველოს კანონმდებლობით ასევე გამიჯნული არაა საზოგადოებრივი მართლწესრიგისა და სახელმწიფო უსაფრთხოებისთვის პოლიციის საქმიანობა. როგორც წესი, სახელმწიფო უსაფრთხოების დაცვის დროს ადამიანის პირად ცხოვრებაში შეჭრის სტანდარტი უფრო დაბალია, თუმცა, გარკვეულ სამართლებრივ ჩარჩოებში აუცილებლად უნდა იყოს მოქცეული. სახელმწიფოს უფლებამოსილებები არც ამ შემთხვევაშია შეუზღუდავი. უსაფრთხოების ინტერესები არ გულისხმობს სახელმწიფოს შეუზღუდავ უფლებამოსილებებს. როგორც ჯორჯ ბუშმა აღნიშნა: „ჩვენ გვაქვს ვალდებულება დავიცვათ თქვენ, მაგრამ ამავე დროს გვაქვს ვალდებულება დავიცვათ თქვენი სამოქალაქო თავისუფლებები“.³³

8. ევროდირექტივის კანონპროექტი

პერსონალურ მონაცემთა დაცვასთან დაკავშირებით არსებობს ევროსაბჭოს 1995 წლის 24 ოქტომბრის დირექტივა „პირთა დაცვის შესახებ მათი პირადი მონაცემების გადამუშავების პროცესში და ასეთი მონაცემების თავისუფალი მიმოქცევის შესახებ“ (Directive 95/46/EC on the protection of individuals with regard to the processing of personal

³² იზორია ლ., კორკელია კ., კუბლაშვილი კ., ზუბუა გ., საქართველოს კონსტიტუციის კომენტარები, თბილისი, 2005, 353.

³³ Anonymity, Privacy and Identity in a Networked Society, edited by Ian Kerr, Valerie Steeves, Carole Luckock, Oxford, 2009, 10, იხ., <<http://www.idtrail.org/content/view/799>> [2/06.2013].

data and on the free movement of such data). სწორედ მოცემულ ღირებულებას ეყრდნობა საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“. საკანონმდებლო ხარვეზების აღმოფხვრის მიზნით ევროსაბჭოში მიმდინარეობს აღნიშნული ღირებულების ცვლილებების კანონპროექტის განხილვა. პირადი ცხოვრების დაცვის სტანდარტის ამაღლების მიზნით პროექტი პერსონალურ მონაცემთა დაცვის შესახებ არსებული საკანონმდებლო მოწესრიგების გამკაცრებას ითვალისწინებს. კანონპროექტი ყველა სფეროს მოიცავს, მათ შორის, მედიას, ინტერნეტს, საპოლიციო ურთიერთობებს, გამოწვევისა და მხოლვით პირადი ურთიერთობები ინტერნეტში. მეორე მხრივ, კანონპროექტი მონაცემთა დამუშავების პროცედურას ამარტივებს. მონაცემთა დამუშავებაზე კომპანიას ევროკავშირის ყველა სახელმწიფოსთვის ინფორმაციის მიწოდების ნაცვლად, მხოლოდ ერთი სუბიექტისთვის მიწოდება მოუწევს. აღნიშნულმა კანონპროექტმა ევროკავშირში მწვავე დისკუსია გამოიწვია, მიიჩნევენ, რომ ეს ხელყოფს გამოხატვის თავისუფლებას და უმჯობესი იქნება, თუ კანონპროექტი არ გავრცელდება ჟურნალისტებზე, სახელოვნებო და ლიტერატურული მიზნებისთვის მონაცემთა დამუშავებაზე. თუმცა, აქვე აღნიშნულია, რომ ამ შემთხვევაში გამოხატვის თავისუფლებით ისარგებლებენ მხოლოდ ჟურნალისტები და არა სხვა მოქალაქეები.³⁴

აღსანიშნავია, რომ პირადი ცხოვრების დაცვას სიტყვის თავისუფლების აბსოლუტიზაცია ართულებს. ცხადია, როცა კანონი ინფორმაციის ბრუნვას ზღუდავს, ის სიტყვის თავისუფლებას პოტენციურ საფრთხეს უქმნის. თუ კანონის მიზანია, ზიანის მომტანი ინფორმაციის შეზღუდვა, როგორ უნდა განისაზღვროს კანონი ისე, რომ არ შეზღუდოს გამოხატვის თავისუფლება. ჯონ მილტონი აცხადებდა, რომ „უფლება – გაიგო, აზრი გამოთქვა და თავისუფლად, საკუთარი სინდისის შესაბამისად იმსჯელო – ყველა სხვა თავისუფლებაზე მაღლა

³⁴ New data rules will collide with fundamental rights, Commission admits, იხ., <<http://www.websites.be/news/new-data-rules-will-collide-fundamental-rights-commission-admits>> [2.06.2013].

დას³⁵. თუმცა, პირადი ცხოვრების დაცვა თვითონ სიტყვის თავისუფლებას სჭირდება, რადგან თუ ადამიანები არ იქნებიან დარწმუნებულნი თავიანთი საუბრისა თუ კომუნიკაციის სხვა ფორმების პრივატულობაში, ისინი აზრის გამოხატვისგან თავს შეიკავენ.³⁶

პერსონალურ მონაცემთა ელექტრონული მიმოქცევა იმდენად შემაფოთებელ ხასიათს იღებს, რომ ევროკავშირი თვით გამოხატვის თავისუფლების ხარჯზეც მზადაა შებოჭოს პირის პერსონალურ მონაცემების უკანონო ბრუნვა.

დასკვნა

დასასრულ შეიძლება „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონთან დაკავშირებით რამდენიმე რეკომენდაცია გაკეთდეს.

კანონის მიზანი – პერსონალური მონაცემების დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობა – შეიძლება ითქვას, რომ ვერ იქნა მიღწეული. პირიქით, კანონი ითვალისწინებს ინფორმაციის შეგროვება-შენახვის უფლებას პირის პირადი ცხოვრების ხარჯზე. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით გათვალისწინებული მოწესრიგებები გაცილებით დაბალ სტანდარტს აწესებს ინდივიდის პირადი ცხოვრების დასაცავად, ვიდრე ეს ზოგადი ადმინისტრაციული კოდექსით იყო გათვალისწინებული. კანონი დახვეწას საჭიროებს. მისი ნაკლოვანებებია:

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-7 მუხლში აღნიშნულია, რომ მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება დასაშვებია მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის თანხმობით ან თუ მონაცემთა სუბიექტის გარდაცვალებიდან გასულია 30 წელი. ეს

³⁵ Daniel J. Solove, The Future of Reputation, 125, იხ., <<http://www.idtrail.org/content/view/799>> [2.06.2013].

³⁶ Anonymity, Privacy and Identity in a Networked Society, edited by Ian Kerr, Valerie Steeves, Carole Luckock, Oxford, 2009, 10, იხ., <<http://www.idtrail.org/content/view/799>> [2/06.2013].

ჩანაწერი წინააღმდეგობაში მოდის „ეროვნული საარქივო ფონდისა და არქივის შესახებ“ კანონის 22-ე მუხლთან და „პაციენტის უფლებების შესახებ“ კანონის 27-ე მუხლთან. ამიტომ უმჯობესი იქნება, თუ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-7 მუხლის პირველ პუნქტს დაემატება ფრაზა „თუ კანონით სხვა რამ არ არის განსაზღვრული“.

მონაცემთა დამუშავების შესაძლო შემთხვევების საკმაოდ ფართო წრეა ჩამოთვლილი. თითქმის ყველა ლეგიტიმური მიზანი ცალ-ცალკეა გამოყოფილი, მიუხედავად ამისა, ცალკე შემთხვევადაა განსაზღვრული მონაცემთა დამუშავება, თუ ეს აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად. ეს ნიშნავს, რომ პერსონალური მონაცემების შეგროვება შესაძლებელია იმ საჯარო ინტერესების დასაცავად, რომელიც კანონში მითითებული არაა. პერსონალურ მონაცემთა დაცვის სტანდარტის ამაღლებისთვის ეს ელემენტი კანონით გათვალისწინებული არ უნდა იყოს.

კანონის თანახმად, თუ მონაცემთა შეგროვება არ ხორციელდება უშუალოდ მონაცემთა სუბიექტისაგან, მონაცემთა დამუშავებელი ან უფლებამოსილი პირი ვალდებულია მოთხოვნის შემთხვევაში მონაცემთა სუბიექტს მიაწოდოს ამ მუხლის პირველ პუნქტში აღნიშნული ინფორმაცია. აუცილებელია, რომ ზემოაღნიშნული ინფორმაციის პირისთვის მიწოდება პირის მოთხოვნის გარეშეც საავალდებულო იყოს. მართლაც, გაუგებარია, როგორ უნდა მოითხოვოს თავად პირმა ინფორმაციის მიწოდება, თუ არ ეცოდინება, ვინ აგროვებს მის შესახებ ინფორმაციას.

კანონი პერსონალური მონაცემების მნიშვნელობის მიხედვით განსაკუთრებული კატეგორიის მონაცემებს გამოყოფს. განსაკუთრებული კატეგორიის მონაცემების დაცვა მინიმუმ უნდა გულისხმობდეს მონაცემთა სუბიექტის მიერ ამ ინფორმაციის კონტროლის საშუალებას. პირის ექსკლუზიურ ნებაზე, მის არჩევანზე უნდა იყოს დამოკიდებული, მონაცემთა დამუშავებელის მიერ მონაცემთა დამუშავების შესაძლებლობა. შესაბამისად, კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემების შეგროვება, როდესაც ის დაკავშირებული

არაა, სახელმწიფო ან საზოგადოებრივ უსაფრთხოებასთან, გამოძიების ინტერესებთან, უნდა იყოს ნებაყოფლობითი. ხოლო თუ კანონი დაუშვებს მის დამუშავებას, მაშინ განსაკუთრებული კატეგორიის მონაცემების დამუშავების წრე უნდა შემცირდეს. უმჯობესია დიფერენცირებულად იქნას განხილული თითოეული განსაკუთრებული კატეგორიის მონაცემების დამუშავების საკითხი. ასევე, კანონის მე-6 მუხლის მე-3 პუნქტში უნდა აღინიშნოს, რომ განსაკუთრებული კატეგორიის მონაცემთა დამუშავების შემთხვევაში დაუშვებელია მონაცემთა მესამე პირისათვის გამჟღავნება მონაცემთა სუბიექტის თანხმობის გარეშე.

მიზანშეწონილი იქნება, თუ პერსონალურ მონაცემთა დაცვის ინსპექტორის დამოუკიდებლობის მეტი გარანტია იქნება გათვალისწინებული. პირველეს ყოვლისა, ის უნდა აირჩეს პარლამენტის მიერ და ანგარიშვალდებულებაც საკანონმდებლო ორგანოს წინაშე უნდა ჰქონდეს, როგორც ეს სახელმწიფოთა უმრავლესობაშია მიღებული. აღმსარულებელი ხელისუფლების მიერ დანიშნული პირის მიერ აღმსარულებელი ხელისუფლების გაკონტროლებისას ინსპექტორის ობიექტურობა ნაკლებად მოსალოდნელია. უმჯობესი იქნება, თუ ინსპექტორს უმაღლესი იურიდიული განათლება მოეთხოვება. ასევე, უფლებამოსილების ვადის თვალსაზრისით 4 ან 5 წელი უფრო მეტ თავისუფლებას მისცემდა მას.

პერსონალურ მონაცემთა დაცვის კუთხით არსებობს სფეროები, რომელზეც არცერთი საკანონმდებლო აქტი არ ვრცელდება, მაგალითად, საზოგადოებრივი მართლწესრიგის დაცვა და საზოგადოებრივი უსაფრთხოება. საქართველოს კანონმდებლობამ უნდა დაადგინოს პოლიციის უფლებამოსილების ფარგლები ინფორმაციის მოპოვებისა და დამუშავების პროცესში.

საბოლოოდ, მთავარია, რომ კანონმა შეძლოს პირადი ცხოვრების ხელშეუხებლობის დაცვა, ამ ურთიერთობის სამართლებრივ ჩარჩოებში მოქცევა. ადამიანები საუკუნეების განმავლობაში სხვადასხვა გზით ცდილობდნენ საკუთარი რეპუტაციის დაცვას. ევროპელი არისტოკრატები თავიანთ ღირსებას ღუელით იცავდნენ. მხოლოდ საფრანგეთში ჰენრი IV-ის მეფობის 21 წლის განმავლობაში საკუთარი

სახელისთვის ათი ათასი ჯენტლმენი მოკვდა.³⁷ კანონმა უნდა შეძლოს თავისი ფუნქციის შესრულება, რათა ადამიანებმა საუკუნეების წინ ნაცად ხერხს – ერთმანეთის სიცოცხლის ხარჯზე საკუთარი სახელისა თუ ღირსების დაცვას არ მიმართონ.

³⁷ Daniel J. Solove, The future of reputation, 114, იხ., <<http://www.idtrail.org/content/view/799>> [2.06.2013]