თამთა არჩუაძე

პერსონალურ მონაცემთა დეპერსონალიზაცია, როგორც მონაცემთა სუბიექტის დაცვის გარანტია

თამთა არჩუაძე
საჯარო სამართლის მაგისტრი,
აღმოსავლეთ ევროპის უნივერსიტეტი.

აბსტრაქტი

თანამედროვე სამყაროში წარმოუდგენელია ადამიანთა არსებობა განსაკუთრებით მნიშვნელოვანი პერსონალური მონაცემების დამცავი მექანიზმის – დეპერსონალიზაციის გარეშე, ვინაიდან ყოველი ინდივიდის ცხოვრება მოიცავს ისეთ დეტალებს, რომელთა გამჟღავნებამაც შესაძლებელია, განუზომელი ზიანი მიაყენოს მონაცემთა სუბიექტს და მის გარშემო მყოფ პირებს.

წინამდებარე ნაშრომი ასახავს სხვადასხვა კატეგორიის მონაცემთა განმარტებას, განიხილავს თითოეულის მნიშვნელობასა და ხარისხს, განსაზღვრავს, რამდენად რელევანტური და მნიშვნელოვანია დეპერსონალიზაციის სამართლებრივი რეგულირება და პრაქტიკული განხორციელება იმისათვის, რომ მიიღწეს მონაცემთა სუბიექტის დაცვის საკანონმდებლო მიზანი.

ნაშრომი საკითხის სრულყოფილად შესწავლის მიზნით მიმოიხილავს არამარტო ქართულ ნორმატიულ ბაზასა და პრაქტიკას, არამედ წარმოაჩენს პერსონალურ მონაცემთა დაცვის გარანტიების შექმნის კუთხით სხვა ქვეყნების გამოცდილებასაც, რაც დეპერსონალიზაციის, როგორც მონაცემთა სუბიექტის დაცვის გარანტიის ავკარგიანობის ანალიზის საშუალებას იძლევა.

შესავალი

პერსონალურ მონაცემთა „ხელშეუხებლობა არის ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობა;“[1] შესაბამისად, მნიშვნელოვანია მონაცემთა სუბიექტის შესახებ ისეთი ინფორმაციის გამჟღავნებისგან დაცვა, რომელმაც შესაძლოა, მას განუზომელი ზიანი მიაყენოს დასაქმების, ოჯახის შექმნის ან თუნდაც გარესამყაროსთან ურთიერთობის კუთხით.

დეპერსონალიზაცია მნიშვნელოვანი გარანტიაა მონაცემთა სუბიექტის დასაცავად. თუმცა პრაქტიკულად მისი განხორციელება რთულია, მაშინ, როდესაც ლეგიტიმური საჯარო ინტერესი მოითხოვს საზოგადოების ინფორმირებას სხვადასხვა საკითხთან დაკავშირებით. ასეთ შემთხვევაში მონაცემთა დამმუშავებელს მართებს სიფრთხილე, რომ შემთხვევით არ გაამჟღავნოს ისეთი ინფორმაცია, რომელიც საზოგადოებას მის მონაცემთა სუბიექტის იდენტიფიცირებაში დაეხმარება.

ნაშრომში განხილულია დეპერსონალიზაციის სამართლებრივი რეგულირების საკითხები და მისი პრაქტიკული განხორციელების შესაძლებლობა. აგრეთვე განსაკუთრებული ყურადღება ეთმობა მონაცემთა ისეთ კატეგორიებს, რომლებიც უპირობოდ იმსახურებენ დეპერსონალიზებული ფორმით არსებობას, როდესაც საქმე ლეგიტიმური საჯარო ინტერესის მიზეზით ინფორმაციის გამჟღავნებას ეხება.

ნაშრომში გამოყენებულია შედარებით-სამართლებრივი, ფორმალურ-ლოგიკური, ანალიტიკური, ისტორიული და სოციოლოგიური კვლევის მეთოდები. შედარებით-სამართლებრივი კვლევის მეთოდი საშუალებას იძლევა, სხვადასხვა ქვეყნის კანონმდებლობის დადებითი და უარყოფითი მხარეების შედარებისა და შეჯერების მეშვეობით ლოგიკურ და თანამიმდევრულ დასკვნამდე იქნეს მსჯელობა წაყვანილი. ანალიტიკური კვლევის მეთოდი თავისთავად გულისხმობს პრობლემათა ანალიზს, რაც კვლავ მსჯელობის ლოგიკურ თანამიმდევრობას განსაზღვრავს და რაციონალური დასკვნის განხორციელების შესაძლებლობას იძლევა. ისტორიული კვლევის მეთოდი პერსონალურ მონაცემთა დამცავი კანონმდებლობის განვითარების ეტაპებს წარმოაჩენს. რაც შეეხება სოციოლოგიური კვლევის მეთოდს, მისი გამოყენება აუცილებელიც კი არის, ვინაიდან პერსონალური მონაცემი, თავისი არსით, სოციუმს უკავშირდება და სოციუმში მყოფ თითოეულ პიროვნებას გააჩნია ის.

1 საქართველოს საკონსტიტუციო სასამართლოს 2009 წლის 10 ივნისის N1/2/458 განჩინება საქმეზე, „საქართველოს მოქალაქეები – დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ.“

1. პერსონალურ მონაცემთა დეპერსონალიზაციის არსი და გამჭვირვალობისა და დაცვის რეჟიმს დაქვემდებარებულ ინფორმაციათა სახეები

1.1. პერსონალურ მონაცემთა დეპერსონალიზაციის განსაზღვრება

სახელისუფლო ორგანოებისა და სხვადასხვა გაერთიანების მიერ ფიზიკურ პირთა შესახებ პერსონალური ინფორმაციის მოპოვებისა და საჭიროებისამებრ დამუშავების პრაქტიკა საუკუნეებს ითვლის, აღსანიშნავია, რომ ჯერ კიდევ რომის იმპერიაში გადასახადის გადამხდელთა შესახებ არსებული ინფორმაცია ხელისუფლების წარმომადგენლების მიერ გროვდებოდა და საკმაოდ სრულყოფილი სახით იწერებოდა პაპირუსის გრაგნილებზე. აღნიშნული ჩანაწერების მეშვეობით ხორციელდებოდა არამარტო გადასახადის გადამხდელის საქმიანობის შესახებ ინფორმაციის მოპოვება, არამედ იმპერიის რეალური და პოტენციური მტრების გამოვლენაც. გადასახადის გადამხდელთა შესახებ არსებული ჩანაწერები მოიცავდა იესო ნაზარეველის, მისი მოწაფეების, მონების ლიდერის – სპარტაკის და ზოგიერთი პოლიტიკური და რელიგიური აქტივისტის შესახებ ინფორმაციას. ბერძნულ და ეგვიპტურ ქალაქებშიც არსებობდა პერსონალურ მონაცემთა შეგროვების პრაქტიკა და ძირითადად გროვდებოდა ინფორმაცია მიწის რეგისტრაციებისა და საკუთრების თაობაზე დადებული კერძო ხელშეკრულებების შესახებ. აღნიშნული მონაცემები მოიცავდა მოსახლის რასობრივი წარმომავლობის შესახებ ინფორმაციას, რათა განესხვავებინათ ებრაელები, მაკედონიელები, ფრიგიელები, ეგვიპტელები და სხვანი.[2] საუკუნეების გამოცდილებამ და ადამიანების მარტივად იდენტიფიცირების სურვილმა, განაპირობა თითოეულ მათგანზე მაქსიმალურად დიდი ოდენობის ინფორმაციის შეგროვების პრაქტიკის დანერგვა, რამაც საფრთხე შეუქმნა ადამიანის პირადი ცხოვრების ხელშეუხებლობის უზენაეს პრინციპს.

მოსამართლე უილიამ დუგლასმა ჯერ კიდევ 1966 წელს განაცხადა, რომ ადამიანები სწრაფად უახლოვდებიან ეპოქას, სადაც აღარ იარსებებს კონფიდენციალურობა, ყოველი მათგანი თავისუფალი თვალთვალის ობიექტი გახდება ნებისმიერ დროს, სახელმწიფოსთვის კი დაფარული აღარაფერი იქნება.[3] ტექნოლოგიების დახვეწასთან ერთად, ადამიანები ამ ეპოქას ძალიან სწრაფად მიუახლოვდნენ.

პიროვნებაზე მაქსიმალურად დიდი და მრავალფეროვანი ინფორმაციის შეგროვების მზარდმა ტენდენციამ განაპირობა საქართველოში პერსონალური მონაცემების დეფინიციის შემდეგი შინაარსით ჩამოყალიბება (რომელიც აბსოლუტურად შეესაბამება განვითარებული ქვეყნების მიერ შექმნილ განმარტებით ტექსტს): პერსონალური მონაცემი ნებისმიერი სახის ინფორმაციაა, რომელიც ემსახურება ფიზიკური პირის იდენტიფიცირებას, შესაბამისად ეს

2 Madsen W., Handbook of Personal Data Protection, New York, 1992, 6.

3 Madsen W., Handbook of Personal Data Protection, New York, 1992, 6.

შეიძლება იყოს საიდენტიფიკაციო ნომერი, პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშანი.[4]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიღებამდე, პერსონალური მონაცემის განმარტებას მოიცავდა „საქართველოს ზოგადი ადმინისტრაციული კოდექსი“, რომელიც პერსონალურ მონაცემს განიხილავდა პირის გასაიდენტიფიცირებლად საჭირო საჯარო ინფორმაციად,[5] რაც სრულიად ეწინააღმდეგებოდა ზოგიერთ შემთხვევაში პერსონალურ მონაცემთა კონფიდენციალურობის აუცილებლობას.[6]

საქართველოს კონსტიტუცია პერსონალურ მონაცემთა გამჟღავნებისგან დაცვის სტანდარტს დეფინიციის განსაზღვრის გარეშე ამკვიდრებს მე-20 მუხლის პირველ ნაწილსა და 41-ე მუხლში. კერძოდ, კონსტიტუციის 41-ე მუხლში წარმოდგენილია მონაცემთა ჩამონათვალი, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, მის ფინანსებთან ან სხვა კერძო საკითხებთან.[7] პირის ჯანმრთელობასთან დაკავშირებული ინფორმაცია უკავშირდება ადამიანის ფიზიკური არსებობის საკითხს, ხოლო ფინანსებთან დაკავშირებული ინფორმაცია მისი ყოფისა და საქმიანობის მატერიალურ საფუძვლებს,[8] რაც შეეხება „კერძო საკითხებს, სავარაუდოა, რომ ისინი განსაზღვრავენ ადამიანის ინტიმური ცხოვრების სფეროს მიკუთვნებულ ურთიერთობებს.[9] საქართველოს საკონსტიტუციო სასამართლოს განმარტებით, კონსტიტუციის ხსენებული მუხლი „კავშირშია კონსტიტუციის მე-20 მუხლთან, რომლითაც დაცულია პირადი ცხოვრების ხელშეუხებლობა, რადგანაც მასში სწორედ ის მონაცემებია მითითებული, რომელიც პირის პრივატულ სფეროს შეეხება.“[10]

პერსონალურ მონაცემთა გამჟღავნებისაგან დაცვა ისეთ შემთხვევებში, როდესაც კონკრეტული გადაწყვეტილებების თუ შეგროვებული ინფორმაციის საჯაროდ ხელმისაწვდომობა გარდაუვალია (მაგალითად: სასამართლოს მიერ მიღებული ყველა გადაწყვეტილება ცხადდება საჯაროდ,[11] პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ ყოველწლიური ანგარიში ითვალისწინებს საჯაროდ გამოქვეყნების მექანიზმს,[12] სახალხო დამცველის ყოველწლიური ანგარიში ქვეყნდება საქართველოს პარლამენტის ოფიციალურ ბეჭდვით ორგანოში,[13] დანაშაულის შესახებ ინფორმაცია ქვეყნდება მასმედიის მეშვეობით და სხვა), შესაძლებელია მონაცემთა დეპერსონალიზაციით, ან ფსევდონიმის გამოყენებით.

4 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის ა)პუნქტი.

5 „საქართველოს ზოგადი ადმინისტრაციული კოდექსის“ 27-ე მუხლის თ) ნაწილი (15.07.1999 წლის რედაქცია).

6 „საქართველოს ზოგადი ადმინისტრაციული კოდექსის“ 44-ე მუხლის 1-ლი ნაწილი (15.07.1999 წლის რედაქცია).

7 საქართველოს კონსტიტუციის 41-ე მუხლის მე-2 ნაწილი.

8 საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406,408 გადაწყვეტილება საქმეზე, „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“.

9 საქართველოს კონსტიტუციის კომენტარი, თბილისი, 2013, გვ. 360.

10 საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406,408 გადაწყვეტილება საქმეზე, „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“.

11 საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-10 მუხლის მე-2 ნაწილი.

12 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ 38-ე მუხლის 1-ლი პუნქტი.

13 საქართველოს ორგანული კანონის „სახალხო დამცველის შესახებ“ 22-ე მუხლის მე-5 პუნქტი.

მონაცემთა სუბიექტის გამჟღავნებისგან დაცვის ამ ორი ვარიანტიდან, საუკეთესო გზა მონაცემთა დეპერსონალიზაციაა, რომელიც ყველაზე მეტად უზრუნველყოფს მიზნის მიღწევას.

ზოგადად საგულისხმოა, რომ დეპერსონალიზაცია გამოიყენება ისეთ შემთხვევებში, როდესაც ინფორმაცია ფაქტის, მოვლენის, პიროვნების და სხვათა შესახებ საზოგადოებისათვის ხელმისაწვდომი უნდა იყოს. გამჟღავნების საკითხის დღის წესრიგში დაყენება რომ არა, დეპერსონალიზაცია საერთოდ არ იქნებოდა საჭირო, ვინაიდან მსგავს შემთხვევაში ინფორმაცია მონაცემთა დამმუშავებლის ფარგლებს არ გასცდებოდა.

სრულყოფილი დეპერსონალიზაცია, რაც გულისხმობს მონაცემთა ანონიმურობის ისეთ მექანიზმს, რომ სუბიექტის იდენტიფიცირება შეუძლებელია, პრაქტიკულად თითქმის მიუღწეველია,[14] შესაბამისად, კანონმდებლობაც მისი განმარტებისას, მართალია, დეპერსონალიზაციად მონაცემთა იმგვარ მოდიფიკაციას მიიჩნევს, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან, მაგრამ ამასთანავე უშვებს შემთხვევას, როდესაც ანონიმურობა შესაძლოა, სრულად ვერ იქნეს დაცული. ასეთ შემთხვევაში მონაცემთა კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებს და დროს უნდა საჭიროებდეს.[15] დეპერსონალიზაციას თითქმის იდენტური შინაარსით განმარტავს გერმანიის ფედერალური მონაცემთა დაცვის აქტი.[16] მსგავს განმარტებას პრაქტიკულ დეპერსონალიზაციას ("faktische Anonymisierung") უწოდებენ,[17] ვინაიდან დეპერსონალიზაციის მაქსიმალურად სრულყოფილი განხორციელება მხოლოდ პრაქტიკაზეა დამოკიდებული, კანონმდებლობა იმის მითითებით შემოიფარგლება, რომ მან მონაცემთა მოდიფიკაციის იმგვარი გზა უნდა გამოიყენოს, სუბიექტის იდენტიფიცირება თავიდან იქნეს აცილებული.

დეპერსონალიზაციის სამართლებრივ დეფინიციას უმეტესი ქვეყნების პერსონალურ მონაცემთა დაცვის აქტები არ მოიცავენ, სრულყოფილი განმარტება გვხვდება მხოლოდ გერმანიის და საქართველოს პერსონალურ მონაცემთა დაცვის კანონმდებლობაში, რაც შეეხება უკრაინას, მართალია, მისი პერსონალურ მონაცემთა დაცვის აქტიც განსაზღვრავს დეპერსონალიზაციას, მაგრამ ძალიან ლაკონურად, კერძოდ: დეპერსონალიზაცია ნიშნავს იმ ინფორმაციათა ამოღებას, რომლებიც პირდაპირ ან არაპირდაპირ აიდენტიფიცირებენ პირს.[18]

ქვეყნებს, სადაც დეპერსონალიზაციის დეფინიცია არ არსებობს, შესაძლოა, ამის მიზეზი გააჩნდეთ. კერძოდ, დეპერსონალიზაციის მიზანი მთლიანად პრაქტიკულ განხორციელებაზეა დამოკიდებული, არ აქვს მნიშვნელობა იმას, თუ როგორი შინაარსით აყალიბებს მას კანონმდებლობა, მთავარია მონაცემთა დამმუშავებელმა, თუ მონაცემთა შემნახველმა მის ხელთ არსებული ინფორმაციის იმგვარი მოდიფიკაცია განახორციელოს, რომ მონაცემთა სუბიექტი დაიცვას გამჟღავნებისგან.

14 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

15 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ" მე-2 მუხლის რ) პუნქტი.

16 იხ. Federal Data Protection Act in Germany, section 3, paragraph 7).

17 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

18 Law of Ukraine on Protection of Personal Data, article 2, sentence 6.

1.2. დეპერსონალიზაციას დაქვემდებარებულ პერსონალურ მონაცემთა კატეგორიები და მათი კონფიდენციალურობის საკანონმდებლო სტანდარტი

1.2.1. განსაკუთრებულ კატეგორიას მიკუთვნებული ინფორმაცია და გამჟღავნებისგან დაცვის ბერკეტები

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიღებამდე, კანონმდებლობა არ მოიცავდა სტანდარტს, რომელიც რომელიმე პერსონალურ მონაცემს განსაკუთრებულ მნიშვნელობას მიანიჭებდა და მათი დაცვისთვის უფრო მკაცრ რეგულირებას დააწესებდა, თუმცა განვითარებული ქვეყნების გავლენით, საქართველოს უზენაესმა სასამართლომ 2010 წლის გადაწყვეტილებაში პერსონალურ მონაცემთა დიფერენციაცია განახორციელა მგრძნობიარე და ჩვეულებრივ პერსონალურ მონაცემებად და განმარტა, რომ „მგრძნობიარე კატეგორიის პერსონალური მონაცემები განსაკუთრებული სამართლებრივი რეჟიმით, გამიჯნულია ჩვეულებრივი პერსონალური მონაცემებისაგან. ამ კატეგორიის პერსონალური მონაცემების დამუშავება-გაცემა საჭიროებს პირის თანხმობას“.[19] აღნიშნული განმარტება, იმ დროისთვის პერსონალური მონაცემების დაცვასთან დაკავშირებული მწირი რეგულაციების გათვალისწინებით, უაღრესად პროგრესული იყო.

დღესდღეობით წარმოუდგენელია, არსებობდეს პერსონალურ მონაცემთა დამცავი კანონმდებლობა და არ იცავდეს ისეთ ინფორმაციას, რომლის მნიშვნელობის გათვალისწინებითაც, ის მიჩნეულია „სენსიტიურ, იგივე სპეციალურ კატეგორიას მიკუთვნებულ მონაცემად“[20] და უკავშირდება პირის რასობრივ ან ეთნიკურ კუთვნილებას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ მრწამსს, პროფესიულ კავშირში გაწევრიანებას, ჯანმრთელობის მდგომარეობას, სქესობრივ ცხოვრებას.[21] ამ მონაცემთა ჩამონათვალი ევროპული პარლამენტისა და საბჭოს დირექტივის შესაბამისად ის მინიმუმია, რომელსაც ყველა ქვეყნის პერსონალურ მონაცემთა დამცავი კანონმდებლობა უნდა ითვალისწინებდეს, შესაბამისად არსებობს მოლოდინი, რომ ევროპული კავშირის ქვეყნები განსაკუთრებულ კატეგორიას მიკუთვნებულ ინფორმაციათა ჩამონათვალს განავრცობენ და უფრო მეტად გაამკაცრებენ, ვინაიდან ისინი თავისუფლები არიან უფრო მკაცრი წესის იმპლემენტაციისას.[22]

ვინაიდან საქართველო მიისწრაფვის ევროკავშირში გაწევრიანებისკენ და ევროპულ სტანდარტებთან შესაბამისობისკენ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი არამარტო იცავს განსაკუთრებულ კატეგორიას მიკუთვნებულ ინფორმაციათა მინიმუმს, არამედ მის დეფინიციაში აქცევს აგრეთვე ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან

19 საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2010 წლის 5 ივლისის განჩინება №ბს-1278-1240 (კ-08).

20 Brouwer E., Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, Leiden, Boston, 2008, 2012.

21 Directive 95/46/EC (ლუქსემბურგის დიდი საჰერცოგო, ლუქსემბურგი) (ძალაში შევიდა 13.12.1995 წელს), Article 8.

22 Klosek J., Data Privacy in the Information Age, Westport, Connecticut, London, 2000, 31.

ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიულ და გენეტიკურ მონაცემებთან დაკავშირებულ ინფორმაციას.[23] უნდა აღინიშნოს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით განსაზღვრული დეფინიცია, რომელიც სისხლის სამართლის პროცესთან დაკავშირებულ განსაკუთრებულ კატეგორიას მიკუთვნებულ პერსონალურ ინფორმაციას განმარტავს, გამოირჩევა თავისი სრულყოფილებით და ყოვლისმომცველობით.

როგორც წესი, სისხლის სამართლის პროცესთან დაკავშირებული ინფორმაციის განსაკუთრებულ მნიშვნელობას უმეტესი ქვეყნების პერსონალურ მონაცემთა დაცვასთან დაკავშირებული კანონი განსაზღვრავს,[24] თუმცა მათგან აღსანიშნავია ესტონეთის „პერსონალურ მონაცემთა დაცვის აქტი“, რომელიც სენსიტიურ ინფორმაციათა კატეგორიაში აქცევს სისხლის სამართლის საქმის ან დანაშაულთან დაკავშირებით სხვა საქმეთა წარმოებისას მოპოვებულ ინფორმაციას და იცავს გამჟღავნებისგან მანამ, სანამ სასამართლო სხდომა საჯაროდ ჩატარდება ან გადაწყვეტილება იქნება მიღებული. სენსიტიურია აგრეთვე ინფორმაცია, რომელიც მოიცავს საზოგადოებრივი მორალის, პირადი ან ოჯახური ცხოვრების დეტალებს, ინფორმაციას, რომელთან მიმართებითაც სხვა ინტერესები ნაკლებად ღირებულია, მსხვერპლისა და მოწმის შესახებ მონაცემებს და ინფორმაციას, რომლის გამჟღავნებისგან დაცვა სამართლიანობის მოთხოვნების შესაბამისად ხორციელდება.[25] ესტონეთის „პერსონალურ მონაცემთა დაცვის აქტისგან“ განსხვავებით, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ სისხლის სამართლის პროცესთან დაკავშირებით კონკრეტულად, სახელდებით მოიხსენიებს იმ მონაცემებს, რომლებიც მიეკუთვნება სენსიტიურ კატეგორიას, აღნიშნული განპირობებულია იმით, რომ სპეციალური ნორმატიული აქტი – „საქართველოს სისხლის სამართლის კოდექსი“ არათუ არ აკონკრეტებს, თუ რომელი ინფორმაციაა განსაკუთრებულ კატეგორიას მიკუთვნებული პერსონალური მონაცემი, არამედ არ მოიცავს დებულებას, რომლითაც სისხლის სამართლის პროცესთან დაკავშირებული ისეთი ინფორმაცია, როგორიცაა ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, უნდა იქნეს გამჟღავნებისგან დაცული.

განსაკუთრებულ კატეგორიას მიკუთვნებული მონაცემები დაცვის უმაღლესი სტანდარტით გამოირჩევა და მათი დამუშავება აკრძალულია[26] გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის წერილობითი თანხმობა ან მონაცემთა დამუშავების აუცილებლობას განაპირობებს შრომითი ვალდებულებების და ურთიერთობების ხასიათი, დასაქმების თაობაზე გადაწყვეტილების მიღების პროცედურა, მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დაცვა. საზოგადოებრივი ჯანმრთელობის დაცვა, ბრალდებულთა/

23 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის ბ) პუნქტი.

24 მაგალითისთვის იხ.„Data Protection Act 1998” of UK part I, paragraph 2, part h), „Law On Legal Protection Of Personal Data” of Republic of Lithuania, article 2, paragraph 9, „ Personal Data Act (523/1999)” of Finland Chapter 3, Section 11, part 6), „The Greek Data Protection Law of 1997 (Law 2472/1997)” Article 2, paragraph b) და სხვა.

25 Estonia: Personal Data Protection Act, article 4, paragraph 7.

26 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის 1-ლი პუნქტი.

მსჯავრდებულთა პირადი საქმეებისა და რეესტრების წარმოება და სხვა.[27] ვინაიდან განსაკუთრებულ კატეგორიას მიკუთვნებული მონაცემები აღმატებული მნიშვნელობისაა და საგულისხმოა, რომ კლასიფიცირდებიან კონფიდენციალურ მონაცემებად,[28] დამმუშავებლის მხრიდან მათდამი კანონიერი წვდომის მიუხედავად, დაუშვებელია მონაცემთა სუბიექტის თანხმობის გარეშე მოპოვებული ინფორმაციის გასაჯაროება და მესამე პირისთვის გამჟღავნება.[29] შესაბამისად მონაცემთა დამმუშავებელი უნდა იყოს კონკრეტული პირი ან დაწესებულება, რომელსაც სამართლებრივი აქტით ან მონაცემთა სუბიექტთან დადებული ხელშეკრულებით უშუალოდ მიენიჭა განსაკუთრებულ კატეგორიას მიკუთვნებულ მონაცემთა დამუშავების უფლება ან ვალდებულება განსაზღვრულ ფარგლებში,[30] დაუშვებელია მის ნაცვლად სხვა დამმუშავებელმა განახორციელოს დამუშავების პროცედურა.

1.2.2. ბიომეტრიული მონაცემი და მათი გამჟღავნებისგან დაცვის სტანდარტები

არის თუ არა ბიომეტრიული მონაცემები პერსონალური ინფორმაცია, დიდი ხნის განსჯის საგანია. დავას წარმოშობს ის, რომ, ერთი მხრივ, საქმე ეხება ბიომეტრიულ ნიმუშებს, რომლებიც უფრო სამედიცინო ინფორმაციაა და წარმოადგენს პერსონალურ ინფორმაციასთან წვდომის გასაღებს, მეორე მხრივ, ბიომეტრიული მონაცემები ნაწარმოებია ადამიანის ქცევითი და ფსიქოლოგიური მახასიათებლებიდან, რომელიც კონკრეტულ პირთან ასოციაციას განაპირობებს, რაც ბიომეტრიულ მონაცემებს აქცევს პერსონალურ მონაცემებად.[31] მიუხედავად იმისა, მიიჩნევა თუ არა ბიომეტრიული მონაცემები პერსონალურ მონაცემებად, აღნიშნული ინფორმაციის დამმუშავებელთა ძირითადი მიზანი ერთია: ჰქონდეს მონაცემთა სუბიექტის პერსონალურ ინფორმაციასთან წვდომა. შესაბამისად, ბიომეტრიული მონაცემების დაცვა და ზოგიერთ შემთხვევაში მათი მოქცევა განსაკუთრებულ კატეგორიაში,[32] განპირობებულია, აღნიშნული ინფორმაციის შეგროვების მასშტაბურობით და მათდამი განსაკუთრებული ინტერესით.

სერიოზულ ბიომეტრიულ კვლევებს საფუძველი ჩაეყარა 1960-იან წლებში, ტექნიკა განვითარდა და დაიხვეწა 1970-იან და 1980-იან წლებში. მნიშვნელოვანი განვითარების ეტაპი დაიწყო 1990-იანი წლების შუა რიცხვებიდან.[33]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ბიომეტრიულ მონაცემს პერსონალურ მონაცემად მიიჩნევს და განმარტავს პირის ფიზიკურ, ფსიქიკურ ან ქცევის მახასიათებლად, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და

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

28 “Who Owns Our Genes?”: Proceedings of an international conference, Tallinn, 1999, 78.

29 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-3 პუნქტი.

30 იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-16 მუხლი.

31 Nanavati S., Thieme M., Nanavati R., Biometrics: Identity Verification in a Networked World, New York, Chichester, Weinheim, Brisbane, Singapore, Toronto, 2002, 243.

32 იხ. „პერსონალურ მონაცემთა დაცვის შესახებ” საქართველოს კანონის მე-2 მუხლის ბ) პუნქტი.

33 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.

რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი).[34]

როგორც წესი, ფიზიკურ ბიომეტრიულ მონაცემთა ჩამონათვალი ბევრად დიდია და მათი გამოყენების პრაქტიკა სხვადასხვა პერიოდს უკავშირდება. დამუშავების ობიექტთაგან პირველ რიგში აღსანიშნავია ხელი, რომლის გეომეტრიული აგებულება 1960 წლიდან პირის იდენტიფიცირების საშუალებად გამოიყენებოდა. 1996 წელს ატლანტის ოლიმპიური თამაშების მიმდინარეობისას ათლეტები უსაფრთხოების სისტემის გავლისას ხელით იდენტიფიცირების მეთოდს იყენებდნენ. დღესდღეობით, ხელის, როგორც ბიომეტრიული მონაცემის, გამოყენება მცირდება და მოძველებულია.[35]

ფიზიკურ ბიომეტრიულ მონაცემთაგან თავისი უნიკალურობის და შეუცვლელობის გამო, ყველაზე აქტიურად გამოყენებადია ადამიანის თითის ანაბეჭდი, რომლის ავტომატური დამუშავების ინიციატივა სისხლის სამართლის სისტემიდან მომდინარეობს. თავდაპირველად თითის ანაბეჭდთა შესწავლა და სხვადასხვა ტიპის მიხედვით კლასიფიცირება ხელით დამუშავებით ხორციელდებოდა. მე-20 საუკუნეში თითის ანაბეჭდთა რაოდენობის მასშტაბური ზრდის შედეგად, ხელით დამუშავების პროცესი ძალიან ძვირი ჯდებოდა და შეცდომებიც გახშირდა. დამუშავების აღნიშნული მეთოდი გამოიყენებოდა 1960-იან წლებამდე, კომპიუტერების შექმნის შემდეგ, პირველი ექსპერიმენტი თითის ანაბეჭდთა ბიომეტრიულ შესაბამისობასთან დაკავშირებით განახორციელა შეერთებული შტატების სტანდარტიზაციის ნაციონალურმა ბიურომ. 1979 წელს თითის ანაბეჭდთა ძებნის სისტემის პირველი საცდელი ნიმუში გამოსცადა შეერთებული შტატების გამოძიების ფედერალურმა ბიურომ. 1983 წლის თითის ანაბეჭდთა იდენტიფიკაციის ავტომატური სისტემები (AFIS) რეგულარულად გამოიყენებოდა.[36]

რაც შეეხება ხმის ნიმუშის მეშვეობით მოსაუბრის იდენტიფიცირების შესაძლებლობას, აღნიშნულზე პირველად 1963 წელს გამოქვეყნდა საგაზეთო სტატია, თუმცა მისი პრაქტიკული გამოცდა განხორციელდა 1974 წელს ამერიკის სატელეფონო და სატელეგრაფო კომპანიის კვლევით ლაბორატორიებში.[37]

გამომდინარე იქიდან, რომ ადამიანები საკუთარი ფიზიკური იდენტობის დასადასტურებლად ხშირად იყენებენ სახის გამოსახულებას (მაგ: პირადობის და მართვის მოწმობებში, პასპორტებსა და სხვა საიდენტიფიკაციო დოკუმენტებში ხშირად აღიბეჭდება ადამიანის სახე), სახე, როგორც ბიომეტრიული მონაცემი, შესწავლის საგნად იქცა 1965 წლიდან, როდესაც ჰელენ ჩანმა და ჩარლს ბისონმა პირველი კვლევები გამოაქვეყნეს. სახის ავტომატური ამომცნობი სისტემის კვლევები 1977 წელს განხორციელდა კანადაში, თუმცა 1990-იან წლებამდე კვლევით საქმიანობაში მნიშვნელოვნად არაფერი შეცვლილა. 1990-იანი წლების

34 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის გ) პუნქტი.

35 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 6.

36 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.

37 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 8.

შუა რიცხვებიდან სახის ამომცნობმა კომერციულმა სისტემებმა დაიწყეს ფუნქციონირება, მათ შორის აღსანიშნავია კომპანიები: Cognitec, ZN, Viisage Technology და Visionics Corporation. 2004 წელს ტექნიკამ მიაღწია სახის ტექსტურის შესწავლის დონესაც.[38]

1970-იანი წლების შუა რიცხვებიდან ტექნოლოგიურად გამოსცადეს თვალის ბადურის მეშვეობით პირის იდენტიფიცირების შესაძლებლობა. აღნიშნული კვლევა, როგორც წესი, გულისხმობს ნიმუშად თვალის უკან მდებარე სისხლძარღვების გამოყენებას, რაც ძალიან ძვირი და სირთულეებთან დაკავშირებული პროცედურაა, კერძოდ რთულია იმ პირის იდენტიფიცირება, რომელიც სათვალეს ატარებს. თუმცა თვალის ბადურა, ისევე, როგორც თვალის ფერადი გარსი, რომლის კვლევის იდეაც წამოაყენა და 1987 წელს დააპატენტა ორმა ოფთალმოლოგმა: ლეონარდ ფლომმა და ალან საფირმა,[39] წარმოადგენს უნიკალურ ბიომეტრიულ მონაცემს, რომლის დუბლირება ძალიან რთულია და შეუცვლელია მთელი სიცოცხლის განმავლობაში. აღნიშნული ნიმუშების კვლევისას კიდევ ერთ სირთულეს წარმოადგენს ის, რომ სკანირება, როგორც კვლევის მეთოდი, რთული გამოსაყენებელია ბავშვებსა და სნეულებში.[40]

ე.წ. კლავიატურის დინამიკა, როგორც ბიომეტრიულ მონაცემთა სახეობა, გულისხმობს კლავიატურაზე ან საბეჭდ მანქანაზე ბეჭდვის რიტმის ნიმუშის მეშვეობით ინდივიდის ამოცნობას. ბეჭდვის რიტმის მეშვეობით, რომელიც მნიშვნელოვნად განსხვავდება სხვადასხვა ინდივიდში, ამოიცნობა მბეჭდავი.[41]

ე.წ. 3D სახის გამოსახულება, როგორც ბიომეტრიული ნიმუში, პირველად გამოიყენეს 1992 წელს და გულისხმობს ადამიანის სახეზე დაკვირვებას, განსაკუთრებით სახის ჩონჩხის ძვლების, სახის უმცირესი ნაწილების შესწავლას კამერების მეშვეობით.[42]

რაც შეეხება ხელისგულის ანაბეჭდის სისტემას, აღნიშნული პირველად უნგრეთში გამოიყენეს 1994 წელს და იდენტურად განხორციელდა AFIS-ის მიერ 1997 წელს. AFIS-ის მიერ ხელისგულის ანაბეჭდის დამუშავება დღესაც აქტიურად ხორციელდება.[43]

პიროვნების იდენტიფიკაციასთან დაკავშირებულმა კვლევებმა და ბიომეტრიულ მონაცემებს მიკუთვნებული ინფორმაციის ეტაპობრივად ზრდამ დაადასტურა, რომ ადამიანის ინდივიდუალური და უნიკალური მახასიათებლები ამოუწურავია და მათი საკვლევ ობიექტად ქცევა მხოლოდ შესაბამისი ტექნიკის არსებობაზეა დამოკიდებული. თანამედროვე სამყაროში სხვა ისეთი ბიომეტრიული ტექნოლოგიების მეშვეობით, როგორიცაა ვენის სკანირება, სახის თერმოგრაფია, დნმ-ის შესაბამისობის დადგენა, სხეულის სუნის განსაზღვრა, სისხლის პულსის,

38 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 7.

39 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 8.

40 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 42.

41 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 53.

42 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 6 და 64.

43 Dunstone T., Yager N., Biometric System and Data Analysis Design, Evaluation, and Data Mining, Eveleigh, NSW, Australia, 2009, 5.

სიარულის მანერის და ყურის ფორმის შესწავლა, შესაძლებელი გახდა ადამიანის ამოცნობა.[44] ტექნიკის განვითარებასთან ერთად ბიომეტრიული კვლევის ობიექტები კვლავ გაიზრდება. სწორედ აღნიშნულის მოლოდინმა განაპირობა ის, რომ სხვადასხვა ქვეყნის კანონმდებელთა უმრავლესობა კონკრეტულად არ ჩამოთვლის იმ ბიომეტრიულ მონაცემთა ნაირსახეობას, რომელთა განსაკუთრებული დაცვა მნიშვნელოვანია, არამედ ბიომეტრიულად მიიჩნევს ზოგადად ადამიანის უნიკალურ და მუდმივად არსებულ ფიზიკურ, ფსიქიკურ და ქცევით მახასიათებელს.

ბიომეტრიულ მონაცემთა მნიშვნელობიდან და მისი ინფორმატიული ბუნებიდან გამომდინარე, საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ განსხვავებულ რეგულაციებს აწესებს საჯარო და კერძო დაწესებულებების მიერ ბიომეტრიულ მონაცემთა დამუშავებისას და აღნიშნავს, რომ ამ ინფორმაციის დამუშავება შესაძლებელია მხოლოდ (საჯარო დაწესებულების მიერ ბიომეტრიული ინფორმაციის დამუშავება შეუზღუდავად შესაძლებელია კანონით დადგენილი წესით პირადობის დამადასტურებელი დოკუმენტის გაცემის ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიცირების, აგრეთვე საქართველოს საკანონმდებლო აქტით პირდაპირ გათვალისწინებულ შემთხვევებში) პირის უსაფრთხოების, საკუთრების დაცვის ან საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით მაშინ, თუ სხვაგვარად აღნიშნული მიზნის მიღწევა შეუძლებელია. კანონმდებელი კერძო დაწესებულებისათვის აწესებს აგრეთვე ბიომეტრიულ მონაცემთა გამოყენებამდე პერსონალურ მონაცემთა დაცვის ინსპექტორისა და მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების აუცილებლობას.[45]

ვინაიდან ქართველი კანონმდებელი ბიომეტრიულ მონაცემთა დამუშავებისას განსაკუთრებულ რეგულაციებს აწესებს, საგულისხმოა, რომ მონაცემთა ეს კატეგორია გამჟღავნებისგან დაცვასაც მოითხოვს. მიიჩნევა, რომ დამმუშავებლის პიროვნება და ბიომეტრიულ მონაცემთა დამუშავების ფარგლები მკაცრად განსაზღვრული უნდა იყოს. საყურადღებოა ის ფაქტიც, რომ კერძო დაწესებულებებს, რომლებიც ამუშავებენ ბიომეტრიულ მონაცემებს, კანონმდებელი დამატებით უწესებს დამუშავებულ მონაცემთა შესახებ, მათ გამოყენებამდე პერსონალურ მონაცემთა დაცვის ინსპექტორისთვის შეტყობინების სავალდებულოობას, ხოლო საჯარო დაწესებულებათა მიმართ მსგავსი შეზღუდვა არ მოქმედებს. მხოლოდ ფარულ საგამოძიებო მოქმედებასთან დაკავშირებით ატყობინებს მონაცემთა დამმუშავებელი პროკურორი პერსონალურ მონაცემთა დაცვის ინსპექტორს, პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით განხორციელებული ან განსახორციელებელი საქმიანობის შესახებ,[46] ვინაიდან საკომუნიკაციო საშუალებების გარეშე ფარული საგამოძიებო საქმიანობა წარმოუდგენელია, აღნიშნულში უშუალოდ მოქმედი საქართველოს კომუნიკაციების ეროვნული კომისიაც ვალდებულია „ელექტრონული კომუნიკაციების მაიდენტიფიცირებელი მონაცემების საქართველოს სისხლის სამართლის საპროცესო კოდექსით დადგენილი წესებით შესაბამისი სახელმწიფო ორგანოებისათვის

44 Newman R., Security and Access Control Using Biometric Technologies, Boston, 2009, 53.

45 იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-9 და მე-10 მუხლები.

46 იხ. საქართველოს სისხლის სამართლის კოდექსის 143^3 მუხლის მე-5, მე-6^1, მე-7 ნაწილები და 143^8 მუხლის მე-3 ნაწილი.

გადაცემის ფაქტების აღრიცხვისა და პერსონალურ მონაცემთა დაცვის ინსპექტორისთვის სათანადო ინფორმაციის მიწოდების“[47] კუთხით. სხვა შემთხვევებში კონკრეტული საჯარო სამსახურების საქმიანობის განხორციელებასთან დაკავშირებული კანონმდებლობა მხოლოდ იმის მითითებით შემოიფარგლება, რომ მონაცემთა დამმუშავებელი პირი ვალდებულია გამჟღავნებისგან დაიცვას დასამუშავებელი პერსონალური მონაცემი.

1.2.3. გენეტიკური მონაცემი და მათი კონფიდენციალურობის სტანდარტები

გენეტიკა არის მეცნიერების დარგი, რომელიც შეისწავლის ორგანიზმების მემკვიდრულობისა და ცვალებადობის კანონზომიერებებს.[48] თანამედროვე დისციპლინად ის იქცა 1860-იანი წლებიდან, გრეგორ მენდელის მუშაობის შედეგად, რომელმაც პირველად წამოაყენა გენის არსებობის იდეა.[49] გენი არის ორმაგი ხვეულისმაგვარი მოლეკულური ძაფი, რომელსაც ეწოდება დეზოქსირიბონუკლეინის მჟავა, შემოკლებით დნმ-ი.[50] 1953 წელს ვატსონის და კრიკის მიერ დნმ-ის სტრუქტურის აღმოჩენის შემდეგ, მოლეკულურმა გენეტიკამ დაიკავა ცენტალური პოზიცია სასიცოცხლო პროცესების მიმდინარეობის ახსნა-განმარტების წარმოდგენის კუთხით.[51] გენების აღმოჩენა, მოლეკულური სტრუქტურის შეცნობა და ფუნქციონირება არის წყარო რომლითაც შეიძლება ბიოლოგიის ორი უდიდესი საიდუმლოების შეცნობა: 1. რა ხდის სახეობას იმად, რადაც ისინი გვევლინებიან? (პრაქტიკული დაკვირვებით მემკვიდრეობითობა გადამწყვეტია, ვინაიდან მაგალითად უნარი, რომ კატას ყველა თაობას უჩნდება კატა, არის მემკვიდრეობითი) და 2. რა იწვევს სახეობათა შიგნით ცვალებადობას? (მაგალითად, უნიკალური ფერის ცხოველებს ხშირად ჰყავთ იგივე ფერის შთამომავლობა, ისეთივე მახასიათებელი თვისებებით, რაც ნიშნავს, რომ ისინი კონკრეტულად „ნაწარმოებნი არიან მხოლოდ ამ ოჯახიდან“).[52] მაშასადამე, გენეტიკა ორგანიზმის „მოკვლევის“ საშუალებაა.[53] მისი მეშვეობით შესაძლებელია იმ უნიკალური და მუდმივი ინფორმაციის მოძიება, რომელიც მხოლოდ კონკრეტული სუბიექტისთვის და მისი ოჯახის სისხლით ნათესავი წევრებისთვის არის დამახასიათებელი.[54] გენეტიკური მონაცემების ცოდნამ შესაძლოა, ინდივიდს თავიდან ააცილებინოს ან მნიშვნელოვნად შეუმციროს მემკვიდრეობითი დაავადებები, ან მოხდეს მათი პროგნოზირება,[55] თუმცა მისმა შემთხვევითმა გაჟღერებამ შესაძლებელია, კონკრეტული პიროვნების მასიდან გარიყვაც გამოიწვიოს.

47 „საქართველოს კომუნიკაციების ეროვნული კომისიის დებულების დამტკიცების შესახებ“ საქართველოს კომუნიკაციების ეროვნული კომისიის დადგენილება N2-ის მე-7 მუხლის მე-3 პუნქტის ლ) ქვეპუნქტი.

48 <http://www.nplg.gov.ge/gwdict/index.php?a=term&d=13&t=2737>[07.03.2016]

49 Griffiths A., Miller J., Suzuki D., Lewontin R., Gelbart W., An Introduction to Genetic Analysis, New York, 2000, 23

50 იქვე, *3*

51 Human Genetic Information: Science, Law and Ethics, UK, 1990, 6.

52 Griffiths A., Miller J., Suzuki D., Lewontin R., Gelbart W., An Introduction to Genetic Analysis, New York, 2000, 3.

53 Human Genetic Information: Science, Law and Ethics, UK, 1990, 7.

54 იქვე, 6.

55 იქვე, 96.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი გენეტიკურ მონაცემს განმარტავს, როგორც „მონაცემთა სუბიექტის უნიკალურ და მუდმივ მონაცემს გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება;“[56] იგი ამავდროულად განსაკუთრებულ მონაცემთა კატეგორიაა, თუკი იძლევა პირის იდენტიფიცირების საშუალებას.[57]

ზოგიერთი გენეტიკური მონაცემი, როგორიცაა გენეტიკური შეუთავსებლობა და სერიოზული დაავადებებისადმი მიდრეკილება, განსაკუთრებულად მგრძნობიარე ბუნებისაა, ხოლო ისეთი გენეტიკური ინფორმაცია, როგორიცაა სქესი, თვალისა და თმის ფერი, ნაკლებ მგრძნობიარე. თუმცა შესაძლოა, შეიცვალოს ამ ინფორმაციისადმი დამოკიდებულება. მაგალითად: ემბრიონის სქესთან დაკავშირებული ინფორმაცია ზოგიერთ მშობელს არ მიეწოდება და დაცულია მისი კონფიდენციალურობა,[58] ვინაიდან ხშირია მშობლებისთვის არასასურველი სქესის ბავშვის ჩასახვისას აბორტის პრეცედენტები.

ადამიანის უჯრედული ქსოვილის დნმ-ის ნიმუში, როგორც პირის ინდივიდუალურობის განმსაზღვრელი, ყოველთვის კონფიდენციალურად იქნება მიჩნეული, რადგან მას შეუძლია საფრთხე შეუქმნას განსაკუთრებით მგრძნობიარე ინფორმაციათა გამჟღავნებას,[59] გაამჟღავნოს ისეთი „ოჯახური საიდუმლოებები“, როგორიცაა მამობის დადგენა და შვილად აყვანა.[60]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი გენეტიკური მონაცემების დამუშავებასთან დაკავშირებით სპეციალურ წესს არ ადგენს, თუმცა განსაკუთრებული კატეგორიის მონაცემთა დამუშავებასთან დაკავშირებული რეგულაცია მასზე ვრცელდება, ვინაიდან აღნიშნულის დეფინიცია თავის თავში გენეტიკურ მონაცემებსაც მოიცავს. შესაბამისად გენეტიკური მონაცემების დაცვა ისევე მკაცრად ხორციელდება, როგორც ნებისმიერი განსაკუთრებული მონაცემის.

2. დეპერსონალიზაციის პრაქტიკული განხორციელების პრობლემები

ვინაიდან დეპერსონალიზაციის საკანონმდებლო დეფინიცია პრაქტიკული განხორციელების შესაძლებლობასაც უნდა მოიცავდეს, აუცილებელია, არსებობდეს რამდენიმე სამართლებრივი პირობა, რომელიც ამას უზრუნველყოფს. მაგალითად, მოსახლეობის აღწერის გადაწყვეტილებაში, გერმანიის საკონსტიტუციო სასამართლომ მოითხოვა აღწერის მონაცემთა ადრეული პრაქტიკული დეპერსონალიზაციის განხორციელება, რათა მონაცემთა სუბიექტის გაიდენტიფიცირება შესაძლებელი არ ყოფილიყო. კერძოდ, გერმანიის ფედერალურ მონაცემთა დაცვის აქტის მე-40 სექციის მე-3 პარაგრაფის თანახმად, პერსონალური

56 „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის გ[1]) პუნქტი.

57 იქვე, მე-2 მუხლის ბ) პუნქტი.

58 “Who Owns Our Genes?”: Proceedings of an international conference, by Nordic Committee on Bioethics, Tallin, 1999, 78.

59 იქვე. 78.

60 Stefanick L., Controlling knowledge: Freedom of Information and Privacy Protection in a Networked World, Canada, 2011. 101.

მონაცემები, რომლებსაც ფლობენ კვლევითი ინსტიტუტები, „უნდა იყოს დეპერსონალიზებული მაშინვე, როგორც კი კვლევითი მიზნები ამის დასაშვებობას განაპირობებენ." მანამდე სუბიექტის მაიდენტიფიცირებელი ინფორმაცია უნდა ინახებოდეს განცალკევებით. თუკი განცალკევება არ განხორციელდება, მინიმუმ ფსევდონიმებით პირდაპირ (ან თუ შესაძლებელია არაპირდაპირი გზით) მაინც უნდა იქნეს ჩანაცვლებული.[61] პიროვნების იდენტიფიცირების პრევენციული დაცვის ღონისძიებების განხორციელების გარეშე, ინფორმაციის ქურდმა, რომელსაც დამატებითი ცნობები აქვს პირის იდენტობის (სახელი, გვარი, მისამართი, პირადი ნომერი), დემოგრაფიული მონაცემების (სქესი, ეროვნება, განათლება, რელიგია, ოჯახური მდგომარეობა), სამედიცინო მონაცემების (დაავადებები, ჩვევები) და სხვათა შესახებ, შესაძლოა გააიდენტიფიციროს მონაცემთა სუბიექტი და გაამჟღავნოს მისი განსაკუთრებით მგრძნობიარე პერსონალური მონაცემები.[62]

სტატისტიკური, სამეცნიერო და ისტორიული მიზნებისათვის მონაცემთა შეგროვებისას სუბიექტის ინტერესების დაცვას „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონიც გაწერს,[63] თუმცა დამმუშავებელ პირს არ უწესებს შეგროვებული ინფორმაციის დეპერსონალიზაციის ვალდებულებას მაშინ, როდესაც ამის საჭიროება არსებობს. აღნიშნულ შემთხვევაში ინფორმაციის გამჟღავნებისგან დაცვის პრაქტიკულ მექანიზმს წარმოადგენს მხოლოდ პერსონალურ მონაცემთა დაცვის ინსპექტორის მოთხოვნა მონაცემთა დეპერსონალიზაციასთან დაკავშირებით, „თუ მიიჩნევს, რომ მონაცემების დამუშავება ხორციელდება კანონის საწინააღმდეგოდ."[64] მაგრამ პრობლემა იჩენს თავს, როდესაც კანონის დარღვევასთან დაკავშირებით ინსპექტორის ინფორმირებამდე, დეპერსონალიზაციის განუხორციელებლობის გამო, პერსონალური მონაცემები გარეშე პირთათვისაც ხელმისაწვდომი ხდება.

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი არ მოიცავს ერთგვაროვან წესს, რომლითაც შესაძლებელია მონაცემთა სუბიექტის ვინაობის გამჟღავნებისგან დაცვა, ვინაიდან აღნიშნული პრაქტიკულად შესაძლოა განხორციელდეს მაიდენტიფიცირებელი ინფორმაციის დაშიფვრით, ამოღებით, გასაიდუმლოებით, ფსევდონიმის მინიჭებით და სხვა მრავალი მეთოდით. ფსევდონიმის მინიჭება უმეტესად ხორციელდება სისხლის სამართლის პროცესში მონაწილე პირის დაცვის მიზნით, კერძოდ, თუ პირი დაცვის სპეციალური ღონისძიების ქვეშ იმყოფება, ღონისძიების სახედ შესაძლოა გამოყენებულ იქნეს ვინაობის შეცვლა, რაც გულისხმობს ფსევდონიმის მინიჭებას, გარეგნობის შეცვლას, ამოცნობისა და იდენტიფიცირების შესაძლებლობის შემცველი საპროცესო და სხვა დოკუმენტების გასაიდუმლოებას.[65] ვინაიდან კანონით დაუშვებელია არასრულწლოვანის პერსონალური მონაცემების გამჟღავნება და გამოქვეყნება, გარდა „პერსონალურ მონაცემთა დაცვის

61 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 112.

62 Fischer-Hübner S., IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2001, 113.

63 იხ. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ" მე-7 მუხლის მე-5 ნაწილი და მე-15 მუხლის მე-4 ნაწილი.

64 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ" 39-ე მუხლის 1-ლი პუნქტის გ) ქვეპუნქტი.

65 საქართველოს სისხლის სამართლის საპროცესო კოდექსის 68-ე მუხლის მე-3 ნაწილის ბ) ქვეპუნქტი.

შესახებ“ საქართველოს კანონით გათვალისწინებული შემთხვევებისა,[66] სისხლის სამართლის და ადმინისტრაციული პასუხისმგებლობის შეფარდების პროცესში არასრულწლოვანის იდენტიფიცირების გამორიცხვის მიზნით, მონაცემთა დამმუშავებელი პირები ვალდებულნი არიან უზრუნველყონ საჯარო ინფორმაციის ხელმისაწვდომობა არასრულწლოვანი პირის საიდენტიფიკაციო მონაცემების ფსევდონიმით ჩანაცვლებით, ინიციალების გამოყენებით, დაშიფვრით ან სხვა მეთოდით.

3. პასუხისმგებლობის მექანიზმები დეპერსონალიზაციის განუხორციელებლობისას

მონაცემთა სუბიექტის უფლება, რომ კანონმდებლობით გათვალისწინებულ შემთხვევებში მისი პერსონალური მონაცემები დაექვემდებაროს დეპერსონალიზაციას, უნდა იქნეს დაცული და გარანტირებული, წინააღმდეგ შემთხვევაში, პერსონალურ მონაცემთა დაცვის ინსპექტორი მონაცემთა სუბიექტის მხრიდან შესაბამისი შეტყობინების მიღების შემთხვევაში ვალდებულია, მიიღოს კანონით გათვალისწინებული ზომები.[67] ინსპექტორი აგრეთვე უფლებამოსილია, მონაცემთა სუბიექტის შეტყობინების გარეშე, საკუთარი ინიციატივით მოითხოვოს დეპერსონალიზაცია, თუკი მიიჩნევს, რომ მონაცემთა დამუშავება ხორციელდება კანონსაწინააღმდეგოდ.[68]

აღსანიშნავია, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორი დამმუშავებლის მიერ მონაცემთა დეპერსონალიზაციის განხორციელებისას, არ მსჯელობს ამ მოქმედების მიზანშეწონილობაზე. კერძოდ, მონაცემთა დამმუშავებელს აქვს უფლება, იმ შემთხვევაშიც მოახდინოს მონაცემთა დეპერსონალიზაცია, როდესაც არსებობს გამჟღავნების აუცილებლობა ამ ინფორმაციის მიმართ ლეგიტიმური საჯარო ინტერესიდან გამომდინარე. მაგალითად, საერთო სასამართლოს მიერ მიღებული გადაწყვეტილებები უმეტესად ქვეყნდება პროცესის მხარეთა ინიციალების მითითებით, მაშინ როდესაც სასამართლო მიმდინარეობდა საჯარო განხილვის ფორმატში და მასზე დასწრების უფლება ყველას ჰქონდა, მსგავს შემთხვევაში სწორი იქნება პერსონალურ მონაცემთა დაცვის ინსპექტორს გააჩნდეს დეპერსონალიზაციის განხორციელების მიზანშეწონილობის განხილვის ფუნქციაც, რათა ინსპექტორის გადაწყვეტილებაზე დაყრდნობით, ნებისმიერ პირს შეეძლოს მონაცემთა გამჟღავნების მოთხოვნა.

66 საქართველოს კანონის „არასრულწლოვანთა მართლმსაჯულების კოდექსის“ მე-13 მუხლის მე-2 ნაწილის მე-2 წინადადება.

67 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ 34-ე მუხლის 1-ლი პუნქტი.

68 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ 39-ე მუხლის 1-ლი პუნქტის გ) ქვეპუნქტი.

პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ მონაცემთა დეპერსონალიზაციის მოთხოვნას სულ ორიოდე შემთხვევაში ჰქონდა ადგილი. კერძოდ, არჩევნების საერთაშორისო სტანდარტებთან შესაბამისობისა და შეზღუდული შესაძლებლობის მქონე პირთათვის ხელმისაწვდომი საარჩევნო გარემოს შექმნის მიზნით, ინსპექტორმა შეზღუდული შესაძლებლობების მქონე პირთა შესახებ (ეტლით მოსარგებლე, სმენადაქვეითებული, უსინათლო) ცენტრალური საარჩევნო კომისიისათვის მონაცემთა დეპერსონალიზებული ფორმით მიწოდება მიზანშეწონილად მიიჩნია.[69]

2015 წლის ანგარიშებში პერსონალურ მონაცემთა დაცვის ინსპექტორი აღწერს ორ შემთხვევას, როდესაც სასამართლომ საჯარო ინფორმაციის სახით, პერსონალური მონაცემების გარეშე, მხოლოდ ინიციალების მითითებით გასცა განაჩენის ასლები და განაჩენის ასლის შინაარსმა შესაძლებელი გახადა მოქალაქეთა იდენტიფიცირება და მათ შესახებ განსაკუთრებულ კატეგორიას მიკუთვნებული ინფორმაციის გამჟღავნება.[70] აღნიშნულმა პრაქტიკამ აჩვენა, რომ დეპერსონალიზაცია მხოლოდ ისეთი მონაცემების ამოღებას ან დაფარვას არ ნიშნავს, როგორიცაა სახელი და გვარი, პირადი საიდენტიფიკაციო ნომერი და მისთანანი, არამედ გულისხმობს ისეთი მონაცემების ანონიმურობას, რომლებიც თავიანთი განსხვავებულობით და ერთადერთობით პირდაპირ მიუთითებენ მონაცემთა სუბიექტზე. ეს შემთხვევა უარყოფითად აისახება ისეთი სისტემის საქმიანობაზე, რომლიც თავად არის ვალდებული განიხილოს დეპერსონალიზაციის განხორციელების მართებულობა პირის მიმართვის შემთხვევაში.

კანონის დარღვევის შემთხვევაში პასუხისმგებლობის მექანიზმებად პერსონალურ მონაცემთა დაცვის ინსპექტორი იყენებს გაფრთხილებას ან ჯარიმას, ჯარიმის ოდენობა დამოკიდებულია იმაზე, თუ რომელი პერსონალური მონაცემის დამუშავებისას განხორციელდა კანონსაწინააღმდეგო ქმედება და ჰქონდა თუ არა ადგილი განმეორებით დარღვევებს პასუხისმგებლობის დაკისრების შემდგომ.[71] კანონი მნიშვნელოვნად არ მიიჩნევს იმას, თუ როგორი ინტენსივობით და რამდენად დიდი მოცულობის მონაცემთა მიმართ ხორციელდებოდა კანონსაწინააღმდეგო ქმედება. ჯარიმის ოდენობა ფიქსირებულია და კანონსაწინააღმდეგო ქმედების ხარისხს და მიყენებული ზიანის ოდენობას არ ითვალისწინებს, რაც, თავის მხრივ, გაუმართლებელია და ჯარიმას, როგორც პასუხისმგებლობის ზომას, ხშირ შემთხვევაში ბიუჯეტის შევსების მექანიზმად მიიჩნევს. გასათვალისწინებელია ის ფაქტიც, რომ მონაცემთა დამმუშავებლისთვის შესაძლოა, დამუშავების აკრძალული ხერხები და ობიექტი ბევრად ღირებული იყოს, ვიდრე დაკისრებული ჯარიმა. ზემოთქმულიდან გამომდინარე საუკეთესო რეგულირება იქნებოდა ის, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორს თითოეული საქმე ინდივიდუალურად შეესწავლა და ჯარიმის ოდენობა თავად განესაზღვრა იმის მიხედვით, თუ რამდენად მომგებიანია დამმუშავებლისთვის კანონსაწინააღმდეგო ქმედება.

69 პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“ თბილისი, 2014, 15.

70 პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიში „პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“ თბილისი, 2015, 26-27.

71 იხ. საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ VII თავი.

პერსონალურ მონაცემთა დეპერსონალიზაციის მოთხოვნების დარღვევის შემთხვევაში მონაცემთა სუბიექტი უფლებამოსილია, მიმართოს იმავე ან ზემდგომ ადმინისტრაციულ ორგანოს ან სასამართლოს.[72] სასამართლო ის უკანასკნელი საშუალებაა, რომლითაც უფლებამოსილ პირს შეუძლია დარღვეული უფლების აღდგენა და დამრღვევისათვის შესაბამისი პასუხისმგებლობის დაკისრების მოთხოვნა.

სასამართლოში განხილულ საქმეთა შორის აღსანიშნავია გადაწყვეტილება, რომლის შესაბამისად, დავა განპირობებული იყო ქალაქ რუსთავის საკრებულოს მხრიდან საჯარო ინფორმაციის გაცემაზე უარის თქმით. ამ გადაწყვეტილებაში სასამართლო მაინც მსჯელობს კონსტიტუციის ცალკეულ მუხლებზე გარკვეული კატეგორიის პერსონალურ მონაცემთა გაცემის წესზე საუბრისას, მიუხედავად იმისა, რომ ამ დროისთვის სპეციალური კანონი მიღებული იყო, თუმცა ამავდროულად ხელმძღვანელობს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონითაც. გადაწყვეტილება მნიშვნელოვანია, რადგან განმარტავს „საჯარო სამსახურში ინტერესთა შეუთავსებლობისა და კორუფციის შესახებ“ კანონის მე-2 მუხლით გათვალისწინებული პირების შესახებ არსებული პერსონალური მონაცემების გაცემის განსხვავებულ სამართლებრივ რეჟიმს და განსაზღვრავს, რომ თანამდებობის პირებთან (აგრეთვე მათი ოჯახის წევრებთან) დაკავშირებული პირადი საიდუმლოების შემცველი ინფორმაციის საჯაროობა ემსახურება ლეგიტიმურ მიზანს – უზრუნველყოს თანამდებობის პირთა შესახებ ინფორმაციის ტრანსფარენტობა, გამჭირვალობა.[73] წინამდებარე განმარტების შინაარსიდან გამომდინარე, სასამართლო მართებულად მიიჩნევს თანამდებობის პირის შესახებ ნებისმიერი ტიპის ინფორმაციის გამჟღავნებას, თუმცა მიუხედავად სტატუსისა და აქედან გამომდინარე გაძლიერებული საზოგადოებრივი ინტერესისა, აუცილებელია ისეთი ინფორმაციის დეპერსონალიზებული ფორმით ხელმისაწვდომობა, რომელიც სენსიტიური ბუნებისაა და აღნიშნულის გამჟღავნება მხოლოდ მონაცემთა სუბიექტის თანხმობაზეა დამოკიდებული.

აღსანიშნავია, რომ სასამართლოს პრაქტიკა ძირითადად ეხება პერსონალურ მონაცემთა შემცველი ინფორმაციის გაცემის, გაცემაზე უარის თქმისა და მონაცემთა შესაბამისი საფუძვლების გარეშე დამუშავების შემთხვევებს. კონკრეტულად დეპერსონალიზაციის მოთხოვნასა და მის მართებულობაზე სასამართლოს ჯერჯერობით არ უმსჯელია.

72 საქართველოს კანონის „პერსონალურ მონაცემთა დაცვის შესახებ“ 26-ე მუხლის 1-ლი პუნქტი.

73 საქართველოს უზენაესი სასამართლოს ადმინისტრაციულ საქმეთა პალატის 2013 წლის 30 მაისის განჩინება, №ბს-527-518(კ-12).

დასკვნა

საქართველო ახალბედაა პერსონალურ მონაცემთა დამცავი კანონმდებლობის შექმნის კუთხით, თუმცა მისასალმებელია ის, რომ ქვეყანა ზედმიწევნით იმეორებს განვითარებული და გამოცდილი სახელმწიფოებისა და ორგანიზაციების საკანონმდებლო და პრაქტიკულ მიღწევებს. დეპერსონალიზაციის განმარტებას ბევრი ქვეყნის კანონმდებლობა საერთოდ არ ითვალისწინებს, თუმცა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ამ კუთხითაც განსაკუთრებული აღმოჩნდა.

ნაშრომში განხილულმა საკითხებმა წარმოაჩინა, რომ დეპერსონალიზაცია მონაცემთა სუბიექტის გამჟღავნებისგან დაცვის საუკეთესო გზაა. შესაბამისად მისი პრაქტიკული დახვეწა აუცილებელია, რათა კანონმდებლობით განსაზღვრული დეფინიციის შესაბამისი იყოს.

ნაშრომში განხილული პრაქტიკის ანალიზის საფუძველზე, შეიძლება ითქვას, რომ აღმოსაფხვრელია დეპერსონალიზაციას დაქვემდებარებულ მონაცემთა გამჟღავნების პრობლემა, რომელიც ისეთი სისტემის მუშაობის შედეგად გამოიკვეთა, როგორიცაა საერთო სასამართლო. მსგავსი შემთხვევები ბევრი საჯარო და კერძო ორგანიზაციისთვისაც ცუდი მაგალითი იქნება, ვინაიდან ისინი თავს ვალდებულად აღარ ჩათვლიან, უზრუნველყონ მონაცემთა დეპერსონალიზაცია, მაშინ როდესაც სასამართლო სისტემისმაგვარი ავტორიტეტის და მნიშვნელობის დაწესებულება არ იცავს კანონმდებლობით დადგენილ სტანდარტს.

კვლევის შედეგად, დადებითად უნდა იქნეს შეფასებული პერსონალურ მონაცემთა დაცვის ინსპექტორის საქმიანობა, რომელიც დაუყოვნებლივ და სწორად რეაგირებს მონაცემთა დეპერსონალიზაციის საკანონმდებლო წესის დარღვევის დროს. თუმცა უკეთესი იქნება, თუკი ინსპექტორის საქმიანობა საქმის უფრო სიღრმისეული შესწავლით და დეპერსონალიზაციის შემთხვევების მართებულობის განხილვითაც განისაზღვრება, რათა მონაცემთა კონკრეტულ შემთხვევებში დეპერსონალიზაციამ არ დააზარალოს ლეგიტიმური საჯარო ინტერესები და დამმუშავებლის მიერ საზოგადოების ინფორმაციის ვაკუუმში მოქცევას არ შეუწყოს ხელი. მსგავს სიტუაციაში ინსპექტორის საქმიანობა კიდევ უფრო საპასუხისმგებლო და დატვირთული იქნება, თუმცა ხელს შეუწყობს მონაცემთა დამმუშავებლის საქმიანობის საფუძვლიან შესწავლას და კანონის დარღვევის პრევენციას.

გარდა აღნიშნულისა, გადასახედია ჯარიმის დაკისრების საკითხი სხვადასხვა კატეგორიის ინფორმაციასთან დაკავშირებულ კანონდარღვევებზე. კერძოდ, ინსპექტორს უნდა მიეცეს საშუალება, რომ ჯარიმის ოდენობა დარღვევით გამოწვეული ზიანიდან და დამმუშავებლის მიერ მიღებული სარგებლიდან გამომდინარე განსაზღვროს. აღნიშნული კვლავ ხელს შეუწყობს ყოველი კონკრეტული შემთხვევის საფუძვლიან შესწავლას და სამართლიანი დამსჯელი ღონისძიებების გატარებას.