საქართველოს ტექნიკური უნივერსიტეტი
GEORGIAN TECHNICAL UNIVERSITY

ნატო გუგავა

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის სტანდარტები საქართველოს საჯარო სექტორში და საერთაშორისო გამოცდილება

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა: საჯარო მმართველობა

შიფრი 1109

საქართველოს ტექნიკური უნივერსიტეტი
თბილისი, 0175, საქართველო
“----------“ 2017 წელი

საქართველოს ტექნიკური უნივერსიტეტი

ბიზნესტექნოლოგიების ფაკულტეტი

ჩვენ, ხელისმომწერნი ვადასტურებთ, რომ გავეცანით ნატო გუგავას მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: ,,განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის სტანდარტები საქართველოს საჯარო სექტორში და საერთაშორისო გამოცდილება“ და ვაძლევთ რეკომენდაციას ----------
საუნივერსიტეტო სადისერტაციო საბჭოში ----------
დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

თარიღი: „-----„ „----------„ 2017 წელი

ხელმძღვანელი: გ. გორაძე

ასოცირებული პროფესორი

რეცენზენტი: ----------

რეცენზენტი: ----------

საქართველოს ტექნიკური უნივერსიტეტი

ნატო გუგავა

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის სტანდარტები საქართველოს საჯარო სექტორში და საერთაშორისო გამოცდილება

საქართველოს ტექნიკური უნივერსიტეტის ბიზნესტექნოლოგიების ფაკულტეტი

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

„----------„ 2017 წელი

ავტორის ხელმოწერა:

რეზიუმე

დემოკრატიულ ქვეყნებში პერსონალური მონაცემების დაცვა ადამიანის ერთ-ერთ ძირითად უფლებად განიხილება, ამ უფლების რეალიზებისთვის კი არსებობს შესაბამისი ინსტიტუციური უწყებები და საკანონმდებლო რეგულაციები.

საქართველოს სახელმწიფომ, ბოლო წლების განმავლობაში, პერსონალური მონაცემების დაცვის კუთხით, რამდენიმე მნიშვნელოვანი ნაბიჯი გადადგა. ეს გამოიხატა საკანონმდებლო დონეზე პერსონალური მონაცემების დაცვის გარანტიების შექმნაში. კერძოდ, 2011 წლის 28 დეკემბერს საქართველოს პარლამენტმა მიიღო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რაც წარმოადგენს მნიშვნელოვან ინსტრუმენტს მოქალაქეთა პერსონალური მონაცემების დაცვის მიმართულებით. 2013 წლის დასაწყისში კი შეიქმნა საზედამხედველო ორგანო პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის სახით, რომლის უფლებამოსილებასაც განეკუთვნება პერსონალური მონაცემების დამუშავების კანონიერებაზე კონტროლი საქართველოში.

გარდა აღნიშნულისა, საქართველოს ევროატლანტიკური ინტეგრაციის პროცესში, ასევე უდიდესი მნიშვნელობა ენიჭება პერსონალური მონაცემების დაცვის მიმართულებით ქვეყანაში არსებულ მდგომარეობას. წლების მანძილზე, ევროკავშირის მხრიდან განსაკუთრებული ყურადღება ეთმობოდა აღნიშნულ საკითხს. 2013 წლის 29 ნოემბერს საქართველოსა და ევროპის კავშირს შორის გაფორმებული ასოცირების შეთანხმებისა და 2014 წლის 27 ივნისს ასოცირების ხელშეკრულების ხელმოწერის საფუძველზე, საქართველომ პერსონალურ მონაცემთა დაცვის ევროპული სტანდარტების დანერგვისა და შესაბამისი საკანონმდებლო და ინსტიტუციური რეფორმების განხორციელების ვალდებულება აიღო. მნიშვნელოვანია, რომ ევროკავშირის ქვეყნებთან თანამშრომლობა, სხვა სისტემურ რეფორმებთან ერთად, მოითხოვს საქართველოს სახელმწიფოს, როგორც საჯარო, ასევე, კერძო სექტორში პერსონალური მონაცემების დამუშავების თანამედროვე სტანდარტების შემოღებასა და დაცვას, საზღვარგარეთის ქვეყნების საუკეთესო გამოცდილების გაზიარებას, ამ მიმართულების განვითარებასა და მოდერნიზებას. აღნიშნული თანამედროვე სტანდარტების იმპლემენტაციის პროცესში კი მნიშვნელოვანია, როგორც სამეცნიერო კვლევის საფუძველზე პუბლიკაციების, ნაშრომების, პროგრამების, მეთოდურ-პრაქტიკული სახელმძღვანელოების გამოცემა, ასევე, განახლებული და თანამედროვეობას მორგებული საუნივერსიტეტო დისციპლინებისა და სხვა ტიპის შემეცნებითი აქტივობების (სასწავლო კურსები, ტრენინგპროგრამები, სამუშაო შეხვედრები, მრგვალი მაგიდები, დისკუსიები და ა.შ.) განხორციელება. ეს, ერთი მხრივ, საგრძნობლად დაეხმარება ამ დარგით დაინტერესებულ ნებისმიერ მოქალაქეს, ხოლო მეორე მხრივ, გაამარტივებს და დააჩქარებს თანამედროვე სტანდარტების დანერგვის პროცესს საქართველოში.

პერსონალური მონაცემების დაცვა წარმოადგენს პირის პირადი ცხოვრების ხელყოფისაგან დაცვას, მისი პერსონალური მონაცემების

უკანონო გამოყენებისა და ამ მონაცემების შეცვლის საფრთხის თავიდან აცილებას. აღსანიშნავია, რომ აღნიშნული მიმართულების განვითარების ისტორია საქართველოში მხოლოდ ოთხ წელს ითვლის. შესაბამისად, პერსონალურ მონაცემთა დაცვის თემატიკა და პრობლემატიკა, როგორც მისი აკადემიური კვლევის, ისე პრაქტიკული გამოყენების თვალსაზრისით, წარმოადგენს სიახლეს ქართული სამართლისათვის. ასეთი რეალობის გათვალისწინებით კი უმნიშვნელოვანეს გამოწვევას წარმოადგენს საქართველოს სახელმწიფოს საჯარო სტრუქტურებში პერსონალური მონაცემების დამუშავებისა და დაცვის კუთხით არსებული მართვითი პრობლემების დანახვა და შეფასება, მით უფრო, რომ კომპიუტერული ტექნოლოგიებისა და ბიოტექნიკის განვითარებამ, სამყაროს გაციფრულების გარდაქმნითმა პროცესმა, სამეცნიერო პროგრესმა, საჭირო გახადა პერსონალურ მონაცემთა დაცვის მიმართულებით უფრო მეტი ყურადღების გამახვილება და დამატებითი საკანონმდებლო რეგულაციების შემოღება.

აღნიშნული ნაშრომი ეძღვნება საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მიმართულებით არსებულ რეალობასა და პრობლემატიკას, ამ მხრივ არსებულ საერთაშორისო გამოცდილებასა და მართვის ეფექტიანი მეთოდების შემუშავებას, ვინაიდან ამ კატეგორიის პერსონალური მონაცემების დაცვისათვის ძალზე მნიშვნელოვანია ქვეყანაში მართვის ეფექტიანი მეთოდების შემუშავება.

წარმოდგენილ სადისერტაციო ნაშრომში კვლევის ობიექტი გამოხატულია შემდეგი საკვლევი ამოცანებით:

- პერსონალური მონაცემების, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების განმარტება და განვითარების ისტორია;
- საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის ეროვნული სტანდარტები, ამ მხრივ არსებული საერთაშორისო გამოცდილება და შედარებითი ანალიზი;
- საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მხრივ არსებული პრობლემების ანალიზი/შეფასება;
- საქართველოში საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დაცვისათვის კონკრეტული რეკომენდაციების შემუშავება.

დასმული ამოცანების გადაწყვეტისას, გამოიყენებოდა სამეცნიერო სფეროში გავრცელებული და კარგად აპრობირებული რამდენიმე მეთოდი. ესენია: ისტორიულ-შედარებითი, ლოგიკური, სისტემურ-სტრუქტურული, ფუნქციური, კონტენტ-ანალიზი, სიტუაციური ანალიზი, სინთეზი, დოკუმენტების შესწავლა-შედარება და პროგნოზირება.

მონაცემების დამუშავებისა და კვლევების შედეგების საფუძველზე, შექმნილია თეორიულ-მეთოდოლოგიური საფუძველი, რომელიც ხელს შეუწყობს საქართველოს სახელმწიფოს საჯარო მმართველობის

ორგანიზაციებს, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის ეფექტიანი მექანიზმის შემუშავებაში.

ნაშრომში წარმოდგენილია საქართველოში პერსონალურ მონაცემთა დაცვაზე საზედამხედველო ინსტიტუტის შექმნის შემდეგ, საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მიმართულებით არსებული ძირითადი პრობლემები, განხილულია კონკრეტული მაგალითები და გამოვლენილია ამ მიმართულების განვითარების ხელშემშლელი კონკრეტული გარემოებები.

ნაშრომში მოცემულია საქართველოს სახელმწიფოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების ეფექტიანი მართვისა და დაცვისათვის მნიშვნელოვანი რეკომენდაციები.

Summary

Protection of personal data is one of the basic human rights in democratic societies and relevant institutions and regulations exist for its realization. Government of Georgia undertook significant steps toward protection of personal data in recent years. This was reflected in the establishment of personal data protection guarantees in legislation. In particular, Parliament of Georgia adopted Law of Georgia on Personal Data Protection in December 28, 2011, representing an important instrument for protection of citizens' personal data. In the beginning of 2013 Data Protection Authority – Office of the Personal Data Protection Inspector was established, which is mandated to monitor legitimacy of personal data processing in Georgia.

Besides, state of personal data protection in the country plays crucial importance to the Georgia's Euro-Atlantic integration process. Over the years, the EU has paid particular attention to this issue. By signing the Association Agreement with the EU on June 27, 2014, Georgia committed itself to implement European standards in personal data protection and to carry out institutional reforms in this field. It is noteworthy, that along with systematic reforms cooperation with the EU member states requires establishment of modern standards of personal data protection in public and private sectors in Georgia, sharing of best international practice, further development of this field and its modernization. In addition, in the process of implementation of modern standards, equal attention shall be payed to the issuance of publications, papers, programmes, methodic and practical guidelines based on scientific research as well as establishment of university disciplines and conduct of other educational activities (such as training courses, workshops, round tables, discussions, etc.) that are revised and adjusted to the contemporary state of play. On the one hand, this will provide valuable assistance to the interested individuals, and on the other, it will simplify and accelerate implementation of modern standards in Georgia.

Personal data protection constitutes protecting of an individual from infringement of his/her privacy, preventing its illegal use or threat to alteration. It shall be mentioned, that development of this field in Georgia has started only four years ago. Therefore, personal data protection and subsequent problems, both in terms of academic research and practical use, constitutes a new phenomenon for Georgian legislation. Taking into account such reality, identification and assessment of problems related to personal data processing and protection in public institutions constitutes an important challenge; paying more attention to personal data protection and establishment of additional legislative regulations became particularly important in the era of development of computer and biotechnology, digitalization processes and scientific progress.

This paper addresses processing of special categories of data (sensitive data) in public sector in Georgia and subsequent problems, international experience and establishment of effective management methods; development of such methods plays crucial importance to the protection of sensitive data in the country.

Following research objectives are set and solved in the presented dissertation work:

➢ Definition of personal data, including sensitive data, and its development;

➢ National standards of sensitive data processing in public sector, international experience in this area and comperative analysis;

➢ Analysis/assessment of problems related to the processing and protection of sensitive data in public sector in Georgia.

➢ Recommendations for the protection of sensitive data in public sector in Georgia.

Widely disseminated and well-tested methods in the scientific field were used in solving above mentioned tasks. These include but are not limited to: historical-comparative, logical, systematic - structural, functional, content analysis, situational analysis, synthesis, study and comparison of documents.

Based on the results of data processing and surveys, theoretical methodological basis is designed to facilitate the establishment of effective data management to protect sensitive data in public sector in Georgia.

This paper addresses basic problems in processing and protection of sensitive data in public sector, concrete examples are discussed and hindering circumstances to the protection of sensitive data are identified.

The paper includes recommendations for effective management and protection of sensitive data in public sector in Georgia.

მადლიერება

უპირველესად, მადლობა მინდა გადაუხადო საქართველოს ტექნიკური უნივერსიტეტის ბიზნესტექნოლოგიების ფაკულტეტის საჯარო მმართველობისა და ელექტრონული ბიზნესის დეპარტამენტის ხელმძღვანელს, პროფესორ გენადი იაშვილს, პროგრამის ხელმძღვანელს პროფესორ შოთა დოღონაძეს, პროგრამის პროფესორებს - გიორგი ბაღათურიას, ოთარ ბაღათურიას, ოთარ ქოჩორაძეს და თამარ რევაზიშვილს, დოქტორანტურაში სწავლის მთელი პერიოდის განმავლობაში, იმ შენიშვნების, მოსაზრებების და რეკომენდაციებისათვის, რომელიც უზრუნველყოფდა ნაშრომის სრულყოფას.

განსაკუთრებული ადგილი უკავია თემის ხელმძღვანელს, ასოცირებულ პროფესორ გიორგი გორაძეს. მადლობას ვუხდი მას, მაღალი პროფესიონალიზმისა და თავდაუზოგავი შრომისათვის, ჩემთვის დახარჯული დროისა და ენერგიისთვის, სამართლიანი კრიტიკისა და ერთგულებისთვის.

განსაკუთრებული მადლობა მინდა გადაუხადო ჩემს მეგობარს, ეკა გორდაძეს, ფასდაუდებელი მასალის მოწოდების, დახმარებისა და გვერდში დგომისთვის.

მადლობა, აგრეთვე, პერსონალურ მონაცემთა დაცვის ინსპექტორს მოწოდებული ინფორმაციისათვის.

და ბოლოს, გულითადი მადლობა ჩემს მშობლებს, ჯამბუ გუგავას და ნარგიზა მუსელიანს, რომელთა სიყვარულისა და მხარდაჭერის გარეშე, წინამდებარე ნაშრომი ვერ დაიწერებოდა.

სარჩევი

შესავალი

„ბოლო წლებში, მონაცემთა ავტომატური დამუშავება სულ უფრო ფართომასშტაბიან ხასიათს იძენს, რამაც ხელი შეუწყო გარკვეული პროცესების ოპტიმიზაციას, მომსახურების გამარტივებას, ბიუროკრატიული საფეხურების შემცირებას. მონაცემთა ბაზების, ელექტრონული ტრანზაქციებისა და თანამედროვე კომუნიკაციის სისტემების განვითარების პარალელურად, გაიოლდა საჯარო და კერძო ორგანიზაციების მიერ მონაცემთა დამუშავება და მათზე წვდომის შესაძლებლობა, რამაც, თავის მხრივ, გაზარდა პერსონალური მონაცემების არამართლზომიერი გამოყენების საფრთხე.

სტატისტიკის მიხედვით, ყოველდღიურად, მილიონნახევრამდე მონაცემი იკარგება ან იპარავენ მას,[1] რის შედეგადაც მონაცემთა დამმუშავებელი ორგანიზაციების გარდა, ზიანი ადგება მონაცემების მესაკუთრეს - მონაცემთა სუბიექტს, ვინაიდან მისი პირადი ცხოვრების ხელშეუხებლობა დგება რისკის ქვეშ. ისეთი პერსონალური მონაცემების გამჟღავნებამ, როგორიცაა მაგალითად, საკრედიტო ბარათის ნომერი, სოციალური ან პირადი ნომერი, შეიძლება, პირს მოუტანოს მატერიალური ზიანი. გარდა ამისა, მისი მონაცემები შეიძლება, გამოყენებული იქნეს დანაშაულებრივი მიზნებისთვისაც.“[2] [1]

საერთაშორისო ექსპერტების მოსაზრებით, მონაცემთა რაოდენობა საკმაოდ სწრაფი ტემპით იზრდება და ორმაგდება ყოველი მომდევნო თვრამეტი თვის განმავლობაში. „Computer Sciences Corporation”-ის მიერ მომზადებული ერთ-ერთი ბოლო ანგარიშის თანახმად, 2020 წლისთვის შექმნილი იქნება 44-ჯერ მეტი მონაცემი, ვიდრე შეიქმნა 2009 წელს. ხოლო

[1] Gemalto's 2015 Breach Level Index, [მოხსენიებულია:„ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, ქალდანი თ., სარიშვილი ნ., სტატია, „პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში, 2016 წელი].

[2] იხ. იგივე.

მსოფლიოში ერთ-ერთი კომპანიის, „IBM“-ის განმარტებით, დღესდღეობით არსებული მონაცემების 90 პროცენტი შექმნილია 2011-2012 წლებში.[3] [2]

საქართველოში მე-20 საუკუნის ბოლოდან დაიწყო და ყოველდღიურად იზრდება ინფორმაციის დამუშავებისას კომპიუტერული ტექნოლოგიების გამოყენების პრაქტიკა კერძო კომპანიებსა თუ საჯარო დაწესებულებებში. მონაცემების დამუშავება და ინფორმაციის მიმოცვლა ქვეყნის შიგნით თუ გარეთ ბევრად მარტივი გახდა. მონაცემთა ბაზაზე წვდომის შემთხვევაში, მარტივადაა შესაძლებელი პერსონალური ინფორმაციის მოძიება და შეცვლა, რაც ასევე ზრდის მონაცემთა არამიზნობრივად და ბოროტად გამოყენების რისკს. „ის ფაქტი, რომ მომხმარებლებს არ ესმით, როგორ იცავენ მათ მონაცემებს, მხოლოდ ერთი პრობლემაა, მეორე არის უსაფრთხოების სისტემის რღვევა, მონაცემებზე უკანონო წვდომის გახშირებული შემთხვევები.“[4] [3] პერსონალური მონაცემების დამუშავების კანონიერება და მაღალ სტანდარტებთან შესაბამისობა არსებითადაა დამოკიდებული მონაცემთა დამუშავების პრინციპებისა და საფუძვლების დაცვაზე. კანონში ასახული პრინციპები და საფუძვლები, „მათი მდგრადი ხასიათიდან გამომდინარე, ამკვიდრებენ მონაცემთა დამუშავების ზოგად წესს და განსაზღვრავენ მონაცემთა დამმუშავებლების ქმედების კანონიერებას.“[5] [4]

პერსონალური მონაცემები სწრაფად და დინამიკურად ვითარდება „როგორც ცალკე აღებული ქვეყნების ფარგლებში, ისე რეგიონალურ დონეზეც - განსაკუთრებით კი, ევროპის საბჭოსა და ევროპის თანამეგობრობის სამოქმედო სივრცეში.“[6] [5] პერსონალური მონაცემები

[3] Tereza M.Payton and Theodore Claypoole „Privacy in the age of big data“.

[4] „Analysis: Why an open and honest approach to personal data use could save you from losing a vital commodity“, see: http://www.cbronline.com/news/cybersecurity/data/data-protection-day-improve-your-privacy-policy-or-lose-your-data-4796165 [უკანასკნელად გადამოწმებულია 2017 წლის თებერვალში].

[5] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში.

[6] „ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო“, კონსტანტინე კორკელია, სტატიათა კრებული, 2011 წელი, თბილისი, გვ. 327.

განიხილება, როგორც ოცდამეერთე საუკუნის ნავთობი, რადგანაც წარმოადგენს მნიშვნელოვან ღირებულებას სამომხმარებლო ბაზარზე.[7] [6]

ასეთი გამოწვევების ფონზე, მნიშვნელოვანია, ყველა ქვეყანამ შექმნას ისეთი სტანდარტები და გარანტიები, რომლითაც დაიცავს მოქალაქეთა პერსონალურ მონაცემებს, მით უფრო, განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს, მათი არამართლზომიერი და არაკანონიერი გამოყენების საფრთხისაგან. საქართველოში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაზღვრავს მონაცემების დაცვის სტანდარტებს, ასევე, იმ სამართლებრივ საფუძვლებს, რომელთა დაცვაც აუცილებელია საქართველოს საჯარო სექტორში პერსონალური მონაცემების, მათ შორის, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას.

ნაშრომის აქტუალურობა

საქართველოში პერსონალური მონაცემების განვითარების ისტორია მხოლოდ ოთხ წელს ითვლის. მიუხედავად იმისა, რომ „2006 წლიდან საქართველო 1981 წლის „პერსონალური მონაცემების ავტომატური გზით დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის მონაწილეა, საქართველოში პერსონალურ მონაცემთა დაცვის მარეგულირებელი საკანონმდებლო ბაზა 2011 წლის ბოლომდე არ არსებობდა. შესაბამისად, არ არსებობდა პერსონალურ მონაცემთა დაცვაზე ზედამხედველობის განმახორციელებელი დამოუკიდებელი ორგანო.“[8]

2011 წელს პარლამენტმა მიიღო „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, რომელიც ძალაში შევიდა და ნაწილობრივ ამოქმედდა 2012 წლის პირველ მაისს. 2013 წლის პირველ ივლისს კი პერსონალურ მონაცემთა დაცვის ინსპექტორის დანიშვნით, ფუნქციონირება

[7] ”The economic value of personal data for online platforms, firms and consumers”, By: Liem C., Petropoulos G., 2016 y, see: http://www.pieria.co.uk/articles/the_economic_value_of_personal_data_for_online_platforms_firms_and_consumers [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[8] „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)”ქალდანი თ., სარიშვილი ნ., სტატია, „პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში”, 2016 წელი.

დაიწყო პერსონალურ მონაცემთა დამუშავების კანონიერებაზე ზედამხედველმა ორგანომ საქართველოში. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ამოქმედებამ, ასევე, დღის წესრიგში დააყენა სახელმწიფო სტრუქტურებში მონაცემთა დამუშავების წესებისა და მათი დაცვის სტანდარტების ინპლემენტაცია. პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის შექმნა და მისი პრაქტიკაში დანერგვა იყო საქართველოსა და ევროპის კავშირს შორის სავიზო დიალოგის ერთ-ერთ მნიშვნელოვანი ნაწილი.

მიუხედავად პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს განვითარების ოთხწლიანი ისტორიისა, მისი როლი, ფუნქციები და დანიშნულება, შეიძლება ითქვას, რომ კვლავაც სიახლეს წარმოადგენს, როგორც საქართველოს მოქალაქეთათვის, ასევე, მონაცემთა დამმუშავებელთათვის, მით უფრო, დედაქალაქის ფარგლებს გარეთ არსებული ორგანიზაციებისა და სუბიექტებისათვის. შესაბამისად, პერსონალურ მონაცემთა დაცვის თემატიკა და პრობლემატიკა, როგორც მისი აკადემიური კვლევის, ისე პრაქტიკული გამოყენების თვალსაზრისით, წარმოადგენს სიახლეს ქართული სამართლისათვის. ამ რეალობის გათვალისწინებით კი, უმნიშვნელოვანეს გამოწვევას წარმოადგენს, საზედამხედველო ორგანოს შექმნის შემდეგ, საქართველოს სახელმწიფოს საჯარო სტრუქტურებში პერსონალური მონაცემების დამუშავებისა და დაცვის კუთხით არსებული პრობლემების დანახვა და შეფასება.

წარმოდგენილ ნაშრომში შესწავლილია, როგორც საერთაშორისო და ეროვნული კანონმდებლობა, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვასთან დაკავშირებით, ასევე, გაანალიზებულია საჯარო სექტორში ამ კატეგორიის მონაცემების დამუშავებისა და დაცვის მხრივ არსებული პრაქტიკა, გამოვლენილია განვითარების დადებითი და ხელშემშლელი ტენდენციები.

ნაშრომს შეუძლია გარკვეული წვლილი შეიტანოს საქართველოს სახელმწიფოს საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დამუშავებისა და დაცვის ეფექტიანი სისტემის

ჩამოყალიბებაში, ვინაიდან ნაშრომში ასახული დასკვნები ეყრდნობა პრაქტიკაში გამოყენებულ გამოცდილებას. შესაბამისად, ნაშრომი სასარგებლო იქნება იმ პირთა წრისათვის, რომლებიც მუშაობენ საჯარო სამსახურში და რომელთა ფუნქცია-მოვალეობებს განეკუთვნება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავება და ამ კატეგორიის მონაცემების დაცვისათვის შესაბამისი ორგანიზაციულ-ტექნიკური ზომების გატარება, ასევე, ამ სფეროში მოღვაწე მეცნიერთათვის, სტუდენტებისა და პერსონალური მონაცემების საკითხით დაინტერესებული ყველა პირისათვის.

კვლევის ობიექტია - საქართველოში პერსონალურ მონაცემთა დაცვაზე საზედამხედველო ორგანოს შექმნის შემდეგ, საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მხრივ არსებული თეორია და პრაქტიკა.

კვლევის საგანია - საქართველოს აღმასრულებელი ხელისუფლების ორგანოებში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებული პრაქტიკის შესწავლა, ეროვნულ კანონმდებლობასთან მისი შესაბამისობის დადგენა და ამ მხრივ, პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილებების გაანალიზება.

კვლევის ამოცანებია:

- პერსონალური მონაცემების, მათ შორის, განსაკუთრებული კატეგორიის პერსონალური მონაცემების განმარტება და განვითარების ისტორია;
- საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის ეროვნული სტანდარტები, ამ მხრივ არსებული საერთაშორისო გამოცდილება და შედარებითი ანალიზი;
- საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მხრივ არსებული პრობლემების ანალიზი/შეფასება;

➢ საქართველოში საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დაცვისთვის კონკრეტული რეკომენდაციების შემუშავება.

კვლევის მიზანია - საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებული პრობლემების გამოვლენა, იდენტიფიცირება, შეფასება, დადებითი და უარყოფითი მხარეების გამოვლენა. ასევე, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვისათვის ეფექტიანი მექანიზმის შემუშავება და ისეთი შინაარსის რეკომენდაციების შეთავაზება, რომლებიც ხელს შეუწყობს საქართველოს სახელმწიფოში მოქმედ საჯარო ორგანიზაციებს არსებული ნაკლოვანებების დაძლევასა და ამ კატეგორიის მონაცემების ეფექტიანი მართვისათვის შესაბამისი სტრუქტურული, ორგანიზაციული და ტექნიკური ზომების გატარებაში.

კვლევის მეთოდოლოგია უშუალოდ გამომდინარეობს საკვლევი ობიექტის არსიდან და თავისებურებებიდან, მიზნიდან და გადასაწყვეტი ამოცანებიდან. ნაშრომის თეორიულ, მეთოდოლოგიურ და წყაროთმცოდნეობის მთავარ ბაზას წარმოადგენს პერსონალური მონაცემების დაცვის სფეროში ეროვნული და საერთაშორისო ნაშრომები, სახელმძღვანელოები და სტატიები. მნიშვნელოვანი ადგილი ეთმობა სხვადასხვა საკანონმდებლო დოკუმენტებს, საცნობარო მასალებსა და ინტერნეტრესურსებს.

კვლევის კონკრეტული მეთოდებიდან ნაშრომში გამოყენებულია სამეცნიერო სფეროში გავრცელებული და კარგად აპრობირებული რამდენიმე მეთოდი. ესენია: ისტორიულ-შედარებითი, ლოგიკური, სისტემურ-სტრუქტურული, ფუნქციური, კონტენტ-ანალიზი, სიტუაციური ანალიზი, სინთეზი, დოკუმენტების შესწავლა-შედარება და პროგნოზირება.

ჰიპოთეზა - სადისერტაციო ნაშრომში შევეცდებით დავამტკიცოთ, რომ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის მიზნით, საქართველოს საჯარო სექტორში

სტრუქტურული რეორგანიზაცია, ფუნქციური გაძლიერება, უახლესი ტექნოლოგიების დანერგვა და შესაბამისი საკანონმდებლო ცვლილებების განხორციელება მნიშვნელოვნად გააუმჯობესებს საჯარო სექტორში ამ კატეგორიის პერსონალური მონაცემების ეფექტიანად მართვის პროცესს.

ნაშრომის მეცნიერული სიახლე:

პერსონალურ მონაცემთა დაცვა წარმოადგენს ერთგვარ სიახლეს ქართულ რეალობაში. შესაბამისად, ამ ნაშრომის მეცნიერული სიახლე, უპირველეს ყოვლისა, მდგომარეობს იმაში, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორის, როგორც მონაცემთა დაცვაზე საზედამხედველო ორგანოს შექმნის შემდეგ, საჯარო დაწესებულებებში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებული მდგომარეობა სიღრმისეულად არ შესწავლილა და საკითხი მეცნიერულად არ დამუშავებულა (თუ არ ჩავთვლით მის ცალკეულ ასპექტებს, გამოქვეყნებულს სამეცნიერო სტატიების სახით). ამასთან, აღსანიშნავია, რომ გარდა ინსპექტორის ცალკეული რეკომენდაციებისა, უშუალოდ საჯარო სექტორისათვის მონაცემთა დაცვის სტანდარტები თითქმის არაა დადგენილი. მეცნიერულ სიახლედ შეიძლება ჩაითვალოს ისიც, რომ ამ ნაშრომის სახით, სამეცნიერო ბრუნვაში შემოდის აქამდე გამოუქვეყნებელი და ნაკლებად გამოკვლეული მასალები. გარდა აღნიშნულისა, წარმოდგენილ ნაშრომში:

- მრავალრიცხოვანი ლიტერატურული მონაცემების დამუშავების საფუძველზე, შექმნილია თეორიულ-მეთოდოლოგიური საფუძველი, რომელიც ხელს უწყობს საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვისა და მონაცემების მართვის ეფექტიანი სისტემის ფორმირებას;
- საზედამხედველო ორგანოს შექმნის შემდეგ, პირველადაა შესწავლილი განსაკუთრებული კატეგორიის მონაცემების მართვისა და დაცვის მხრივ საქართველოს საჯარო სექტორში არსებული ვითარება, თეორიული და პრაქტიკული ასპექტები. გაანალიზებულია ამ კატეგორიის მონაცემების მართვისთვის ეფექტიანი მექანიზმის აუცილებლობა

საქართველოს სახელმწიფოს საჯარო მმართველობის ორგანიზაციებში;

➢ წარმოდგენილია საერთაშორისო კანონმდებლობა და პრაქტიკა მსოფლიოს ზოგიერთი დიდი ქვეყნის (ამერიკის შეერთებული შტატების, დიდი ბრიტანეთის გაერთიანებული სამეფოს, იტალიის და სხვა) მაგალითზე, მოცემულია შედარებითი ანალიზი და განვითარების პერსპექტივები;

➢ წარმოდგენილია ფასეული და პრაგმატული ხასიათის დასკვნები, ასევე, რეკომენდაციები განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვისა და მართვის ეფექტიანი სისტემის შესაქმნელად.

წარმოდგენილი ნაშრომი მნიშვნელოვანია თეორიული და პრაქტიკული თვალსაზრისით.

თეორიული თვალსაზრისით - პერსონალური მონაცემების, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების განვითარების, ამ მხრივ, საქართველოს საჯარო სექტორში არსებული ვითარების თეორიული და პრაქტიკული ასპექტების ანალიზი საშუალებას გვაძლევს, ერთიანად წარმოვაჩინოთ და შევაფასოთ ამ დარგის განვითარების თეორიული ასპექტები, დადებითი და უარყოფითი ტენდენციები.

პრაქტიკული თვალსაზრისით - განსაკუთრებული კატეგორიის პერსონალური მონაცემების ეფექტიანად დაცვა მნიშვნელოვანია საქართველოს საჯარო სექტორის მონაცემთა დამმუშავებლებისათვის. შესაბამისად, ამ მხრივ, ნაშრომში მოცემული მეცნიერული კვლევის შედეგი მიმართულია, როგორც პრაქტიკული შედეგების მიღებაზე, ასევე, სიახლეების პრაქტიკაში დანერგვაზე.

სადისერტაციო ნაშრომი ხელს შეუწყობს საქართველოს სახელმწიფოს საჯარო სექტორის მონაცემთა დამმუშავებლებს, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების დროს, მიიღონ ეფექტიანი გადაწყვეტილებები და მისი დაცვისთვის გაატარონ აუცილებელი ორგანიზაციულ-ტექნიკური ზომები. შესაბამისად,

ნაშრომი დაეხმარება ამ საკითხით დაინტერესებულ ყველა პირს, საჯარო სექტორის მონაცემთა დამმუშავებლებს, გაიაზრონ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვისთვის აუცილებელი მნიშვნელოვანი თეორიული და პრაქტიკული ასპექტები, რათა მათი საქმიანობა, ამ მხრივ, იყოს სტანდარტების შესაბამისი და შედეგზე ორიენტირებული.

ნაშრომის სტრუქტურა:

ნაშრომი შედგება შესავალი ნაწილის, ლიტერატურის მიმოხილვის, საერთაშორისო და ადგილობრივი კანონმდებლობის ანალიზის, საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემთა დამუშავების პროცესში ინსპექტორის მანდატის წარმოჩენის, საჯარო მმართველობის ორგანიზაციებში განსაკუთრებული კატეგორიის მონაცემთა დაცვის მხრივ გამოვლენილი პრობლემების იდენტიფიცრების, განსჯის, დასკვნისა და შესაბამისი რეკომენდაციებისგან.

რეზიუმე - ქართულ და ინგლისურ ენებზე მოკლედ არის გადმოცემული შესრულებული სამუშაოს შინაარსი, ნაშრომის სიახლე, მიღწევები, შედეგები და ღირებულებები.

შესავალი ნაწილი - დასაბუთებულია საკვლევი თემატიკის აქტუალობა და მნიშვნელობა, განსაზღვრულია კვლევის საგანი, კვლევის ობიექტი, კვლევის მიზანი. დასახული მიზნის მისაღწევად, მოცემულია შესასრულებელი ამოცანები, კვლევის თეორიულ-მეთოდოლოგიური საფუძვლები, ასევე, დასაბუთებულია კვლევის სიახლე, მისი თეორიული და პრაქტიკული მნიშვნელობა.

ლიტერატურის მიმოხილვა - შესწავლილია ეროვნული და საერთაშორისო კანონმდებლობა, ლიტერატურა, საცნობარო მასალები, დოკუმენტური და კომპიუტერული წყაროები.

ნაშრომის პირველი თავი - „საერთაშორისო კანონმდებლობა პერსონალური მონაცემების დაცვის თაობაზე“ - შედგება ოთხი ქვეთავისაგან, სადაც მოცემულია მონაცემთა დაცვის შესახებ კანონის შექმნის ისტორია, მონაცემთა დამუშავებისთვის ევროპული სამართლით

დადგენილი საკვანძო პრინციპები და საფუძვლები, განხილულია ადამიანის უფლებათა ევროპული სასამართლოს ზოგიერთი მნიშვნელოვანი გადაწყვეტილება. ასევე, ცალკე ქვეთავად წარმოდგენილია სხვა ქვეყნების გამოცდილება, მათ შორის, ამერიკის შეერთებულ შტატებში, აზიის ქვეყნებსა და რუსეთში არსებული მდგომარეობა.

ნაშრომის მეორე თავი - „განსაკუთრებული კატეგორიის პერსონალური მონაცემები და ადგილობრივი კანონმდებლობა“ - შედგება ოთხი ქვეთავისაგან და მოცემულია პერსონალური მონაცემების, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების ცნება, მნიშვნელობა, ეროვნული კანონმდებლობით, მონაცემთა დამუშავებისთვის დადგენილი ისეთი ძირითადი პრინციპების განმარტება, როგორიცაა: სამართლიანობა და კანონიერება, მონაცემთა სუბიექტის ღირსების დაცვა, მონაცემების ნამდვილობა და სიზუსტე, მონაცემთა პროპორციულობა და ადეკვატურობა, მისი დამუშავებისათვის მკაფიოდ განსაზღვრული კანონიერი მიზნის არსებობა და მონაცემთა შენახვა მხოლოდ მიზნის მისაღწევად განსაზღვრული აუცილებელი ვადის განმავლობაში. ასევე, წარმოდგენილია ის სამართლებრივი საფუძვლები, რომელთა არსებობის შემთხვევაშიც, შესაძლებელია განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავება და განმარტებულია განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას, მონაცემთა დამმუშავებლის უფლება-მოვალეობები. ამასთან, ამავე თავში, განხილულია საზღვარგარეთის ზოგიერთი ქვეყნის (შვედეთი, ნორვეგია, დიდი ბრიტანეთი და იტალია) ეროვნული კანონის მიხედვით, განსაკუთრებული კატეგორიის პერსონალური მონაცემების განმარტება, მისი დამუშავებისთვის დადგენილი საფუძვლები და მოცემულია შედარებითი ანალიზი.

ნაშრომის მესამე თავი - „პერსონალურ მონაცემთა დამუშავების კანონიერებაზე ზედამხედველი ორგანო და მისი მანდატი“ - ითვალისწინებს ორ ქვეთავს და მასში განხილულია, ერთი მხრივ, საქართველოში პერსონალურ მონაცემთა დაცვის ინსპექტორის, ხოლო,

მეორე მხრივ, სხვა ქვეყნების საზედამხედველო ორგანოების მანდატი, სტრუქტურა, უფლება-მოვალეობები, საქმიანობის მიმართულებები, საჯარო სექტორზე მონაცემთა დაცვისა და ზედამხედველობის განხორციელების ფორმები და საჯარო უწყებების ანგარიშვალდებულება ამ ინსტიტუტის წინაშე.

ნაშრომის მეოთხე თავი - „საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას გამოვლენილი პრობლემები“- წარმოდგენილია სამ ქვეთავად. წლების მიხედვით, მოცემულია საქართველოს საჯარო სექტორში ამ კატეგორიის პერსონალური მონაცემების დამუშავებისა თუ დაცვის მხრივ არსებული სიტუაცია და გამოწვევები, დადებითი და უარყოფითი ტენდენციები. ნაშრომში განხილულია საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის ის მნიშვნელოვანი გადაწყვეტილებები, რომლებიც შეეხება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმებას საჯარო ორგანიზაციებში და გაანალიზებულია ამ მხრივ არსებული პრაქტიკა.

ნაშრომის ბოლოს, დასკვნის სახით, წარმოდგენილია საქართველოს სახელმწიფოს საჯარო სექტორში იდენტიფიცირებული პრობლემები და შემოთავაზებულია რეკომენდაციები.

ლიტერატურის მიმოხილვა

საქართველოში პერსონალური მონაცემების დაცვა განსაკუთრებით მნიშვნელოვანი გახდა მას შემდეგ, რაც 2012 წლის პირველ მაისს ამოქმედდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი და 2013 წელს სახელმწიფოში შეიქმნა პერსონალურ მონაცემთა დაცვაზე საზედამხედველო ინსტიტუტი, პერსონალურ მონაცემთა დაცვის ინსპექტორის სახით. შესაბამისად, ნაშრომის მთავარ გამოწვევას წარმოადგენს კანონის ამოქმედებისა და საზედამხედველო ორგანოს შექმნის შემდეგ, საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებული თეორიისა და პრაქტიკის შესწავლა, იმ პრობლემების წარმოჩენა, რომლებიც ხელს უშლის საჯარო სექტორში ამ კატეგორიის მონაცემების ეფექტიანად დაცვის პროცესს.

წარმოდგენილი ნაშრომი ეფუძნება მის დამუშავებამდე არსებულ ეროვნულ და საერთაშორისო კანონმდებლობას, ასევე, იმ სპეციალურ ლიტერატურას, წყაროებსა და ანგარიშებს, რომლებიც ძირითად საფუძველს წარმოადგენს წინამდებარე კვლევისათვის.

ნაშრომი იწყება პერსონალური მონაცემების დაცვის შესახებ კანონის შექმნის ისტორიის მიმოხილვით. საქართველოში პერსონალურ მონაცემთა განმარტება და მისი კატეგორიზაცია, სპეციალური კანონის მიღებამდე, ხორციელდებოდა ,,საქართველოს ზოგადი ადმინისტრაციული კოდექსის“ მეშვეობით, ასევე, მონაცემთა დაცვის შესახებ ცალკეული დებულებები არსებობდა სხვადასხვა სპეციალურ კანონებში. საქართველოს სახელმწიფოს ევროპისაკენ სწრაფვის პოლიტიკამ კი განაპირობა ამ საკითხის ცალკე საკანონმდებლო აქტით მოწესრიგების აუცილებლობა. საზღვარგარეთის ქვეყნებისა და საქართველოს პერსონალურ მონაცემთა დაცვის კანონის განვითარების ისტორია საფუძვლიანადაა წარმოდგენილი მარიამ ცაცანაშვილის სახელმძღვანელოში - „ინფორმაციული სამართალი“ [7]. ნაშრომში განხილულია ინფორმაციის ცნებისა და ინფორმაციული სივრცის ფილოსოფიური ასპექტები, თუმცა ცალკე თავად მოცემულია პერსონალური

მონაცემების სამართლებრივი რეგულირების საკითხი. პერსონალური მონაცემების ისტორიას, კატეგორიზაციასა და მათი განსაზღვრის საკანონმდებლო კრიტერიუმებს შეეხება ასევე, თამთა არჩუაძის სამაგისტრო ნაშრომი, „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას“[8].

აღსანიშნავია, რომ პირადი ცხოვრების პატივისცემასა და მონაცემთა დაცვას დიდი ყურადღება ექცევა ევროპის მასშტაბით. ევროპის საბჭოს ძირითადი საერთაშორისო სამართლებრივი დოკუმენტი, როგორიც არის **ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენცია** [9], პირადი ცხოვრების პატივისცემის უფლებას ადამიანის ერთ-ერთ ძირითად უფლებად აღიარებს, რომლის დაცვის უზრუნველყოფაც თითოეული სახელმწიფოს ვალდებულებაა. ხოლო, რაც შეეხება მონაცემთა დაცვას, ამ მხრივ, ევროპის კავშირისა და ევროპის საბჭოს ფარგლებში, მიღებულია არაერთი სავალდებულო სამართლებრივი თუ სარეკომენდაციო ხასიათის დოკუმენტი. შესაბამისად, ნაშრომში დეტალურადაა განხილული **პერსონალური მონაცემების ავტომატური დამუშავებისას, ფიზიკური პირების დაცვის შესახებ ევროპის საბჭოს 108-ე კონვენცია**[9] [10], რომელიც პირველი საერთაშორისო სავალდებულო დოკუმენტია და ითვალისწინებს მონაცემთა დაცვის სახელმძღვანელო პრინციპებს. კონვენცია ადგენს წევრ სახელმწიფოთა ვალდებულებებს, როგორც საჯარო, ისე კერძო სექტორის მიმართ, შეიმუშაონ და დანერგონ მონაცემთა დაცვის შიდა საკანონმდებლო რეგულაციები. იგი ადგენს მონაცემთა სუბიექტების უფლებებს და მონაცემთა დამმუშავებლების მოვალეობებს, ასევე, განსაზღვრავს მონაცემთა კანონიერად დამუშავების პრინციპებსა და საფუძვლებს. ნაშრომში განხილულია, ასევე, **108-ე კონვენციის დამატებითი ოქმი (ETS. 181)** [11], რომელიც განსაზღვრავს პერსონალურ მონაცემთა დამუშავებაზე კონტროლის განმახორციელებელი, დამოუკიდებელი საზედამხედველო ორგანოს შექმნას, მის აღჭურვას სათანადო უფლებამოსილებითა და

[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS. 180) adopted in Strasburg by the Council of Europe on 28 January 1981.

მანდატით. ოქმში მოცემულია სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის მონაცემთა გადაცემის წესები. ასევე, დეტალურად არის წარმოდგენილი **პერსონალური მონაცემების დაცვისა და მონაცემთა გადაცემის შესახებ ევროპის კავშირის დირექტივა 95/46/EC**[10] [12], რომელიც ევროპის საბჭოს 108-ე კონვენციის მსგავსად, მონაცემთა დაცვის თვალსაზრისით, ერთ-ერთი ძირითადი დოკუმენტია და ითვალისწინებს მონაცემთა სუბიექტების უფლებებსა და მონაცემთა დამმუშავებლების მოვალეობებს, ასევე, განსაზღვრავს მონაცემთა კანონიერად დამუშავების საფუძვლებსა და პრინციპებს. დირექტივა, კონვენციისაგან განსხვავებით, ვრცელდება როგორც ავტომატური, ისე არაავტომატური საშუალებებით მონაცემთა დამუშავებაზე. დირექტივა ავალდებულებს წევრ სახელმწიფოებს, შექმნან დამოუკიდებელი საზედამხედველო ორგანო, რომელიც გააკონტროლებს ქვეყანაში პერსონალური მონაცემების დამუშავების კანონიერებას. დირექტივაში დეტალურად არის გაწერილი პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული საკითხები, მათ შორის, მონაცემთა დამუშავების კანონიერი საფუძვლები და პრინციპები, მონაცემთა სუბიექტის უფლებები, დამმუშავებლის ვალდებულებები, მონაცემთა უსაფრთხოება და სხვა. **ევროპის საბჭოს მინისტრთა კომიტეტის რეკომენდაცია R (87) 15**[11] **[13],** რომელზეც საუბარია ნაშრომში, შეეხება პოლიციის მიზნებისათვის მონაცემთა დამუშავებას და ითვალისწინებს ძირითად სახელმძღვანელო პრინციპებს, პოლიციის სექტორში პერსონალურ მონაცემთა დაცვის შესახებ. რეკომენდაციაში მოცემულია მონაცემთა შეგროვების, შენახვის, გამოყენების და გადაცემის, მონაცემთა უსაფრთხოების სტანდარტები, ასევე, მონაცემთა სუბიექტის უფლებები, ჰქონდეს წვდომა მის შესახებ არსებულ მონაცემებთან. რეკომენდაცია ითვალისწინებს დამოუკიდებელი სახელმწიფო ორგანოს ჩამოყალიბებას,

[10] 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.

[11] Recommendation No. R(87)15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector, adopted by the Committee of Ministers on 17 September 1987.

რომელიც პასუხისმგებელი იქნება ქვეყანაში იმ პრინციპების დაცვაზე, რომელიც მოცემულია ამ რეკომენდაციაში. **ევროპის კავშირის 2008 წლის 27 ნოემბრის ჩარჩო გადაწყვეტილება (2008/977/ JHA)**[12] [14] კი შეეხება პოლიციის სექტორში პერსონალურ მონაცემთა დამუშავებას. იგი ადგენს სამართალდამცავი ორგანოების მიერ პერსონალურ მონაცემთა დამუშავების პრინციპებს, განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძვლებს, მონაცემთა სუბიექტის უფლებებს და სხვა. ჩარჩო გადაწყვეტილების თანახმად, სახელმწიფომ უნდა უზრუნველყოს სამართალდამცავი ორგანოების მიერ საჯარო წესრიგის შენარჩუნების, დანაშაულის პრევენციისა და დევნის მიზნით, მონაცემთა დამუშავებაზე კონტროლის განმახორციელებელი, დამოუკიდებელი საზედამხედველო ორგანოს შექმნა, რომელიც აღჭურვილი იქნება შემდეგი უფლებამოსილებით:

➢ **საგამოძიებო უფლებამოსილება** - ორგანოს უნდა ჰქონდეს უფლება, განახორციელოს შეუზღუდავი წვდომა მონაცემთა დამუშავებასთან დაკავშირებულ ინფორმაციაზე და შეაგროვოს ასეთი ინფორმაცია, საზედამხედველო ფუნქციების ეფექტურად წარმოების მიზნით;

➢ **ინტერვენციის ეფექტური უფლებამოსილება** - საზედამხედველო ორგანოს უნდა ჰქონდეს საშუალება, გამოხატოს საკუთარი მოსაზრება მონაცემთა დამუშავების განხორციელებამდე, მათ შორის, გამოსცეს მონაცემთა დაბლოკვის, მონაცემთა განადგურების, წაშლის ბრძანება, ასევე, დროებით ან მუდმივად აკრძალოს მონაცემთა დამუშავება;

➢ **სამართალწარმოების პროცესში ჩართვის უფლებამოსილება** - პერსონალურ მონაცემთა დაცვის კანონმდებლობის დარღვევის შემთხვევებში, საზედამხედველო ორგანოს უნდა ჰქონდეს სასამართლო ხელისუფლებისადმი მიმართვის უფლებამოსილება. თანამედროვე ციფრული გამოწვევების გათვალისწინებით, მონაცემთა დამუშავების

[12] Framework Decision of the Council of European Union 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

საკითხების უფრო მეტი აქტუალობისა და კიბერუსაფრთხეების ზრდის ფონზე, მიღებულ იქნა გადაწყვეტილება №108, კონვენციის მოდერნიზების შესახებ, რათა ციფრულ სფეროში უფრო მეტად იქნეს დაცული პირადი ცხოვრების ხელშეუხებლობა და გაძლიერდეს კონვენციის მაკონტროლებელი მექანიზმები.

ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით დადგენილი სტანდარტები, თარგმანის სახით, გამოცემულია კახაბერ გოშაძის სახელმძღვანელოში „მონაცემთა დაცვის ევროპული სამართალი“ [15]. აღნიშნული სახელმძღვანელო საკმაოდ დეტალურად განიხილავს ევროპის მასშტაბით მოქმედ იმ სამართლებრივ თუ სარეკომენდაციო სახის დოკუმენტებს, რომლებიც ეხება პერსონალური მონაცემების დაცვას. სახელმძღვანელოში მოცემულია ადამიანის უფლებათა ევროპული სასამართლოსა და მართლმსაჯულების ევროპული კავშირის სასამართლოს მიერ გამოტანილი გადაწყვეტილებები, რომლებიც ეხება პირადი ცხოვრების, მათ შორის, პერსონალური მონაცემების დაცვას.

პერსონალურ მონაცემთა დაცვის მიმართულებით, უმნიშვნელოვანეს დოკუმენტს წარმოადგენს „პერსონალურ მონაცემთა დამუშავებისას ფიზიკური პირების დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის, ასევე, №95/46/EC დირექტივის გაუქმების შესახებ“ ევროპის პარლამენტისა და ევროპული საბჭოს 2016 წლის 27 აპრილის №2016/679 რეგულაცია, რომელიც ევროკავშირის ფარგლებში, სხვადასხვა დონეზე მიმდინარე განხილვის შედეგად შეთანხმდა და 2016 წლის 24 მაისიდან შევიდა ძალაში. სწორედ, ეს რეგულაცია ჩაანაცვლებს არსებულ №95-46-EC დირექტივას და ექნება პირდაპირი მოქმედება ევროკავშირის წევრ სახელმწიფოებში. რეგულაცია ძალაში შევა 2018 წლის 25 მაისიდან.[13] [16]

ნაშრომში წარმოდგენილია ევროკავშირის ახალი რეგულაციის მიხედვით მონაცემთა დაცვის კუთხით არსებული მნიშვნელოვანი სიახლეები, როგორიცაა მონაცემთა სუბიექტის თანხმობის სრულყოფა,

[13] Regulation 2016/679 of the European Parlament and of the Council 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), 27 April 2016.

საზედამხედველო ორგანოს ინფორმირების ვალდებულება, მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების ვალდებულება, მონაცემთა დაცვის ოფიცრის დანიშვნის სავალდებულოობა და სხვა.

მნიშვნელოვანი ცვლილებებია გათვალისწინებული ევროპის საბჭოს განახლებული 108-ე კონვენციის სამუშაო ვერსიაშიც, რომლითაც პერსონალურ მონაცემთა დაცვის მარეგულირებელი ნორმების მოქმედების სფეროდან ერთადერთი დაშვებული გამონაკლისი მონაცემთა აშკარად გამოხატული პირადი და საოჯახო მიზნით დამუშავებაა. კონვენციით, გარკვეული შეზღუდვები შეიძლება დაწესდეს მხოლოდ მაშინ, თუ ეს აუცილებელი და პროპორციული ღონისძიებაა, დემოკრატიულ საზოგადოებაში ეროვნული უსაფრთხოების, საზოგადოებრივი უსაფრთხოების, თავდაცვის, ქვეყნის მნიშვნელოვანი ეკონომიკური და ფინანსური ინტერესების დასაცავად, სასამართლოს დამოუკიდებლობისა და მიუკერძოებლობის დასაცავად, სისხლის სამართლის დანაშაულის გამოძიებისა და ბრალდების, სისხლის სამართლის სასჯელის აღსრულების ან სხვა მიზნებიდან გამომდინარე, მონაცემთა სუბიექტის დასაცავად ან სხვათა უფლებებისა და ძირითადი თავისუფლებების დასაცავად.

ევროკავშირის ახალ რეგულაციას, ევროპის საბჭოს მოდერნიზებულ კონვენციას, პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტებსა და მის საქართველოში დანერგვას განიხილავენ ქალდანი თ. და სარიშვილი ნ., სტატიაში - „პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში“ და ასევე, ცერცვაძე მ. სტატიით - „პიროვნების დაცვის საერთო ევროპული სამართლებრივი სტანდარტები პერსონალური მონაცემების ავტომატიზებული დამუშავებისას“ [17]. აღნიშნული სტატია ეძღვნება ევროპის საბჭოს მიერ შემუშავებულ ადამიანის უფლებათა დაცვის სტანდარტებს პერსონალური მონაცემების ავტომატიზებული დამუშავებისას. ავტორი განიხილავს კონკრეტულ სფეროებში კონვენციის დებულებების ასამოქმედებლად ევროპის საბჭოს მინისტრთა კომიტეტის მიერ მიღებულ რეკომენდაციებს, რომელთა

შესრულება ევალებათ კონვენციის მონაწილე სახელმწიფოთა მთავრობებს, ევროპის საბჭოს წესდების მე-15 b მუხლის შესაბამისად.

ნაშრომში წარმოდგენილია ასევე სხვა ქვეყნების გამოცდილება, მათ შორის, ამერიკის შეერთებულ შტატებში, აზიის ქვეყნებსა და რუსეთში არსებული ვითარება, Daniel J. Solove & Paul M. Schwartz „Privacy law Fundamentals“ [18] სახელმძღვანელოზე დაყრდნობით, რომლის თანახმადაც, სახელმწიფოთა უმრავლესობას არ აქვს პირადი ცხოვრების დაცვის შესახებ ფედერალური კანონის მსგავსი აქტები. კალიფორნიას, მასაჩუსეტს, მინესოტას, ნიუ-იორკსა და ვისკონსინიას კი გააჩნია მსგავსი კანონმდებლობა. ამ კანონებს აქვთ სპეციალურად დაწესებულებებისათვის გამიზნული დამატებები. სახელმწიფოები ასეთი ფართო ინფორმაციული პრაქტიკული სამართლის გარეშე, ხშირად, ყურადღებას ამახვილებენ მთავრობის მიერ პერსონალური მონაცემების შემცველი ინფორმაციის გამოყენებაზე.

რაც შეეხება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის ეროვნულ სტანდარტებს, იმის გათვალისწინებით, რომ საზედამხედველო ინსტიტუტის შექმნის შემდეგ, საქართველოს სახელმწიფოს საჯარო სექტორში არსებული მდგომარეობა მეცნიერულ დონეზე არ არის შესწავლილი, ნაშრომი, ძირითადად, ეყრდნობა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონს, როგორც საქართველოში განსაკუთრებული კატეგორიის მონაცემების დაცვის ეროვნული სტანდარტების განმსაზღვრელ ერთადერთ ძირითად ნორმატიულ აქტს [19], ასევე, „პერსონალური მონაცემების დაცვისა და დამუშავების სახელმძღვანელოს“ [20], რომელიც გამოსცა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა 2013 წელს და შეიძლება ითქვას, რომ წარმოადგენს პირველ განმარტებით სახელმძღვანელოს. პერსონალური მონაცემების დაცვისა და პირადი ხელშეუხებლობის საკითხებს მიმოიხილავს ასევე, ნ. საგინაშვილი თავის სამეცნიერო სტატიაში [21], სადაც მითითებულია თუ რატომ გახდა მნიშვნელოვანი პერსონალური მონაცემების დაცვის ცალკე უფლებად გამოყოფა, რამ გამოიწვია მისი

პირადი ცხოვრების ხელშეუხებლობის კონცეფციიდან გამოყოფა და ცალკე რეგულირება. სტატიაში, პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის კონცეფციების მნიშვნელობის, აქტუალობისა და ისტორიული განვითარების ფონზე, წარმოდგენილია პერსონალური მონაცემების დეფინიცია, საქართველოს კანონის, ევროკავშირისა და ევროპის საბჭოს მიდგომები.

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ამოქმედების შემდეგ, საქართველოში, კანონის ინპლემენტაციის მიზნით, შეიქმნა არასახარბიელო მდგომარეობა. კერძოდ, საქართველოს სამინისტროებში იყო პერსონალურ მონაცემთა დაცვის საკითხისადმი დაბალი ცნობადობა, კანონის ინპლემენტაციისადმი გაუაზრებელი მიდგომა, კონკრეტული გეგმის და ხედვის უქონლობა, არ იდგმებოდა არანაირი ქმედითი ნაბიჯები, არ არსებობდა არანაირი წინაპირობა ვარაუდისთვის, რომ საქართველოს სამინისტროებში არსებობს მკაფიო ნება და სერიოზული განზრახვა პერსონალური მონაცემების დაცვის საკითხის მოწესრიგებისა [22].

რაც შეეხება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის საერთაშორისო დოკუმენტებთან შესაბამისობას, ინოვაციებისა და რეფორმების ცენტრის ჩატარებულ კვლევაში, რომელიც „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვის“ [23] სახით გამოქვეყნდა 2015 წელს, ნათქვამია, რომ მიუხედევად ნაკლოვანებებისა, რომელიც კანონს გააჩნია, შეიძლება ითქვას, რომ საბოლოო ჯამში, ის თანხვედრაშია თანამედროვე ევროპულ სტანდარტებთან. ამასთან, აღსანიშნავია, რომ კანონი ძალაში შევიდა მის შესასრულებლად საკმაოდ არასახარბიელო პერიოდსა და გარემოში: საზოგადოების დაბალი ცნობადობის გამო, მსგავსი უფლებებისა და მისი მნიშვნელობის შესახებ, ფაქტობრივად, არ არსებობდა მოთხოვნა პერსონალურ მონაცემთა დაცვაზე, არ არსებობდნენ საჯარო მოხელეები და სამართლის სპეციალისტები, რომლებსაც ამ საკითხების სიღრმისეული ცოდნა ექნებოდათ; კარგად ჩამოყალიბებული ელექტრონული

მმართველობა შეიქმნა იმ პერიოდში, როდესაც საჯარო სექტორში პერსონალურ მონაცემთა დაცვის წესები არ არსებობდა; ხელმძღვანელებს არ ჰქონდათ მზაობა, გამოეყოთ კანონის შესრულებისთვის საჭირო ფინანსური რესურსები; არ არსებობდნენ პერსონალურ მონაცემთა დაცვაზე მომუშავე აქტივისტები და ადვოკატები; არ იყო შექმნილი პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო.

2013 წელს, პერსონალურ მონაცემთა დაცვის საზედამხედველო ინსტიტუტის შექმნის შემდეგ კი საქართველოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებულ მდგომარეობას აღწერს ინსპექტორი 2013-2014 [23], 2014 [24], 2015 [25] და 2016 [26] წლის ანგარიშებში, სადაც სხვა თემებთან ერთად, საუბარია განსაკუთრებული კატეგორიის მონაცემთა დამუშავებასთან დაკავშირებულ დარღვევებზე.

ანგარიშში, კონკრეტული მაგალითების სახით, განიხილულია ზოგიერთ საჯარო უწყებაში არსებული პრობლემები და შემოწმების საფუძველზე მიღებული კონკრეტული გადაწყვეტილებები. ამ მიმართულებით, ნაშრომში, ასევე, გაანალიზებულია პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2017 წლის 16 მაისის №PDP 5 17 00001756 წერილით მოწოდებული საჯარო ინფორმაცია, კერძოდ, საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების შედეგად, ინსპექტორის მიერ გამოტანილი გადაწყვეტილებები (28 გადაწყვეტილება). [27]

ინსპექტორის ანგარიშებისა და აპარტიდან მოწოდებული ინფორმაციის თანახმად, საჯარო სექტორში ხშირ და ყოველწლიურად განმეორებად გამოწვევას წარმოადგენს ამ კატეგორიის მონაცემთა პრინციპების დარღვევითა და სამართლებრივი საფუძვლის გარეშე დამუშავება. წარმოდგენილ ნაშრომში დასმული პრობლემაც სწორედ არსებულმა პრაქტიკამ განაპირობა. კერძოდ, იმ გარემოებამ, რომ საჯარო სექტორში საჭიროა გარკვეული სახის სტრუქტურული, ორგანიზაციული და

სამართლებრივი ხასიათის ცვლილებების განხორციელება, რასაც საჯარო სექტორში მონაცემთა დამმუშავებლები რატომღაც გვერდს უვლიან.

გარდა აღნიშნულისა, ნაშრომში ასევე, გამოყენებულია ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა, ინტერნეტრესურსები და ისეთი ლიტერატურა, როგორიცაა : „The Right to Privacy“, „Privacy vs Security“, „Hhe EU General Data Protection Regulation“, „Controlling knowledge: Freedom of Information and Privacy Protection in a Networked World“. აგრეთვე, ცალკეული კატეგორიის მონაცემთა დამუშავებასთან დაკავშირებული ნაშრომები -„Working Document on Genetic Data“, „Advice paper on special categories of data (sensitive data)“ და სხვა.

თავი I. საერთაშორისო კანონმდებლობა პერსონალური მონაცემების დაცვის თაობაზე

ადამიანის პირადი უფლებების, მათ შორის პერსონალური მონაცემების დაცვისა და უზრუნველყოფის საკითხები, დიდი ხანია საერთაშორისო სამართლებრივი რეგულირების უმნიშვნელოვანესი ობიექტია. „პრინციპი, რომ ადამიანს აქვს სრული უფლება, დაიცვას პირადი მონაცემები, არსებობს საერთო სამართალის ჩამოყალიბებიდან მოყოლებული, მაგრამ დროდადრო, საჭირო ხდება ამ უფლების დაცვის გზების ჩამოყალიბება და განახლება“ „....ადრეულ საუკუნეებში, სამართალი აწესებდა რეგულაციებს პირადი ცხოვრებასა და საკუთრებაში ფიზიკური ჩარევისათვის, „vie et armis“ პრინციპის მიხედვით. შემდგომ, „ცხოვრების უფლების“ დაცვისათვის საჭირო გახდა სხვადასხვა ფორმების შემუშავება.“[14] [28]

აღსანიშნავია, რომ პერსონალური მონაცემების დაცვის მხრივ, „საერთაშორისო აქტებით დგინდება და მყარდება გარკვეული უნივერსალური თუ რეგიონულ-კონტინენტური, მაგალითად ევროპული, სამართლებრივი სტანდარტები. სტანდარტი (ინგლ. *Standart* – ნორმა, ნიმუში, საზომი), ფართო გაგებით, ნიშნავს ნორმატიულ-ტექნიკურ დოკუმენტს, რომელიც ადგენს ნორმების, წესების, მოთხოვნების კომპლექსს სტანდარტიზაციის ობიექტისათვის და რომელსაც ამტკიცებს კომპეტენტური ორგანო.“[15] მნიშვნელოვანია, რომ ევროპის საბჭო და ევროპის კავშირის კანონმდებლობა პერსონალურ მონაცემთა დაცვის სფეროში მთელ რიგ რეგულაციებსა და სტანდარტებს აწესებს. მათ შორისაა ადამიანის უფლებათა ევროპული კონვენცია, დირექტივა 95/46/EC „პერსონალურ მონაცემთა დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის შესახებ“, ასევე, ევროპის საბჭოს

[14] Hhe Right To Privacy, Samuel D. Warren & Luis D. Brandies, Published in the 2015 Hardcover Edition By Quid Pro Books.

[15] ცერცვაძე მ., „პიროვნების დაცვის საერთოევროპული სამართლებრივი სტანდარტები პერსონალური მონაცემების ავტომატიზებული დამუშავებისას“,საქართველოს ელექტრონული სამეცნიერო ჟურნალი იურისპრუდენცია №1, 2002 წელი, გვ. 27-36.

108-ე კონვენცია, ევროპის ადამიანის უფლებათა სასამართლოს გადაწყვეტილებები და განმარტებები.

1.1. პერსონალურ მონაცემთა დაცვის ტერმინოლოგია და ისტორია

„მეორე მსოფლიო ომის შემდგომ, ნელ-ნელა დაიწყო რა ინფორმაციული ერა, სულ უფრო რთულდება პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვა“.[16] [29] რაც შეეხება პირად, ანუ კერძო ცხოვრებას, „იგი საკმაოდ ფართო სფეროა. სწორედ აღნიშნულის გათვალისწინებით განასხვავებენ კერძო ცხოვრების ოთხ სფეროს: 1. ინფორმაციულ კერძო ცხოვრებას (პერსონალური მონაცემების დაცვა); 2. სხეულებრივ პირად ცხოვრებას (სხეულის ხელშეუხებლობისა და ინტიმური სფეროს დაცვა); 3. საკომუნიკაციო კერძო ცხოვრებას (საფოსტო და სატელეგრაფო საიდუმლოება, კომუნიკაციის საშუალებათა უსაფრთხოება); 4. ტერიტორიის ხელშეუხებლობას (საცხოვრებლის, სამუშაო ადგილის და სხვა)“[17]. [30] ამასთან, ადამიანის „პირადი სფერო შეიძლება გამოვლინდეს პერსონალური მონაცემების დაცვაში“.[18][31]

მე-20 საუკუნეში პირადი ცხოვრების ხელშეუხებლობა, „რომელის ერთი ნაწილია პერსონალური მონაცემების დაცვა, ცნობილი კონცეფციის, „ფრაივერსის“ (Privacy -პირადი ცხოვრების სამართლის სტატუსით აღჭურვა) კვლევის განსაკუთრებული ობიექტი გახდა.“ ... „ამ კონცეფციას საფუძვლად დაედო ბოსტონის გაზეთებში ერთ-ერთი ქორწილის წვრილმანი დეტალების პუბლიკაცია. ახალდაქორწინებულთა განრისხებული მამა, ბოსტონელი იურისტი სამუელ უერონი და მისი კოლეგა ლუის ბრანდეისი დაფიქრდნენ პირად ცხოვრებაში პრესის ჩარევის დასაშვებ საზღვრებზე და შექმნეს ესე „პირად ცხოვრებაში ჩაურევლობის

---

[16] Prof.dr. Lokke Moerel, Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof, 2014, ხელმისაწვდომია: http://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[17] ბიჭია მ., „პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით“, გამომცემლობა „ბონა-კაუზა“, თბილისი, 2012 წელი, გვ. 60.

[18] Иванский В., „Правовая зашита информации о частной жизни граждан“, 1999, ст. 141.

უფლება“ (1980 წ), რომელიც ყველაზე გავლენიან სტატიად იქცა პირადი ცხოვრების სამართლებრივ საკითხებზე“. ....„მე-20 საუკუნის შუა წლებიდან, საკმარისი პრეცედენტული ბაზა შეიქმნა „ფრაივერსის“ ცნების სტრუქტურიზაციისა და თეორიული განზოგადებისთვის.“ [19]

თუ გადავხედავთ პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან დაკავშირებულ ისტორიას, „პირველი კანონი, ამოქმედდა ჰესსეში, გერმანიაში. ამ პროცესს მოჰყვა კანონთა მიღება შვედეთში 1973 წელს, ამერიკის შეერთებულ შტატებში - 1974 წელს, გერმანიაში - 1977 წელს, საფრანგეთსა და ნორვეგიაში - 1978 წელს. დღესდღეობით, ყველა დასავლეთ ევროპულ ქვეყანას გააჩნია საკუთარი რეგულირება პერსონალურ მონაცემთა დაცვასთან დაკავშირებით“[20]. [32] „2016 წლის მონაცემებით კი, „111 ქვეყანას აქვს შემუშავებული პერსონალური მონაცემების დაცვის მარეგულირებელი ეროვნული კანონმდებლობა, საიდანაც 54 ევროპული ქვეყანაა.“[21]

პერსონალურ მონაცემებთან დაკავშირებული საკითხების განხილვამდე, „მართებული იქნება ჩამოვაყალიბოთ, თუ რა არის პერსონალური მონაცემი“.[22] [33] ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით, „პერსონალური მონაცემი“ აღნიშნავს ნებისმიერ ინფორმაციას, რომელიც შეეხება განსაზღვრულ ან განმსაზღვრელ პირს („ინფორმაციის სუბიექტს“), ანუ ინფორმაციას იმ პირის თაობაზე, რომლის ვინაობაც ცნობილია ან შეიძლება დადგინდეს, დამატებითი მონაცემების თანახმად. შესაბამისად, მონაცემთა დაცვის ევროპული სამართლისათვის აუცილებლობას არ წარმოადგენს მონაცემთა სუბიექტის იდენტიფიცირება მაღალი სიზუსტით, საკმრისია, პირის მიმართ ინფორმაცია შეიცავდეს პირდაპირი ან არაპირდაპირი იდენტიფიკაციის ელემენტებს, თუმცა

[19] ცაცანაშვილი მ., „ინფორმაციული სამართალი“, თბილისი, 2004 წელი, გვ. 101-102.

[20] Karanja S., Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Netherlands, Martinus Nijhoff Publishers, 2008. p. 123. [მოხსენიებულია თამთა არჩუაძის სამაგისტრო ნაშრომში, „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე დამუშავებისას“].

[21] „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, ქალდანი თ., სარიშვილი ნ., 2016 წელი.

[22] თემიდა, სამეცნიერო პრაქტიკული ჟურნალი, უგრეხელიძე ნ., სტატია „პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზა საქართველოში“, 2011 წელი, №5(7), გვ. 162.

კანონმდებლობა ცალკე გამოყოფს პერსონალური მონაცემების იმ კატეგორიას, რომელთა დამუშავება, მათი ბუნებიდან გამომდინარე, შესაძლოა, შეიცავდეს რისკებს მონაცემთა სუბიექტებისათვის და შესაბამისად, საჭიროებდეს გაძლიერებულ დაცვას. ასეთ მონაცემებს უწოდებენ მგრძნობიარე ანუ „სენსიტიურ“ პერსონალურ მონაცემებს. შეიძლება ითქვას, რომ „მგრძნობიარობის“ კრიტერიუმი სუბიექტივიზმს უკავშირდება, მაგრამ განსაკუთრებულად „სენსიტიურად“ უნდა მივიჩნიოთ ისეთი ინფორმაცია, რომლის გამოქვეყნებას საჩოთიროდ მიიჩნევდა ყველა ჩვეულებრივი მგრძნობიარე ადამიანი.“[23] ამ კატეგორიის მონაცემების დამუშავება კი ევროპული კანონმდებლობით, ნებადართულია მხოლოდ შესაბამისი დაცვის სპეციალური ზომების არსებობისას.

ევროპის საჭოს 108-ე კონვენციის მე-6 მუხლი „სენსიტიური“ ანუ „მგრძნობიარე“ მონაცემების სპეციალურ კატეგორიებად განიხილავს პირის რასობრივ წარმომავლობას, პოლიტიკურ, რელიგიურ ან სხვა მრწამსს, ჯანმრთელობის მდგომარეობასა თუ სექსუალურ ცხოვრებასთან დაკავშირებულ პერსონალური მონაცემებს და განმარტავს, რომ ეს მონაცემები არ ექვემდებარება ავტომატიზებულ დამუშავებას, გარდა იმ შემთხვევისა, როცა ადგილობრივი კანონმდებლობა უზრუნველყოფს მათი დაცვის შესაბამის გარანტიებს. იგივე დათქმა არსებობს სისხლის სამართლებრივ პასუხისმგებლობასთან დაკავშირებულ მონაცემებთან დაკავშირებითაც.

მონაცემთა დაცვის დირექტივა კი დამატებით, „სავაჭრო გაერთიანების წევრობას“ განსაზღვრავს, როგორც სენსიტიურ მონაცემს, რამდენადაც ეს ინფორმაცია შესაძლებელია იყოს პოლიტიკური შეხედულების ან ასოცირების მკაფიო მაჩვენებელი. თუმცა „სენსიტიური მონაცემების წრე უფრო ფართოა, ვიდრე ევროდირექტივაშია მოცემული.“[24] ამასთან, მნიშვნელოვანია ის გარემოებაც, რომ „დირექტივის მე-8 მუხლის

[23] ბიჭია მ., „პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით“, თბილისი, 2012 წელი, გვ76.

[24] ინოვაციებისა და რეფორმების ცენტრი, „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, გვ.10.

მე-7 პუნქტი ავალდებულებს წევრ ქვეყნებს, განსაზღვრონ ის პირობები, თუ რა შემთხვევაში ექვემდებარება დამუშავებას ეროვნული საიდენტიფიკაციო ნომერი ან ნებისმიერი სხვა იდენტიფიკატორი“.[25]

1.2. მონაცემთა დამუშავების ევროპული სამართლის საკვანძო პრინციპები

მონაცემთა დამუშავების საკვანძო პრინციპების არსი მოცემულია პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ ევროპის საბჭოს 108-ე კონვენციის მე-5 მუხლში და პერსონალური მონაცემების ავტომატიზებული დამუშავებისას, მოითხოვს, რომ მონაცემები: ა) მიღებული და დამუშავებული უნდა იყოს პირდაპირი და კანონიერი გზით; ბ) შენახული უნდა იქნეს ზუსტად განსაზღვრული კანონიერი მიზნებისთვის და არ იყოს გამოყენებული მათთან შეუთავსებელი გზით; გ) უნდა იყოს ადეკვატური და არ აღემატებოდეს იმ მიზნებს, რომლებისთვისაც ისინი ინახება; დ) უნდა იყოს ზუსტი და საჭიროებისამებრ, განახლებადი; ე) დაცული უნდა იყოს იმ ფორმით, რომელიც იძლევა მონაცემთა სუბიექტის იდენტიფიკაციის საშუალებას მხოლოდ იმ დროში, რაც საჭიროა იმ მიზნებისათვის, რისთვისაც ინახება ეს მონაცემები. „იგივე პრინციპები მოცემულია ევროკავშირის მონაცემთა დაცვის დირექტივის მე-6 მუხლში და პერსონალურ მონაცემთა დაცვის საკითხებზე ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპების მეორე ნაწილში, თუმცა ნაწილობრივ განსხვავებული ფორმულირებით.“[26] აღნიშნული საერთაშორისო სამართლებრივი დოკუმენტების გაანალიზების საფუძველზე, შეიძლება ითქვას, რომ მონაცემთა დაცვის ევროპული სამართლის საკვანძო პრინციპებად განიხილება: „კანონიერი დამუშავების პრინციპი, მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი,

[25] გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 57

[26] ინოვაციებისა და რეფორმების ცენტრი, „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, 2015 წელი, გვ.9.

მონაცემთა ხარისხის პრინციპი, მონაცემთა სამართლიანი დამუშავების პრინციპი, ანგარიშვალდებულების პრინციპი.“[27]

კანონიერი დამუშავების პრინციპი, ევროპული კავშირისა და ევროპის საბჭოს მონაცემთა დაცვის კანონმდებლობის მიხედვით, თითქმის ერთნაირი ფორმითაა განმტკიცებული პერსონალური მონაცემების ევროპის საბჭოს 108-ე კონვენციის მე-5 მუხლსა და ევროპის კავშირის დირექტივის 95/46/EC[4] მე-6 მუხლში, თუმცა არც ერთი ზემოაღნიშნული მუხლი არ შეიცავს „კანონიერი დამუშავების“ განმარტებას. მოცემული სამართლებრივი ცნების გასაგებად, აუცილებელია, ყურადღება გავამახვილოთ ადამიანის უფლებათა ევროპული კონვენციით გათვალისწინებულ მართლზომიერ ჩარევაზე. პერსონალურ მონაცემთა დამუშავება არის კანონიერი მხოლოდ იმ შემთხვევაში, თუ შესაბამისობაშია კანონთან, ემსახურება ლეგიტიმურ მიზანს და აუცილებელია დემოკრატიულ საზოგადოებაში ამ მიზნის მისაღწევად. პერსონალურ მონაცემთა დამუშავებამ შეიძლება, გამოიწვიოს მონაცემთა სუბიექტის პირადი ცხოვრების პატივისცემის უფლების დარღვევა და ამ უფლებაში ჩარევა. თუმცა, ეს უფლება არ წარმოადგენს აბსოლუტურ უფლებას და მონაცემთა დაცვის უფლებაში ჩარევა შესაძლებელი და გარდაუვალია, როდესაც არსებობს სხვათა ან საზოგადოების ლეგიტიმური ინტერესი.

ადამიანის უფლებათა დაცვის ევროპული სასამართლოს პრაქტიკის თანახმად, შიდასახელმწიფოებრივი სტანდარტის შესაბამისად, ჩარევა **კანონთან შესაბამისად ჩაითვლება** იმ შემთხვევაში, თუ იგი არის „ხელმისაწვდომი მოცემული პირებისთვის, ხოლო მისი შედეგები - განჭვრეტადი.“[28] წესი განჭვრეტადია, თუ „არის ფორმულირებული საკმარისი სიზუსტით, რათა ნებისმიერ ინდივიდს მიეცეს საშუალება, საჭიროების შემთხვევაში, შესაბამისი მითითების საფუძველზე,

[27] გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 82

[28] ადამიანის უფლებათა დაცვის ევროპული სასამართლო Amann v. Switzerland [GC], No. 27798/95 16 თებერვალი 2000 წელი, პარაგრაფი 50.

განსაზღვროს მისი მოქმედება.[29] ამ შემთხვევაში, კანონით მოთხოვნილი სიზუსტის ხარისხი დამოკიდებული იქნება კონკრეტულ გარემოებებზე.[30]

პერსონალურ მონაცემთა დაცვის უფლებაში კანონთან შესაბამისობით ჩარევის მაგალითისთვის განვიხილოთ საქმე Copland v. The United Kingdom[31]. მოცემულ საქმეზე განმცხადებელი დასაქმებული იყო Carmarthenshire College-ში და 1995 წელს კოლეჯის დირექტორის პირად თანაშემწედ დაინიშნა. საჭირო გახდა მისი მჭიდრო თანამშრომლობა დირექტორის მოადგილესთან, რომლის დავალებითაც, სამუშაო პერიოდში, განმცხადებლის ტელეფონი, ელექტრონული ფოსტა და ინტერნეტი დაექვემდებარა მონიტორინგს. მონიტორინგის მიზანს წარმოადგენდა იმის დადგენა, რამდენად იყენებდა განმცხადებელი კოლეჯის მოწყობილობებს პირადი მიზნებისთვის. განმცხადებლის განმარტებით, მუშავდებოდა დეტალური და ყოვლისმომცველი მონაცემები განხორციელებული ზარების ხანგრძლივობის, შემომავალი და გამავალი ზარების, ასევე, იმ ტელეფონის ნომრების შესახებ, რომლიდანაც განმცხადებელს უკავშირდებოდნენ. მონიტორინგს დაექვემდებარა განმცხადებლის მიერ ინტერნეტის გამოყენების საკითხი და შესწავლილ იქნა განმცხადებლის მიერ რამდენიმე თვის განმავლობაში ვებპორტალების, მათზე განხორციელებული ვიზიტების, თარიღებისა და წვდომის ხანგრძლივობის ანალიზი, ასევე, მისი სამსახურებრივი ელექტრონული ფოსტის გამოყენების საკითხიც. ამასთან, კოლეჯში არ არსებობდა პოლიტიკა, რომელიც არეგულირებდა თანამშრომლების მიერ ტელეფონის, ელექტრონული ფოსტისა და ინტერნეტის გამოყენების მონიტორინგს.

სასამართლომ, გადაწყვეტილების მიღებისას, ხაზი გაუსვა იმ ფაქტს, რომ განმცხადებელი არ იყო გაფრთხილებული მისი ზარების მონიტორინგთან დაკავშირებით და შესაბამისად, მას ჰქონდა ლეგიტიმური მოლოდინი იმისა, რომ მისი სამუშაო ტელეფონის ნომრიდან

[29] იგივე, პარაგრაფი 56.

[30] ადამიანის უფლებათა დაცის ევროპული სასამართლო The Sunday Times v. the United Kingdom, No. 6538/74, 26 აპრილი, 1979 წელი, პარაგრაფი 49.

[31] ადამიანის უფლებათა დაცვის ევროპული სასამართლო, Copland v. The United Kingdom, No. 62617/00, 03 ივლისი, 2007 წელი.

განხორციელებული ზარების კონფიდენციალურობა დაცული იქნებოდა. კონკრეტულ შემთხვევაში, სასამართლომ მხედველობაში მიიღო ის ფაქტი, რომ არ არსებობდა არც ეროვნული კანონმდებლობა და არც კოლეჯის რაიმე სახის შიდა რეგულაცია, რომელიც ითვალისწინებდა დამსაქმებლის მიერ დასაქმებულთა ტელეფონის, ელექტრონული ფოსტისა და ინტერნეტის გამოყენების მონიტორინგს. შესაბამისად, სასამართლომ მიიჩნია, რომ მის უფლებებში ჩარევა არ იყო „კანონთან შესაბამისი“. განმცხადებლის ტელეფონის, ელექტრონული ფოსტისა და ინტერნეტის გამოყენებასთან დაკავშირებული პერსონალური მონაცემების შეგროვება და შენახვა, განმცხადებლის ცოდნის გარეშე, წარმოადგენდა ადამიანის უფლებაში ჩარევას და მოცემულ შემთხვევაში, სასამართლომ დაადგინა ადამიანის უფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლის დარღვევა.

ასევე მნიშვნელოვანი გადაწყვეტილება მიიღო ადამიანის უფლებათა დაცვის ევროპულმა სასამართლომ 2016 წლის იანვარში, რომლითაც პირიქით, ლეგიტიმურად ცნო დამსაქმებლის მიერ სამუშაო საათებში დასაქმებულის პირადი მიმოწერის კონტროლი.

აღნიშნული საქმეზე განმცხადებელი იყო რუმინელი მოქალაქე, რომელიც იყენებდა Yahoo massanger-ს სამუშაო მიზნით, პროფესიული კონტაქტების დასამყარებლად. საკომუნიკაციო აპლიკაციის ანგარიშის შექმნის მიზანი სწორედ საქმიანი მიმოწერის წარმოება იყო. თუმცა განმცხადებელმა კომუნიკაციის ეს საშუალება გამოიყენა პირადი მიმოწერისთვისაც. დამსაქმებელი კომპანიის პოლიტიკით მკაცრად იყო აკრძალული ამ სახის საკომუნიკაციო საშუალებების გამოყენება პირადი მიზნებისათვის. ამიტომ დამსაქმებელმა პირადი მიმოწერის ფაქტის აღმოჩენის შემდგომ, დასაქმებული სამსახურიდან დაითხოვა, კომპანიის შიდა რეგულაციის უხეში დარღვევისათვის. რუმინელი მოქალაქე ამტკიცებდა, რომ ეს ქმედება და მის პირად კომუნიკაციაში ჩარევა იყო, მისი პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევა. ევროპის ადამიანის უფლებათა საერთაშორისო სასამართლომ დაადგინა, რომ დამსაქმებლის მხრიდან ადგილი არ ჰქონია პირადი ცხოვრების

ხელშეუხებლობის დარღვევის ფაქტს და დასაქმებულის მიმოწერის ნახვა იყო დაუსაბუთებელი და გაუმართლებელი. დამსაქმებელს უნდოდა დარწმუნებულიყო, რომ დასაქმებული კეთილსინდისიერად ასრულებს თავის პროფესიულ მოვალეობას სამუშაო საათებში და არ არღვევს შიდა რეგულაციას.

აღნიშნულ გადაწყვეტილებას მოჰყვა დიდი გამოხმაურება ევროპულ მედიაში, განსაკუთრებით დიდ ბრიტანეთში. ისეთმა მედიასაშუალებებმა, როგორიც არის Telegraph, Guardian, BBC, Times, Mirror და სხვებმა არაერთი სტატია მიუძღვნეს ამ საკითხს. სტატიებში აღნიშნული გადაწყვეტილება გაშუქდა, როგორც უფლება დამსაქმებლებისათვის, გააკონტროლონ დასაქმებულთა პირადი მიმოწერა Facebook, Twitter, What's app, Gmail და სხვა საკომუნიკაციო საშუალებებით, ნებისმიერ დროს. სწორედ ამის გამო, ევროპის საბჭოს პრესსამსახური იძულებული გახდა, საგანგებო განცხადება გაეკეთებინა ევროპის ადამიანის უფლებათა ევროპული სასამართლოს მიერ მიღებულ გადაწყვეტილებაზე და აღენიშნა, რომ პრესის მიერ გადაწყვეტილების გაშუქება არ ხდება სწორად და სამართლიანად.[32] [34]

აღსანიშნავია, რომ პერსონალურ მონაცემთა კანონიერი დამუშავების პრინციპი მოიცავს, ერთი მხრივ, ლეგიტიმური მიზნისა და მეორე მხრივ, აუცილებელი საზოგადოებრივი საჭიროების არსებობის შეფასებას დემოკრატიულ საზოგადოებაში. ლეგიტიმური მიზნის არსებობაზე ადამიანის უფლებათა დაცვის ევროპულმა სასამართლომ იმსჯელა საქმეზე Peck v. the United Kingdom[33], სადაც განმცხადებელმა გადაწყვიტა თავის მოკვლა ქუჩაში, მაჯაზე ვენის გადაჭრით. მან არ იცოდა, რომ ამ მცდელობას ვიდეოსათვალთვალო (CCTV) კამერა იღებდა. პოლიციამ, რომელიც ახორციელებდა მონიტორინგს, იგი გადაარჩინა, თუმცა ვიდეოჩანაწერი გადაეცა მედიას, რომელმაც განმცხადებლის სახის დაფარვის გარეშე გამოაქვეყნა ფირი. სასამართლომ დაადგინა, რომ რელევანტური და

[32] Rawlinson K., „UK press accused of 'misinformed media storm' over email spying story", 2016, see: http://www.theguardian.com/technology/2016/jan/16/uk-press-accused-of-misinformed-media-storm-over-email-spying-story [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[33] ადამიანის უფლებათა დაცვის ევროპული სასამართლო, Peck v. the United Kingdom, No. 44647/98, 28 იანვარი 2003 წელი.

საკმარისი მიზეზი, სახელმწიფო ორგანოს მიერ ჩანაწერის საჯაროდ, პირდაპირ გადაცემის მართლზომიერებისთვის, განმცხადებლის თანხმობის ან მისი ვინაობის დაფარვის გარეშე, არ არსებობდა. ამ საქმეში არ არსებობდა მონაცემთა დამუშავების ლეგიტიმური მიზანი და შესაბამისად, სასამართლომ დადგინა კონვენციის მე-8 მუხლის დარღვევა.

რაც შეეხება საქმეს Khelili v. Switzerland[34], ამ შემთხვევაში, განმცხადებელს პოლიციის მიერ შემოწმებისას, აღმოაჩნდა სატარებელი საკონტაქტო ბარათები, რომელზეც ეწერა: „სასიამოვნო, მოხდენილი ქალი, ორმოც წლამდე ასაკის, შეხვდება მამაკაცს, სასმელის დალევისა და პერიოდულად სეირნობის მიზნით. ტელეფონის ნომერი.“ განმცხადებელი იუწყებოდა, რომ აღნიშნული აღმოჩენის შედეგად, პოლიციამ თავის ბაზაში იგი „მეძავად“ მოიხსენია, რა საქმიანობასაც იგი კატეგორიულად უარყოფდა. განმცხადებელმა მოითხოვა სიტყვა „მეძავის“ ამოშლა პოლიციის კომპიუტერული ბაზიდან. სასამართლომ აღიარა, რომ, ზოგადად, ინდივიდის პერსონალური მონაცემების შენახვა იმ საფუძვლით, რომ პირმა შესაძლოა, ჩაიდინოს სხვა სამართალდარღვევა, გარკვეული შემთხვევების გათვალისწინებით, შესაძლოა, იყოს თანაზომიერი. თუმცა განმცხადებლის საქმეში, პროსტიტუციაზე მითითება იყო ძალიან ბუნდოვანი და ზოგადი, არ იყო გამყარებული კონკრეტული ფაქტებით, რამდენადაც იგი არასდროს ყოფილა გასამართლებული პროსტიტუციისთვის და, შესაბამისად, კონვენციის მე-8 მუხლის თანახმად, ვერ იქნებოდა მიჩნეული მომეტებული საზოგადოებრივი საჭიროების ხარისხის მქონედ. სასამართლომ დაადგინა, რომ წლების განმავლობაში, პოლიციის მიერ სიტყვა „მეძავის“ შენახვა შესაბამის ჩანაწერებში არ წარმოადგენდა აუცილებლობას დემოკრატიულ საზოგადოებაში. შესაბამისად, ამ საქმეზეც სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

ევროპული სამართლით, ასევე, ხაზგასმულია მონაცემთა დამუშავებისას **მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი,** რაც ნიშნავს, რომ პერსონალურ მონაცემთა დამუშავების ლეგიტიმურობის

[34] ადამიანის უფლებათა დაცვის ევროპული სასამართლო, Khelili v. Switzerland, , No. 16188/07, 18 ოქტომბერი, 2011 წელი.

საკითხი დამოკიდებულია დამუშავების მიზანზე.[35] მიზანი უნდა იყოს განსაზღვრული და გაცხადებული დამმუშავებლის მიერ, მონაცემთა დამუშავების დაწყებამდე.[36] [35]

„ევროპული კავშირის კანონმდებლობის მიხედვით, მონაცემთა დამუშავების მიზანი ნათლად უნდა იყოს განსაზღვრული დამუშავების დაწყებამდე. ევროპის საბჭოს კანონმდებლობის თანახმად კი, ამ საკითხის განსაზღვრის უფლება აქვთ უშუალოდ სახელმწიფოებს. ამასთან, ორივე კანონმდებლობით, მონაცემთა დამუშავება განუსაზღვრელი მიზნისთვის არ არის შესაბამისობაში მონაცემთა დაცვის სამართალთან. ასევე, მონაცემთა შემდგომი გამოყენება სხვა მიზნისთვის საჭიროებს დამატებით სამართლებრივ საფუძველს, თუ დამუშავების ახალი მიზანი შეუთავსებელია თავდაპირველ მიზანთან და რაც შეეხება მესამე მხარისთვის მონაცემთა გადაცემას, ეს წარმოადგენს ახალ მიზანს, რაც ასევე საჭიროებს დამატებით სამართლებრივ საფუძველს. “[37]

მონაცემების, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას, როდესაც განიხილება კონკრეტული მონაცემის დამუშავების მიზანი, მისი არეალი და მოცულობა, ევროპის კავშირისა და ევროპის საბჭოს კანონმდებლობა მნიშვნელოვანად მიიჩნევს თავსებადობის კონცეფციას. ხაზგასმულია, რომ მონაცემთა გამოყენება თავსებადი მიზნებისთვის დაშვებულია მხოლოდ საწყისი სამართლებრივი საფუძვლით. თუმცა, რას ნიშნავს „თავსებადი“ ცალსახად განმარტებული არ არის და შეფასებას ექვემდებარება ყოველი კონკრეტული გარემოებებიდან გამომდინარე. მონაცემთა დაცვის დირექტივა მკაფიოდ ადგენს, რომ „მონაცემთა შემდგომი დამუშავება ისტორიული, სტატისტიკური ან სამეცნიერო მიზნებისთვის არ უნდა ჩაითვალოს

[35] 108-ე კონვენცია მე-5 მუხლის „ბ“ ქვეპუნქტი, მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის „ა“ ქვეპუნქტი.

[36] მუხლი 29 სამუშაო ჯგუფი (2013), მოსაზრება 03/2013 მიზნის ლიმიტირების შესახებ, WB 203, ბრიუსელი, 2 აპრილი, 2013 წელი.

[37] გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 92.

შეუსაბამოდ, თუ წევრი ქვეყნები ადგენენ დაცვის შესაბამის მექანიზმებს“.[38] [36]

ევროპული სამართალი მონაცემთა დამუშავებისას, ასევე მნიშვნელოვნად მიიჩნევს **მონაცემთა ხარისხის პრინციპების დაცვას, რაც თავის მხრივ, აერთიანებს მონაცემთა შესაბამისობის, მონაცემთა სიზუსტისა და მონაცემთა ლიმიტირებული შენახვის პრინციპების დაცვას.**

მონაცემთა შესაბამისობის პრინციპი ნიშნავს, რომ მხოლოდ ისეთი მონაცემები შეიძლება დამუშავდეს, რომლებიც არის „ადეკვატური, შესაბამისი და არ არის ჭარბი იმ მიზნიდან გამომდინარე, რომლისთვისაც ისინი შეგროვდა ან/და შემდგომში დამუშავდა.“[39]

რაც შეეხება მონაცემთა სიზუსტის პრინციპს, ეს გულისხმობს, რომ დამმუშავებელმა არ უნდა გამოიყენოს მასთან არსებული პერსონალური ინფორმაცია, თუ არ უზრუნველყოფს მონაცემთა სიზუსტესა და მისი განახლებისათვის შესაბამისი ზომების მიღებას.

მონაცემთა სიზუსტის ვალდებულება განიხილება მონაცემთა დამუშავების მიზნიდან გამომდინარე. ერთი მხრივ, შესაძლებელია, იყოს შემთხვევები, როდესაც შენახული მონაცემების განახლება სამართლებრივად იყოს აკრძალული, რამდენადაც არ უნდა შეიცვალოს მონაცემთა შენახვის მიზანი, ხოლო მეორე მხრივ, არსებობს შემთხვევები, სადაც მონაცემთა სისწორის რეგულარული შემოწმება, მათ შორის განახლება აუცილებელია, იმ პოტენციური ზიანის გამო, რაც შეიძლება მიადგეს მონაცემთა სუბიექტს არაზუსტი მონაცემების დატოვების შემთხვევაში.

მონაცემთა ლიმიტირებული შენახვის პრინციპი განმტკიცებულია მონაცემთა დაცვის დირექტივის მე-6 მუხლის პირველი პუნქტის „e“ ქვეპუნქტით, ისევე, როგორც 108-ე კონვენციის მე-5 მუხლის „e“

[38] ამგვარი შიდასახელმწიფოებრივი საკანონმდებლო დებულების მაგალითი მოცემულია ავსტრიის მონაცემთა დაცვის აქტში (Datenschutzgesetz), Fed. Law Gazette I No. 165/1999, პარაგრაფი 46, ხელმისაწვდომია ინგლისურ ენაზე: www.dsk.gv.at. [მოხსენიებულია გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი].

[39] 108-ე კონვეცია, მე-5 მუხლის „c’ ქვეპუნქტი, მონაცემთა დაცვის დირექტივა მე-6 მუხლის პირველი პუნქტის „c“ ქვეპუნქტი

ქვეპუნქტით, რომელიც ავალდებულებს წევრ ქვეყნებს პერსონალური მონაცემების „შენახვას იმგვარი ფორმით, რომელიც იძლევა მონაცემთა სუბიექტების იდენტიფიცირების საშუალებას იმ ვადით, რაც საჭიროა მონაცემთა შეგროვების მიზნის მიღწევისთვის ან შემდგომი დამუშავების მიზნისთვის“. შესაბამისად, მონაცემები უნდა იქნეს განადგურებული ამ მიზნების მიღწევისთანავე. მაგალითისთვის, საქმეზე S. and Marper v. the United Kingdom[40], სადაც გაერთიანებული სამეფოს “საპოლიციო და სისხლის სამართლებრივი მტკიცებულებების შესახებ” აქტის 64-ე სექციის თანახმად, ეჭვმიტანილი პირის თითის ანაბეჭდების, უჯრედოვანი ნიმუშებისა და დნმ-ის პროფილის შენახვა შესაძლებელი იყო უვადოდ, იმ შემთხვევაშიც კი, როდესაც სისხლის სამართლის პროცესის დასრულების შემდეგ, პირი გათავისუფლდა ან არ წაეყენა ბრალი. აღნიშნულ საქმეზე შესწავლილ იქნა ადამიანის უფლებათა ევროპული კონვენციის მაღალი ხელშემკვრელი მხარეების პრაქტიკა და აღინიშნა, რომ გაერთიანებული სამეფოს მიერ დნმ მონაცემთა შენახვა შეზღუდული პერიოდით და კონკრეტული მიზნებით ხორციელდებოდა. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ იმ პირთა თითის ანაბეჭდების, უჯრედოვანი ნიმუშებისა და დნმ პროფილების შენახვის შეუზღუდავი და არადისკრიმინაციული ბუნება, რომლებიც იყვნენ დანაშაულში ეჭვმიტანილები, მაგრამ არა მსჯავრდებულები, არ უზრუნველყოფდა სამართლიან ბალანსს საჯარო და კერძო ინტერესებს შორის. შესაბამისად, სასამართლომ მიიჩნია, რომ პერსონალურ მონაცემთა შენახვა, აღნიშნულ შემთხვევაში, წარმოადგენდა არაპროპორციულ ზომას მიზანთან მიმართებაში და ვერ იქნებოდა მიჩნეული აუცილებლად დემოკრატიულ საზოგადოებაში. შედეგად, მან ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა. „პერსონალურ მონაცემთა შენახვის ვადების შეზღუდვა ვრცელდება მხოლოდ იმ მონაცემებზე, რომლითაც შესაძლებელია მონაცემთა სუბიექტის იდენტიფიცირება. იმ მონაცემების კანონიერი

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

შენახვა, რომელიც აღარ არის საჭირო, შესაძლოა, უზრუნველყოფილ იქნეს ანონიმირებით ან ფსევდონიმირებით.“[41]

მონაცემთა შენახვა სამომავლო სამეცნიერო, ისტორიული ან სტატისტიკური გამოყენებისთვის, მონაცემთა დაცვის დირექტივის მიხედვით, არის მკაფიოდ გამოცალკევებული მონაცემთა ლიმიტირებული შენახვის პრინციპისგან.[42] პერსონალურ მონაცემთა მიმდინარე შენახვასა და გამოყენებას თან უნდა სდევდეს შიდასახელმწიფოებრივი კანონმდებლობით დადგენილი უსაფრთხოების ზომები.

მონაცემთა სამართლიანი დამუშავების პრინციპი, ევროპული კანონმდებლობის მიხედვით, არეგულირებს, უპირველეს ყოვლისა, მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის ურთიერთობას. სამართლიანი დამუშავება გულისხმობს მის გამჭვირვალობას და დამმუშავებელთა ვალდებულებას მონაცემთა სუბიექტების მიმართ, მათ შესახებ მონაცემთა დამუშავებამდე, აცნობონ, სულ მცირე, დამუშავების მიზნის, დამმუშავებლის ვინაობისა და მისი მისამართის შესახებ. გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, პერსონალურ მონაცემთა საიდუმლო და ფარული დამუშავება არ უნდა ხორციელდებოდეს. მონაცემთა სუბიექტებს უფლება აქვთ, განახორციელონ წვდომა საკუთარ მონაცემებზე, დამუშავების ადგილის მიუხედავად.

სამართლიანი დამუშავების პრინციპი ევროპული სამართლის მიხედვით, მოიცავს ასევე, მონაცემთა დამმუშავებლის მხრიდან გამჭვირვალობის დაცვასა და ნდობის დამყარების შესაძლებლობას. მონაცემთა დამუშავების **გამჭვირვალობის პრინციპი განსაზღვრავს** დამმუშავებლის ვალდებულებას, მონაცემთა სუბიექტების ინფორმირების თაობაზე, მათი მონაცემების გამოყენების საკითხთან დაკავშირებით. მაგალითისთვის, საქმეზე Haralambie v. Romania[43] განმცხადებელი ითხოვდა

---

[41] გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 98.

[42] მონაცემთა დაცვის დირექტივა, მე-6 მუხლის პირველი პუნქტის „e“ ქვეპუნქტი.

[43] ადამიანის უფლებათა ევროპული სასამართლო Haralambie v. Romania, No. 21737/03, 27 ოქტომბერი, 2009 წელი.

საიდუმლო სამსახურის მიერ მის შესახებ შენახულ ინფორმაციაზე წვდომას, თუმცა მისი მოთხოვნა დაკმაყოფილებულ იქნა მხოლოდ ხუთი წლის შემდეგ. ადამიანის უფლებათა ევროპულმა სასამართლომ არაერთხელ აღნიშნა, რომ ინდივიდებს, რომელთა შესახებაც სახელმწიფო დაწესებულების მიერ შენახული იყო პერსონალური ფაილები, წვდომასთან მიმართებით, გააჩნდათ სასიცოცხლო ინტერესი. სახელმწიფო ორგანოს ჰქონდა ამგვარ ინფორმაციასთან წვდომის უზრუნველსაყოფად ეფექტური პროცედურის დადგენის ვალდებულება. სასამართლომ აღნიშნა, რომ არც შენახული ფაილების რიცხვი და არც არქივირებასთან დაკავშირებული პრობლემები არ ხდიდა მართლზომიერს განმცხადებლის ფაილებზე წვდომის მოთხოვნის ხუთი წლით გადავადებას. სახელმწიფო ორგანოებმა ვერ უზრუნველყვეს განმცხადებლისთვის ეფექტური და ხელმისაწვდომი პროცედურის არსებობა, რათა მას გონივრულ ვადაში ჰქონოდა საკუთარ პერსონალურ ფაილებზე წვდომის განხორციელების შესაძლებლობა. სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

რაც შეეხება სამართლიანი ნდობის დამყარებას მონაცემთა სუბიექტთან, ამ თვალსაზრისით, ევროპული კანონმდებლობა გულისხმობს, რომ დამმუშავებლებმა უნდა შეძლონ, დაუსაბუთონ მოქალაქეებს რომ მონაცემებს ისინი ამუშავებენ კანონიერად და გამჭვირვალედ; ამასთან, დამუშავების მოქმედებებს არ აწარმოებენ საიდუმლოდ და ამას არ გააჩნია გაუთვალისწინებელი ნეგატიური ეფექტი. დამმუშავებლები უნდა იყვნენ დარწმუნებულნი, რომ მოქალაქეები არიან ინფორმირებულნი მათი მონაცემების გამოყენების თაობაზე, განსაკუთრებით მაშინ, თუ თანხმობა წარმოადგენს მონაცემთა დამუშავების სამართლებრივ საფუძველს. მაგალითისთვის განვიხილოთ საქმე K.H. and Others v. Slovakia,[44] სადაც განმცხადებელი იყო რომანული ეთნიკური წარმოშობის მქონე რვა ქალბატონი, რომლებიც ორსულობისა და მშობიარობის დროს, განთავსებულნი იყვნენ აღმოსავლეთ სლოვაკეთის ორ ჰოსპიტალში. მცდელობების მიუხედავად, ვერც ერთი მათგანი ვერ დაფეხმძიმდა.

[44] ადამიანის უფლებათა ევროპული სასამართლო, K.H. and Others v. Slovakia, No. 32881/04, 28 აპრილი, 2009 წელი.

ეროვნულმა სასამართლოებმა დაავალდებულეს ჰოსპიტლები, რომ დაეშვათ განმცხადებლები და მათი წარმომადგენლები სამედიცინო ჩანაწერებთან, წერილობითი ამონაწერების გაკეთების მიზნით, თუმცა უარი მიიღეს დოკუმენტების ფოტოასლების გაკეთების თაობაზე, მათი უკანონოდ გამოყენების თავიდან ასაცილებლად. განმცხადებლების საქმეზე, შიდასახელმწიფოებრივმა სასამართლოებმა მართლზომიერად ჩათვალეს სამედიცინო ჩანაწერების ასლის გადაღების აკრძალვა, თუმცა ადამიანის უფლებათა ევროპულმა სასამართლომ ვერ დაადგინა, თუ რამდენად შეეძლოთ განმცხადებლებს, რომლებსაც მიეცათ წვდომის უფლება სრულ სამედიცინო ჩანაწერებზე, უკანონოდ გამოეყენებინათ ინფორმაცია მათ შესახებ. ამ საქმეზე ადამიანის უფლებათა დაცვის ევროპულმა სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

მონაცემების დამუშავების **ანგარიშვალდებულების** პრინციპი კი მოიცავს და მოითხოვს დამმუშავებლის მიერ მონაცემთა დაცვის უზრუნველსაყოფად ზომების ინპლემენტაციას, პასუხისმგებლობას, მონაცემთა დამუშავება წარმართოს კანონმდებლობის დაცვით და საზედამხედველო ორგანოსა და საზოგადოებისათვის დასაბუთების შესაძლებლობას, მის მიერ განხორციელებული მოქმედებები შესაბამისობაში იყოს მონაცემთა დაცვის დებულებებთან.

„იმ დროს, როდესაც 108-ე კონვენცია არ აკეთებს დათქმას დამმუშავებლების ანგარიშვალდებულების პრინციპზე, ტოვებს რა, ამ საკითხს ღიად შიდასახელმწიფოებრივი კანონით რეგულირებისთვის, მონაცემთა დაცვის დირექტივის მე-6 მუხლის მე-2 პუნქტი ადგენს, რომ დამმუშავებელმა უნდა უზრუნველყოს პირველი პუნქტით დადგენილი პრინციპების შესრულება“[45]

ზემოაღნიშნული დებულებებიდან ნათლად გამომდინარეობს, რომ მონაცემთა დამმუშავებლებმა თავად უნდა მოახდინონ მონაცემთა დამუშავების პროცესის ამ წესებთან ინტეგრირება და ამისთვის არ უნდა

[45] „მონაცემთა დაცვის ევროპული სამართალი“, კ. გოშაძე, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 102.

დაელოდონ გამოვლენილ ნაკლოვანებებზე მონაცემთა სუბიექტების ან საზედამხედველო ორგანოების მხრიდან მითითებას.

1.3. განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების საფუძვლები ევროპული კანონმდებლობის მიხედვით

„პრინციპი, რომელიც ამბობს, რომ პერსონალურ მონაცემთა ნებისმიერი დამუშავება უნდა იყოს კანონიერი, მოითხოვს, რომ დამუშავების ყველა შემთხვევა ეფუძნებოდეს კანონით გათვალისწინებულ საფუძველს. საჯარო სექტორში მონაცემთა დამმუშავებლისთვის ასეთი საფუძველი არის ვალდებულება ან მინიმუმ, კანონით განსაზღვრული ნებართვა.“[46] „განსაკუთრებული კატეგორიის მონაცემები დაცული უნდა იყოს, როგორც ფიზიკურ სივრცეში (offline), ისე - ინტერნეტში (online).“[47] [37] მაშინ, როდესაც ევროპის საბჭოს კონვენცია ნებას რთავს შიდასახელმწიფოებრივ კანონმდებლობას, განსაზღვროს შესაბამისი დაცვის ზომები და დაადგინოს, როდის არის განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება კანონიერი, მონაცემთა დაცვის ევროპული დირექტივის მე-8 მუხლმა პირველად სცადა, განესაზღვრა შემთხვევები „სენსიტიური“ კატეგორიის მონაცემთა დამუშავებისთვის. ზოგადად, სენსიტიური, ანუ „განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება აკრძალულია.“[48] თუმცა, არსებობს მოცემული აკრძალვის გამონაკლისთა ამომწურავი ჩამონათვალი, რომელიც დადგენილია დირექტივის მე-8 მუხლის მე-2 და მე-3 პუნქტებით. ეს გამონაკლისები შეიცავს მონაცემთა სუბიექტის აშკარა თანხმობას, მონაცემთა სუბიექტის სასიცოცხლო ინტერესებს, სხვათა ლეგიტიმურ ინტერესებსა და საჯარო ინტერესს.

---

[46] ინოვაციებისა და რეფორმების ცენტრი, „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, 2015 წელი, გვ.10.

[47] ევროპის კომისიის სპეციალური ევრობარომეტრი 431, გვ. 15, ხელმისაწვდომია: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[48] მონაცემთა დაცვის დირექტივა, მე-8 მუხლის პირველი პუნქტი.

მონაცემთა სუბიექტის მკაფიო თანხმობა - „მონაცემთა კანონიერი დამუშავების უპირველესი პირობა, მიუხედავად იმისა, განსაკუთრებულია თუ არა იგი, არის მონაცემთა სუბიექტის თანხმობა. განსაკუთრებული კატეგორიის მონაცემის შემთხვევაში, თანხმობა უნდა იყოს მკაფიო. შიდასახელმწიფოებრივი კანონით, შესაძლებელია განისაზღვროს, რომ განსაკუთრებული მონაცემების გამოყენებაზე თანხმობა არ არის საკმარისი საფუძველი მათი დამუშავებისთვის, მაგალითად, თუ განსაკუთრებულ შემთხვევებში, დამუშავება მოიცავს დიდ რისკებს მონაცემთა სუბიექტისთვის.

ზოგიერთ შემთხვევაში, შინაარსობრივი თანხმობაც კი შესაძლებელია აღიარებული იყოს განსაკუთრებული კატეგორიის მონაცემთა დამუშავების სამართლებრივ საფუძვლად: დირექტივის მე-8 მუხლის მე-2 პუნქტი ადგენს, რომ დამუშავება არ არის აკრძალული, თუ იგი მოიცავს მონაცემებს, რომელიც მონაცემთა სუბიექტმა აშკარად საჯარო გახადა.“[49]

მონაცემთა სუბიექტის სასიცოცხლო ინტერესები - არასენსიტიური მონაცემების მსგავსად, განსაკუთრებული კატეგორიის მონაცემები შესაძლებელია, დამუშავებული იქნეს მონაცემთა სუბიექტის სასიცოცხლო ინტერესებისთვის.[50] ამ საფუძვლით განსაკუთრებული კატეგორიის მონაცემთა კანონიერი დამუშავებისთვის აუცილებელია, რომ შეუძლებელი იყოს მონაცემთა სუბიექტისთვის საკითხის დასმა მის გადასაწყვეტად, მაგალითად, მონაცემთა სუბიექტის უგონო მდგომარეობის ან მისი მიუწვდომლობის გამო.

სხვათა ლეგიტიმური ინტერესები - არასენსიტიური მონაცემების მსგავსად, სხვათა ლეგიტიმური ინტერესების დაცვა შესაძლოა, წარმოადგენდეს განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძველს. მათი დამუშავება, მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-2 პუნქტის მიხედვით, ნებადართულია მხოლოდ შემდეგ შემთხვევებში:

---

[49] გოშაძე, კ. „მონაცემთა დაცვის ევროპული სამართალი“, თარგმანი, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 115-116.

[50] მონაცემთა დაცვის დირექტივა, მე-8 მუხლის c ქვეპუნქტი.

➢ თუ დამუშავება აუცილებელია სხვა პირის სასიცოცხლო ინტერესებისთვის, როდესაც მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად არ შესწევს უნარი, განაცხადოს თანხმობა;

➢ თუ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, როგორიცაა ჯანმრთელობის შესახებ მონაცემები, ხორციელდება შრომით-სამართლებრივი მიზნებისთვის, განსაკუთრებით სახიფათო სამუშაო ადგილის გათვალისწინებით ან რელიგიური მრწამსის შესახებ მონაცემები – დასვენების დღეების განსასაზღვრად;[51]

➢ როდესაც ფონდები, ასოციაციები ან სხვა არასამეწარმეო ორგანოები პოლიტიკური, ფილოსოფიური, რელიგიური ან სავაჭრო კავშირის მიზნებიდან გამომდინარე, ამუშავებენ მონაცემებს მათი წევრების, სპონსორების ან სხვა დაინტერესებული პირების შესახებ (ამგვარი მონაცემები განსაკუთრებული კატეგორისაა, ვინაიდან ისინი შესაძლებელია, ავლენდეს კონკრეტული ინდივიდის რელიგიურ ან პოლიტიკურ შეხედულებებს);[52]

➢ თუ განსაკუთრებული კატეგორიის მონაცემები არის გამოყენებული სასამართლოში პროცესისთვის ან ადმინისტრაციულ ორგანოში სამართლებრივი მოთხოვნით მიმართვისთვის, მისი განხილვისათვის ან დაცვისთვის;[53]

➢ ამასთან, მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-3 პუნქტის თანახმად, თუ ჯანმრთელობის შესახებ მონაცემები გამოიყენება სამედიცინო გამოკვლევისა და მკურნალობისთვის შესაბამისი ჯანდაცვის დაწესებულების მომსახურე პირის მიერ, ამ მომსახურებათა მართვა, ასევე, გათვალისწინებულია დადგენილი გამონაკლისებით. განსაკუთრებული უსაფრთხოებისთვის, პირები მიიჩნევიან „ჯანდაცვის დაწესებულების მომსახურე პირებად“ იმ შემთხვევაში, თუ ისინი ექვემდებარებიან კონფიდენციალურობის სპეციალურ, პროფესიულ ვალდებულებას.[54]

---

[51] მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-2 პუნქტის b ქვეპუნქტი.

[52] იქვე, d ქვეპუნქტი.

[53] იქვე, მე-8 მუხლის მე-2 პუნქტის e ქვეპუნქტი.

[54] გოშაძე კ., „მონაცემთა დაცვის ევროპული სამართალი“, თარგმანი, 2015 წელი, გამომცემლობა „იურისტის სამყარო“, თბილისი, გვ. 118.

საჯარო ინტერესი - მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-4 პუნქტის თანახმად, წევრ ქვეყნებს შეუძლიათ, დაადგინონ დამატებითი მიზნები, რომელთათვისაც შესაძლებელია, დამუშავდეს განსაკუთრებული მონაცემები, კერძოდ, მონაცემთა დამუშავება აუცილებელია არსებითი საჯარო ინტერესისთვის, იგი განსაზღვრულია შიდასახელმწიფოებრივი კანონით ან ზედამხედველი ორგანოს გადაწყვეტილებით. შიდასახელმწიფოებრივი კანონი ან ზედამხედველი ორგანოს გადაწყვეტილება შეიცავს უსაფრთხოების აუცილებელ ზომებს მონაცემთა სუბიექტის ინტერესთა ეფექტური დაცვისთვის.[55] თვალსაჩინო მაგალითია ჯანმრთელობის ელექტრონული ფაილური სისტემები, რომლის შექმნაც იგეგმება ევროპული კავშირის ბევრ ქვეყანაში. აღსანიშნავია, რომ საქართველოშიც დაწყებულია ჯანმრთელობის ელექტრონული ფაილური სისტემის დანერგვა. ამგვარი სისტემით შესაძლებელია, რომ ჯანმრთელობის მდგომარეობის შესახებ მონაცემები, რომელიც შეგროვებულ იქნა ჯანდაცვის დაწესებულების მომსახურე პირის მიერ პაციენტის მკურნალობის პროცესში, ფართოდ გახდეს ხელმისაწვდომი ჯანდაცვის სხვა დაწესებულების მომსახურეთათვის, ძირითადად, მთელი ქვეყნის მასშტაბით. თუმცა, „29-ე მუხლის სამუშაო ჯგუფმა“[56] [38] დაასკვნა, რომ ამგვარი სისტემების დანერგვა ვერ მოხერხდება პაციენტის მონაცემების დამუშავებისთვის განკუთვნილი, არსებული სამართლებრივი წესების საფუძველზე, რაც დადგენილია მონაცემთა დაცვის დირექტივის მე-8 მუხლის მე-3 პუნქტით. იმის გათვალისწინებით, რომ ჯანმრთელობის შესახებ მოცემული ელექტრონული ფაილური სისტემის არსებობა წარმოადგენს არსებით საჯარო ინტერესს, იგი შესაძლებელია, დაეყრდნოს დირექტივის მე-8 მუხლის მე-4 პუნქტს, რაც მოითხოვს მკაფიო

[55] მონაცემთა დაცვის დირექტივა, მე-8 მუხლის მე-4 პუნქტი.

[56] 29-ე მუხლის სამუშაო ჯგუფის დამატებითი ინფორმაცია, ხელისაწვდომია: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Art29 [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

სამართლებრივ საფუძველს მისი განხორციელებისთვის და უსაფრთხოების აუცილებელ ზომებს სისტემის დაცული ფუნქციონირებისთვის.[57] [39]

ზემოაღნიშნული დებულებების გარდა, ევროპის საბჭოსა და ევროკავშირის კანონმდებლობით დადგენილ „საერთაშორისო სტანდარტებთან დაახლოებაზე საუბრისას, მხედველობაშია მისაღები როგორც ევროპის საბჭოს 108-ე კონვენციის განახლების, ისე ევროკავშირის ფარგლებში განხორციელებული პერსონალურ მონაცემთა დაცვის რეფორმის საკითხი.“[58] [40]

ამ მხრივ, აუცილებლად უნდა განვიხილოთ განახლებული 108-ე კონვენციის სამუშაო ვერსია, რომლის მიხედვითაც, „პერსონალურ მონაცემთა დაცვის მარეგულირებელი ნორმების მოქმედების სფეროდან ერთადერთი დაშვებული გამონაკლისი მონაცემთა აშკარად გამოხატული პირადი და საოჯახო მიზნით დამუშავებაა.“[59] რაც შეეხება ევროპის კავშირის პერსონალურ მონაცემთა დაცვის ზოგად რეგულაციას, რომელიც 2018 წლის 25 მაისიდან ამოქმედდება, იგი ითვალისწინებს მთელ რიგ ისეთ ვალდებულებებს, რომლებიც საქართველოს კანონმდებლობაში ამ ეტაპზე ასახული არ არის. **რეგულაციით გათვალისწინებულია მნიშვნელოვანი ცვლილებები, კერძოდ:**

თანხმობა - დოკუმენტში ცალკე არის გამოყოფილი თანხმობის მუხლი, რომელშიც აღნიშნულია, რომ თანხმობის არსებობის მტკიცების ტვირთი ეკისრება მონაცემთა დამმუშავებელს. ამასთან, წერილობითი ფორმით გამოთქმული თანხმობა შედგენილი უნდა იყოს მარტივ და გასაგებ ენაზე. მონაცემთა სუბიექტს უფლება ექნება, ნებისმიერ დროს გამოითხოვოს მის მიერ გამოთქმული თანხმობა და ეს პროცედურა უნდა იყოს ისეთივე მარტივი, როგორც მისი გაცხადება. ცალკე არის გამოყოფილი თანხმობა არასრულწლოვანთა პერსონალური მონაცემების დამუშავების შემთხვევაში.

---

[57] მუხლი 29 სამუშაო ჯგუფი (2007) სამუშაო დოკუმენტი, ჯანმრთელობის ელექტრონულ რეესტრში (HER) ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების თაობაზე, WP131, ბრიუსელი, 15 თებერვალი 2007 წელი.

[58] Association Agenda between the European Union and Georgia, see: [www.eeas.europa.eu], [მოხენიებულია ქალდანი თ., სარიშვილი ნ., „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, 2016 წელი].

[59] Article 9, text of the modernised Convention 108; see: [www.coe.int]

საზედამხედველო ორგანოს ინფორმირების ვალდებულება - მონაცემთა დამმუშავებლებს ეკისრებათ ვალდებულება პერსონალური მონაცემების უკანონო ხელყოფისა და გამჟღავნების შემთხვევაში (data breach), დაუყოვნებლივ, მაგარამ ფაქტის დადგომიდან არაუგვიანეს 72 საათისა, მის შესახებ აცნობონ პერსონალური მონაცემების დაცვის საზედამხედველო ორგანოს. თუ ვადა დაცული არ იქნა, მონაცემთა დამმუშავებელმა საზედამხედველო ორგანოს უნდა წარუდგინოს შესაბამისი ახსნა-განმარტება. ინფორმაციის მიწოდება სავალდებულო არ არის, თუ მონაცემთა უკანონო გამჟღავნების ან ხელყოფის ფაქტი არ იქნება დიდი ზიანის მომტანი ადამიანის უფლებებისა და თავისუფლებების ხელყოფის კუთხით.

მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების ვალდებულება - მონაცემთა სუბიექტს უნდა მიეწოდოს ინფორმაცია მონაცემთა უკანონო ხელყოფისა და გამჟღავნების შემთხვევაში, თუ არსებობს მათი უფლებებისა და თავისუფლებებისათვის ზიანის მიყენების რისკი. შეტყობინება გაკეთებული უნდა იყოს მარტივი და გასაგები ფორმით, ასევე, უნდა შეიცავდეს რეკომენდაციებს მონაცემთა სუბიექტისათვის.

უფლებამოსილი პირი - ცვლილებებს შორის აღსანიშნავია, რომ უფლებამოსილ პირებს აქვთ გარკვეული ვალდებულებები, რომლებიც აქამდე განსაზღვრული იყო მხოლოდ მონაცემთა დამმუშავებელთათვის. ამასთან, შესაძლებელი იქნება უფლებამოსილი პირის მიერ პერსონალური მონაცემების დამუშავების რეგულაციასთან შესაბამისობის ფაქტის გასაჩივრებაც.

სანქციები - ევროკავშირის განახლებული რეგულაცია გამოირჩევა გაზრდილი სანქციებით. მონაცემთა დაცვის საზედამხედველო ორგანოებს საშუალება ექნებათ, მონაცემთა დაცვის დამუშავების წესების დარღვევისათვის, მონაცემთა დამმუშვებელსა და უფლებამოსილ პირს დააკისრონ ჯარიმა 10-20 მილიონი ევროს ან წლიური ბრუნვის 2-4%-ის ოდენობით (დაეკისრება იმ სახის სახდელი, რომელიც მეტი იქნება).

საერთაშორისო გადაცემა - მონაცემთა საერთაშორისო გადაცემის წესები არსებითად არ შეცვლილა. ცვლილებებს შორის აღსანიშნავია კომპანიების ვალდებულება, ჰქონდეთ სავალდებულო კორპორაციული წესები, თუ აქვთ წარმომადგენლობა ევროკავშირის ფარგლებს გარეთ ან არიან ერთიანი ჯგუფის წევრები, ახორციელებენ ერთობლივ ეკონომიკურ საქმიანობას ევროკავშირის ფარგლებს გარეთ არსებულ კომპანიასთან. აღნიშნული წესები სავალდებულო უნდა იყოს შესასრულებლად ყველა იმ წარმომადგენლობისა და პარტნიორისათვის, რომელსაც შეიძლება, შეხება ჰქონდეს მონაცემებთან. რეგულაციაში მოცემულია გარემოებების ამომწურავი ჩამონათვალი, როდესაც შესაძლებელია პერსონალური მონაცემების მესამე სახელმწიფოსათვის გადაცემა, თუ ამ სახელმწიფოში არ არის მონაცემთა დაცვის სათანადო გარანტიები ან სახეზე არ არის სავალდებულო კორპორატიული წესები. ამ გარემოებებს შორის არის მონაცემთა სუბიექტის თანხმობა, გამოთქმული მონაცემთა გადაცემასთან დაკავშირებული რისკების შესახებ მისი სრულად ინფორმირების შემდგომ.

მონაცემთა დაცვის ოფიცერი - მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირებისათვის, გარკვეულ შემთხვევებში, სავალდებულო გახდება პერსონალური მონაცემების დაცვის ოფიცრების ყოლა, ეს შემთხვევებია: მონაცემების დამუშავება საჯარო დაწესებულების მიერ; მონაცემების დამუშავების სპეციფიკიდან გამომდინარე, აუცილებელია მასზე მუდმივი მონიტორინგის განხორციელება ან თუ საქმე გვაქვს დიდი ოდენობით მონაცემების დამუშავებასთან; მონაცემთა დამმუშავებლის საქმიანობის მთავარი ნაწილი არის დიდი ოდენობით და „სენსიტიური“ მონაცემების დამუშავება. პერსონალური მონაცემების დაცვის ოფიცერს მოეთხოვება, ჰქონდეს შესაბამისი ცოდნა, რაც დამოკიდებული იქნება იმ მონაცემებზე, რომელთა კონტროლიც მას მოუწევს.

დავიწყების უფლება - რეგულაციაში გამოყოფილია დავიწყების უფლება, რომელიც, თავისი არსით, მოიცავს მონაცემთა სუბიექტის უფლებას, მოითხოვოს მისი პერსონალური მონაცემების წაშლა ან

გამოითხოვოს მის მიერ გამოთქმული თანხმობა, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.

მონაცემთა დაცვა წინასწარ (privacy by design) - მონაცემთა დაცვის უზრუნველყოფა წინასწარ, პრევენციული ღონისძიებებით, რაც გულისხმობს ისეთი ქმედებების განხორციელებას, რომლებიც თავიდან აგვარიდებს პერსონალური მონაცემების დაცვის რეგულაციის შემდგომ დარღვევას და მონაცემების უკანონო ხელყოფასა და გამჟღავნებას. ეს ქმედებები მოიცავს: მონაცემთა დაცვის წესების არსებობას, დამუშავების რისკების შეფასებას, რეგულაციის დებულებებისა და მონაცემთა დაცვის წესების იმპლემენტაციას, ასევე, დამუშავებული მონაცემების ოდენობის შემცირებას.

ჩანაწერების წარმოება (records of processing activities) - მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებულნი არიან, აწარმოონ იმ მონაცემების აღწერა (იგივეა შინაარსით, რაც ფაილური სისტემის კატალოგი), რომლებიც მუშავდება მათ მიერ. ჩანაწერებში მოცემული უნდა იყოს ინფორმაცია მონაცემთა დამმუშავებლის (უფლებამოსილი პირის) შესახებ, მონაცემთა დამუშავების მიზანი, დამუშავებული მონაცემების კატეგორიები, მონაცემთა შენახვის ვადები და ა.შ. აღნიშნული ჩანაწერები უნდა არსებობდეს წერილობითი ფორმით, მათ შორის, ელექტრონული ფორმით. მონაცემთა დამმუშვებელმა (უფლებამოსილმა პირმა) აღნიშნული ჩანაწერები, მოთხოვნის შემთხვევაში, უნდა წარუდგინოს საზედამხედველო ორგანოს. ჩანაწერების წარმოება არ ევალებათ ორგანიზაციებს, რომელთაც ჰყავთ 250-ზე ნაკლები დასაქმებული, თუ აღნიშნული ორგანიზიაციები არ ამუშავებენ ადამიანის უფლებებისა და თავისუფლებებისათვის რისკის შემცველ მონაცემებს, დამუშავება არ არის შემთხვევითი ან მოიცავს განსაკუთრებული კატეგორიის მონაცემებს და ნასამართლობის შესახებ ინფორმაციას.

სერტიფიცირება - წევრმა სახელმწიფოებმა, საზედამხედველო ორგანოებმა, ევროკავშირის პერსონალური მონაცემების დაცვის საბჭომ და კომისიამ უნდა წაახალისონ რეგულაციის დაცვა სერტიფიცირების

მექანიზმის დანერგვით, რომლითაც შეფასდება მონაცემთა დამმუშავებლების მიერ რეგულაციის მოთხოვნების დაცვის დონე. სერტიფიკატები იქნება ნებაყოფლობითი და მათი გაცემა მოხდება გამჭვირვალე შეფასების პროცესის გავლის შემდგომ.

აღსანიშნავია, რომ რეგულაციის მოქმედება ვრცელდება სასამართლოში სამართალწარმოების პროცესში მონაცემების დამუშავებაზე, თუმცა სასამართლოს მიერ მონაცემების დამუშავების წესები შეიძლება, დამატებით განისაზღვროს ევროკავშირის წევრი სახელმწიფოს კანონმდებლობით. საზედამხედველო ორგანოების უფლებამოსილება არ გავრცელდება სასამართლოს სისტემაზე, რათა არ მოხდეს მართლმსაჯულების სისტემაზე კონტროლის განხორციელება.

აღსანიშნავია, რომ რეგულაციის მოქმედება ვრცელდება ევროკავშირის ტერიტორიაზე დარეგისტრირებულ ყველა მონაცემთა დამმუშვებელსა და უფლებამოსილ პირზე, იმისდა მიუხედავად, ხდება თუ არა პერსონალური მონაცემების დამუშავება ევროკავშირის ტერიტორიაზე. ასევე, იმ მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირების საქმიანობაზე, რომლებიც რეგისტრირებულნი არ არიან ევროკავშირის ტერიტორიაზე, მაგრამ სთავაზობენ საქონელსა და მომსახურებას ევროკავშირის ტერიტორიაზე მყოფ პირებს ან/და ახდენენ ევროკავშირის ტერიტორიაზე მყოფი პირების ქმედებათა შესწავლას (მაგალითად, ინტერნეტში აქტივობის განხორციელების შესახებ ინფორმაციის შეგროვება და პროფილის შექმნა).

1.4. სხვა ქვეყნების გამოცდილება

ამერიკის შეერთებული შტატები

პირადი ცხოვრების შესახებ კანონი ამერიკის შეერთებული შტატებში მიიღეს 1974 წელს, რომლის ძირითად ამოცანას წარმოადგენს „სახელმწიფო ორგანოების მიერ პერსონალურ მონაცემთა შემცველი მონაცემების მოპოვების, გამოყენებისა და გავრცელების რეგულირება. კანონი ვრცელდება სახელმწიფო ორგანოებზე. არ ვრცელდება ბიზნესის, კერძო

სექტორის ორგანიზაციებზე, სასამართლოებზე ან ადგილობრივ ხელისუფლებაზე. აგრეთვე, სახელმწიფო და ადგილობრივ ორგანოებზე, იმ შემთხვევაში, თუ სარგებლობენ სოციალური დაცვით. რაც შეეხება მოქალაქეებისა და მოქალაქეობის არმქონე პირთა უფლებების დაცვას, ეს კანონი იცავს „აშშ-ის მოქალაქეებს ან აშშ-ში ცხოვრების უფლების მქონე, მოქალაქეობის არმქონე პირებს, რომელთაც აშშ-ში აქვთ მუდმივი საცხოვრებელი“ (5 §552 (ა) (2). ამასთანავე, ამ კანონის მოქმედება უფრო ფართოდ ვრცელდება „ნებისმიერ პიროვნებაზე“ (5 §552 (ა)(3).

კანონის მოქმედება ვრცელდება მხოლოდ იმ შემთხვევაში, თუ „ჩანაწერი“ შეიცავს „ჩანაწერთა სისტემას“. ჩანაწერის იდენტიფიცირება შესაძლებელი უნდა იყოს ინდივიდუალურად (5. §552ა(ა)(4). ჩანაწერი უნდა ინახებოდეს „ჩანაწერების სისტემაში“, რომელიც არის ადამიანების სახელების ან სხვა იდენტიფიცირებადი ინფორმაციის შემცველი ჩანაწერების ნაკრები.

კანონი ითვალისწინებს პერსონალურ მონაცემთა შემცველი ინფორმაციის შეგროვება-შენახვის შეზღუდვას. დაწესებულებებს შეუძლიათ, ფლობდნენ „მხოლოდ ისეთ ინფორმაციას, რომელიც არის ამ დაწესებულებათა მოთხოვნებისათვის საჭირო და შესაბამისი“ (5 §552ა(ე)(1). ამასთან, თუ პირი მოითხოვს ინფორმაციას, როგორ გამოიყენება მისი პერსონალური მონაცემები, დაწესებულებამ უნდა მიაწოდოს მას ამის შესახებ საჭირო ცნობები ინდივიდუალურად. დაწესებულებებმა უნდა გამოაქვეყნონ სახელმწიფო რეგისტრაციის შენიშვნებში იმ ჩანაწერების შესახებ, რომლებსაც ისინი განახორციელებენ (5§552ა(ე)(3)-(4).

მონაცემების დაცვისათვის კანონით დადგენილია, რომ „დაწესებულებებმა, ასევე, უნდა „შეიმუშაონ შესაბამისი ადმინისტრაციული, ტექნიკური და ფიზიკური დაცვითი მექანიზმები ამ ჩანაწერების კონფიდენციალობის დაცვისათვის (5§552ა(ე)(10). მოთხოვნის საფუძველზე, პიროვნებას შეუძლია, გადახედოს თავის მონაცემებს და უზუსტობების შემთხვევაში, მოითხოვოს დაწესებულების მიერ მისი გასწორება (5 §552ა(დ).

კანონში გათვალისწინებულია ჩანაწერებზე გავრცელებული რიგი გამონაკლისები, რომლებზეც არ ვრცელდება ამ კანონის მოქმედება. ეს გამონაკლისები მოიცავს: 1) ჩანაწერებს სასამართლო ძალდატანებისა და სასამართლო დევნის გამოცხადების შესახებ; 2) ჩანაწერებს, რომელთა გავრცელებაც გათვალისწინებულია ამ კანონით; 3) ჩანაწერებს, რომლებიც მუდმივად გამოიყენება და რომელთა გამოყენებაც არ ხელყოფს იმ მიზანს, რა მიზნითაც მოხდა ამ ინფორმაციის შეგროვება დაწესებულების მიერ; 4) მოსახლეობის აღმწერი ბიუროს ჩანაწერებს; 5) იმ ჩანაწერებს, რომელთა გავრცელებაც მოხდა დაუძლეველი ძალის - ადამიანის ჯანმრთელობისა და უსაფრთხოების გამო; 6)კონგრესისათვის გადაცემა; 7) აშშ-ის მთავარი საკონტროლო-ფინანსური სამმართველოს უფროსისთვის ამ მონაცემების გადაცემა; 8) სასამართლო ბრძანებით ამგვარი ინფორმაციის გადაცემა; 9) საკრედიტო დაწესებულებებისათვის ამგვარი ინფორმაციის გადაცემა (5 §552ა(ბ). ამასთან, იმისათვის, რომ ქმედება კანონით იქნეს დასჯადად ცნობილი, მოსარჩელემ უნდა დაამტკიცოს, რომ ინფორმაცია, რომელსაც შეიცავს „ჩანაწერი“ ერთიანდება „ჩანაწერთა სისტემაში“. ამასთან, დაწესებულებამ დაარღვია კანონი თავისი მოქმედებით, ქმედება იყო „წინასწარგანზრახული, მოფიქრებული“ და მოსარჩელეს მიადგა ზიანი.[60]

აღსანიშნავია, რომ „ამერიკის შეერთებულ შტატებში სახელმწიფოთა უმრავლესობას არ აქვს პირადი ცხოვრების დაცვის შესახებ ფედერალური კანონის მსგავსი აქტები. კალიფორნიას, მასაჩუსეტს, მინესოტას, ნიუ-იორკსა და ვისკონსინის აქვთ მსგავსი კანონმდებლობა.“[61]

კალიფორნიის პრაქტიკა, სამოქალაქო სამართალი, §1798, სექტემბერი (1977) - ეს კანონი მოითხოვს, რომ დაწესებულებებმა თავიანთ ჩანაწერებში აღნიშნონ „მიზნისთვის საჭირო და შესაფერისი ან კალიფორნიის კონსტიტუციით ან სახელმწიფოს აქტებით დადგენილი“ ინფორმაცია, რაც ანაცვლებს დაწესებულებების მიერ შეგროვებულ მეორად ინფორმაციას. ეს კანონი შეიცავს ასევე, გამონაკლის შემთხვევებს, რომლითაც

[60] Solove J., & Schwartz P. M., „Privacy law Fundamentals“, Edited by the International Association of Privacy Professionals (IAPP), 2015 years, p 135-144.

[61] იგივე, p. 145-146.

ნებადართულია მეორადი ინფორმაციის გავრცელება (§1798.24). სახელმწიფო დაწესებულებების მიერ პერსონალური მონაცემების შემცველი ინფორმაციის გავრცელება/გაზიარება სახელმწიფოს გარეთ დაწესებულებებთან დასაშვებია მხოლოდ იმ შემთხვევაში, თუ კანონით ამგვარი ინფორმაციის გაცვლა გათვალისწინებულია (§1798.24(ფ). ნებისმიერ პირს შეუძლია, გამოიკვლიოს და შეასწოროს თავისი პერსონალური ინფორმაცია სააგენტოს ჩანაწერებში (§1978.32).[62]

მასაჩუსეტსის პრაქტიკა, კანონი Mass. Gen. Ann. 66ა§1 (1975) - ეს კანონი უყენებს მოთხოვნებს პერსონალური ინფორმაციის დამმუშავებელ პირებს. პერსონალური მონაცემების დამმუშავებელი პირი წარმოადგენს „დაწესებულებას, რომელიც აგროვებს, იყენებს, ასწორებს ან ავრცელებს იმ პირის პერსონალურ მონაცემებს, რომელსაც აქვს კონტრაქტი ან სხვა რაიმე შეთანხმება ამ დაწესებულებასთან“ (Mass. Gen. Ann. 66ა§1). ამგვარი ინფორმაციის დამმუშავებელი უნდა დარწმუნდეს, რომ ინფორმაციას აგროვებს კანონით გათვალისწინებული წესებით (§2 (ა). მან უნდა „მოიპოვოს ამგვარი ინფორმაცია ზუსტი, სრული, დროული, რელევანტური ქმედებითა და მიზეზით, ამ ინფორმაციის სუბიექტის ხასიათს, უფლების, შესაძლებლობების და სარგებლის ობიექტური განსაზღვრით“ (§2(ჰ). კანონი ასევე, მოითხოვს, რომ ამგვარი ინფორმაცია გამჟღავნდეს „მოთხოვნის შემთხვევაში, სასამართლო პროცესზე“ (§2 (კ).[63]

მინესოტას მთავრობის მიერ გამოცემული საკანონმდებლო აქტები პერსონალურ მონაცემებთან დაკავშირებით (13.01.1974) - აღნიშნული კანონი ვრცელდება მთავრობის ყველა იმ დაწესებულებაზე, რომელიც აგროვებს, ამუშავებს და ავრცელებს პერსონალურ მონაცემებს (§13.01(1974). სახელმწიფო დაწესებულებებმა აუცილებლად ნათლად უნდა განუმარტონ მხარეებს, თუ რა მიზნით აგროვებენ მათ პერსონალურ მონაცემებს. (§13.04(2) ეს კანონი დაწესებულებებს უფლებას აძლევს, გაავრცელონ არასაჯარო ინფორმაცია იმ შემთხვევაში, თუ ეს დაშვებულია სახელმწიფო

[62] იხ. იგივე

[63] Solove J., & Schwartz P. M., „Privacy law Fundamentals“, Edited by the International Association of Privacy Professionals (IAPP), 2015 years, p 145-146.

ან ფედერალური კანონით, ან სხვა განსაკუთრებულ შემთხვევებში“ (§13.05 (4). თავის მხრივ, მონაცემთა სუბიექტსაც შეუძლია მოითხოვოს მისი ჩანაწერების გადაცემა (§13.04(3).[64]

ნიუ -იორკის პერსონალურ მონაცემთა დაცვის შესახებ კანონი, 46§94 (1983) - სახელმწიფოს თითოეული სააგენტოსთვის ობიექტური ინფორმაციაა, „რომ შეინახოს და აწარმოოს ჩანაწერების სიტემა“ (46. ნიუ-იორკი, კანონმდებლობა §94). აღნიშნული ავალდებულებს სააგენტოს, რომ „შეაგროვოს ისეთი პერსონალური ინფორმაცია, რომელიც სააგენტოს მიზნებისათვის არის შესაფერისი და საჭირო ან განსაზღვრულია კანონით ან სავალდებულოა კანონის სპეციალური დათქმით.“ ასეთი ჩანაწერები, რომლებიც გამოიყენება „რომელიმე პერსონალური მონაცემის განსაზღვრისათვის“, აუცილებლად უნდა შეგროვდეს „ზუსტი, რელევანტური, დროული და კომპეტენტური“ ფაქტორით. მონაცემთა სუბიექტს, მონაცემთა გამოთხოვნისთანავე, უნდა ეცნობოს ინფორმაცია ამ მონაცემების მოპოვების მიზეზის შესახებ (§94 (დ). სახელმწიფო სააგენტოები უფლებამოსილნი არიან, აწარმოონ პერსონალურ მონაცემთა შემცველი მონაცემების ჩანაწერები“ (§95). კანონით აკრძალულია პერსონალური მონაცემების შემცველი ინფორმაციის გავრცელება, გარდა კანონით გათვალისწინებული გამონაკლისი შემთხვევისა (§96)[65].

ვისკონსინის მნიშვნელოვანი ინფორმაციული პრაქტიკა, კანონი, §19.62 (1991) - ეს კანონი სააგენტოებს უწესებს პერსონალური ინფორმაციის მოპოვების სპეციალურ სტანდარტებს (§19.62). ვისკონსინის კანონი ითვალისწინებს კომპიუტერების მეშვეობით ინფორმაციის მოპოვებაზე შეზღუდვებს (§19.69). ვისკონსინის კანონით. ასევე, აკრძალულია სახელმწიფოს მთავრობის ვებგვერდებიდან ინტერნეტმომხმარებლების პერსონალური მონაცემების შემცველი ინფორმაციის მოპოვება (§19.68), თუმცა, იგივე კანონი ითვალისწინებს გამონაკლისს, IP მისამართის შემთხვევაში. ასევე, აკრძალულია „პირის სახელის ან საცხოვრებელი

[64] იხ. იგივე

[65] Solove J., & Schwartz P. M., „Privacy law Fundamentals“, Edited by the International Association of Privacy Professionals (IAPP), 2015 years, p 145-146.

ადგილის ჩანაწერის გავრცელებაც, თუ ეს გათვალისწინებული არ არის კანონით“ (§19.71)[66]

სამხრეთ ამერიკა, არგენტინა - არგენტინის სახელმწიფოს კონსტიტუციის 43-ე მუხლით დაცულია პერსონალური მონაცემები („habeas data“). პიროვნებას შეუძლია, „ფლობდეს ინფორმაციას საჯარო ჩანაწერებში მის შესახებ არსებული პერსონალური მონაცემების ან სხვა პირადი ინფორმაციის შემცველი მონაცემების შესახებ.“ არგენტინა იყო პირველი ქვეყანა სამხრეთ ამერიკაში, რომელმაც მიიღო პერსონალურ მონაცემთა დაცვის შესახებ კანონი (2000 წელი). ეს კანონი ეფუძნება ევროკავშირის დირექტივას პერსონალურ მონაცემთა შესახებ, არგენტინის კონსტიტუციის რამდენიმე მუხლს და უახლეს შიდასახელმწიფოებრივ კანონმდებლობას. ამ კანონებს შორის არის წესები „habeas data“-ს დაცვითი პროცედურების შესახებ. არგენტინის პერსონალურ მონაცემთა დაცვის შესახებ კანონი კრძალავს პერსონალური მონაცემების საერთაშორისო მიმოცვლას ადეკვატური დაცვის გარეშე. 2003 წლის ივნისში, ევროგაერთიანებამ მიიღო გადაწყვეტილება, რომ არგენტინა პერსონალური მონაცემებს ადეკვატურად იცავს.[67]

შუა აღმოსავლეთი, დუბაი - დუბაიში პერსონალურ მონაცემთა დაცვის შესახებ კანონი მიიღეს 2004 წელს. არაბეთის გაერთიანებული საამიროების შვიდიდან ერთი საამირო - დუბაი შუა აღმოსავლეთის უმნიშვნელოვანესი ბიზნესცენტრია. 2007 წელს, მან გააუმჯობესა და სხვადასხვა გზებით გაამკაცრა პერსონალურ მონაცემთა დაცვის შესახებ კანონი, პერსონალურ მონაცემთა ინსპექტორის ინსტიტუტის დამოუკიდებლობის ჩათვლით. [68]

აზია, იაპონია - იაპონიის კონსტიტუციის მე-13 მუხლით დაცულია „სიცოცხლის, თავისუფლების უფლება“, 1963 წელს კი უზენაესმა სასამართლომ გამოსცა დებულება პირადი ცხოვრების დაცვის შესახებ. პერსონალურ მონაცემთა დაცვის შესახებ კანონი, რომელიც იაპონიაში 2005

[66] იგივე.
[67]იგივე, 285-286.
[68] იგივე.

წელს მიიღეს წარმომადგენლებს ავალდებულებს, მონაცემთა სუბიექტებს მიაწოდონ ინფორმაცია, თუ მათ რომელ პერსონალურ მონაცემს იყენებენ ან ამუშავებენ. ეს კანონი ასევე, ზღუდავს მესამე პირებზე ამ ინფორმაციის გავრცელებას, კანონიერი საფუძვლის გარეშე. ინფორმაციის გავრცელება დასაშვებია მხოლოდ კანონით ან ბრძანებულებით.[69]

აზია, ჩინეთი - ჩინეთს არ აქვს პირადი ცხოვრების დაცვის ერთიანი კანონი. აქ მოქმედი სამოქალაქო სამართლით დაცულია რეპუტაცია, ხოლო სისხლის სამართალი იცავს „სიტყვის გამოხატვის თავისუფლებას“. ჩინეთის ინტერნეტმომსახურების ბაზრის შესახებ კანონის რამდენიმე დებულება (2011 წელი) კრძალავს პერსონალური მონაცემების შემცველი ინფორმაციის მესამე პირებისათვის გადაცემას, შეგროვებასა და დამუშავებას სათანადო საფუძვლის გარეშე. სატელეკომუნიკაციო დაწესებულებებმა მომხმარებლებს უნდა შეატყობინონ ამგვარი ინფორმაციის გავრცელების ფაქტის შესახებ.[70]

რუსეთი - რუსეთის სახელმწიფოს კონსტიტუციის 23-ე მუხლით დაცულია „პირადი ცხოვრების, პერსონალური მონაცემებისა და ოჯახური ცხოვრების, პატივისცემისა და ღირსების უფლება“. ამ მუხლით დაცულია მიმოწერის უფლებაც. 24-ე მუხლი კრძალავს, მონაცემთა სუბიექტის თანხმობის გარეშე, პერსონალური მონაცემების შემცველი ინფორმაციის შეგროვებას, გამოყენებასა და გავრცელებას. პერსონალური მონაცემების შესახებ კანონით, რომელიც მიიღეს 2006 წელს, აკრძალულია პირადი ცხოვრების შესახებ ინფორმაციის გავრცელება და განხილულია მთავრობის ჩანაწერების სისტემის რეგულაცია.

რუსეთის პერსონალური მონაცემების დაცვის შესახებ კანონი ითვალისწინებს პერსონალური მონაცემების საზღვარგარეთ გადაცემის საკითხს. კანონი ამის უფლებას აძლევს მხოლოდ იმ სახელმწიფოებს, რომლებიც არიან პერსონალური მონაცემების დაცვის კუთხით ევროპის კონვენციის მონაწილე ქვეყნები (1981). რუსეთის კანონმდებლობით დადგენილია, რომ კომუნიკაციების სააგენტოს შეუძლია, შეადგინოს იმ

[69] იგივე.
[70] იგივე.

ქვეყნების ე. წ. whitelist-ი, რომლებისთვისაც შეეძლებათ პერსონალური მონაცემების შემცველი ინფორმაციის გადაცემა. ეს ქვეყნები აუცილებლად უნდა ითვალისწინებდნენ პერსონალური მონაცემების დაცვის ადეკვატურ შესაძლებლობას. პერსონალური ინფორმაციის გადაცემა ასევე შესაძლებელია, თუ პერსონალური მონაცემი ექვემდებარება გადაცემას.[71]

[71] იგივე.

თავი II. განსაკუთრებული კატეგორიის პერსონალური მონაცემები, ადგილობრივი კანონმდებლობა და შედარებითი ანალიზი

2.1. პერსონალური მონაცემები და მათი კატეგორიები

საქართველოს სახელმწიფოში „დამოუკიდებლობის მოპოვების შემდეგ, განსაკუთრებით 1995-2000 წლებში, საკანონმდებლო მუშაობა მთლიანად ორიენტირებული იყო ადამიანის უფლებებისა და თავისუფლებების დაცვისაკენ მიმართულ კანონშემოქმედებაზე.“[72] [41] ამ პერიოდს უკავშირდება საქართველოს კონსტიტუციის, ანუ სახელმწიფოს ძირითადი საკანონმდებლო აქტის მიღებაც, რომელიც სუბიექტის „პერსონალური მონაცემების დაცვას ცალკე უფლებად არ გამოყოფს. ის მოიაზრება პირადი და ოჯახური ცხოვრების ხელშეუხებლობის კონსტიტუციური უფლების დაცულ სფეროში“.[73] [42]

საქართველოს კონსტიტუცია, ითვალისწინებს რა, ადამიანის პირადი ცხოვრების ხელშეუხებლობის, პიროვნების განვითარების, მისი ღირსების დაცვის, მოქალაქის შესახებ სახელმწიფო დაწესებულებაში არსებული ინფორმაციის გაცნობის უფლებებსა და სახელმწიფოს ვალდებულებას, დაიცვას ოფიციალურ ჩანაწერებში არსებული ჯანმრთელობასთან, ფინანსებთან ან სხვა კერძო საკითხებთან დაკავშირებული ინფორმაცია, ამით ქმნის პერსონალურ მონაცემთა დაცვის კანონმდებლობის კონსტიტუციურ გარანტიასა და საფუძველს. საქართველოს კონსტიტუციის 41-ე მუხლის პირველი და მეორე პუნქტით დაცული სიკეთეები სხვადასხვაა. „პირველ შემთხვევაში, დაცულია დაინტერესებული პირის უფლება, მიიღოს ინფორმაცია ოფიციალური წყაროებიდან, ხოლო მეორე შემთხვევაში, პირადი მონაცემების საიდუმლოება“.[74] [43] „პირის ინტერესი, არ დაუშვას კერძო საკითხებთან დაკავშირებული ინფორმაციის გამჟღავნება

[72] გაგნიძე ე., საიქოძე ნ., „ პერსონალური მონაცემების დაცვასთან დაკავშირებული კერძო და საჯარო ინტერესის თანაფარდობა და უფლებაში ჩარევის საფუძვლიანობის კრიტერიუმები“, სტუდენტური სამართლებრივი ჟურნალი, 2016 წელი, გვ.64.

[73] იზორია ლ., ბერიაია ი. და სხვები, „საპოლიციო სამართალი“, 2015 წელი, თბილისი, შსს-ს აკადემიის გამომცემლობა, გვ.83.

[74] საღარაძე ს., „ინფორმაციის თავისუფლება და პერსონალურ მონაცემთა დაცვა“, 2014 წელი, გვ. 5.

და აკონტროლოს ამ ინფორმაციის გავრცელება, პირადი ცხოვრების ხელშეუხებლობის უფლების ერთ-ერთი უმთავრესი ასპექტია.“[75] [44] თუმცა „პირადი ცხოვრების ხელშეუხებლობის დაცვა სოციალური კონცეფციაა და მისი აღქმა მუდმივ ცვლილებებს განიცდის“,[76] [45] ამასთან, მონაცემთა „უსაფრთხოებასა და პირადი ცხოვრების ხელშეუხებლობას შორის ბალანსის დაცვა მიღწეული უნდა იქნეს სამართლიან პირობებში.“ [77] [46]

რაც შეეხება პერსონალურ მონაცემთა დაცვას, ისტორიულად, საქართველოს პარლამენტმა 2005 წლის 28 ოქტომბერს მოახდინა „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკურ პირთა დაცვის შესახებ“ ევროპის საბჭოს 108-ე კონვენციის რატიფიცირება, 2013 წლის 27 ივლისს კი განახორციელა 108-ე კონვენციის დამატებითი ოქმის რატიფიცირებაც.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მიღებულ იქნა 2011 წელს, რომელიც ნაწილობრივად ძალაში შევიდა 2012 წლის პირველ მაისს, ხოლო პერსონალურ მონაცემთა დაცვის ინსპექტორი, როგორც საზედამხედველო ინსტიტუტი, დაინიშნა 2013 წელს. ოდნავ მოგვიანებით, 2013 წლის 29 ნოემბერს, საქართველოსა და ევროპის კავშირს შორის გაფორმებული ასოცირების შეთანხმებისა და 2014 წლის 27 ივნისს ასოცირების ხელშეკრულების ხელმოწერის საფუძველზე, საქართველომ ვალდებულება აიღო, უზრუნველეყო პერსონალურ მონაცემთა დაცვის სტანდარტების შესაბამისობა პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ ევროპის საბჭოს 108-ე კონვენციასა და მის დამატებით ოქმთან, ასევე, პერსონალური მონაცემების დაცვისა და მონაცემთა გადაცემის შესახებ ევროპარლამენტისა და ევროპული საბჭოს 95/46/EC დირექტივასთან, ევროპის კავშირის 2008 წლის 27 ნოემბრის ჩარჩო გადაწყვეტილებასა (2008/977/JHA) და ევროპის საბჭოს მინისტრთა კომიტეტის № R (87) 15 რეკომენდაციასთან.

---

[75] საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406.408 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი და ,,საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“.

[76] S.D. Warren & L.D. Brandeis, ‘The Right to Privacy’, Harvard Law Review, 1890 y, p. 193

[77] Sophie Stalla-Bourdillon, Joshua Phillips, Mark D. Ryan, Privacy vs. Security, 2010 y, p. 16.

აღებული ვალდებულებების შესრულების მიზნით კი 2014 წელს, აგვისტოსა და ნოემბერში, განხორციელდა მნიშვნელოვანი საკანონმდებლო ცვლილებები „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში. თუმცა, კანონის მიღებამდე, „პირის პერსონალური ინფორმაციის დაცვა საქართველოში აქამდე სხვადასხვა კანონმდებლობით გაბნეულად რეგულირდებოდა.“[78] [47] კერძოდ, „საქართველოს ზოგად ადმინისტრაციულ კოდექსში იყო დებულებები, რომლებიც ძირითადად, ვრცელდებოდა საჯარო დაწესებულებებზე, თუმცა იყო სხვა დებულებებიც, რომლებიც დღემდე მოქმედებს. ასეთი კანონებია: საქართველოს ორგანული კანონი „კომერციული ბანკების შესახებ“, საქართველოს კანონი „პაციენტის უფლებების შესახებ“, კანონი „ზოგადი განათლების შესახებ“ და სხვა.“[79] [48]

პერსონალური მონაცემი, კანონის თანახმად, „არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს“.[80] „ეს, ერთი შეხედვით, მარტივი დეფინიციაა, მაგრამ პრაქტიკაში მისი გამოყენებისას, ხშირად ჩნდება კითხვები, თუ რა შეიძლება ჩაითვალოს პერსონალურ მონაცემად და შესაბამისად, რაზე უნდა გავრცელდეს კანონით განსაზღვრული რეგულირების წესები.“[81] ამიტომაც, საკითხის სიახლისა და განმარტების თავისებურების გამო, წინამდებარე თავში, მეტი სიცხადისათვის, წარმოდგენილი იქნება შესაბამისი განმარტებითი სიტუაციები და მაგალითები.

ტერმინი „პერსონალური მონაცემი“ მოიცავს მონაცემთა საკმაოდ ფართო სპექტრს და გულისხმობს ნებისმიერი სახის მონაცემს, რომელიც უკავშირდება ფიზიკურ პირს. იმისთვის, რომ მონაცემი ჩაითვალოს პერსონალურ მონაცემად, იგი უნდა იძლეოდეს პირის პირდაპირი ან

[78] ქვაკუთხედი, ეროვნულ-სარწმუნოებრივი ჟურნალი, თბილისი, 2011 წელი, №1(52), გვ.10

[79] სამეცნიერო-პრაქტიკული ჟურნალი თემიდა №6(8), მოსახლიშვილი ლ., სტატია - „პერსონალური მონაცემების დაცვის კანონდებლობა საქართველოში“, 2012 წელი, გვ. 78.

[80] საქართველოს კანონი “პერსონალურ მონაცემთა დაცვის შესახებ“, 28.12.2011 წელი, მუხლი 2 (ა).

[81]„ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე“, სატიათა კრებული, კორკელია კ.-ს რედაქტორობით, საგინაშვილი ნ., „პესრონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა“, თბილისი, 2015 წელი, გვ.169.

არაპირდაპირი გზით იდენტიფიკაციის საშულებას. ფიზიკური პირის იდენტიფიკაცია შეიძლება სხვადასხვა საშუალებით, უმეტეს შემთხვევაში იდენტიფიკაცია ხდება სახელის, გვარის, პირადი ნომრის, მართვის მოწმობის საშუალებით, თუმცა შესაძლოა, სხვა, უფრო რთული საშუალებები იყოს გამოყენებული, როგორიცაა ფიზიკური მახასიათებლები, თითის ანაბეჭდი, დნმ-ის კოდი, საბანკო ანგარიშის ნომერი და სხვა. „თუმცა არის მთელი რიგი სიტუაციები, როდესაც პირის ვინაობის დაკონკრეტების გარეშეც შეიძლება მოხდეს მისი ამოცნობა. მაგალითად, ქვეყნის დღევანდელი პრეზიდენტი. ამ შემთხვევაში, პირის პერსონალური მონაცემია პირის თანამდებობა. დამნაშავის ავტორობოტის შექმნისას, პირის იდენტიფიცირების მთავარი საშუალებაა მისი გარეგნობა. შესაძლოა, პირის სახელი და გვარი არც იყოს ცნობილი. ამ შემთხვევაში, მისი პერსონალური მონაცემი არის პირის გარეგნული აღწერილობა.

იდენტიფიცირება მნიშვნელოვნად არის დამოკიდებული თითოეული შემთხვევის კონკრეტულ გარემოებებზე. ერთი და იგივე მონაცემი ერთ შემთხვევაში, შეიძლება ჩაითვალოს პერსონალურ მონაცემად, სხვა შემთხვევაში - არა. მაგალითად, მანქანის სანომრე ნიშანი, ცალკე აღებული, არ არის პერსონალური მონაცემი, მაგრამ იგივე სანომრე ნიშანი პოლიციის ხელში, რომელიც ფლობს შესაბამის ბაზას და შეუძლია, ამ ნომრით მისი მფლობელის ამოცნობა, უკვე პერსონალური მონაცემია,“[82] შესაბამისად, იდენტიფიცირება დამოკიდებულია გონივრულ და არა მაინცადამაინც მაღალტექნოლოგიურ და ტექნიკურ საშუალებებზე. ამასთან, „არანაირი შეზღუდვა არ არსებობს - რითაც შეგვიძლია დავადასტუროთ, რომ ეს მონაცემი უკავშირდება ადამიანს, არის პერსონალური მონაცემი, მთავარი ფიგურა არის ადამიანი. პერსონალური მონაცემები აქვს ადამიანს, იურიდიულ პირს კი აქვს სხვა ტიპის მონაცემები.“[83] თუმცა, „საერთაშორისო საკანონმდებლო პრაქტიკა იმაზეც მეტყველებს, რომ პერსონალურ

[82] იგივე, გვ.172.

[83] ჟურნალი „თბილისელები“, ხაჩიძე ნ., „როგორ გროვდება ადამიანის პერსონალური მონაცემები, სად ინახება ისინი და რა უნდა ვიცოდეთ იმისთვის, რომ თავიდან ავიცილოთ ჩვენივე მონაცემების ბოროტად გამოყენება“, 31.03.14-06.04.14., №13 (692).

მონაცემთა ცნება იურიდიულ პირებზეც ვრცელდება. ამ მხრივ საინტერესოა ისლანდიის 1989 წლის კანონი პერსონალურ მონაცემთა რეგისტრაციის შესახებ“, რომლის მიხედვითაც, პერსონალურ მონაცემებს ეკუთვნის ცნობები ინდივიდის, კომპანიის თუ სხვა იურიდიული პირების ფინანსური თუ სხვაგვარი საქმიანობის შესახებ, რომელიც საიდუმლოდ უნდა ინახებოდეს.“[84] [49]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ცალკე განსაკუთრებული კატეგორიის დეფინიციით გამოყოფს და სპეციალურ გარანტიებს ადგენს იმგვარი პერსონალური მონაცემების მიმართ, რომლებიც დაკავშირებულია „პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან. ეს მონაცემები, ისევე, როგორც გარკვეული სახის ბიომეტრიული მონაცემები, მათი სენსიტიური ხასიათიდან გამომდინარე, განეკუთვნება განსაკუთრებულ კატეგორიას, ვინაიდან ამ ტიპის მონაცემთა უკანონოდ შეგროვება, შენახვა ან გავრცელება შესაძლოა, ქმნიდეს პირადი ცხოვრების ხელყოფის, ადამიანის დევნის, შევიწროების ან სხვაგვარი დისკრიმინაციის საფრთხეს. აღსანიშნავია ისიც, რომ „განსაკუთრებული კატეგორიის მონაცემთა არასწორმა გამოყენებამ (მაგალითად, როგორიცაა ჯანმრთელობის ან სექსუალური ორიენტაციის შესახებ ინფორმაცია), განსაკუთრებით კი მისმა საჯაროდ გავრცელებამ, შესაძლოა, გამოუსწორებელი და ძალზე ხანგრძლივი შედეგები გამოიწვიოს, როგორც სუბიექტისათვის, ისე სოციალური გრემოსათვის.“[85] [50] სწორედ

[84]ცაცანაშვილი მ., „ინფორმაციული სამართალი“, 2004 წელი, გვ.106.

[85] Articls 29, Data Protection Working Party, Advice paper on special categories of data (“sensitive data”), 2011, p. 4, see: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-

ამიტომაცაა ხაზგასასმელი ის გარემოება, რომ „განსაკუთრებული კატეგორიის მონაცემთა დამუშავება უნდა მოექცეს მკაცრ სამართლებრივ რეჟიმში“ [86] [51] და მისი დამუშავება „უნდა მოხდეს მხოლოდ მკაცრად განსაზღვრულ შემთხვევებში.“[87] [52]

აღსანიშნავია, ის ფაქტიც, რომ პერსონალურ მონაცემთა დაცვაზე ზოგადი ადმინისტრაციული კოდექსის მოწესრიგება, რომელიც 2012 წელს გაუქმდა, ასევე „კრძალავდა საჯარო დაწესებულების მიერ იმგვარი პერსონალური მონაცემების დამუშავებას, რომელიც დაკავშირებულია პირის რელიგიურ, სექსუალურ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ ან მსოფლმხედველობრივ შეხედულებებთან.“[88] [53]

რაც შეეხება ბიომეტრიულ მონაცემს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „გ“ ქვეპუნქტი ცალკე გამოყოფს ამ მონაცემების კატეგორიას და მიუთითებს, რომ ბიომეტრიული მონაცემი არის „ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი).“ ამასთან, ბიომეტრიული მონაცემი განსაკუთრებული კატეგორიის პერსონალურ მონაცემად შეიძლება ჩაითვალოს მხოლოდ იმ შემთხვევაში, როდესაც ის იძლევა ფიზიკური პირის იდენტიფიცირების საშუალებას განსაკუთრებული კატეგორიის მონაცემის ნიშნით, როგორიცაა რასობრივი

---

document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[86] Handbook on European data protection law, Council of Europe, 2014, p. 81, see: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[87] Louise Wiseman, Jenny Gordon, Data protection: Guidelines for the use of personal data in system testing, Second edition, 2009, p. 2, see: http://shop.bsigroup.com/upload/Shop/Download/Books/BIP0002sample.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში]

[88] „ადმინისტრაციული სამართლის პრობლემები“, სტატიათა კრებული, გიორგაძე ლ. -ს საერთო რედაქტორობით, ცანავა ლ., „პერსონალურ მონაცემთა დამუშავებისა და საჯაროობის სამართლებრივი მოწესრიგება“, დავით ბატონიშვილის სამართლის ინსტიტუტის გამომცემლობა, 2013 წელი, გვ.63.

ან ეთნიკური კუთვნილება, ჯანმრთელობის მდგომარეობა, ნასამართლობა და სხვა. ბიომეტრიული მონაცემი დაკავშირებულია ფიზიკურ პირთან, არის მუდმივი, უნიკალური, იძლევა პირის ზუსტი და უტყუარი იდენტიფიცირების საშუალებას, სწორედ ამიტომ კანონი ცალკე მუხლად არეგულრებს საჯარო და კერძო დაწესებულების მიერ ბიომეტრიული მონაცემების დამუშავების მიზნებს.

პერსონალურ მონაცემთა დაცვის ინპექტორის აპარატის მიერ მომზადებულ რეკომედაციაში[89] აღნიშნულია, რომ „საჯარო დაწესებულების მიერ ბიომეტრიულ მონაცემთა დამუშავება შეიძლება მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნებისათვის, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით, თუ აღნიშნული მიზნის მიღწევა სხვა საშუალებებით შეუძლებელია, ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. მაგალითად: საჯარო დაწესებულების მიერ თანამშრომელთა შენობაში შესვლისა და გასვლის კონტროლი (დასაქმებულთა მხრიდან სამსახურში გამოცხადების აღრიცხვის მიზნით), თითის ანაბეჭდის გამოყენებით, ცალსახად ჩაითვლება არაადეკვატურ და არაპროპორციულ საშუალებად. შესაბამისად, დასაქმებულის კონტროლის მიზნებისათვის ბიომეტრული მონაცემების დამუშავება არამართლზომიერია. თუმცა, თითის ანაბეჭდის გამოყენებით ფიზიკური შეღწევა შენობის იმ კონკრეტულ ნაწილში/ფლიგელში, სადაც ინახება საიდუმლოების შემცველი ინფორმაცია, ჩაითვლება მიზნის მიღწევის პროპორციულ საშუალებად. [54] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-9 მუხლის მეორე პუნქტის თანახმად, კანონიერად მიიჩნევა ბიომეტრიულ მონაცემთა დამუშავება პირადობის დამადასტურებელი დოკუმენტის გაცემის ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიკაციის მიზნებისათვის.“[90] სწორედ, ბიომეტრული მონაცემების სენსიტიური ბუნების გამო, მონაცემთა

[89] „რეკომენდაციები ბიომეტრიულ მონაცემების დამუშავების შესახებ“, გვ.3. ხელმისაწვდომია: www.pdp.ge

[90] „რეკომენდაციები ბიომეტრიულ მონაცემთა დაცვის შესახებ“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ხელმისაწვდომია: www.pdp.ge.

დამმუშავებლებმა მის მიმართ უნდა გამოიჩინონ განსაკუთრებული სიფრთხილე და მიიღოს შესაბამისი დაცვის ზომები.[91] [55]

კანონი გენეტიკურ მონაცემსაც გასაზღვრავს და ასეთად მიიჩნევს „მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემი გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება.“[92] მოცემული განმარტება მსგავსია ბიომეტრიული მონაცემების განმარტების, თუმცა არ არის ერთნაირი. „გენეტიკური მონაცემი გარდა იმისა, რომ მუდმივი და უნიკალურია, და უკავშირდება ფიზიკურ პირს შეიცავს ინფორმაციას ერთდროულად რამდენიმე პირის შესახებ და იძლევა მათი იდენტიფიცირების საშუალებას (მაგალითად, ოჯახის ბიოლოგიური წევრების, სისხლით ნათესავების, მომავალი და წარსული თაობების, რაც მნიშველოვნად ამარტივებს ამოცნობის პროცესს“[93]. [56]

ბიომეტრიულ და გენეტიკურ მონაცემებთან დაკავშირებით დაზუსტებას საჭიროებს შემდეგი გარემოება: „იმის გარკვევისას მონაცემი მიეკუთვნება თუ არა განსაკუთრებულ კატეგორიას, განმსაზღვრელია დეფინიციის ნიშნების ჩამონათვალი და, არა ის, მონაცემი ბიომეტრიულია, გენეტიკურია თუ არა. ეს საკითხი აქტუალობას იძენს ეთნიკური ნიშნის საფუძველზე პირთა გარეგნობის მიხედვით გამორჩევისას. მაგალითად, თუ სამოდელო სააგენტოში პირთა შერჩევა ხორციელდება პირთა მახასიათებლების მიხედვით (ბიომეტრული მონაცემი) აქ განსაკუთრებული არაფერია, მაგრამ თუ შერჩევის პროცესში გარეგნული მახასიათებლების დაკავშირება ხდება ეთნიკურ წარმომავლობასთან, ასეთ შემთხვევაში, პირის იდენტიფიცირების მიზნიდან გამომდინარე, ბიომეტრიული მონაცემი

---

[91] Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective (2nd Edition), Offi ce of the Privacy Commissioner for Personal Data, Hong Kong, 2010, p. 44, see: https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[92]„ პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მუხლი 2 (გ[1])

[93] Article 29, Data Protection Working Party, Working Document on Genetic Data,WP 91, 2004, see: http://ec.europa.eu/;

მიეკუთვნება სენსიტიური მონაცემების კატეგორიას.“[94] ამასთან, „ზოგიერთი გენეტიკური მონაცემი, როგორიცაა გენეტიკური შეუთავსებლობა და სერიოზული დაავადებებისადმი მიდრეკილება, განსაკუთრებულად მგრძნობიარე ბუნებით ხოლო ისეთი გენეტიკური ინფორმაცია, როგორიცაა სქესი, თვალისა და თმის ფერი ნაკლებ მგრძნოებიარე ხასიათისაა, თუმცა შესაძლოა შეიცვალოს ამ ინფორმაციისადმი დამოკიდებულება. მაგალითად: ემბრიონის სქესთან დაკავშირებული ინფორმაცია ზოგიერთ მშობელს არ მიეწოდება და დაცულია მისი კონფიდენციალურობა[95] [57] ვინაიდან ხშირია მშობლებისთვის არასასურველი სქესის ბავშვის ჩასახვისას აბორტის პრეცენდენტები. ხოლო, ადამიანის უჯრედული ქსოვილის დნმ-ის ნიმუში, როგორც პირის ინდივიდუალურობას განმსაზღვრელი, ყოველთვის კონფიდენციალურად იქნება მიჩნეული, რადგან მას შეუძლია „გაამჟღავნოს ისეთი ,,ოჯახური საიდუმლობები“, როგორიცაა მამობის დადგენა და შვილად აყვანა“.[96] [58]

„მრავალმა ქვეყანამ აამოქმედა კანონები მონაცემთა დაცვის თუ პირადი ცხოვრების ხელშეუხებლობის შესახებ“.[97] [59] თუ გადავხედავთ სხვა ქვეყნების ეროვნულ კანონმდებლობას განსაკუთრებული კატეგორიის პერსონალური მონაცემების ანუ ე.წ. „სენსიტიური“ მონაცემების დეფინიციასთან დაკავშირებით, ნორვეგიის პერსონალურ მონაცემთა დაცვის აქტის (2000 წლის 14 აპრლი) მე-2 მუხლი ასეთი კატეგორიის პერსონალურ მონაცემად მიიჩნევს „ინფორმაციას, რომელიც უკავშირდება რასობრივ და ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებას, ფილოსოფიურ ან რელიგიურ მრწამსს, პირის ეჭვმიტანილად ან/და ბრალდებულად ყოფნის, დამნაშავედ ცნობისა და მსჯავრდების შესახებ

---

[94] „ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე“, სატიათა კრებული კორკელია კ. რედაქტორობით, საგინაშვილი ნ., „პესრონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა“, თბილისი, 2015 წ, გვ.175.

[95] Who Owns Our Genes?": Proceedings of an international conference, by Nordic Committee on Bioethics, Tallin, October, 1999, p. 78.

[96] Stefanick L., Controlling knowledge: Freedom of Information and Privacy Protection in a Networked World, Canada, AU Press, 2011. p. 101.

[97] ბორნი ჰ.,უილსი ა., „დაზვერვის სამსახურებზე ზედამხედველობის განხორციელება“, 2012 წელი, გვ.162.

მონაცემებს, ასევე ჯანმრთლობასთან, სექსუალურ ცხოვრებასთან და სავაჭრო კავშირის წევრობასთან დაკავშირებული ინფორმაციას.“[98] [60] დიდი ბრიტანეთის პერსონალურ მონაცემთა დაცვის აქტით (1988 წელი) ასეთ კატეგორიის პერსონალურ მონაცემად ითვლება ის პერსონალური მონაცემი, რომელიც შეიცავს ინფორმაციას მონაცემთა სუბიექტის რასობრივი ან ეთნიკური კუთვნილების შესახებ, პოლიტიკური შეხედულების შესახებ, რელიგიური რწმენის ან მსგავსი რწმენის შესახებ, სავაჭრო კავშირის წევრობის შესახებ, ფიზიკური ან ფსიქიკური ჯანმრთელობის მდგომარეობის შესახებ, სექსუალური ცხოვრების შესახებ, სუბიექტის მხრიდან დანაშაულის/სავარაუდო დანაშაულის ჩადენისა და მსჯავრდების შესახებ, ინფორმაციას ნებისმიერი სამართალწარმოების შესახებ, რომელიც შეეხება სუბიექტის მხრიდან დანაშაულის/შესაძლო დანაშაულის ჩადენას და საპროცესო შედეგების დადგომის ან მსჯავრის დადების შესახებ.“[99] [61] იტალიის მონაცემთა დაცვის კოდექსის მე-4 მუხლის თანახმად, სენსიტიური კატეგორიის მონაცემად ითვლება ის პერსონალური მონაცემი, რომლის გამჟღავნებაც იძლევა პირის რასობრივი, ეთნიკური წარმოშობის, რელიგიის, ფილოსოფიური ან სხვა მრწამსის, პოლიტიკური შეხედულების, პარტიის წევრობის, სავაჭრო კავშირის, ფილოსოფიური, პოლიტიკური, რელიგიური თუ სავაჭრო ხასიათის ასოციაციების/ორგანიზაციების წევრობის შესახებ ინფორმაციას, ასევე ინფორმაციას, რომელიც ჯანმრთელობასა და სექსუალურ ცხოვრებას უკავშირდება.“[100] [62]

დასკვნის სახით შეიძლება ითქვას, რომ პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში „განსაკუთრებული კატეგორიის

---

[98] ნორვეგიის პერსონალურ მონაცემთა დაცვის აქტი (2000 წლის 14 აპრლი), ხელმისაწვდომია: https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[99] დიდი ბრიტანეთის პერსონალურ მონაცემთა დაცვის აქტი (1988 წელი), ხელმისაწვდომია: http://www.legislation.gov.uk/ukpga/1998/29/section/2, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[100] იტალიის მონაცემთა დაცვის კოდექსი (2003 წელი), ხელმისაწვდომია: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

პერსონალურ მონაცემების დეფინიცია თეორიულად თითქმის სრულად ასახავს ევროპის საბჭოსა და ევროკავშირის დოკუმენტებით განსაკუთრებული დაცვას მიკუთვნებულ „სენსიტიურ“ პერსონალური მონაცემების ჩამონათვალს.

2.2. განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების პრინციპები

„პერსონალური მონაცემების დაცვის მაღალ სტანდარტს მონაცემთა დამუშავების პრინციპების დაცვა, მკაფიოდ განსაზღვრული მიზნითა და სამართლებრივი საფუძვლით მონაცემთა დამუშავება განაპირობებს.“[101] „სიტყვა „პრინციპი“ (Principium) ლათინური წარმოშობისაა და „საწყისს“ „საფუძველს“ ნიშნავს, იგი განმარტებულია როგორც სახელმძღვანელო იდეა, რომელიც ერთგვარი გარანტორია ზოგადი წესების დამკვიდრების თვალსაზრისით.“[102] [63] ძირითადი პრინციპებს, რომელთა დაცვის ვალდებულებაც საქართველოს საჯარო სექტორში ყველა მონაცემთა დამმუშავებელსა ან მის უფლებამოსილ პირს გააჩნია, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაზღვრავს და პერსონალური მონაცემების ყველა კატეგორიის, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის, დადგენილ ეროვნულ სტანდარტს წარმოადგენს. მათ შორის ერთ-ერთია **განსაკუთრებული კატეგორიის მონაცემების სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად დამუშავება.** „ტერმინი „კანონიერი“ გულისხმობს ზოგადად ქვეყნაში მოქმედ კანონმდებლობასა და საერთაშორისო ხელშეკრულებებს. მიუხედავად იმისა, რომ მონაცემთა დამუშავების პროცესი შესაძლოა სრულად შეესაბამებოდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დებულებებს, შესაძლოა დაირღვეს კანონიერების

[101] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის ანგარიში, ხელმისაწვდომია:www.pdp.ge.

[102] თათია ცეცხლაძე, სამაგისტრო ნაშრომი „ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემის დაცვა სადაზღვევო სფეროში“, კავკასიის უნივერსიტეტი, 2017 წელი, გვ. 33-34.

პრინციპი. კანონიერებისა და სამართლიანობის უზრუნველყოფა მონაცემთა დამუშავების პროცესში მნიშვნელოვნად არის დამოკიდებული პერსონალური მონაცემების მოპოვების გზებზე, იმაზე თუ რამდენად კანონიერად ხდება ინფორმაციის შეგროვება. თუ პერსონალური მონაცემები შეგროვებულია შესაბამისი საფუძვლის გარეშე, ხდება კანონიერებისა და სამართლიანობის პრინციპის დარღვევა. არის შემთხვევები, როდესაც მონაცემთა შეგროვება მონაცემთა სუბიექტების გარკვეული ჯგუფის მიმართ ხდება ერთი და იგივე მეთოდით, თუმცა ამა თუ იმ მონაცემთა სუბიექტის შესახებ ინფორმაციის მოპოვება უკანონოა, დანარჩენების მიმართ კი კანონიერი.

მონაცემთა დამუშავების პროცესში კანონიერებისა და სამართლიანობის პრინციპი მოიცავს ისეთ საკითხის შეფასებასაც, როგორიცაა მონაცემთა სუბიექტზე მონაცემთა დამუშავების პროცესის უარყოფითი გავლენა. იმისათვის რომ აღნიშნული უარყოფითი გავლენა ჩაითვალოს კანონიერად და სამართლიანად, ის უნდა იყოს დასაბუთებული. მაგალითისათვის, პერსონალური მონაცემების დამუშვებას, რომელიც ხორციელდება საგზაო მოძრაობის წესების დაცვის მიზნით, შესაძლოა მოჰყვეს პიროვნებისათვის ადმინისტრაციული პასუხისმგებლობის დაკისრება, ამას, თავის მხრივ უარყოფითი გავლენა აქვს მონაცემთა სუბიექტზე. თუმცა, აღნიშნული უარყოფითი გავლენა არის დასაბუთებული საზოგადოებრივი წესრიგის დაცვის და უსაფრთხოების უზრუნველყოფის საჭიროებით და, შესაბამისად, ვერ იქნება მიჩნეული უკანონოდ და უსამართლოდ.“[103]კანონიერებისა და სამართლიანობის პრინციპთან ერთად უმნიშვნელოვანესი გარემოებაა, რომ პერსონალური მონაცემების დამუშავება განხორციელდეს პიროვნების ღირსების შეულახავად.

განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას **მონაცემთა დაუშავებლის ვალდებულებას წარმოადგენს, მონაცემები დაამუშაოს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი**

[103] „პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.17-18.

მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან შეუთავსებელი მიზნით;

აღნიშნული პრინციპი უნდა განვიხილოთ შემდეგი კომპონენტების გათვალისწინებით: პერსონალური მონაცემების დამუშავების მიზანი, მონაცემების მოცულობის განსაზღვრა და კონკრეტული სუბიექტი/სუბიექტთა ჯგუფი, რომლის მონაცემთა დამუშავებაც ხდება.

მონაცემთა დამუშავების შინაარსის და მოცულობის პროპორციულობა და ადეკვატურობა დამოკიდებულია მონაცემების დამუშავების მიზანზე. შესაბამისად, ძალიან მნიშვნელოვანია პერსონალური მონაცემების დამუშვების კონკრეტული მიზნის განსაზღვრა. ეს არის „ე.წ. „მონაცემთა მინიმიზაციის“ პრინციპი - მონაცემთა დამმუშავებელმა არ უნდა დაამუშავოს იმაზე მეტი მონაცემი ვიდერე საჭიროა დამუშავების მიზნის მისაღწევად. გარდა ამისა, მის მიერ შენახული მონაცემები არ უნდა შეიცავდეს საჭიროზე მეტ დეტალებს. ადეკვატურობისა და პროპორციულობის პრინციპიც კავშირშია ასევე კონკრეტულ ინდივიდთან, თუ მონაცემთა დამმუშავებელს სჭირდება ინფორმაცია კონკრეტული პირის შესახებ, არაადეკვატურია სხვა პირების შესახებ იმავე მონაცემების ამ მიზნით შეგროვება. მაგალითისათვის, დამსაქმებელი დასაქმებულებს სთხოვს, რომ მიაწოდონ ინფორმაცია სისხლის ჯგუფის შესახებ, რადგან ზოგიერთი მათგანი აყვანილია იმ სამუშაოზე, რომელიც შეიცავს ჯანმრთელობის დაზიანების რისკს. ამ შემთხვევაში სისხლის ჯგუფის შესახებ ინფორმაციის მოთხოვნა საჭიროა, თუმცა სხვა თანამშრომლების მიმართ, რომლებიც მხოლოდ საოფისე სამუშაოს ასრულებენ, იგივე მოთხოვნის დაწესება არაპროპორციული და არაადეკვატურია.“[104]

მონაცემები არ უნდა ინახებოდეს და მუშავდებოდეს ისეთი ზოგადი მიზნით, როგორიცაა „მომავალში შეიძლება გამომადგეს“. თუმცა, ინფორმაციის შენახვა შესაძლებელია ისეთი შემთხვევებისთვის, რომელთა დადგომის დიდი ალბათობაც არსებობს. მაგალითისათვის, სისხლის

[104] იხ. იგივე, გვ. 18-19.

ჯგუფის შესახებ მონაცემების შეგროვება დამსაქმებლის მიერ ხდება ჯანმრთელობის დაზიანების შემთხვევისათვის, რომლის დადგომის ალბათობა გამომდინარეობს სამუშაოს სპეციფიკიდან, თუმცა შეიძლება ამ შემთხვევას ადგილი არც ჰქონდეს.

მნიშვნელოვანია, რომ შეგროვებული მონაცემები ნამდვილი და ზუსტი იყოს და, საჭიროების შემთხვევაში, აუცილებლად განახლდეს. ამ პრინციპის დაცვისთვის „მონაცემთა დამმუშავებელმა უნდა მიიღოს ყველა საჭირო ზომა, რომ უზრუნველყოს შეგროვებული ინფორმაციის სანდოობა და სიზუსტე, ასვეე საჭიროებისამებრ მათი განახლება. საჯარო უწყებამ ყურადღება უნდა გაამახვილოს მონაცემების სწორად ასახვაზე, ვინაიდან ერთი და იგივე ინფორმაცია შეიძლება იყოს ზუსტიც და ამასთან არაზუსტიც, მითითებისას არსებული სხვაობის გამო. მაგალითად, თუ პიროვნებამ კომპანიას დაუკვეთა პროდუქცია და ამ უკანასკნელმა შეინახა მისი პერსონალური მონაცემები (მისამართი, ტელეფონის ნომერი) შესაძლო საჩივრის შემთხვევაში პირის იდენტიფიკაციის მიზნით, კომპანის არ წარმოეშობა ვალდებულება სისტემატიურად ამოწმოს პირი იმავე მისამართზე ცხოვრობს თუ არა და ამ მიზინით განაახლოს მის ხელთ არსებული ინფორმაცია, რასაც ვერ ვიტყვით საჯარო ორგანიზაციების მიერ მონაცემთა დამუშავებაზე.“[105] ამასთან, „განახლებული მონაცემების ქონა მნიშვნელოვანია, რადგან ხშირად იცვლება დამუშავების გარემოებები.“ [106] [64]

არაზუსტი ან არასწორი მონაცემების ჩასწორება არ ნიშნავს, რომ ყველა შემთხვევაში უნდა წაიშალოს არასწორი მონაცემები და განადგურდეს. მონაცემების ისტორიული, სტატისტიკური და კვლევის მიზნებისათვის დამუშვებისას მისმა განახლებამ შესაძლოა უარყოფითი შედეგი იქონიოს და აზრიც კი დაუკარგოს პერსონალური მონაცემები

[105] იხ. იგივე, გვ.19-20

[106] Arthur J. Winfield, Judith Rees, Ian Smit, Pharmaceutical Practice, 2009, see: https://books.google.ge/books?id=G0lZEGZi9SMC&pg=PT489&lpg=PT489&dq=sensitive+personal+data+book&source=bl&ots=CXPbFwpXGu&sig=EMUJJJb6-NknQ3rVTSN7UB9H7ms&hl=en&sa=X&ved=0ahUKEwjSs8XOvMHTAhVD1BoKHW19Dcs4ChDoAQhAMAU#v=onepage&q=sensitive%20personal%20data%20book&f=false [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

შენახვის მიზანს. მაგალითისათვის, „სამედიცინო ისტორიაში ახალი დიაგნოზის დასმის შემდეგ ძველი არასწორი სამედიცინო დიაგნოზის ჩანაწერის დატოვება აუცილებელია, რადგანაც აიხსნას იმ მკურნალობის დანიშვნის საფუძველი, რაც მანამდე პირის მიმართ მიმდინარეობდა. ზოგიერთ შემთხვევაში, მონაცემთა ჩასწორებისას აუცილებელია მითითება მომხდარი შეცდომის შესახებ. ასევე, მაგალითისათვის, თუ პიროვნებას დამსაქმებლის მიერ გამოეცხადა საყვედური და მოხდა მისი ხელფასიდან თანხის დაქვითვა, მაგრამ შემდეგ გაირკვა რომ მოხდა შეცდომა და დასაქმებულს თანხა უკან დაუბრუნდა. კომპანიის ანგარიშზე თანხის მოძრაობის ასახსნელად აუცილებელია ჩანაწერის დატოვება და დასაქმებულის მიმართ ადმინისტრაციული ღონისძიების გამოყენების შესახებ იმის მითითება, რომ მოხდა შეცდომა.“[107] კანონით მონაცემთა სიზუსტესა და ნამდვილობაზე პასუხისმგებლობა ეკისრება მონაცემთა დამმუშავებელს.

მონაცემთა დამუშავების პროცესში აუცილებელია, რომ **განსაკუთრებული კატეგორიის პერსონალური მონაცემები შენახონ მხოლოდ იმ ვადით, რომელიც საჭიროა მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს ან შენახული უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით, თუ კანონით სხვა რამ არ არის დადგენილი.** ეს პრინციპი არ განსაზღვრავს პერსონალური მონაცემების შენახვის ზუსტ ვადას და ასეთად განიხილავს იმ ვადას, რაც დამოკიდებულია მონაცემთა დამუშავების მიზანზე. მაგალითისათვის, სასტუმროში გაკეთებული ვიდეო ჩანაწერი ადმინისტრაციამ შეიძლება შეინახოს ხანმოკლე ვადით, რადგან ვიდეოთვალთვალის სისტემა, როგორც წესი, დამონტაჟებულია უსაფრთხოების უზრუნველყოფის მიზნით; ხოლო ბანკებში ბანკომატთან დამონტაჟებული ვიდეოკამერის მიერ დაფიქსირებული ვიდეოჩანაწერი

[107] „პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.20.

რეკომენდირებულია შეინახონ უფრო ხანგძლივი დროის განმავლობაში, რადგან საეჭვო ტრანზაქციის განხორციელების შემთხვევაში მის გამოვლენას შესაძლოა დრო დასჭირდეს.

„მონაცემთა ვადაზე ადრე წაშლამ, მათი დამუშავების მიზნიდან გამომდინარე, ასევე შესაძლოა გამოიწვიოს პრობლემა, თუმცა დიდი ხნის განმავლობაში მონაცემთა შენახვაც მოიცავს ისეთ რისკებს, როგორიცაა მოძველებული ინფორმაციის გამოყენებისას შეცდომის დაშვების რისკი, რადგან გარკვეული დროის გასვლა მონაცემთა სიზუსტის დადგენას ართულებს. ასევე, თუ უწყება საჭიროზე მეტი მონაცემებს ინახავს, მონაცემთა სუბიექტის მოთხოვნის შემთხვევაში იგი ვალდებულია ამ უკანასკნელს მიაწოდოს ყველა მის ხელთ არსებული მონაცემი, რაც საჯარო უწყების მხრიდან ასევე საჭიროებს დამატებით რესურსსა და ძალისხმევას.“[108]

თუკი შევადარებთ ევროპულ და ეროვნულ კანონმდებლობას განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის დადგენილი პრინციპების მხრივ, თავისუფლად შეიძლება ითქვას, რომ „საქართველოს კანონის მე-4 მუხლში მოცემული პრინციპები თანხვედრაშია კონვენციის მე-5 მუხლში მოცემულ პრინციპებთან (და ევროკავშირის დირექტივის მე-6 მუხლთან). პირველი პრინციპი, რომ პერსონალური მონაცემები „დამუშავებული უნდა იყოს სამართლიანად და კანონიერად“ მოცემულია კონვენციის მე–5 მუხლის ა ქვეპუნქტში და საქართველოს კანონის მე–4 (ა) მუხლში. კონვენციის მე–5 (ბ) მუხლი და საქართველოს კანონის მე–4 (ბ) მუხლი ეხება განსაზღვრული მიზნიდან გამომდინარე მონაცემების დამუშავების პრინციპს, რაც პერსონალურ მონაცემთა დაცვის ევროპული კანონის კიდევ ერთი ქვაკუთხედია. კონვენციისა და სხვა დოკუმენტების დამატებითი პრინციპები მოიცავს: (1) დამუშავებულ მონაცემთა კატეგორიების შეზღუდვას მხოლოდ აბსოლუტური აუცილებლობისთვის და (2) ზუსტი მონაცემების შენახვის ვალდებულებას, სადაც საჭიროა განახლებული

[108] „პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.21.

სახით. ეს პრინციპები განმეორებულია პერსონალურ მონაცემთა დაცვის საქართველოს კანონის მე–4 (გ), (დ) მუხლში.“[109]

2.3. განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების საფუძვლები

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას აუცილებლად უნდა შევეხოთ ორ ისეთ მნიშვნელოვან საკითხს, როგორიცაა მონაცემთა დამუშავება და კანონის გავრცელების ფარგლები. აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმდება ვრცელდება საქართველოს ტერიტორიაზე ავტომატური ან ნახევრად ავტომატური საშუალებებით მონაცემთა დამუშავებასა და აგრეთვე არაავტომატური საშუალებებით იმ მონაცემთა დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შეტანის მიზნით მუშავდება. ასევე, დანაშაულის თავიდან აცილებისა და გამოძიების, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისათვის სახელმწიფო საიდუმლოებისთვის მიკუთვნებულ მონაცემთა ავტომატურ დამუშავებაზე. ხოლო, რაც შეეხება მონაცემთა დამუშავებას, საქართველოს კანონი ამ ცნებას განმარტავს, როგორც ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით მონაცემთა მიმართ შესრულებულ ნებისმიერ მოქმედებას. კერძოდ, შეგროვებას, ჩაწერას, ფოტოზე აღბეჭდვას, აუდიოჩაწერას, ვიდეოჩაწერას, ორგანიზებას, შენახვას, შეცვლას, აღდგენას, გამოთხოვას, გამოყენებას ან გამჟღავნებას მონაცემთა გადაცემის, გავრცელების ან სხვაგვარად ხელმისაწვდომად გახდომის გზით, დაჯგუფებით ან კომბინაციით, დაბლოკვით, წაშლით ან განადგურებით. აღსანიშნავია, რომ მონაცემთა ავტომატური საშუალებებით დამუშავება მოიცავს მონაცემთა ინფორმაციული ტექნოლოგიების გამოყენებით დამუშვებას. არაავტომატური საშუალებებით მონაცემთა დამუშავება კი ამ კანონის მოქმედების სფეროში ექცევა მხოლოდ იმ შემთხვევაში, თუ ის

[109] ინოვაციებისა და რეფორმების ცენტრი, „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, გვ 9.

გარკვეული სისტემით და კონკრეტული კრიტერიუმების მიხედვით დალაგებულ მონაცემთა ბაზაშია გაერთიანებული. ამასთან, მონაცემთა ნახევრად ავტომატური დამუშავების სახეს უფრო ეფექტურად მიიჩნევენ, ვინაიდან, „ვინაიდან კომპიუტერს არ შეუძლია ჩაანაცვლოს ინფორმაციის განმმარტებლის ცოდნა, გამოცდილება და გაგების უნარი, თუმცა შეუძლია შეინახოს უზარმაზარი რაოდენობის მონაცემები, გაამარტივოს მათი ძიება და რაოდენობრივი ანალიზი“[110] [65] არაავტომატური საშუალებებით მონაცემთა დამუშავება „ხელით წერის მეშვეობით „ხელნაწერი ფაილების“ შექმნას გულისხმობს და ხშირად გამოიყენება საავადმყოფოებში.“[111] [66]

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-6 მუხლი ცალკე გამოყოფს განსაკუთრებული კატეგორიის პესრონალური მონაცემების დამუშავების საკითხს, თუმცა ეს საფუძვლები არ არის ამომწურავი, ამიტომაც იყო, რომ წლების განმავლობაში (მოყოლებული 2013 წლიდან) ამ მუხლმა განიცადა არაერთი ცვლილება და დაემატა სხვა სპეციალური საფუძვლებიც. აღსანიშნავია, რომ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების მიმართ მოქმედებს საერთო წესი, რომლის თანახმადაც, განსაკუთრებული ამ კატეგორიის მონაცემთა დამუშავება აკრძალულია. თუმცა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილია ის გამონაკლისი შემთხვევები, როდესაც შესაძლებელია ამ კატეგორიის მონაცემების დამუშავება. ასეთ შემთხვევებად ადგილობრივი კანონმდებლობით განიხილება:

ა) მონაცემთა სუბიექტის წერილობითი თანხმობა - რაც მოიზარებს იმას, რომ განსაკუთებული კატეგორიის პერსონალურ მონაცემთა დამუშავებისას წერილობით თანხმობაში აშკარად უნდა ჩანდეს პირის მიერ ამ კატეგორიის მონაცემების დამუშავებაზე გამოხატული ნებაყოფლობითი თანხმობა. კერძოდ, კონკრეტულად რომელი მონაცემის, რა მიზნით და რომელი სამართლებრივი საფუძვლით დამუშავებას დათანხმდა პიროვნება.

[110] Satellite Remote Sensing, A New Tool for Archaeology, Editors: Rosa Lasaponara and Nicola Masin, UK, 2012. p. 8.
[111] Büllesbach A., Concise European IT Law, USA, Kluwer Law International, 2010, p. 94.

მონაცემთა სუბიექტის მიერ მისი პერსონალური მონაცემების დამუშავებაზე გაცემული თანხმობა ისევე მარტივად უნდა იყოს გამოთხოვადი, როგორც თავის დროზე - თანხმობის გაცემის პროცესი. როდესაც საქმე ეხება განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას, თანხმობა უნდა იყოს ნათელი და მკაფიო.[112] [67] მაგალითად, „სამედიცინო დაწესებულებების მიერ ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებისას აუცილებელია პაციენტის წერილობითი თანხმობის მოპოვება, თუ სახეზე არ არის კანონით გათვალისწინებული სხვა საფუძველი. ამასთან, კანონი ადგენს თანხმობის კანონიერების წინაპირობებს. კერძოდ, იმისათვის, რომ პაციენტის თანხმობა განვიხილოთ მონაცემთა დამუშავების საფუძვლად, პაციენტს წინასწარ უნდა მიეწოდოს ინფორმაცია მონაცემთა დამუშავების მიზნების შესახებ და მის თანხმობას უნდა ჰქონდეს ნებაყოფლობითი ხასიათი";[113] [68] ვინაიდან განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისას მკაფიო თანხმობის გაცემა ემსახურება მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვას. [114] [69]

გ) მონაცემთა სუბიექტის მიერ მონაცემების გასაჯაროება - მაგალითად, პოლიტიკური შეხედულებების ან რელიგიური კუთვნილების მითითება სოციალურ ქსელში;

გ) მონაცემთა დამუშავება შრომითი ვალდებულების შესრულებისა ან მასთან დაკავშირებული უფლების განხორციელებისათვის - მაგალითისთვის შესაძლებელია განვიხილოთ დამსაქმებლის მიერ ჯანმთელობისთვის საშიშ სამუშაოზე ადამიანების აყვანისას მათი

---

[112] Allen & Overy, The EU General Data Protection Regulation, 2017, p. 4, see: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf. [უკანასკნელად ნანახია 2017 წლის აპრილში].

[113] „რეკომენდაცია ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ", 2016 წელი, ხელმისაწვდომია www.pdp.ge.

[114] Bridgit Dimond, Legal Aspects of Midwifery, third edition, 2006, p. 183., see: https://books.google.ge/books?id=pjsHBgAAQBAJ&pg=PA180&lpg=PA180&dq=sensitive+personal+data+book&source=bl&ots=kX5a8U1dpI&sig=QAi-AadIz2Ur_EDVtPijyNl8rl0&hl=en&sa=X&ved=0ahUKEwjpmbGxucHTAhXDtRQKHZrBDvw4ChDoAQg0MAM#v=onepage&q=sensitive%20personal%20data%20book&f=false, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

ჯანმრთელობის შესახებ სრული ინფორმაციის მოთხოვნა, რათა საქმიანობის პროცესში არ მოხდეს დასაქმებულის ჯანმრთელობის გაუარესება;

დ) სასიცოცხლო ინტერესის დაცვა, როდესაც მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად არ აქვს მონაცემთა დამუშავებაზე თანხმობის გამოხატვის უნარი - მაგალითად, ავტოსატრანსპორტო შემთხვევის შემდგომ მკურნალი ექიმის მიერ სასწრაფო დახმარების სამსახურისათვის პაციენტის სამედიცინო ისტორიის გადაცემა მისთვის სწორი მკურნალობის უზრუნველსაყოფად;

ე) მონაცემთა დამუშავება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნებისათვის, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისთვის და ფუნქციონირებისათვის - მაგალითად, საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრომ შეიძლება აწარმოოს სხვადასხვა ქრონიკული დაავადების მქონე პირთა აღრიცხვა, რათა მათ დაუწესდეს გარკვეული შეღავათები მედიკამენტოზურ მკურნალობაზე;

ვ) მონაცემთა დამუშავება პოლიტიკური, ფილოსოფიური, რელიგიური ან სავაჭრო გაერთიანების, ასოციაციის ან სხვა არაკომერციული ორგანიზაციის მიერ ლეგიტიმური საქმიანობის განხორციელებისათვის - ამ საფუძლით მონაცემთა დამუშავება შესაძლობას აძლევს ამ ტიპის ორგანიზაციებს დაამუშაონ მათი წევრების ან იმ პირების განსაკუთრებული კატეგორიის მონაცემები, რომლებსაც მუდმივი კავშირი აქვთ მათთან. როგორც წესი, ამ ინფორმაციის მონაცემთა სუბიექტის თანხმობის გარეშე მესამე პირისათვის გამჟღავნება დაუშვებელია. თუმცა, „შესაძლებელია ერთ შემთხვევაში მონაცემთა გადაცემის ფაქტი იყოს მიზნის ადეკვატური და პროპორციული, ხოლო სხვა შემთხვევაში - არა. მაგალითად, უგონო მდგომარეობაში მყოფი პაციენტის ოჯახის წევრებს, რომლებიც იღებენ პასუხისმგებლობას პაციენტის შემდგომ მკურნალობასა და მოვლაზე, უფლება აქვთ იცოდნენ პაციენტის ჯანმრთელობის მდგომარეობა. ამ შემთხვევაში მონაცემების დამუშავება ხდება

ჯანმრთელობის დაცვის დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით. ამასთან, ინფორმაციის გაცემა არის მიზნის პროპორციული და ადეკვატური. მეორე მხრივ, მონაცემთა დამუშავების საფუძველი სახეზე არ იქნება და პრინციპების დარღვევა მოხდება, თუ პაციენტის ჯანმრთელობის მდგომარეობის შესახებ ოჯახის წევრისათვის ინფორმაციის მიწოდება მოხდება მაშინ, როდესაც პაციენტი არ საჭიროებს სხვათა დახმარებას მკურნალობის ან თავის მოვლის პროცესში და შეუძლია თავად გადაწყვიტოს, რა ინფორმაციას მიაწვდის ოჯახის წევრებს.";[115]

ზ) მონაცემთა დამუშავება ბრალდებულთა/მსჯავრდებულთა პირადი საქმეებისა და რეესტრების წარმოების, მსჯავრდებულის მიმართ მის მიერ სასჯელის მოხდის ინდივიდუალური დაგეგმვის ან/და მსჯავრდებულის სასჯელის მოხდისგან პირობით ვადამდე გათავისუფლებასთან და მისთვის სასჯელის მოუხდელი ნაწილის უფრო მსუბუქი სახის სასჯელით შეცვლასთან დაკავშირებული საკითხების განხილვის მიზნით - ამ საფუძვლით მონაცემთა დამუშავება უკავშირდება პენიტენციურ სისტემაში ბრალდებულის/მსჯავრდებულის მიღებასთან, გადაადგილებასთან, მკურნალობასთან, გათავისუფლებასთან და ა.შ.;

თ) მონაცემების დამუშავება „არასაპატიმრო სასჯელთა აღსრულების წესისა და პრობაციის შესახებ" საქართველოს კანონის მე-2 მუხლით გათვალისწინებული სამართლებრივი აქტების აღსრულების მიზნით, რაც გულისხმობს საქართველოს საჯელაღსრულებისა და პრობაციის სამინისტროს შესაძლებლობას, მონაცემები დაამუშაოს არასაპატიმრო სასჯელთა სახის შემდეგი სამართლებრივი აქტებს აღსრულებისას: სასჯელის სახით თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევა, სასჯელის სახით იურიდიული პირისათვის საქმიანობის უფლების ჩამორთმევა, სასჯელის სახით საზოგადოებისათვის სასარგებლო შრომის დანიშვნა, სასჯელის სახით გამასწორებელი სამუშაოს დანიშვნა, სასჯელის სახით თავისუფლების შეზღუდვია და სასჯელის სახით

[115] „რეკომენდაცია ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ", 2016 წელი, ხელმისაწვდომია www.pdp.ge.

შინაპატიმრობის დანიშვნა. ასევე, პირობითი მსჯავრის დანიშვნის, სასჯელის მოხდისაგან პირობით ვადამდე გათავისუფლებისა და სასჯელის მოხდის გადავადების (ორსული ქალისათვის – მშობიარობის შემდეგ 1 წლამდე) აღსრულებისას. თუ აღნიშნული სამართლებრივი აქტები სასჯელის სახის განსაზღვრასთან ერთად შესაძლოა შეიცავდეს აღმზრდელობითი ზემოქმედების ან/და სამედიცინო ხასიათის მოთხოვნებს, ასეთ შემთხვევაში ამ ღონისძლებებისა და ასევე განრიდების სუბიექტის მიერ ნაკისრი საზოგადოებისათვის სასარგებლო უსასყიდლო სამუშაოს შესრულების აღსრულებისასაც. [116] [70]

ი) მონაცემების დამუშავება „საერთაშორისო დაცვის შესახებ“ საქართველოს კანონით პირდაპირ გათვალისწინებულ შემთხვევებში - აღსანიშნავია, რომ ამ კანონის მოქმედების სფეროს წარმოადგენს უცხოელისა და იმ მოქალაქეობის არმქონე პირის, რომელიც არ არის საქართველოში სტატუსის მქონე მოქალაქეობის არმქონე პირი, საქართველოს ტერიტორიაზე შემოსვლის და ყოფნის (რომლებმაც ამ კანონის შესაბამისად მოითხოვეს საერთაშორისო დაცვა) აგრეთვე მათ მიმართ მოპყრობის სტანდარტების განსაზღვრა; თავშესაფრის მაძიებლის, ლტოლვილის, ჰუმანიტარული სტატუსის მქონე პირისა და დროებითი დაცვის ქვეშ მყოფი პირის სამართლებრივ მდგომარეობის, უფლება-მოვალეობების და სოციალურ-ეკონომიკურ გარანტიების დადგენა; უცხოელისა და მოქალაქეობის არმქონე პირისათვის საქართველოში ლტოლვილის, ჰუმანიტარული ან დროებითი დაცვის ქვეშ მყოფი პირის სტატუსის მინიჭების, შეწყვეტის, გაუქმებისა და ჩამორთმევის და შესაბამისი სტატუსიდან გამორიცხვის საფუძვლებისა და პროცედურების დადგენა; სახელმწიფო უწყებათა კომპეტენციების განსაზღვრა თავშესაფრის პროცედურის უზრუნველყოფის სფეროში. ხოლო ამ კანონის მიზანია: შექმნას თავშესაფრის პროცედურისთვის საჭირო სამართლებრივი ჩარჩო; ამ კანონით დადგენილი წესით უზრუნველყოს თავშესაფრის მაძიებლის, ლტოლვილის, ჰუმანიტარული სტატუსის მქონე პირისა და დროებითი

[116] „არასაპატიმრო სასჯელთა აღსრულების წესისა და პრობაციის შესახებ“ საქართველოს კანონი, მუხლი 2.

დაცვის ქვეშ მყოფი პირის უფლებების დაცვა; ასევე უზრუნველყოს თავშესაფრის პროცედურა ამ კანონით გათვალისწინებული საერთაშორისო დაცვის მექანიზმების გამოყენებით.[117] [71] ამ კანონით პირდაპირ გათვალიწინებულ შემთხვევის მაგალითად შეგვიძლია განვიხილოთ საქართველოს ოკუპირებული ტერიტორიებიდან იძულებით გადაადგილებულ პირთა, განსახლებისა და ლტოლვილთა სამინისტროს მიერ თავშესაფრის მაძიებელთა და საერთაშორისო დაცვის მქონე პირთა შესახებ მონაცემთა ბაზის წარმოება, რომელიც მოიცავს ამ პირების შესახებ პერსონალურ, მათ შორის განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს.

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვა და მისი თანმდევი შედეგები თანაბრად შეეხება თითოეულ მოქალაქეს, რომელიც აქტიურადაა ჩაბმული საჯარო თუ კერძო სამართალურთიერთობებში. შესაბამისად, კანონის მოქმედების მასშტაბი საკმაოდ ფართოა.“[118] თუმცა, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი განსაზღვრავს იმ შემთხვევებს, როდესაც განსაკუთრებული კატეგორიის პესრონალური მონაცემების დამუშავებისათვის არ მოითხოვება კანონით გათვალისწინებული საფუძვლების არსებობა, ანუ მათზე არ ვრცელედება ზემოაღნიშნული შეზღუდვები. ასეთად ეროვნული კანონმდელობა განიხილავს საზოგადოებრივი უსაფრთხოების, ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნით მონაცემთა დამუშავებას, თუ საკითხი პირდაპირ და სპეციალურად რეგულირდება საქართველოს სისხლის სამართლის საპროცესო კოდექსით ან „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ საქართველოს კანონით ან სხვა სპეციალური კანონით. ასევე „ოფიციალური სტატისტიკის შესახებ“ საქართველოს კანონით გათვალისწინებული მოსახლეობის საყოველთაო აღწერის მიზნით მონაცემთა დამუშავებას. მაგალითისთვის, სამართალდამცავი ორგანოების

[117] „საერთაშორისო დაცვის შესახებ“ საქართველოს კანონი, მუხლი 2.

[118] სამეცნიერო პრაქტიკული ჟურნალი „თემიდა“, მოსახლიშვილი ლ., სტატია „პერსონალური მონაცემების დაცვის კანონმდებლობა საქართველოში“, 2012 წელი, №6(8), გვ 77.

მიერ ჯანმრთელობასთან დაკავშირებული ინფორმაციის გამოთხოვა სისხლის სამართლის საპროცესო კოდექსის საფუძველზე.

მნიშვნელოვანია შევეხოთ ასევე გარდაცვლილი პირის შესახებ არსებული პერსონალურ მონაცემების დაცვის საკითხს, ვინიდან „პერსონალურ მონაცემთა ,,ქურდმა“ შესაძლოა აღნიშნული ინფორმაცია გამოიყენოს ახალი ყალბი ანგარიშების შესაქმნელად, ან გარდაცვლილი პირის სოციალური დაცვის ნომერი მიითვისოს.“[119] [72] საზღვარგარეთის ქვეყნებში განსხვავებული პრაქტიკაა, ზოგიერთი ქვეყანა არ არეგულირებს გარდაცვლილი პირის შესახებ მონაცემთა დამუშავების წესს, რაც შეეხება საქართველოს კანონს, იგი ითვალისწინებს დებულებებს გარდაცვლილი ფიზიკური პირის შესახებ პერსონალური მონაცემების დამუშავებაზე. მონაცემთა სუბიექტის გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავება, მათ შორის განსაკუთრებული კატეგორიის მონაცემების დამუშავება გარდა ამ კანონის განსაზღვრული საფუძვლებისა, დასაშვებია მხოლოდ მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის თანხმობით ან თუ მონაცემთა სუბიექტის გარდაცვალებიდან გასულია 30 წელი. სუბექტის გარდაცვალების შემდეგ მის შესახებ მონაცემთა დამუშავებას კანონი დასაშვებად უშვებს თუ ეს აუცილებელია მემკვიდრეობასთან დაკავშირებული უფლებების რეალიზაციისათვის. თუმცა ზემოაღნიშნული საფუძვლებით დამუშავება დაუშვებელია, თუ მონაცემთა სუბიექტმა გარდაცვალებამდე წერილობითი ფორმით აკრძალა მის შესახებ მონაცემთა მისი გარდაცვალების შემდეგ დამუშავება. ამასთან, გარდაცვლილი პირის შესახებ მონაცემები შეიძლება გამჟღავნდეს ისტორიული, სტატისტიკური და კვლევითი მიზნებისათვის, გარდა იმ შემთხვევისა, როდესაც გარდაცვლილმა პირმა წერილობითი ფორმით აკრძალა მათი გამჟღავნება. რაც შეეხება გარდაცვლილი პირის სახელს, სქესს, დაბადებისა და გარდაცვალების თარიღებს მათი დამუშავება არ

[119] Acohido B., Swarts J., Zero Day Threat: The Shocking Truth of how Banks and Credit Bureaus Help Cyber Crooks Steal Your Monay and Identity, NY and London, Union Square Press an imprinted of Sterling Publishers Co., 2008. p. 101

საჭიროებს კანონით გათვალისწინებული მონაცემთა დამუშავების საფუძვლის არსებობას.

საზღვარგარეთის ქვეყნების ეროვნულ კანონმდებლობას თუ გადავხედავთ, დიდი ბრიტანეთის პერსონალურ მონაცემთა დაცვის აქტის (1988 წელი) მე-4 მუხლის მე-3 ნაწილის თანახმად, სესიტიური მონაცემების დამუშავების საფუძველია, თუ „ა) მონაცემთა დამუშავება ემსახურება დამსაქმებლის მხრიდან კანონმდებლობით დაკისრებული მოვალეობების შესრულების მიზანს; ბ) დამუშავება ემსახურება თავად მონაცემთა სუბიექტის ან სხვა მესამე პირის სასიცოცხო ინტერესების დაცვას (ამ დროს თანხმობის მოპოვება შეუძლებელი უნდა იყოს); გ) დამუშვება ნებისმიერი ორგანიზაციის და დაწესებულების კანონმდებლობით განსაზღვრულ მიზნებსა და საქმიანობას შეესაბამება (მათ შორის, პოლიტიკური, ფილოსოფიური, რელიგიური და სავაჭრო კავშირის მიზნებისათვის მოქმედებს), თუ თავად ეს ორგანიზაცია/დაწესებულება არ არის შექმნილი და ორიენტირებული მოგების მიღებაზე; დ) დამუშავება ემსახურება მონაცემთა სუბიექტის კანონმდებლობით გათვალისწინებული უფლებებისა და ინტერესების დაცვას; ე) დამუშავება ემსახურება სამართალწარმოების მიზნებს ან მართლმსაჯულების აღსრულებას (მათ შორის, ადვოკატის, წარმომადგენლის აყვანა, სუბიექტის უფლებების დაცვა სასამართლოსა და სხვა ადგილას; ვ) დამუშავება პარლამენტის, სამინისტროებისა და სახელმწიფო დეპარტამენტების მიერ, მათთვის დაკისრებული ფუნქციების შესასრულებლად; ზ) მონაცემთა სუბიექტმა თავად გახადა საჯარო მის შესახებ ინფორმაცია.“[120] იტალიის მონაცემთა დაცვის კოდექსის მე-20 და 26-ე მუხლებით განსაზღვრულია ამ კატეგორიის მონაცემების დამუშავების საფუძვლები, კერძოდ, „ა) საჯარო დაწესებულებების მიერ სენსიტიური მონაცემების დამუშავება დასაშვებია მხოლოდ კანონმდებლობით პირდაპირ გათვალისწინებულ შემთხვევებში: ა) თუ დამუშავება ემსახურება საჯარო ინტერესს; ბ) არსებობს მკაფიოდ გამოხატული საჯარო ინტერესი; გ) არსებობს სუბიექტის მკაფიო წერილობითი თანხმობა; დ) მონაცემები

[120] იხ. http://www.legislation.gov.uk/ukpga/1998/29/section/2, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

მუშავდება სავაჭრო კავშირის, ფილოსოფიური, პოლიტიკური, რელიგიური თუ სავაჭრო ხასიათის ასოციაციების/ორგანიზაციების მიერ; ე) მონაცემთა დამუშავება ემსახურება მესამე პირთა სასიცოცხლო ინტერესების დაცვას; ვ) მონაცემთა დამუშავება აუცილებელია საგამოძებო მოქმედებებისათვის; ზ) მონაცემთა დამუშავებას ითვალისწინებს სპეციალური კანონმდებლობა.“[121] რაც შეეხება შვედეთის პერსონალურ მონაცემთა დაცვის აქტს (Personal Data Act) „მთლიანად აკრძალულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება და ამისთვის მხოლოდ გამონაკლისებია დაშვებული. გამონაკლისებია, თუ: არსებობს მკაფიო თანხმობა; მონაცემები საჯაროდ ხელმისაწვდომი გახადა თავად სუბიექტმა; მონაცემთა დამმუშავებლის მიერ შრომითი კანონმდებლობიდან გამომდნარე ვალდებულებების შესასრულება; მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დაცვა (როდესაც მას თავად არ აქვს საშუალება, გამოხატოს თანხმობა); სამართლებრივი ინტერესების დაცვა; ემსახურება ჯანმრთელობის დაცვის (მათ შორის, დიაგნოზის დასმის, მკურნალობის) მიზნებს; არაკომერციული ორგანიზაციების მხრიდან მათი წევრების პოლიტიკური, ფილოსოფიური და რელიგიური შეხედულებების დამუშავება ამ ორგანიზაციის მიზნებისათვის; სტატისტიკური და კვლევითი მიზნებისათვის.“[122] [73]

წარმოდგენილი მასალის ანალიზის საფუძველზე ნათლად ჩანს, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისთვის დადგენილი საფუძვლები თეორიულად თითქმის სრულად ასახავს ევროსაბჭოსა და ევროკავშირის კანინმდებლობით დადგენილ სტანდარტებს, უფრო მეტიც კი, ზოგიერთი საზღვარგარეთის ქვეყნის ეროვნული კანონმდებლობის ანალოგიურია. მაგალითად,

[121]იხ. http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[122] Susanna Norelid and Emanuel Hollstrand, Data protection in Sweden: overview, 2017, see: https://uk.practicallaw.thomsonreuters.com/8-502-0348?__lrTS=20170426060701848&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1[უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

საქართველოს კანონსა და შვედეთის პერსონალურ მონაცემთა დაცვის აქტში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის დადგენილი საფუძვლები შეიძლება ითქვას რომ სრულიად იდენტურია. თუმცა, აქვე უნდა აღინიშნოს, საქართველოს კანონში იკვეთება „ევროდირექტივის მე-8 მუხლის მე-4 დებულების მსგავსი ჩანაწერის არ არსებობა, რომელიც ამბობს, რომ სენსიტიური მონაცემების დამუშავების დამატებით შემთხვევები შესაძლოა იყოს გათვალისწინებული კანონით, სადაც მათი დამუშავება ხდება მნიშვნელოვანი საჯარო ინტერესების დაცვისთვის და იმ პირობით, რომ მონაცემთა დაცვის სუბიექტისთვის სათანადო დაცვის მექანიზმებია უზრუნველყოფილი. შეიძლება მსჯელობა, რომ პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი შეიძლება შეიცვალოს ან გაძლიერდეს უფრო გვიან მიღებული სამართლებრივი დებულებებით“, ... „ვინაიდან საქართველოს კანონს არ აქვს უპირატესი სტატუსი სხვა კანონებთან შედარებით, მე-6 მუხლით განსაზღვრული შეზღუდვები არ არის ეფექტური. ისინი ასევე არასაკმარისია იმ შემთხვევებში, როდესაც მე–6 მუხლით სენსიტიური მონაცემების დამუშავება არ არის ნებადართული, მაგრამ ცხადია, რომ აუცილებელია. რეკომენდებულია, დამატებითი ყურადღება მიექცეს, თუ როგორ არის შესაძლებელი მე–6 მუხლის მიზნის რეალიზება.“ [123]

2.4. მონაცემთა დამმუშავებლის უფლებამოსილებანი

პერსონალურ მონაცემთა დაცვის სამართლებრივი რეგულირება ეს არის, ერთი მხრივ, „პიროვნების შეთანხმება სახელმწიფოსთან, ბანკებთან, სატელეფონო კომუნიკაციებთან და სხვა დაწესებულებებთან, იმის შესახებ, რომ პიროვნება მზად არის, თავად უზრუნველყოს საკუთარი თავის შესახებ არსებული ინფორმაციის მიწოდება ზემოთქმული ორგანიზაციებისა და სახელმწიფოსათვის“[124] [74], ხოლო მეორე მხრივ, მონაცემთა დამუშავების

[123] ინოვაციებისა და რეფორმების ცენტრი, „საქართველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, გვ.10-15.

[124] Симонов Алексей., Предисловие, Волчинская Е.К., Защита персональных данных, Россия, 2001, ст.6.

პროცესში მონაცემთა დამმუშავებელი/უფლებამოსილი პირის მიერ კანონით განსაზღვრული ვალდებულებების შესრულება. ვინაიდან, იქ, სადაც „მოქალაქე დაუცველია, სახელმწიფო ვერ იტყვის, რომ დემოკრატიული სისტემა შექმნა.“[125] [75]

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, საჯარო სექტორის მონაცემთა დამმუშავებელი ვალდებულია, მონაცემთა დამუშავებისას, დაიცვას ყველა პრინციპი ერთდროულად. როდესაც მონაცემთა დამმუშავებელი პერსონალური მონაცემების შეგროვებას/მოპოვებას ახორციელებს უშუალოდ მონაცემთა სუბიექტისაგან, მონაცემთა დამმუშავებელი ვალდებულია, მიაწოდოს მას შემდეგი ინფორმაცია: „მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) 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.“[126]

მონაცემთა დამმუშავებელი ვალდებულია, მოთხოვნის შემთხვევაში, მონაცემთა სუბიექტს მიაწოდოს ინფორმაცია მისი პერსონალური მონაცემების დამუშავების სამართლებრივი საფუძვლების, მონაცემთა დამუშავების მიზნის, მონაცემთა შეგროვების საშუალებებისა და დამუშავებული მონაცემების მოცულობის შესახებ. „მსგავს შემთხვევაში, მონაცემთა სუბიექტი არამარტო მიღებულ გადაწყვეტილებაზე იღებს პასუხისმგებლობას, არამედ მის შედეგებზეც“.[127] [76] თუ მონაცემთა სუბიექტი ითხოვს ან მონაცემთა დამმუშავებელი ნებაყოფლობით აწვდის მას ინფორმაციას მისი პერსონალური მონაცემების დამუშავების შესახებ,

[125] ახალი თაობა, ხურცილავა ნ., „რა ბედი ელის პერსონალურ მონაცემებს“ თბილისი, 2014 წლის 29 იანვარი, №23, გვ.7.

[126] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“; მუხლი 16.

[127] Петров М.И., Постатейный комментарий к Федеральному закону О персональных данных, Россия, Юстицинформ, 2007, ст. 28.

აუცილებელია მონაცემთა დამმუშავებლის/უფლებამოსილი პირის მიერ პროპორციულობის პრინციპის დაცვა და მონაცემთა სუბიექტისათვის მხოლოდ მის მიერ მოთხოვნილი პერსონალური მონაცემების ან/და კანონით გათვალისწინებული მონაცემების მიწოდება, რათა ზედმეტი მონაცემების გადაცემით, არ მოხდეს სხვათა უფლებების ხელყოფა ან თვითონ მონაცემთა სუბიექტისათვის ზიანის მიყენება. ამასთან, „მონაცემთა დამუშავებისას, დამსაქმებელი ვალდებულია, გააფრთხილოს მონაცემთა სუბიექტი დამუშავების ფაქტის შესახებ, გარდა იმ შემთხვევისა, როდესაც მისთვის ისედაც ცნობილია ამის შესახებ. გაფრთხილება, ძირითადად, ხდება ზეპირი ან წერილობითი ფორმით, მაგრამ ეს შეიძლება განხორციელდეს სხვა ფორმითაც“.[128] [77] თუმცა კანონი იმპერატიულად ადგენს, რომ „დავის წარმოშობის შემთხვევაში, მონაცემთა დამმუშავებელს ეკისრება მონაცემთა სუბიექტის თანხმობის ფაქტის არსებობის მტკიცების ტვირთი. შესაბამისად, მტკიცების ტვირთის მიზნებისათვის მიზანშეწონილია, თუ მონაცემთა დამმუშავებელი მოიპოვებს მონაცემთა სუბიექტის წერილობით თანხმობას.“[129] [78]

ინფორმაციული ტექნოლოგიებისა და ციფრული მოწყობილობების განვითარებასთან ერთად, გაიზარდა პერსონალური მონაცემების ავტომატურად დამუშავების რაოდენობა. „ტექნოლოგიების განვითარების პარალელურად, ინტერნეტში კომუნიკაციის დროს, (როგორიცაა ელექტრონული ფოსტა, სოციალური მედია და სხვა) დიდი ყურადღება უნდა დაეთმოს განსაკუთრებული კატეგორიის მონაცემთა დაცვას.“[130] [79;

---

[128] სამეცნიერო შრომების კრებული, რეფერატი და რეცენზირებული სამეცნიერო პრაქტიკული ჟურნალი, მოსახლიშვილი ლ., სტატია „პერსონალური მონაცემების დაცვა შრომით ურთიერთობებში“, თბილისის ღია სასწავლო უნივერსიტეტი, თბილისი, 2013 წელი, №4, გვ. 16-25.

[129]წლიური ალმანახი, სტატიათა კრებული, ფალავანდიშვილი ბ., „პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი - ზოგადი მიმოხილვა, იურიდიული ფირმა „მგალობლიშვილი, ყიფიანი, ძიძიგური“, თბილისი, 2013 წელი, გვ.48-52.

[130] ევროპის კომისია, კვლევა „Study on the economic benefits of privacy- enhancing technologies (PETS)“, გვ. 17, ხელმისაწვდომია: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში]; ასევე, Madsen, Wayne, Handbook of Personal Data Protection, 1992, p.16-62 და Winnie Chang, A Practical Guide to Singapore Data Protection Law, 2013, ხელმისაწვდომია: http://www.cnplaw.com/en/media/files/Brochure%20for%20A%20Practical%20Guide%20to%20Sin

80; 81] აღნიშნულიდან გამომდინარე, „მონაცემთა დამმუშავებელი ვალდებულია, მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომელიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით, უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.“[131]

კანონი არ განმარტავს ტერმინს „შესაბამისი ორგანიზაციულ-ტექნიკური ზომები“. ერთიანი უსაფრთხოების სტანდარტის დადგენა საკმაოდ რთულია, რადგან სხვადასხვა სახის და მოცულობის მონაცემები საჭიროებს განსხვავებული დონის უსაფრთხოების სისტემის არსებობას. „საჯარო სექტორში მონაცემთა დამმუშავებელმა უსაფრთხოების ზომების განსაზღვრისას, მხედველობაში უნდა მიიღოს ორი მნიშვნელოვანი საკითხი:

➢ **ინფორმაციის შინაარსი** - მონაცემთა დამმუშავებელმა უნდა შეაფასოს მის მიერ დამუშავებული პერსონალური მონაცემების მოცულობა და შინაარსი, მაგალითად, ამუშავებს თუ არა განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს.

➢ **ზიანის შეფასება** - უსაფრთხოების სისტემის გაუმართაობის ან ხელყოფის შედეგად მოპოვებული პერსონალური მონაცემების არამართლზომიერმა გამოყენებამ შესაძლოა, გამოიწვიოს სერიოზული ზიანი მონაცემთა სუბიექტისთვის, მაგალითად, სიცოცხლისათვის საფრთხის შექმნა, სერიოზული ფინანსური დანაკარგი. შესაბამისად, იმ მონაცემთა დაცვას, რომლის უსაფრთხოების რღვევამ შესაძლოა, გამოიწვიოს მძიმე შედეგი, სჭირდება უფრო მეტი რესურსი, ვიდრე სხვა მონაცემებს."[132]

მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშვებასთან დაკავშირებული რისკების ადეკვატური და პროპორციული უნდა იყოს. რისკების შეფასებისას, მხედველობაში მიიღება როგორც დამუშავებული მონაცემების ხასიათი, ასევე, ორგანიზაციის

---

gapore%20Data%20Protection%20Law%20by%20Winnie%20Chang.pdf[უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

[131] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 17.1.

[132] „პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მოანცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.42.

თანამშრომელთა რაოდენობა და მონაცემთა ბაზასთან მათი წვდომის ხარისხი, მონაცემთა ბაზაზე წვდომის უფლების მქონე მესამე პირები და მათი რაოდენობა.

საჯარო სექტორში უსაფრთხოების სისტემის ეფექტურობისთვის მნიშვნელოვანია რამდენიმე ფაქტორის გათვალისწინება:

„მენეჯმენტი და ორგანიზაციული ზომები, რაც გულისხმობს: უსაფრთხოების პოლიტიკის შემუშავებას/მონაცემთა უსაფრთხოების წესების განსაზღვრას; უსაფრთხოების უზრუნველყოფაზე პასუხისმგებელი პირის/პირების განსაზღვრას დაწესებულებაში; კოორდინაციას ორგანიზაციის თანამშრომლებს შორის აღნიშნულ საკითხთან მიმართებაში; პერსონალური მონაცემების დაცვის არამარტო ადეკვატური საშუალებების დანერგვას, არამედ უსაფრთხოების თანამედროვე სტანდარტების შესაბამისი ზომების მიღებას.“[133]

პერსონალური მონაცემების დაცვითი სისტემის მნიშვნელობას შეხება „Electronic Frontier Foundation (EFF)“ („ელექტრონული სასაზღვრო ფონდი“) - ის მიერ გამოქვეყნებული კვლევა. კვლევაში შეფასებულია 24 უმსხვილესი სატელეკომუნიკაციო და ინფორმაციული ტექნოლოგიების კომპანიის პერსონალური მონაცემების დაცვის სისტემა. საინტერესოა, რომ აღნიშნული შეფასების შედეგად კომპანია WhatsApp-მა მიიღო მხოლოდ ერთი ვარსკვლავი ხუთიდან. მიუხედავად იმისა, რომ WhatsApp-ს ჰქონდა დრო ანგარიშში პირველად გამოჩენამდე, მან არ განახორციელა არცერთი ცვლილება, რომელშიც გათვალისწინებული იქნებოდა პერსონალური მონაცემების დაცვის სფეროში სხვა კომპანიების საუკეთესო პრაქტიკა. აღსანიშნავია, რომ მისი დედობილი კომპანია Facebook-ი ბევრად უკეთ, ოთხი ვარსკვლავით შეფასდა. EFF-ის მიერ კომპანიების შეფასება მოხდა ხუთი კრიტერიუმის მიხედვით, მიყვებიან თუ არა კომპანიები საყოველთაოდ აღიარებულ საუკეთესო პრაქტიკას, გამჭვირვალეა თუ არა მათი საქმიანობა მთავრობისათვის მოთხოვნილი ინფორმაციის გაცემასთან დაკავშირებით, აქვთ თუ არა გამოქვეყნებული მონაცემთა შენახვის

[133] იხ.იგივე, გვ. 43

პოლიტიკა და ასაჯაროებენ თუ არა ინფორმაციას მთავრობის მხრიდან ინფორმაციის წაშლის მოთხოვნებთან დაკავშირებით. Apple-ი აღმოჩნდა იმ მცირერიცხოვან კომპანიებს შორის, რომლებმაც სრული ხუთი ვარსკვლავი მიიღეს. ხუთი ვარსკვლავი მიიღეს ისეთმა კომპანიებმა, როგორებიც არიან Wordpress-ი, Dropbox-ი, Yahoo, CREDO, Sonic-ი, Wickr-ი და Wikimedia.[134] [82]

2015 წლის განმავლობაში, მოხდა არაერთი კიბერთავდასხმა სხვადასხვა დიდ კომპანიაზე, როგორებიც არიან Ashley Madison-ი, Moonpig-ი, TalkTalk-ი და სხვა. აღნიშნულ შემთხვევებს შედეგად მოჰყვა დიდი ოდენობით მონაცემების გამჟღავნება და დაკარგვა. ამდენად, მონაცემთა დამმუშავებელი კომპანიები იძულებული გახდნენ, შეეცვალათ საკუთარი კიბერუსაფრთხოების მიდგომები. პრაქტიკამ აჩვენა, რომ ანტივირუსი, დამცავი კედელი, საფრთხეების აღმოჩენა და მონიტორინგი აღარ იყო საკმარისი. ევროკავშირის პერსონალური მონაცემების მარეგულირებელი ნორმები კომპანიებს ავალდებულებს, მიიღონ პრევენციული ზომები მონაცემების დასაცავად და ასევე, მოახდინონ სწრაფი რეაგირება მონაცემთა უსაფრთხოებისათვის, თუმცა ეს არ უზრუნველყოფს მონაცემთა სათანადო დაცვას. კომპანიების უსაფრთხოების სტრატეგია უსუსური აღმოჩნდა. კომპანიებმა უნდა იზრუნონ არამარტო სისტემის უსაფრთხოებაზე, არამედ იმაზეც, რომ მონაცემები იყოს უსაფრთხოდ მაშინაც კი, როდესაც მესამე პირები შეაღწევენ სისტემაში, ამდენად, მნიშვნელოვანია უსაფრთხოების მართვის სტანდარტების დანერგვა. 2016 წლის უსაფრთხოების ტენდენციაა ორმაგი ავთენტიფიკაციის აუცილებლობა, მონაცემების დაშიფვრა და გასაღების სწორი მართვა. ყოველივე აღნიშნული, იქნება წინაპირობა იმისა, რომ სისტემის უსაფრთხოების რღვევის შემთხვევაშიც კი, მონაცემები იქნება მაქსიმალურად დაცული[135]. [83]

---

[134] Shepher A., „Electronic Frontier Foundation gives messaging app one star out of five for security“, ხელმისაწვდომია: http://www.itpro.co.uk/security/24839/whatsapp-among-worst-rated-companies-in-privacy-study, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში].

[135] Hart J., „New cyber security trends and new approaches to data protection“ December 2015y,. ხელმისაწვდომია: http://www.itproportal.com/2015/12/17/2016-new-cyber-security-trends-new-approaches-data-protection/? [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

საჯარო სექტორში მონაცემთა დამმუშავებლის ვალდებულებაა დაიცვას მონაცემები მათი უკანონო გამჟღავნებისაგან. მონაცემთა გამჟღავნება არის მონაცემთა დამუშავების ფორმა, რომელმაც შესაძლოა, გამოიწვიოს საკმაოდ მძიმე შედეგი მონაცემთა სუბიექტისათვის, კანონმდებელი მონაცემთა დამმუშავებელს ავალდებულებს, აღრიცხოს მონაცემთა გამჟღავნების ყველა შემთხვევა, ანუ მათი მესამე პირისათვის გადაცემა.

მონაცემთა გამჟღავნებისთვის, ისევე, როგორც მონაცემთა დამუშავების სხვა შემთხვევებშიც, აუცილებელია კანონით დადგენილი საფუძვლის არსებობა. ზოგადი წესის თანახმად, მონაცემთა სუბიექტმა თვითონ უნდა გადაწყვიტოს, ვის და რა მოცულობით გადაეცეს თავისი პერსონალური მონაცემები, ამ შემთხვევაში, მონაცემთა გამჟღავნების საფუძველი არის მონაცემთა სუბიექტის თანხმობა.

მონაცემთა გამჟღავნების აღრიცხვისას, უნდა მოხდეს ისეთი ინფორმაციის რეგისტრაცია, როგორიცაა: რომელი პერსონალური მონაცემის გამჟღავნება მოხდა, ვისთვის მოხდა პერსონალური მონაცემების გამჟღავნება, პერსონალური მონაცემების გამჟღავნების თარიღი და პერსონალური მონაცემების გამჟღავნების სამართლებრივი საფუძველი. აღნიშნული მონაცემები უნდა ინახებოდეს პირის პერსონალურ მონაცემებთან ერთად, პერსონალური მონაცემების შენახვის ვადით.

საჯარო სექტორის მონაცემთა დამმუშავებელი ვალდებულია, თითოეულ ფაილურ სისტემასთან დაკავშირებით, აწარმოოს ფაილური სისტემის კატალოგი, რაც გულისხმობს ფაილური სისტემის სტრუქტურისა და შინაარსის დეტალურ აღწერილობას. კატალოგში აღირიცხება შემდეგი ინფორმაცია: „ა) ფაილური სისტემის სახელწოდება; ბ) მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის დასახელებები და მისამართები, მონაცემთა შენახვის ან/და დამუშავების ადგილი; გ) მონაცემთა დამუშავების სამართლებრივი საფუძველი; დ) მონაცემთა სუბიექტის კატეგორია; ე) მონაცემთა კატეგორია ფაილურ სისტემაში; ვ)

მონაცემთა დამუშავების მიზანი; ზ) მონაცემთა შენახვის ვადა; თ) მონაცემთა სუბიექტის უფლების შეზღუდვის ფაქტი და საფუძვლები; ი) ფაილურ სისტემაში განთავსებულ მონაცემთა მიმღები და მათი კატეგორიები; კ) ინფორმაცია მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის შესახებ და ასეთი გადაცემის სამართლებრივი საფუძველი; ლ) მონაცემთა უსაფრთხოების დაცვისათვის დადგენილი პროცედურის ზოგადი აღწერილობა.“[136]

პერსონალურ მონაცემთა დაცვის ინსპექტორი აწარმოებს ფაილურ სისტემათა კატალოგების რეესტრს. რეესტრში შეტანილი ინფორმაცია საჯაროა და განთავსდება ოფიციალურ ვებგვერდზე.[137] ინსპექტორის აპარატიდან გამოთხოვილი სტატისტიკური მონაცემებით, 2013 წლიდან 2017 წლის 10 მაისის ჩათვლით, პერსონალურ მონაცემთა დაცვის ინსპექტორს შეტყობინება, ფაილური სისტემის კატალოგების სახით, წარუდგინა 1845 საჯარო დაწესებულებამ (მათ შორის, საჯარო სკოლებმა). ამასთან, წარმოდგენილი ფაილურ სისტემათა კატალოგების რეესტრის მიხედვით:

- საჯარო სექტორის მონაცემთა დამმუშავებლების მიერ პირის რასობრივ ან ეთნიკურ კუთვნილებასთან დაკავშირებული ინფორმაცია არ მუშავდება;
- პოლიტიკური შეხედულებების შესახებ ინფორმაციას ამუშავებს საჯარო სექტორის 02 მონაცემთა დამმუშავებელი;
- რელიგიურ ან/და ფილოსოფიურ მრწამსთან დაკავშირებულ ინფორმაციას - საჯარო სექტორის 06 მონაცემთა დამმუშავებელი;
- პროფესიული კავშირის წევრობის შესახებ ინფორმაციას - საჯარო სექტორის 04 მონაცემთა დამმუშავებელი;
- ჯანმრთელობის მდგომარეობასთან დაკავშირებულ ინფორმაციას - საჯარო სექტორის 971 მონაცემთა დამმუშავებელი;
- სქესობრივ ცხოვრებასთან დაკავშირებულ ინფორმაციას - საჯარო სექტორის 01 მონაცემთა დამმუშავებელი;

[136] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 19.1.
[137] იხ. ვებგვერდი: www.catalog.pdp.ge.

➢ ინფორმაციას ნასამართლობის შესახებ - საჯარო სექტორის 79 მონაცემთა დამმუშავებელი;

➢ ადმინისტრაციულ პატიმრობასთან დაკავშირებით - საჯარო სექტორის 02 მონაცემთა დამმუშავებელი;

➢ პირისთვის აღკვეთის ღონისძიების შეფარდებასთან დაკავშირებულ ინფორმაციას - საჯარო სექტორის 02 მონაცემთა დამმუშავებელი;

➢ პირთან საპროცესო შეთანხმების დადების შესახებ ინფორმაციას - საჯარო სექტორის 01 მონაცემთა დამმუშავებელი;

➢ განრიდებასთან დაკავშირებით, ინფორმაცია არ იძებნება ;

➢ დანაშაულის მსხვერპლად აღიარებასა და პირის დაზარალებულად ცნობის შესახებ ინფორმაციას - საჯარო სექტორის 01 მონაცემთა დამმუშავებელი.

კითხვაზე, აქვს თუ არა წარმოდგენილი ყველა საჯარო დაწესებულებას ინფორმაცია ფაილური სისტემის კატალოგის სახით, საპასუხო წერილში განმარტებულია, რომ აპარატში დაცული ინფორმაციით, მოკლებულნი არიან შესაძლებლობას, მოგვაწოდონ ზუსტი ინფორმაცია, აქვს თუ არა ყველა საჯარო დაწესებულებას მოწოდებული ფაილური სისტემის კატალოგი. წერილში ასევე, მითითებულია, რომ ფაილურ სისტემათა კატალოგების რეესტრის ფორმატიდან გამომდინარე, ვინაიდან მონაცემთა დამმუშავებლების მიერ ზემოაღნიშნული მონაცემები შესაძლოა, მითითებული იყოს „სხვა კატეგორიის მონაცემის“ სახით, დასაშვებია, განსაკუთრებული კატეგორიის მონაცემებს ამუშავებდეს საჯარო სექტორის მეტი მონაცემთა დამმუშავებელი.[138]

აღსანიშნავია, რომ „ფაილური სისტემის კატალოგის“ წარმოება არ არის უბრალო ფორმალობა ან/და მხოლოდ მონაცემთა სუბიექტისა თუ ინსპექტორის ინფორმირების საშუალება.“[139] ვინაიდან, „პრაქტიკაში, ერთი

[138] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2017 წლის 16 მაისის №5 17 00001756 წერილი.

[139] ინოვაციების და რეფორმების ცენტრი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ინპლემენტაცია საქართველოს სამინისტროებში, მონიტორინგის ანგარიში, 2013 წელი, გვ.16, ხელმისაწვდომია ვებგვერდზე:www. irc.ge.

მხრივ, არსებობენ მცირე ზომის ორგანიზაციები (დამმუშავებლები), რომელთაც უმნიშვნელო მოცულობის, არამგრძნობიარე მონაცემებთან აქვთ შეხება, თანამშრომელთა რაოდენობა ერთეულებს ან რამდენიმე ათეულს არ აღემატება, არ გააჩნიათ რთული საინფორმაციო სისტემები და მრავალსუბიექტიანი ბიზნესპროცესები, არ აწარმოებენ პერსონალურ მონაცემთა გადაცემას სხვა დამმუშავებლებისადმი და შესაბამისად, მათ მიერ გასატარებელი ორგანიზაციული და ტექნიკური ზომები მინიმალურია, არ არის დაკავშირებული დიდ დანახარჯებთან. ამის საპირისპიროდ, არსებობს ორგანიზაციათა მეორე კატეგორია, რომლებიც თანამშრომელთა მრავალრიცხოვანი შემადგენლობისა და კომპიუტერული პროგრამების გამოყენებით, დიდი მოცულობის მგრძნობიარე მონაცემებს ამუშავებენ, რაც მაღალ რისკებს წარმოშობს.“[140] შესაბამისად, ძალზე მნიშვნელოვანია, რომ ერთი მხრივ, ინსპექტორის აპარატში მონაცემთა დამმუშავებლის მიერ ზუსტად და ოპერატიულად იქნას წარდგენილი ინფორმაცია ფაილური სისტემის კატალგის სახით, ხოლო, მეორე მხრივ, პერსონალურ მონაცემთა დაცვის ინსპექტორმა განახორციელოს ეფექტიანი კონტროლი, რომ აღნიშნული კატალოგის შევსება არ ატარებდეს ფორმალურ ხასიათს. ვინაიდან, სწორედ აღნიშნული სისტემა წარმოადგენს ქვეყანაში მონაცემთა დამმუშავებელთა რაოდენობის ფლობის, მისი დეტალურად გაწერის, მოცულობითი მონაცემების დამმუშავებლების განსაზღვრის, რისკების იდენტიფიცირების საშუალებას, რომლის გააზრების გარეშე, პრაქტიკულად შეუძლებელია მონაცემთა დამუშავების კანონიერების მიღწევა სახელმწიფოში. ინსპექტორის აპარატიდან წარმოდგენილი ინფორმაციის საფუძველზე კი შეიძლება ითქვას, რომ მიუხედავად ფაილური სისტემის კატალოგის ელექტრონული რეესტრის არსებობისა, ინსპექტორს არ აქვს სრული ინფორმაცია და ზუსტად ვერ აიდენტიფიცირებს, რამდენი საჯარო უწყება ამუშავებს ამა თუ იმ განსაკუთრებული კატეგორიის პერსონალურ მონაცემს და ასევე, ვერ

[140] იხ. იგივე, გვ.17

აკონტროლებს, წარმოდგენილი აქვს თუ არა ფაილური სისტემის სავალდებულო კატალოგი ყველა საჯარო უწყებას.

თავი III. პერსონალურ მონაცემთა დაცვაზე ზედამხედველი ორგანო და მისი უფლებამოსილება

3.1. პერსონალურ მონაცემთა დამუშავების პროცესში ინსპექტორის მანდატი

პერსონალურ მონაცემთა დაცვის შესახებ ევროპული კანონმდებლობის თანახმად, „მონაცემთა სუბიექტს უნდა გააჩნდეს უფლება, რომ ეროვნული კანონმდებლობის დონეზე, უზრუნველყოფილი იყოს მისი პერსონალური მონაცემების დაცვის მექანიზმები. ამასთან, ევროპული კანონმდებლობის თანახმად, უნდა შეიქმნას ისეთი სახის საზედამხედველო ორგანოები, რომლებიც ადგილობრივ დონეზე განახორციელებენ პერსონალურ მონაცემთა დამუშავების კანონიერების ზედამხედველობას და ამავდროულად, დაეხმარებიან მოქალაქეებს, რათა დაიცვან თავიანთი უფლებები.“[141] [84]

საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერებაზე კონტროლს და ზედამხედველობას ახორციელებს პერსონალურ მონაცემთა დაცვის ინსპექტორი, რომელიც თანამდებობაზე ინიშნება სამი წლის ვადით, ღია კონკურსის წესით. პერსონალურ მონაცემთა დაცვის ინსპექტორის შერჩევის წესი, თანამდებობრივი შეუთავსებლობა და უფლებამოსილების შეწყვეტის საფუძვლები განისაზღვრება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით. ინსპექტორი თავისი უფლებამოსილების განხორციელებისას, დამოუკიდებელია და არ ექვემდებარება არცერთ სხვა თანამდებობის პირსა და ორგანოს, მასზე რაიმე ზემოქმედება ან მის საქმიანობაში ჩარევა აკრძალულია და ისჯება კანონით. ინსპექტორის საქმიანობის ერთერთ ძირითად მიმართულებას წარმოადგენს როგორც საჯარო, ასევე, კერძო დაწესებულებებისთვის და მოქალაქეებისთვის კონსულტაციის გაწევა, პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე. სტატისტიკური მონაცემების თანახმად, 2013 წლის 1 ივლისიდან 2016 წლის 01 ნოემბრამდე პერიოდში,

[141] Handbook on European data protection law, 2014, see: http://www.echr.coe.int/documents/handbook_data_protection_eng.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა გასცა 4178 კონსულტაცია შემდეგ თემებზე: ფაილური კატალოგის რეესტრის წარმოება -28%, მონაცემთა დამუშავების პრინციპები და საფუძვლები -22 %, სუბიექტის უფლებები და მონაცემთა უსაფრთხოება -12 %, ფარული საგამოძიებო მოქმედებები -5% და სხვა.[142]

პერსონალურ მონაცემთა დაცვის ინსპექტორის ერთ-ერთ ძირითად ფუნქციას წარმოადგენს მონაცემთა სუბიექტის განცხადებების განხილვა პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, რა დროსაც ინსპექტორმა უნდა შეისწავლოს და შეაფასოს განცხადებით წარმოდგენილი ფაქტები და გარემოებები. საჭიროების შემთხვევაში, შესაბამისი პირებისგან გამოითხოვება დამატებითი მასალა ან ხორციელდება მონაცემთა დამმუშავებლის ან/და უფლებამოსილი პირის შემოწმება (ინსპექტირება). [143] 2013 წლის 1 ივლისიდან - 2016 წლის 01 ნოემბრამდე პერიოდში, ინსპექტორმა განიხილა 254 განცხადება, რომელთაგან ყველაზე აქტუალურ საკითხებს წარმოადგენდა პირდაპირი მარკეტინგი, მონაცემთა დამმუშავებლის მიერ მოქალაქისათვის ინფორმაციის მიუწოდებლობა, მონაცემთა გასაჯაროება, სამართალდამცავი ორგანოების მიერ მონაცემების დამუშავების კანონიერება, მონაცემებზე წვდომის კანონიერება, აუდიო-ვიდეოთვალთვალის კანონიერება[144].

პერსონალურ მონაცემთა დაცვის ინსპექტორი ახორციელებს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის მიერ მონაცემთა დამუშავების კანონიერების შემოწმებას (ინსპექტირება), რომელსაც ახორციელებს დაინტერესებული პირის განცხადების საფუძველზე ან საკუთარი ინიციატივით. ინსპექტირება მოიცავს პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვისა და მონაცემთა დამუშავების კანონიერი საფუძვლების არსებობის დადგენას; პერსონალურ მონაცემთა დაცვისათვის მიღებული პროცედურებისა და ორგანიზაციულ-ტექნიკური ზომების კანონმდებლობასთან შესაბამისობის შემოწმებას; ფაილური სისტემის

[142] სტატისტიკური მონაცემები ხელმისაწვდომია ვებგვერდზე: www.pdp.ge.
[143] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ.
[144] სტატისტიკური მონაცემები ხელმისაწვდომია ვებგვერდზე: www.pdp.ge.

კატალოგის, ფაილურ სისტემათა კატალოგების რეესტრისა და პერსონალურ მონაცემთა გაცემის აღრიცხვის შესახებ კანონით დადგენილი მოთხოვნების შესრულების შემოწმებას; პერსონალურ მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის კანონიერების შემოწმებას; პერსონალურ მონაცემთა დაცვასთან დაკავშირებული კანონმდებლობით გათვალისწინებული სხვა მოთხოვნების დაცვის შემოწმებას.[145]

2013 წლის 1 ივლისიდან - 2017 წლის 01 იანვრამდე პერიოდში, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის მიერ განხორციელდა 134 ინსპექტირება. შემოწმდა შემდეგი საჯარო დაწესებულებები: საქართველოს პროკურატურა - 11-ჯერ, შინაგან საქმეთა სამინისტრო - 10-ჯერ, შსს-ს პოლიციის დეპარტამენტის რაიონული განყოფილების სამმართველოები - 7 ჯერ, სასჯელაღსრულებისა და პრობაციის სამინისტრო - 2-ჯერ, ოკუპირებული ტერიტორიებიდან იძულებით გადაადგილებულ პირთა, განსახლებისა და ლტოლვილთა სამინისტრო - 2-ჯერ, სახელმწიფო სერვისების განვითარების სააგენტო - 2 ჯერ, განათლებისა და მეცნიერების სამინისტრო, გარემოს დაცვისა და ბუნებრივი რესურსების სამინისტრო, დიასპორის საკითხებში სახელმწიფო მინისტრის აპარატი, ეკონომიკისა და მდგრადი განვითარების სამინისტრო, ენერგეტიკის სამინისტრო, რეგიონული განვითარებისა და ინფრასტრუქტურის სამინისტრო, შერიგებისა და სამოქალაქო თანასწორობის საკითხებში საქართველოს სახელმწიფო მინისტრის აპარატი, სოფლის მეურნეობის სამინისტრო, სპორტისა და ახალგაზრდობის სამინისტრო, ფინანსთა სამინისტრო, ცენტრალური საარჩევნო კომისია, საქართველოს სახელწიფო უსაფრთხოების სამსახური, მთავრობის კანცელარია, სსიპ „112“, სსიპ „ლ. სამხარაულის სახ. სასამართლო ექსპერტიზის ეროვნული ბიურო“, ახმეტის მუნიციპალიტეტი, ბაღდათის მუნიციპალიტეტის საკრებულო, ბაღდათის მუნიციპალიტეტის გამგეობა, წალკის №2 საჯარო სკოლა, წალკის №1 საჯარო სკოლა, თბილისის №114-ე

[145] იხ. იგივე

საჯარო სკოლა.[146] რაც შეეხება 2013 წლის 1 ივლისიდან 2017 წლის 10 მაისის ჩათვლით, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერებაზე ზედამხედველობას საჯარო სექტორში, ინსპექტორის აპარატიდან მოწოდებული სტატისტიკური ინფორმაციის თანახმად, სულ განხორციელდა 10 ინსპექტირება და 21 განცხადების განხილვა. [147]

აღსანიშნავია, რომ შემოწმების პროცესში, ინსპექტორი უფლებამოსილია, ნებისმიერი დაწესებულებისგან, ფიზიკური და იურიდიული პირისაგან გამოითხოვოს დოკუმენტები და ინფორმაცია, რომლებიც აუცილებელია შემოწმების განსახორციელებლად. მონაცემთა დამმუშავებელი და უფლებამოსილი პირი ვალდებული არიან, ინსპექტორს დაუყოვნებლივ მიაწოდონ ნებისმიერი მოთხოვნილი ინფორმაცია და დოკუმენტი. ინსპექტორი უფლებამოსილია, შემოწმების განხორციელების მიზნით, შევიდეს ნებისმიერ დაწესებულებაში, გაეცნოს მისთვის საინტერესო ნებისმიერ დოკუმენტსა და ინფორმაციას, მიუხედავად მათი შინაარსისა და შენახვის ფორმისა. ისეთი დაწესებულების შემოწმების შემთხვევაში, რომლის საქმიანობაც დაკავშირებულია სახელმწიფო უსაფრთხოებასა და თავდაცვასთან ან რომელიც ახორციელებს ოპერატიულ-სამძებრო საქმიანობას, პერსონალურ მონაცემთა დაცვის ინსპექტორი ვალდებულია, დაგეგმილი შემოწმებისა და მისი ფარგლების შესახებ აღნიშნულ დაწესებულებას აცნობოს წინასწარ, არანაკლებ 3 დღით ადრე.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე საზოგადოების ცნობიერების ამაღლება ასევე პერსონალურ მონაცემთა დაცვის ინსპექტორის მნიშვნელოვანი ფუნქციაა. საზოგადოების ცნობიერების ამაღლების მიზნით, პერსონალურ მონაცემთა დაცვის ინსპექტორი ორგანიზებას უწევს საინფორმაციო შეხვედრებს და სემინარებს, ავრცელებს განცხადებებს და სხვა. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის პრაქტიკაში დანერგვისა და ერთგვაროვანი

[146] სტატისტიკური მონაცემები ხელმისაწვდომია ვებგვერდზე: www.pdp.ge.
[147] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2017 წლის 16 მაისის №PDP 5 17 00001756 წერილი.

განმარტების მიზნით, ინსპექტორი ასევე, უზრუნველყოფს ტრენინგებს მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირებისათვის, შეიმუშავებს სასწავლო და საგანმანათლებლო მასალებს.

ინსპექტორი, როგორც პერსონალურ მონაცემთა დამუშავების კანონიერებაზე ზედამხედველი, საქართველოს პარლამენტსა და მთავრობას წარუდგენს ასევე, წინადადებებს, დასკვნებსა და რეკომენდაციებს, ქვეყანაში პერსონალურ მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებული საკანონმდებლო გარემოს გაუმჯობესების მიზნით, აღნიშნული კი მოიცავს სხვა ქვეყნებისა და საერთაშორისო ორგანიზაციების საუკეთესო პრაქტიკის გაცნობას საჯარო დაწესებულებებისათვის, მონაცემთა დამუშავებასა და დაცვასთან დაკავშირებული კვლევების ჩატარებას, პრაქტიკაში წამოჭრილ სირთულეებზე დაყრდნობით, სასურველი საკანონმდებლო ცვლილებების პროექტის შემუშავებას და სხვა.

დღეის მდგომარეობით, პერსონალურ მონაცემთა დაცვის ინსპექტორს წარდგენილი აქვს ოთხი წლიური ანგარიში საქართველოს პარლამენტში, ასევე, შემუშავებული აქვს რეკომენდაციები ისეთ მნიშვნელოვან თემებზე, როგორიცაა შრომით ურთიერთობებში პერსონალური მონაცემების დაცვა, ბიომეტრიულ და ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემების დამუშავება, უსაფრთხოების წესების დაცვა ონლაინ შესყიდვისას და სხვა.[148]

პერსონალურ მონაცემთა დაცვის ინსპექტორი მასზე დაკისრებულ ფუნქციებს ახორციელებს აპარატის საშუალებით, აპარატის სტრუქტურა და საქმიანობა განისაზღვრება პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის დებულებით. სამართალდარღვევის ფაქტის აღმოჩენის შემთხვევაში და მისი აღსრულების მიზნით, ინსპექტორი უფლებამოსილია, გაატაროს შემდეგი ღონისძიებები: მოითხოვოს დარღვევისა და მონაცემთა დამუშავებასთან დაკავშირებული ნაკლოვანებების მის მიერ მითითებული ფორმით, მითითებულ ვადაში გამოსწორება; მოითხოვოს მონაცემთა დამუშავების დროებით ან სამუდამოდ შეწყვეტა, თუ მონაცემთა

[148] პერსონალურ მოანცემთა დაცვის ინსპექტორის რეკომენდაციები ხელმისაწვდომია ვებგვერდზე: www.pdp.ge

დამმუშავებლის ან უფლებამოსილი პირის მიერ მონაცემთა უსაფრთხოებისთვის მიღებული ზომები და პროცედურები არ შეესაბამება კანონის მოთხოვნებს; მოითხოვოს მონაცემთა დამუშავების შეწყვეტა, მათი დაბლოკვა, წაშლა, განადგურება ან დეპერსონალიზაცია, თუ მიიჩნევს, რომ მონაცემთა დამუშავება ხორციელდება კანონის საწინააღმდეგოდ; მოითხოვოს მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის შეწყვეტა, თუ მათი გადაცემა ხორციელდება კანონმდებლობით განსაზღვრული მოთხოვნების დარღვევით; წერილობით მისცეს რჩევები და გაუწიოს რეკომენდაციები მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს, მათ მიერ მონაცემთა დამუშავებასთან დაკავშირებული წესების უმნიშვნელოდ დარღვევის შემთხვევაში.[149]

ადმინისტრაციული სამართალდარღვევის შემთხვევაში, პერსონალურ მონაცემთა დაცვის ინსპექტორი უფლებამოსილია, კანონმდებლობით განსაზღვრული წესით, მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს დააკისროს შესაბამისი ადმინისტრაციული პასუხისმგებლობა. პერსონალურ მონაცემთა დაცვის ინსპექტორი მონაცემთა დამმუშავებლის მიერ კანონის მოთხოვნათა დარღვევის შემთხვევაში, უფლებამოსილია, გამოიყენოს კანონის აღსრულების ერთი ან რამდენიმე ღონისძიება ერთდროულად, გარკვეული რიგითობის დაცვით ან პარალელურ რეჟიმში. ინსპექტორის გადაწყვეტილება შესასრულებლად სავალდებულოა და მისი გასაჩივრება შეიძლება სასამართლოში, კანონმდებლობით განსაზღვრული წესის შესაბამისად.

2013 წლის 1 ივლისიდან - 2017 წლის 01 იანვრამდე პერიოდში, ინსპექტორის აპარატის მიერ საჯარო და კერძო ორგანიზაციების შემოწმების შედეგად, გამოვლინდა 197 სამართალდარღვევა. მათ შორის, პირდაპირი მარკეტინგის წესების დარღვევა, სუბიექტის ინფორმირების წესების დარღვევა -33%, პრინციპების და საფუძვლების გარეშე მონაცემთა

[149] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“.

დამუშავება-30%, სამართალდამცავი ორგანოების მიერ მონაცემთა მოპოვების წესების დარღვევა -6% და სხვა.[150]

3.2 საზღვარგარეთის ქვეყნების მონაცემთა დაცვაზე ზედამხედველი ორგანოები

აღსანიშნავია, რომ სხვადასხვა ქვეყნებში პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოები სხვადასხვა სახელწოდებით მოქმედებენ. ისევე, როგორც საქართველოში, ჩამონათვალს შორის ვხვდებით პერსონალურ მონაცემთა დაცვის ინსპექტორებს, ასევე, კომისრებს, ომბუდსმენებს და გარანტორებს.

სახელწოდების ვარიაციებთან ერთად, განსხვავებულია საზედამხედველო ორაგნოების მოწყობის ფორმებიც. მაგალითად, საზედამხედველო ორგანოს ხელმძღვანელს შეიძლება, წარმოადგენდეს ერთი პირი, ან კოლეგიური ორგანო. იმ შეთხვევაში, თუ საზედამხედველო ორგანოს წარმოადგენს კოლეგია, მასში შემავალ პირთა რაოდენობა, მათი უფლება-მოვალეობები ეროვნული კანონმდებლობით არის განსაზღვრული. საერთაშორისო სტანდარტები ამ მხრივ რაიმე სახის მოთხოვნას არ აწესებს. განვიხილოთ ევროპის იმ ქვეყნების რამდენიმე საზედამხედველო ორგანოს მოწყობა, რომლებიც მოწინავე როლს ასრულებენ პერსონალურ მონაცემთა დაცვის საერთაშორისო/ეროვნული სტანდარტების დამკვიდრებაში.

იტალია - იტალიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო (პერსონალურ მონაცემთა დაცვის გარანტე) შეიქმნა 1997 წელს, იმ დროს არსებული „პერსონალურ მონაცემთა დაცვის შესახებ“ აქტის საფუძველზე. საზედამხედველო ორგანო არის კოლეგია, რომელსაც ირჩევს პარლამენტი 7 წლის ვადით (მეორე ვადით მათი არჩევა არ შეიძლება). საზედამხედველო ორგანოს ოფისი მდებარეობს ქ.რომში, მისი თანამშრომლების რაოდენობა კი შეადგენს 125 პირს. იტალიის საზედამხედველო ორგანოს კოლეგია შედგება ოთხი პირისგან: პრეზიდენტი, ვიცე-პრეზიდენტი და ორი წევრი. კოლეგიის ორ წევრს

[150] მონაცემები ხელმისაწვდომია ვებგვერდზე: www.pdp.ge.

ირჩევს დეპუტატთა პალატა, დანარჩენ ორს კი სენატი, სპეციალური საარჩევნო პროცედურის საფუძველზე. წევრებს უნდა ჰქონდეთ სამართლებრივი და ტექნიკური (ინფორმაციული ტექნოლოგიების განხრით) გამოცდილება. კოლეგიის შემადგენლობა ამ ორივე მიმართულებით განისაზღვრება. წევრები ირჩევენ პრეზიდენტს, რომელსაც აქვს გადამწყვეტი ხმის უფლება. ისინი ასევე, ირჩევენ ვიცე-პრეზიდენტს, რომელიც პრეზიდენტის ფუნქციებს, ასრულებს მისი არყოფნის შემთხვევაში.[151]

იტალიის საზედამხედველო ორგანოში საქმიანობის განმავლობაში, კოლეგიის შემადგენლობას არ აქვს სხვა თანამდებობის დაკავების უფლება, მათ შორის, არჩევითი თანამდებობის ან პროფესიული/საკონსულტაციო აქტივობების განხორციელების უფლება[152] იტალიის საზედამხედველო ორგანოს შემადგენლობაში, ასევე, მნიშვნელოვანი როლი უკავია აღმასრულებელ მდივანს, რომელიც ხელმძღვანელობს გარანტეს ოფისს.[153]

საფრანგეთი - კნილი (საფრანგეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანო - კომისია) დაფუძნდა 1978 წელს იმ დროს „საფრანგეთის პერსონალურ მონაცემთა დაცვის შესახებ“ აქტის თანახმად. ორგანოს დამოუკიდებლობის გარანტს სწორედ მისი კომპოზიცია წარმოადგენს. იგი შედგება 17 წევრისგან, რომლებსაც ირჩევენ ასამბლეები და სხვადასხვა სახელისუფლებო ორგანოები. წევრები ირჩევენ თავმჯდომარეს. კნილის შემადგელობაში შედის: პარლამენტის ოთხი წევრი (ასამბლეის ორი წევრი, სენატის ორი წევრი); საფრანგეთის ეკონომიკური, სოციალური და გარემოს საბჭოს ორი წევრი; უმაღლესი ხელისუფლების ექვსი წარმომადგენელი (სახელმწიფო საბჭოს ორი წევრი, უზენაესი სასამართლოს ორი წევრი, აუდიტის სასამართლოს ორი წევრი); ხუთი საჯარო მოხელე, რომლებსაც ნიშნავს: ეროვნული ასამბლეის პრეზიდენტი (1 საჯარო ფიგურა), სენატის პრეზიდენტი (1 საჯარო ფიგურა), საფრანგეთის კაბინეტი (3 საჯარო ფიგურა).

---

[151] იტალიის პერსონალურ მონაცემთა დაცვის კოდექსი, მუხლი 153 (1,2,3,4).
[152]იგივე, მუხლი 153 (4)).
[153] მუხლი 156 (1)).

კომისრების მანდატი 5 წელია, პარლამენტარების კი - მათი საპარლამენტო მანდატების მიხედვით განისაზღვრება. კომისიის წევრები კვირაში ერთხელ იწვევენ პლენარულ სესიას, თავმჯდომარის მიერ გაწერილი დღის წესრიგის მიხედვით. სესიების დიდი ნაწილი ეთმობა კანონმდებლობისა და კანონპროექტების განხილვას, რომლებიც მთავრობამ მიაწოდა კნილს მოსაზრებისთვის. ამასთან, კნილი გასცემს ნებართვასაც განსაკუთრებული კატეგორიის მონაცემების დამუშავებაზე. იგი ასევე, აანალიზებს ახალი ტექნოლოგიების გავლენას მოქალაქეთა პერსონალურ მონაცემთა დაცვის საკითხზე.

კნილის შემადგენლობაში ასევე, იქმნება კომიტეტი, რომელიც შედგება 5 წევრისა და თავმჯდომარისგან (რომელიც არ შეიძლება იყოს კნილის თავმჯდომარე). კომიტეტი პერსონალური მონაცემების დაცვის კანონმდებლობის დარღვევისთვის აწესებს სანქციებს, რომელთა რაოდენობამ შეიძლება 300 000 ევროს მიაღწიოს. [154] [85]

ბულგარეთი - პერსონალურ მონაცემთა დაცვის კომისია შედგება თავმჯდომარისა და 4 წევრისგან. წევრების არჩევა ხდება პარლამენტის მიერ, მინისტრთა საბჭოს ინიციატივის საფუძველზე, 5 წლის ვადით. მათი ხელახალი არჩევა მეორე მანდატით შესაძლებელია. კომისია პირველად 2002 წელს შეიქმნა. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-11 მუხლის თანახმად, კომისიის პრეზიდენტი ახორციელებს კომისიის საქმიანობის ორგანიზებასა და ადმინისტრირებას, წარმოადგენს კომისიას მესამე პირებთან ურთიერთობებში, ნიშნავს და ათავისუფლებს მოხელეებს, ამტკიცებს სისხლის სამართლებრივ ბრძანებებს. ისევე, როგორც იტალიაში, აღმასრულებელი მდივანი ახორციელებს ოფისის მენეჯმენტსა და ადმინისტრირებას. ოფისი შედგება 87 თანამშრომლისგან.[155] [86]

---

[154] საფრანგეთში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებგვერდი: https://www.cnil.fr/en/node/287 [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[155] ბულგარეთში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებგვერდი: https://www.cpdp.bg/en/index.php?p=element&aid=39 [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

ბელგია - პირადი ცხოვრების პატივისცემის კომისია შეიქმნა 1992 წელს ბელგიის ფედერალურ წარმომადგენელთა ორგანოს მიერ, „პირადი ცხოვრების პატივისცემის უფლების შესახებ“ აქტის საფუძველზე. კომისია შედგება 16 წევრისგან: პრეზიდენტი, ვიცე-პრეზიდენტი, 6 მუდმივი წევრი და 8 მონაცვლე პირი. პრეზიდენტი და ვიცე-პრეზიდენტი სრულ განაკვეთზე მომუშავე წევრები არიან. იმ შემთხვევაში, თუ პრეზიდენტის მშობლიური ენა ჰოლანდიურია, მაშინ ვიცე-პრეზიდენტის მშობლიური ენა უნდა იყოს ფრანგული და პირიქით. კომისია უნდა შედგებოდეს მინიმუმ, შემდეგი 4 კატეგორიის პირებისგან: სამართლებრივი ექსპერტები, ინფორმაციული ტექნოლოგიების ექსპერტები და 2 ინდივიდი, რომლებსაც აქვთ გამოცდილება საჯარო და კერძო სექტორში პერსონალურ მონაცემთა მართვაში. კომისიის 16-ვე წევრი ინიშნება 6 წლის მანდატით, რომელიც შეიძლება განახლდეს ერთხელ.

2009 წლის შემდეგ, ასევე, არსებობს ელექტრონულ-ადმინისტრაციულ მონაცემთა მიმოცვლის ფლამანდიის საზედამხედველო კომისია. ფლამანდიურ კომისიას იგივე უფლებამოსილებები აქვს, უბრალოდ, ფლამანდიის დონეზე. კონკრეტულ სექტორზე ზედამხედველობის განხორციელების მიზნით, კომისიაში შეიქმნა სექტორული კომიტეტები. სექტორული კომიტეტები შეიქმნა „პირადი ცხოვრების პატივისცემის შესახებ“ აქტის ან კონკრეტული სექტორის მარეგულირებელი აქტის საფუძველზე. მათ ხელმძღვანელობს კომისიის პრეზიდენტი. სექტორული კომიტეტების ერთ წარმომადგენელს ნიშნავს კომისიის პრეზიდენტი, დანარჩენებს კი ირჩევს წარმომადგენელთა პალატა. მათი მანდატიც 6 წლით შემოიფარგლება და წევრები პერსონალურ მონაცემთა დაცვის ექსპერტები არიან. სექტორული კომიტეტების პრეზიდენტებმა უნდა უზრუნველყონ, რომ მათი გადაწყვეტილებები არ ეწინააღმდეგებოდეს კომისიის ხედვას. წინააღმდეგ შემთხვევაში, მათ შეუძლიათ საქმის წარმოების შეჩერება და მისი გადაცემა კომისიისთვის. სექტორული კომიტეტების უფლებები შეიძლება განსხვავდებოდეს ერთმანეთისგან. სექტორული კომიტეტები

ადგენენ წლიურ ანგარიშს, რომელიც კომისიის წლიურ ანგარიშში ქვეყნდება. ამ ეტაპზე, მოქმედებს 5 სექტორული კომიტეტი:

➢ ეროვნული რეესტრი (პირადი ნომრების გამოყენებაზე ზედამხედველობა. კომიტეტი შედგება 6 მუდმივი და 6 მონაცვლე წევრისგან);

➢ ფედერალური ხელისუფლება (ფედერალური ხელისუფლების მიერ პერსონალურ მონაცემთა ელექტრონულ კომუნიკაციაზე ზედამხედველობა. კომიტეტი შედგება 6 მუდმივი და 6 მონაცვლე წევრისგან);

➢ სოციალური უზრუნველყოფა და ჯანდაცვა (კომიტეტი იცავს ბელგიის სოციალური უზრუნველყოფის ქსელის ბენეფიციარებს და ზედამხედველობს ჯანმრთელობასთან დაკავშირებული მონაცემების დამუშავებას. იგი შედგება ორი სექციისგან: სოციალური უზრუნველყოფის და ჯანმრთელობის დაცვის სექციები. ორივე შედგება 6-6 წევრისგან: 2 პირადი ცხოვრების კომისიისა და 4 გარე წევრისგან).

➢ სტატისტიკური ზედამხედველობის კომიტეტი (ზედამხედველობს სტატისტიკის საკითხებს. კომიტეტი შედგება 6 მუდმივი და 6 მონაცვლე წევრისგან. თითოეულ კატეგორიაში ვხვდებით 3 გარე წევრს და კომისიის 3 წარმომადგენელს).

➢ Crossroads Bank of Enterprises (კომიტეტი ზედამხედველობს მონაცემთა დამუშავების უსაფრთხოების საკითხებს ამ ბანკში. კომიტეტი შედგება 6 მუდმივი და 6 მონაცვლე წევრისგან. თითოეულ კატეგორიაში ვხვდებით 3 გარე წევრს და კომისიის 3 წარმომადგენელს).

კომისიას ფუნქციების განხორციელებაში ეხმარება სამდივნო, რომელიც დაახლოებით 50 თანამშრომლისგან შედგება. სამდივნო ასევე, ეხმარება სექტორულ კომიტეტებს.[156] [87]

ჰოლანდია - ჰოლანდიის საზედამხედველო ორგანოს ხელმძღვანელობს კომისართა კოლეგია, რომელიც შედგება თავმჯდომარისა

[156] ბელგიაში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებგვერდი: https://www.privacycommission.be/en/in-a-nutshell [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

და 2 წევრისგან. კოლეგიის წევრები ინიშნებიან მონარქის ბრძანებით, უსაფრთხოებისა და იუსტიციის მინისტრის წარდგინების საფუძველზე. თავმჯდომარე თანამდებობაზე ინიშნება 6 წლის ვადით, რომელიც შეიძლება განახლდეს მხოლოდ ერთხელ. კოლეგიის დანარჩენი წევრების ვადა შემოიფარგლება 4 წლით, რომლის განახლება კიდევ შემდეგი 4 წლით, მხოლოდ ერთხელ შეიძლება. საზედამხედველო ორგანოს მართვის რეგულაციები განსაზღვრავს კოლეგიის პასუხისმგებლობას და საქმიანობის განხორციელების წესებს.[157] [88]

ესპანეთი - ესპანეთის საზედამხედველო ორგანო (სააგენტო) შეიქმნა 1992 წელს. სააგენტოს ხელმძღვანელი ინიშნება სააგენტოს საკონსულტაციო საბჭოს წევრებისგან, მონარქის ბრძანებით, იუსტიციის მინისტრის წარდგინების საფუძველზე. სააგენტოს დირექტორი ინიშნება 4 წლის ვადით. იგი ხელმძღვანელობს სააგენტოს, წარმოადგენს მას საერთაშორისო დონეზე, სააგენტოს საქმიანობის განსახორციელებლად, იღებს რეზოლუციებსა და ინსტრუქციებს.

სააგენტოში ასევე, ფუნქციონირებს საკონსულტაციო საბჭო, რომელიც შედგება 10 წევრისგან. წევრები 4 წლის ვადით ინიშნებიან. საკონსულტაციო საბჭო სამდივნოს ფუნქციასაც ასრულებს. საკონსულტაციო საბჭო იკრიბება სააგენტოს დირექტორის მოწვევით, ყოველ 6 თვეში ერთხელ. იგი პერსონალურ მონაცემთა დაცვის სფეროში, სააგენტოს დირექტორს აძლევს რჩევებს. მის შემადგენლობაში შედის: დეპუტატთა კონგრესის წარმომადგენელი, სენატის წარმომადგენელი, სახელმწიფო ადმინისტრაციის წარმომადგენელი, კატალონიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს წარმომადგენელი, ბასკეთის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს წარმომადგენელი, ესპანეთის მუნიციპალიტეტებისა და პროვინციების ფედერაციის წარმომადგენელი, ისტორიის სამეფო აკადემიის წარმომადგენელი, უნივერსიტეტების საბჭოს წარმომადგენელი,

[157] ჰოლანდიაში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებგვერდი: https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/commissioners-dutch-dpa [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

მომხმარებელთა წარმომადგენელი, კერძო სექტორის წარმომადგენელი. ესპანეთში ასევე, მოქმედებს კატალონიისა და ბასკეთის ავტონომიური სააგენტოები.[158] [89]

დიდ ბრიტანეთში, პოლონეთში, გერმანიაში, ჩეხეთში, ესტონეთში, ირლანდიაში, საზედამხედველო ორგანოს ხელმძღვანელობს ერთი პირი და მათი ფუნქციები დაახლოებით საქართველოს საზედამხედველო ორგანოს ანალოგია.

რაც შეეხება საზღვარგარეთის ქვეყნების სტატისტიკურ მონაცემებს, დიდი ბრიტანეთის პერსონალური მონაცემების დაცვის საზედამხედველო ორგანომ (ICO) გამოაქვეყნა 2016 წლის პირველი სამი თვის სტატისტიკა, მონაცემთა უსაფრთხოების რღვევასთან და მათზე უკანონო წვდომასთან დაკავშირებით. დიდ ბრიტანეთში, 2016 წლის იანვრიდან მარტის ჩათვლით, დაფიქსირდა მონაცემთა უსაფრთხოების რღვევის ან დაკარგვის 448 შემთხვევა. უნდა აღინიშნოს, რომ ამ შემთხვევების უმეტესობა არის ადამიანის მიერ დაშვებული შეცდომის შედეგი. ზემოაღნიშნული 448 შემთხვევიდან, 74 გამოწვეული იყო ქაღალდური დოკუმენტების დაკარგვით, ასევე, 74 შემთხვევაში მონაცემები ფაქსით ან ელექტრონული ფოსტით გაეგზავნა შეუსაბამო მიმღებს, დაკარგული და მოპარული იქნა 20 დაუბლოკავი ელექტრონული მოწყობილობა, 24 შემთხვევაში კი ქაღალდური დოკუმენტაცია უმეთვალყურეოდ იქნა დატოვებული. ასევე, დაფიქსირდა მონაცემების ზეპირსიტყვიერი გამჟღავნება, ინფორმაციის განთავსება დაუცველ ელექტრონულ მოწყობილობაზე და სხვა. რაც შეეხება დაუცველი ვებგვერდებისა და ჰაკერული თავდასხმების შედეგად მონაცემების დაკარგვას, დაფიქსირდა მხოლოდ 39 ასეთი შემთხვევა. ბრიტანეთის საზედამხედველო ორგანოს ცნობით მონაცემთა უსაფრთხოების რღვევის ან დაკარგვის 448 შემთხვევიდან, 184 შემთხვევა ჯანდაცვის სექტორში დაფიქსირდა; ადგილობრივ მთავრობებზე, საგანმანათლებლო დაწესებულებებზე და ბიზნესზე 115 ინციდენტი

[158] ესპანეთში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებგვერდი: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/historia-iden-idphp.php [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

მოვიდა, რაც შეეხება საფინანსო, სადაზღვევო და საკრედიტო სექტორს, აქ დაფიქსირებულმა დარღვევებმა 25 შემთხვევა შეადგინა. გარდა ამისა, დამატებით დაფიქსირდა მონაცემთა უსაფრთხოების რღვევის 176 ფაქტი ელექტრონული კომუნიკაციის მომსახურების განმახორციელებელი კომპანიებიდან. [159] [90]

გარდა სტატისტიკური მონაცემებისა, მნიშვნელოვანია დიდი ბრიტანეთის პერსონალური მონაცემების დაცვაზე ზედამხედველობის ორგანოს (ICO) მიერ მიღებული გადაწყვეტილებები. ერთ-ერთ საქმეზე, რომელიც შეეხებოდა ყოფილი მეუღლისთვის პაციენტზე და მის შვილზე კონფიდენციალური ინფორმაციის გადაცემას, ICO-მ სამედიცინო დაწესებულება 40 000 ფუნტი სტერლინგით დააჯარიმა.

საქმის შესწავლისას, ICO-მ გამოავლინა, რომ სამედიცინო დაწესებულებამ ერთ-ერთი პაციენტის ყოფილი მეუღლის მოთხოვნის საფუძველზე, ამ უკანასკნელს მიაწოდა ინფორმაცია პაციენტისა და მისი შვილის შესახებ. გაიცა საკმაოდ მოცულობითი ინფორმაცია, რომელიც მოიცავდა 62-გვერდიან დოკუმენტს. აღნიშნული ფაქტი დაამძიმა გარემოებამ, რომ პაციენტმა, ვისი მონაცემებიც იქნა გამჟღავნებული, ფაქტის დადგომამდე გააფრთხილა დაწესებულება, რომ მისი პერსონალური ფაილი არავისთვის მიეწოდებინათ.

ICO-ს წარმომადგენელმა განაცხადა, რომ ადამიანებისთვის ძალიან დამთრგუნველია ის ფაქტი, რომ ინფორმაცია, რომელსაც ისინი უზიარებენ საკუთარ ექიმს, შეიძლება, ხელმისაწვდომი გახდეს მესამე პირებისთვის. ამასთან, მეტად მნიშვნელოვანია, რომ სამედიცინო დაწესებულებებმა უზრუნველყონ სწავლება და ტრენინგები საკუთარი თანამშრომლებისათვის, რათა შემდგომში ინფორმაციის გამჟღავნების მსგავსი ფაქტები თავიდან იქნეს არიდებული.[160] [91]

---

[159] „Human error is the main cause of data breaches, according to the UK's data protection watchdog“ 2016, see: http://www.out-law.com/en/articles/2016/june/human-error-remains-main-cause-of-data-breaches-ico-data-shows/? [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[160] „Watchdog fines GP for data breach“, 2016, see: http://www.professionalsecurity.co.uk/news/case-studies/watchdog-fines-gp-for-data-breach/? [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

ინგლისის საქალაქო საბჭო კი 100-ზე მეტი ადამიანის შესახებ პერსონალური მონაცემების შემცველი ფაილების მიტოვებულ შენობაში უყურადღებოდ დატოვების გამო, დიდი ბრიტანეთის საზედამხედველო ორგანომ 100 ათასი ფუნტი სტერლინგით დააჯარიმა.

ჰემფშირის საქალაქო საბჭო ინგლისში საზოგადოებრივი სერვისის მიწოდებაზეა პასუხისმგებელი და მისი ბენეფიციარების შესახებ უყურადღებოდ მიტოვებული დოკუმენტაცია შენობის ახალმა მესაკუთრემ იპოვა. ნაპოვნი დოკუმენტაცია შეიცავდა ზრდასრულთა და არასრულწლოვანთა სენსიტიურ ინფორმაციას და დატოვებული იყო ისეთ პირობებში, სადაც შეიძლებოდა, მარტივად ხელმისაწვდომი გამხდარიყო მესამე პირებისთვის. ბრიტანეთის საზედამხედველო ორგანოს წარმომადგენელთა განცხადებით, ამ ინფორმაციის გამჟღავნებას შესაძლოა, მეტად დიდი ზიანი მოჰყოლოდა. საქალაქო საბჭოს მიერ შენობის დატოვებასა და ახალი მფლობელების მიერ მასში შესახლებას შორის ორწლიანი პერიოდი იყო გასული, რაც მეტად დიდი დროა, კონფიდენციალური მონაცემების უყურადღებოდ დატოვების თვალსაზრისით.[161] [92]

დიდი რეზონანსი მოჰყვა ასევე, ჰაკერების მიერ სექსუალური მომსახურების ერთ-ერთი ვებგვერდის Ashley Madison-ის გატეხვას, რის საფუძველზეც, მოიპარეს 33 მილიონი მომხმარებლის სახელი, მისამართი, ელფოსტა და ინფორმაცია მომხმარებელთა სქესობრივი ცხოვრების შესახებ. აღსანიშნავია, რომ ჰაკერებმა შექმნეს ონლაინ პროგრამა, სადაც ელფოსტის ცოდნის შემთხვევაში, შესაძლებელი იყო იმის გარკვევა, იყო თუ არა მომხმარებელი დარეგისტრირებული Ashley Madison-ის ვებგვერდზე.

კიბერ თავდასხმამდე, ვებგვერდზე რეგისტრირებული იყო მილიონობით მომხმარებელი, მთელი მსოფლიოს მასშტაბით, მათ შორის, სამთავრობო და დიდი კომპანიების საფოსტო სერვერებიდან.

[161] „Council fined £100,000 after social care files left in empty building“, 2016, see: https://www.theguardian.com/society/2016/aug/17/council-fined-100000-after-social-care-files-left-empty-building [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

გავრცელებული ინფორმაციის თანახმად, 100 მომხმარებელზე მეტი დარეგისტრირებული იყო დიდი ბრიტანეთის თავდაცვის სამინისტროს ელფოსტის მეშვეობით, და დაახლოებით ამდენივე სამთავრობო ელფოსტით, რომლის დაბოლოებაა gov.uk. პარლამენტის ერთ-ერთი წევრი, რომლის მონაცემებიც აღმოჩნდა ვებგვერდზე, აცხადებს, რომ არანაირი კავშირი აღნიშნულ ვებგვერდთან არ აქვს და იგი არის თაღლითობის მსხვერპლი.

ვებგვერდს ჰქონდა ფასიანი მომსახურება, რომლის საშუალებითაც მომხმარებელს შეეძლო საკუთარი მონაცემების სრული წაშლა, თუმცა აღნიშნული სერვისი, სავარაუდოდ, არ მუშაობდა, რადგან მასზე დარჩენილი ინფორმაცია საკმარისი იყო მომხმარებლების და მათი ინტერესების იდენტიფიკაციისათვის. ვებგვერდზე არსებული ინფორმაციის დიდი ნაწილი სპეციალური სისტემით იყო დაცული, რაც მოპარვის შემთხვევაში, ამ მონაცემების ნახვას შეუძლებელს ხდიდა. თუმცა ისეთი მონაცემები, როგორიცაა ელფოსტის მისამართი, ბარათის ნომერი და ინტერესთა სფერო, არ იყო დაშიფრული, ამიტომ ჰაკერებმა შეძლეს ამ ინფორმაციის გამოყენება და გავრცელება.[162] [93]

თავი IV. საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას გამოვლენილი პრობლემები (ინსპექტორის გადაწყვეტილებების ანალიზი)

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვა, შესაძლებელია ითქვას, რომ ყველა ქვეყნის საზედამხედველო ორგანოს დღის წესრიგის მთავარ საკითხს უნდა წარმოადგენდეს, ვინაიდან ადამიანის ჯანმრთელობის მდგომარეობისა თუ სექსუალური ცხოვრების, ნასამართლეობისა თუ სხვა ამ კატეგორიას მიკუთვნებული მონაცემების უსაფუძვლო დამუშავებამ და გამჟღავნებამ შესაძლოა, პირს გამოუსწორებელი პირადი და რეპუტაციული ზიანი მიაყენოს. საკითხის

[162] „Ashley Madison hackers release vast database of 33m accounts“, 2015, see: http://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

პრიორიტეტულობიდან გამომდინარე, საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის მხრივ არსებული პრობლემებისა და ინსპექტორის საზედამხედველო ფუნქციის ეფექტიანობის შესაფასებლად, შესაბამისი კითხვარის საფუძველზე, ინსპექტორის აპარატიდან გამოვითხოვეთ სტატისტიკური და საჯარო ინფორმაცია.

ინსპექტორის აპარატში გაგზავნილი კითხვარი, სხვა საკითხებთნ ერთად, მოიცავდა შემდეგ კითხვებს:

1. განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების მიზნით, რამდენი და რომელი საჯარო დაწესებულებები შეამოწმა პერსონალურ მონაცემთა დაცვის ინსპექტორმა, 2013 წლიდან 2017 წლის 30 აპრილის პერიოდში? გთხოვთ, აღნიშნული სტატისტიკური ინფორმაცია წარმოადგინოთ წლების მიხედვით და ამასთან, ასევე, გადმოგვიგზავნოთ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების საფუძველზე ინსპექტორის მიერ გამოტანილი გადაწყვეტილებების ასლები.

2. 2013 წლიდან 2017 წლის 30 აპრილის პერიოდში, რამდენმა მოქალაქემ მომართა პერსონალურ მონაცემთა დაცვის ინსპექტორს, მისი განსაკუთრებული კატეგორიის პერსონალური მონაცემის დამუშავებასთან დაკავშირებით? გთხოვთ, სტატისტიკური ინფორმაცია წარმოადგინოთ წლების მიხედვით, ასევე, გადმოგვიგზავნოთ აღნიშნული განცხადებების განხილვის საფუძველზე ინსპექტორის მიერ გამოტანილი გადაწყვეტილებების ასლები.

ინსპექტორის აპარატიდან სრულად მოგვეწოდა სტატისტიკური ინფორმაცია, რომლის თანახმადაც, საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემთა დამუშავების კანონიერების შემოწმების მიზნით, მითითებულ პერიოდში, განხორციელდა 11 ინსპექტირება, მათგან წლების მიხედვით ჩატარებული შემოწმებების რაოდენობის სტატისტიკური მაჩვენებელი შემდეგია:

➢ 2013 წელს შემოწმება არ ჩატარებულა;

➢ 2014 წელს ჩატარდა 02 შემოწმება - საქართველოს შინაგან საქმეთა სამინისტრო (განცხადების ფარგლებში) და საქართველოს მთავარი პროკურატურა;

➢ 2015 წელს ჩატარდა 03 შემოწმება - სსიპ ,,ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიურო'' (განცხადების ფარგლებში), სსიპ ქალაქ წალკის №1 საჯარო სკოლა, სსიპ ქალაქ წალკის №2 საჯარო სკოლა;

➢ 2016 წელს ჩატარდა 06 შემოწმება - სსიპ თბილისის №114 საჯარო სკოლა, სსიპ ადიგენის მუნიციპალიტეტის სოფელ აბასთუმნის საჯარო სკოლა, საქართველოს შინაგან საქმეთა სამინისტრო (2-ჯერ), სსიპ ქაქუცა ჩოლოყაშვილის სახელობის ქალაქ თბილისის №178-ე საჯარო სკოლა, საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო (კვლავ მიმდინარეობს);

➢ 2017 წელს განსაკუთრებული კატეგორიის მონაცემებთან დაკავშირებით, შემოწმება არ ჩატარებულა.

რაც შეეხება მოქალაქეთა განცხადებებს, 2017 წლის 30 აპრილის ჩათვლით, განსაკუთრებული კატეგორიის მონაცემების დამუშავების კანონიერების შესწავლის მიზნით, ინსპექტორის აპარატმა მიიღო მოქალაქეთა 22 განცხადება, რომელთა რაოდენობის სტატისტიკური მაჩვენებელი წლების მიხედვით შემდეგნაირად გამოიყურება:

➢ 2013 წელს ასეთი განცხადება არ შემოსულა;

➢ 2014 წელს – 02 განცხადება;

➢ 2015 წელს - 07 განცხადება;

➢ 2016 წელს – 12 განცხადება (ერთის განხილვა კვლავ მიმდინარეობს);

➢ 2017 წელს – 01 განცხადება.

დანართის სახით, აპარატის მიერ გამოიგზავნა ინსპექტორის მიერ მიღებული ზემოაღნიშნული გადაწყვეტილებების მნიშვნელოვანი ნაწილი, 28 (ოცდარვა) გადაწყვეტილება დაფარვით, თუმცა ინფორმაციის სრულად

მოწოდება ვერ მოხერხდა. წერილში მითითებული განმარტების თანახმად, ვერ მოხდა მოწოდება იმ გადაწყვეტილებებისა, რომელთა დეპერსონალიზაცია შეუძლებელია გადაწყვეტილების არსებითი ნაწილების დაფარვის გარეშე. შესაბამისად, საკითხის შესწავლისას, ვიხელმძღვანელეთ, ერთი მხრივ, ინსპექტორის აპარატის მიერ მოწოდებული გადაწყვეტილებებით, ხოლო მეორე მხრივ, პერსონალურ მონაცემთა დაცვის ინსპექტორის ყოველწლიური ანგარიშებით.

4.1. 2013-2014 წლებში გამოვლენილი პრობლემები

ინსპექტორის აპარატს 2013 წელს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერება არ შეუმოწმებია და არც მოქალაქეებს მიუმართვათ ასეთი შინაარსის განცხადებით, რაც სავარაუდოდ, განპირობებული იყო ინსპექტორის, როგორც საზედამხედველო ინსტიტუტის სიახლითა და პერსონალურ მონაცემთა დაცვის საკითხებისადმი ცნობადობის დაბალი მაჩვენებლით. აღნიშნულ გარემოებას ადასტურებს ინოვაციებისა და რეფორმების ცენტრის მიერ 2013 წელს განხორციელებული მონიტორინგის ანგარიში, რომლის თანახმადაც, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ამოქმედების შემდგომ, მისი საჯარო უწყებებში ინპლემენტაციის მიზნით განხორციელებული მონიტორინგის შედეგად, საქართველოს სამინისტროებში გამოვლინდა, რომ „პერსონალურ მონაცემთა დაცვის საკითხისადმი ცნობადობა დაბალია, ზოგან კი უბრალოდ, არ არსებობს. სამინისტროების უმრავლესობას არ აქვს გააზრებული პერსონალურ მონაცემთა დაცვის შესახებ კანონმდებლობის ინპლემენტაციისთვის გასატარებელი ღონისძიებები. არცერთ სამინისტროს არ გადაუდგამს ქმედითი ნაბიჯები კანონის იმპლემენტაციისათვის. არ არსებობს კანონის იმპლემენტაციის კონკრეტული ხედვა და გეგმები. არ არსებობს წინაპირობები და მტკიცებულებები ვარაუდისთვის, რომ მონიტორინგის პერიოდისთვის, საქართველოს სამინისტროებში არსებობს მკაფიო ნება და სერიოზული განზრახვა პერსონალურ მონაცემთა დაცვის

საკითხის მოწესრიგებისათვის.“[163] 2013 წელს საჯარო სექტორში მონაცემთა დამუშავების კუთხით არსებულ მნიშვნელოვან პრობლემებზე საუბრობს ინსპექტორი 2013-2014 წლების ანგარიშში და მონაცემთა ავტომატური დამუშავების პროცესში, ერთ-ერთ მთავარ გამოწვევად მიუთითებს **უწყებებს შორის მონაცემთა გაცვლის ან/და წვდომის მინიჭებისთვის სამართლებრივი საფუძვლის არარსებობას.** ანგარიშში აღნიშნულია, რომ „ხშირად ახალ ტექნოლოგიებზე გადასვლა შესაბამისი საკანონმდებლო ბაზის განახლების გარეშე მიმდინარეობდა. მონაცემთა ავტომატური დამუშავების პროცესში, ერთ-ერთ მთავარ პრობლემას წარმოადგენს უწყებებს შორის მონაცემთა გაცვლის ან/და წვდომის მინიჭებისთვის სამართლებრივი საფუძვლის არარსებობა. ბოლო დროს, განსაკუთრებით იზრდება სხვადასხვა საჯარო უწყებებს შორის მონაცემთა გაცვლის, ასევე, კერძო სექტორის მიერ დამუშავებულ მონაცემებზე საჯარო უწყებების წვდომის მაჩვენებლები, რაც კიდევ უფრო ამძიმებს მონაცემთა დამუშავების კუთხით არსებულ არცთუ სახარბიელო მდგომარეობას და ქმნის მონაცემთა უკანონო დამუშავებისთვის ხელსაყრელ გარემოს. მონაცემთა დამმუშავებლები ყურადღების მიღმა ტოვებენ იმ მნიშვნელოვან გარემოებას, რომ მონაცემების მოპოვებისა და შენახვის უფლებამოსილება ორგანიზაციას ავტომატურად არ ანიჭებს ამ მონაცემების სხვა უწყებისათვის გადაცემის უფლებას.“[164] მითითებულ ანგარიშში, განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას გამოვლენილ დარღვევებთან დაკავშირებით ნათქვამია, რომ „2013 წლის აგვისტო-სექტემბერში, ეროვნული უშიშროების საბჭოს მდივნის მომართვის საფუძველზე, ინსპექტორმა შეისწავლა წინასაარჩევნო პერიოდში, ერთ-ერთი უნივერსიტეტის კვლევის ფარგლებში, მთავრობის კანცელარიის კოორდინირებით, 12 სამინისტროში მოხელეთა პოლიტიკური შეხედულებების შესახებ მონაცემთა დამუშავების საკითხი. დადგინდა, რომ

[163] ინოვაციებისა და რეფორმების ცენტრი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ინპლემენტაცია საქართველოს სამინისტროებში“, მონიტორინგის ანგარიში, 2013 წელი, გვ.6

[164] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

კვლევის მიზანს წარმოადგენდა საჯარო სექტორში მოქალაქეთა დასაქმების განმაპირობებელი ფაქტორების გამოვლენა. მთავრობის კანცელარია კოორდინაციას უწევდა სამინისტროების მონაწილეობას კვლევაში და არ წარმოადგენდა მონაცემთა დამმუშავებელს. საჯარო მოსამსახურეებისთვის დარიგებული კითხვარები იყო ანონიმური, მათი შევსება არ ატარებდა სავალდებულო ხასიათს, თუმცა კითხვარს არ ახლდა შესაბამისი განმარტება და დასმული კითხვების ერთობლიობა იძლეოდა კვლევაში მონაწილე მოხელეთა იდენტიფიცირების შესაძლებლობას. შევსებული კითხვარების შეგროვება ხდებოდა თითოეულ უწყებაში სპეციალურად განსაზღვრულ პირთან. მიუხედავად იმისა, რომ საკითხის შესწავლის დროისთვის, მთავრობის კანცელარიის ინიციატივით, კვლევა შეწყდა, არსებობდა პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-4, მე-5 და მე-6 მუხლების დარღვევის საფრთხე. ამიტომ პერსონალურ მონაცემთა დაცვის ინსპექტორის მიმართვის საფუძველზე შევსებული კითხვარები განადგურდა.“[165]

ამავე ანგარიშში, ასევე საჯარო სექტორში არსებულ მნიშვნელოვან პრობლემად განსაკუთრებული კატეგორიის მონაცემთა დამუშავებისას, პრაქტიკაში **დამმუშავებლების მიერ თანხმობის ამსახველი დოკუმენტის წარმოუდგენლობა სახელდება.** მონაცემთა დამმუშავებლები ვერ უზრუნველყოფენ წარმოდგენას დოკუმენტისა, რომელშიც მკაფიოდ და ნათლად იქნებოდა გამოხატული სუბიექტის ნება. უფრო მეტიც, დამმუშავებლები არ არიან ინფორმირებულნი მათ მიერ დამუშავებული მონაცემების სენსიტიური ხასიათისა და კანონით დადგენილი მოთხოვნების შესახებ, რის გამოც უზრუნველყოფილი არ არის მონაცემთა უსაფრთხოების მინიმალური სტანდარტი.

პერსონალურ მონაცემთა დაცვის ინსპექტორი 2013-2014 წლების ანგარიშში ყურადღებას ამახვილებს **სამართალდამცავი ორგანოების მიერ სატელეკომუნიკაციო კომპანიების მონაცემთა ბაზებში არსებულ ინფორმაციასთან პირდაპირი წვდომის საკითხზე** (მათ შორის სატელეფონო

[165] პერსონალურ მონაცემთა დაცვის ინპექტორის 2013-2014 წლების ანგარიში, ხელმისაწვდომია: www.pdp.ge.

კომუნიკაციისა და პირის ადგილმდებარეობის შესახებ), ფარული მიყურადებისა და თვალთვალის განხორციელებაზე, რაც განპირობებულია მათი უფლებამოსილებით, დანაშაულის გამოძიების მიზნებისთვის, აწარმოონ ფარული ვიდეო და აუდიოჩაწერა, ფოტოგადაღება, სატელეფონო საუბრის მოსმენა და სხვა.

„ფარული მიყურადებისა და თვალთვალის საკითხი განსაკუთრებული სიმწვავით წარმოჩნდა 2013 წლის გაზაფხულზე, როდესაც შინაგან საქმეთა სამინისტრომ გაავრცელა ინფორმაცია 2005-2012 წლებში შექმნილი ათასობით ფარული აუდიო და ვიდეოჩანაწერის შესახებ, რომელთა საერთო მოცულობა 260 678 მეგაბაიტი იყო, ხოლო ჩანაწერების ხანგრძლივობა 1760 საათს აჭარბებდა.“ „....აღმოჩენილი მასალა მოიცავდა პოლიტიკოსების, ბიზნესის და სამოქალაქო საზოგადოების წარმომადგენლების პირადი ცხოვრების ამსახველ კადრებს, აუდიოჩანაწერებსა და ფოტოებს. რამდენიმე ჩანაწერზე ასახული იყო პატიმართა წამების ფაქტები.

კომისიამ, მუშაობის პროცესში, ვერ მოიძია პირადი ცხოვრების ამსახველი ვიდეო და აუდიომასალის კანონიერად მოპოვების დამადასტურებელი ოფიციალური დოკუმენტი. პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაციით, კომისიამ შეიმუშავა ინტიმური ცხოვრების ამსახველი მასალის აღრიცხვის, უსაფრთხოებისა და განადგურების მეთოდოლოგია, რის შედეგადაც განადგურდა ინფორმაციის 112 ელექტრონული მატარებელი, ხოლო ძირითადი მასალა (633 ელექტრონული მატარებელი) გამოძიების მიზნით, გადაეცა მთავარ პროკურატურას.“[166]

2013-2014 წლების ანგარიშში მნიშვნელოვანი ადგილი უკავია მოქალაქეთა **ჯანმრთელობის მდგომარეობასთან და ნასამართლობასთან დაკავშირებული მონაცემების უკანონო გასაჯაროებას.** „ინსპექტორის აპარატის მიერ ჩატარებული კონსულტაციების შედეგად, გამოიკვეთა, რომ

[166] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

შრომით ურთიერთობებში განსაკუთრებული კატეგორიის მონაცემთა დამუშავება ერთ-ერთ გავრცელებულ პრობლემას წარმოადგენს. საჯარო დაწესებულებების მიერ ისეთი განსაკუთრებული კატეგორიის მონაცემების დამუშავება, როგორიცაა ნასამართლობა და სამედიცინო-ნარკოლოგიური შემოწმების შედეგი, რეგულირდება „საჯარო სამსახურის შესახებ“ საქართველოს კანონით. შესაბამისად, არსებობს მონაცემთა დამუშავების სამართლებრივი საფუძველი. სხვა სახის განსაკუთრებული კატეგორიის მონაცემებთან დაკავშირებით, აუცილებელია სუბიექტის ინფორმირებული და წერილობითი თანხმობის არსებობა“,- ნათქვამია ამ ანგარიშში.

რაც შეეხება 2014 წელს, ინსპექტორის აპარატიდან მიღებულ ინფორმაციაზე დაყრდნობით, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების მიზნით, ინსპექტორმა 2014 წელს განახორციელა 02 შემოწმება და ამავე საკითხზე განიხილა მოქალაქეთა 02 განცხადება. შემოწმებები ჩატარდა საქართველოს მთავარ პროკურატურასა და საქართველოს შინაგან საქმეთა სამინისტროში, ამ კონკრეტულ საქმეებს, გამოტანილ გადაწყვეტილებებთან ერთად, განიხილავს ინსპექტორი 2014 წლის ანგარიშში.

მოქალაქეთა მომართვები ადასტურებს, რომ ისინი ხშირ შემთხვევაში, **არასათანადოდ ან საერთოდ არ არიან ინფორმირებულნი მონაცემთა დამუშავების მიზნის შესახებ,** რამდენიმე მათგანმა ასევე, მიუთითა ღირსების შემლახავ გარემოში მონაცემთა დამუშავების თაობაზე. მაგალითად, პირებმა, რომელთაც ნებაყოფლობით გაიარეს ნარკოლოგიური შემოწმება, განაცხადეს, რომ შემოწმება ხორციელდებოდა ვიდეოკონტროლის პირობებში, ყოველგვარი ალტერნატიული საშუალების შეთავაზების გარეშე. იმავდროულად, დაკვირვების ოთახში განთავსებულ მონიტორზე გამოსახულების ნახვა არა მხოლოდ პერსონალს, არამედ ნარკოლოგიური შემოწმების სხვა მსურველებსაც შეეძლოთ. „პრაქტიკაში ყველაზე პრობლემურია მკაფიოდ განსაზღვრული კანონიერი მიზნით მონაცემთა დამუშავება. როგორც საჯარო, ისე კერძო ორგანიზაციების უმრავლესობა ვერ ახდენს მონაცემთა დამუშავების (მაგალითად,

შეგროვების, შენახვის, გასაჯაროების და სხვა) კონკრეტული და ლეგიტიმური მიზნის იდენტიფიცირებას. შესაძლოა, ორგანიზაციას ჰქონდეს მონაცემთა შეგროვებისა და გარკვეული ვადით შენახვის მიზანი, რაც იმთავითვე, არ გულისხმობს მის მიერ ამ მონაცემების სხვა ორგანიზაციისთვის გადაცემის უფლებამოსილებას. საჯარო სექტორის მიერ მონაცემთა დამუშავების მიზნის განსაზღვრისას, ხშირად ხდება მათი საქმიანობის მარეგულირებელი ნორმატიული აქტების ზოგადად მითითება, რასაც მონაცემთა დამუშავების პირდაპირ განსაზღვრული კანონიერი მიზნის არარსებობა განაპირობებს. ეს კი წინააღმდეგობაში მოდის საჯარო სამართლის უმთავრეს პრინციპთან - „რაც კანონით დაშვებული არ არის, აკრძალულია“, - ნათქვამია 2013-2014 წლების ანგარიშში.

ამავე პერიოდის ერთ-ერთ მთავარ პრობლემას **საჯარო უწყებების მიერ მონაცემთა დამუშავების პრინციპების დარღვევა წარმოადგენდა.** „პრაქტიკაში მრავლად გვხვდება **მიზნის არაპროპორციულად, არაადეკვატურად დიდი მოცულობით და განუსაზღვრელი ვადით მონაცემების დამუშავების ფაქტები.** მონაცემთა დამუშავების პროცესში, არ ხდება მიზნის შესაბამისი მონაცემების მოცულობის შეფასება. ზოგიერთი დამმუშავებელი აცნობიერებს, რომ მის მიერ მოთხოვნილი ან მიღებული ინფორმაცია არაპროპორციული და არაადეკვატურია, თუმცა ელექტრონული პროგრამის ან მონაცემთა ბაზის სტრუქტურა და ფორმატი არ იძლევა უფრო მცირე მოცულობით მონაცემთა დამუშავების საშუალებას. სამწუხაროა, რომ ძვირადღირებულ მონაცემთა ბაზების შექმნა წინა წლებში ხორციელდებოდა პერსონალური მონაცემების დაცვის სტანდარტების უგულებელყოფით, რაც ნეგატიურად აისახება დღეს არსებულ მდგომარეობაზე.“

„...საანგარიშო პერიოდში, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა, მოქალაქეთა განცხადების საფუძველზე, ჩაატარა საქართველოს შინაგან საქმეთა სამინისტროს რამდენიმე დანაყოფის ინსპექტირება (შემოწმება), რაც მოიცავდა შრომითი ურთიერთობის ფარგლებში, მონაცემთა დამუშავების, მოქალაქის შესახებ შსს-ს მონაცემთა ბაზებში

დაცული ინფორმაციის კანონიერების შემოწმებას და სასაზღვრო–გამშვებ პუნქტებზე შეგროვებული ინფორმაციის სხვა უწყებებისთვის ხელმისაწვდომობას. ინსპექტირების შედეგად, შინაგან საქმეთა სამინისტროს დაევალა ხარვეზების გამოსწორება და მიმდინარეობს მონიტორინგი გადაწყვეტილების შესრულებაზე.“[167]

2014 წელს ინსპექტორის აპარატმა, საკუთარი ინიციატივით, შეამოწმა ასევე საქართველოს შინაგან საქმეთა სამინისტროს მიერ საზღვრის კვეთის პროცესში პერსონალური მონაცემების დამუშავების კანონიერება. პროცესში აღმოჩნდა, რომ საზღვრის კვეთის დროს, ადგილი ჰქონდა ყველა მგზავრისათვის ფოტოსურათის გადაღებას და მათ ასახვას მონაცემთა ავტომატიზებულ ბაზაში. ფოტოსურათის გადაღება ხდებოდა საზღვრის გადაკვეთის ყველა შემთხვევაში სტანდარტულად, მაშინაც კი, როდესაც პირის მიმართ არ არსებობდა რაიმე ეჭვი ან/და მონაცემთა ბაზაში ასახული იყო პირის იდენტიფირებისთვის გამოსადეგი ხარისხის ფოტოსურათი. შემოწმების პროცესში, სამინისტრომ დაიწყო ახალი სტანდარტის დანერგვა, რომლის თანახმადაც, სახელმწიფო საზღვარზე ფოტოგადაღება მოხდება მხოლოდ გამონაკლის შემთხვევებში. ამასთან, სასაზღვრო გამტარ პუნქტებზე თვალსაჩინო ადგილას განთავსდა ვიდეოთვალთვალის შესახებ გამაფრთხილებელი ნიშნები და განისაზღვრა საზღვრის კვეთის პროცესში მოპოვებული მონაცემების შენახვის ვადა.“

2014 წლის ანგარიშში კი პერსონალურ მონაცემთა დაცვის ინსპექტორი, განსაკუთრებული კატეგორიის მონაცემების დამუშავების კუთხით, უკვე მიუთითებს საჯარო სექტორში არსებულ სხვა პრობლემატიკაზე, რომელთა შორის მნიშვნელოვანი ადგილი **პირის ჯანმრთელობის შესახებ ინფორმაციის დამუშავებას ეხება.** საჯარო უწყებების მხრიდან ასეთი ხასიათის ინფორმაციის დამუშავება და გავრცელება სავარაუდოდ, მიზნად ისახავს საზოგადოებაში უწყების იმიჯის დაცვას, თუმცაღა აღნიშნული ქმედების შედეგად, მიიღება პირის ცხოვრებაში უნებართვო, უკანონო ჩარევა და განსაკუთრებული კატეგორიის

[167] იხ. იგივე

პერსონალური მონაცემების საჯარო გავრცელება, მისი ნების საწინააღმდეგოდ.

ინსპექტორი 2014 წლის ანგარიშში განიხილავს საქართველოს მთავარი პროკურატურის მიერ მის ოფიციალურ ვებგვერდზე გამოქვეყნებული სისხლის სამართლებრივი დევნის მასალებს, რომელთა შორისაც იყო ბრალდებულის ოჯახის წევრის სამედიცინო დიაგნოზი. „ინსპექტირების შედეგად დადგინდა, რომ ადგილი ჰქონდა განსაკუთრებული კატეგორიის მონაცემების კანონით გათვალისწინებული საფუძვლის გარეშე გავრცელებას, რისთვისაც „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად, მთავარ პროკურატურას ადმინისტრაციული სახდელის სახით, შეეფარდა ჯარიმა 1000 ლარის ოდენობით. ინსპექტორის გადაწყვეტილება გასაჩივრდა სასამართლოში, თუმცა თბილისის საქალაქო სასამართლომ საჩივარი არ დააკმაყოფილა და საქართველოს მთავარი პროკურატურის მხრიდან ადმინისტრაციული სამართალდარღვევის ჩადენის ფაქტი დაადასტურა. სასამართლომ ასევე არ გაიზიარა საჩივრის ავტორის განმარტება, რომ გამოძიების მიზნებისთვის მონაცემთა დამუშავება-გავრცელებაზე არ ვრცელდებოდა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოქმედება. მოცემულ შემთხვევაში, მთავარი პროკურატურა გასცდა სისხლის სამართლის საპროცესო კოდექსითა და დანაშაულის გამოძიების სხვა მარეგულირებელი ნორმატიული აქტებით განსაზღვრულ მიზნებს, შესაბამისად, საზოგადოების ინფორმირების მიზნით, დიაგნოზის გასაჯაროების დროს, მასზე ვრცელდებოდა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მოქმედება.“[168]

განსაკუთრებული კატეგორიის მონაცემთა კანონიერი საფუძვლის გარეშე გამჟღავნებისთვის ადმინისტრაციული პასუხისმგებლობა 2014 წელს ასევე, დაეკისრა სასჯელაღსრულებისა და პრობაციის სამინისტროსაც, რომელმაც „ერთ-ერთი მსჯავრდებულის გარდაცვალების შემდგომ, საზოგადოების ინფორმირების მიზნით და გარდაცვალების ფაქტის მიმართ

[168] პერსონალურ მონაცემთა დაცვის ინპექტორის 2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

გაჩენილი ეჭვების გასაქარწყლებლად, ვებგვერდზე გამოაქვეყნა მსჯავრდებულის სახელი, გვარი, მსჯავრდებულის მიერ გარდაცვალებამდე ჩატარებული მკურნალობის, მისი სამედიცინო დიაგნოზისა და გაწეული სამედიცინო მომსახურების შესახებ ინფორმაცია. ინსპექტირების შედეგად დადგინდა, რომ მონაცემთა სუბიექტის (ან კანონით გათვალისწინებული მემკვიდრეების) წერილობითი თანხმობის გარეშე განსაკუთრებული კატეგორიის მონაცემის ვებგვერდზე ხელმისაწვდომობა არღვევდა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6.3 მუხლს, რომლის თანახმადაც, მონაცემთა დამუშავების საფუძვლის არსებობის მიუხედავად, დაუშვებელია სუბიექტის თანხმობის გარეშე განსაკუთრებული კატეგორიის მონაცემთა გასაჯაროება. კანონის შესაბამისად, სამინისტროს დაეკისრა ადმინისტრაციული სახდელი - ჯარიმა 1000 ლარის ოდენობით.“[169]

4.2. 2015 წელს გამოვლენილი პრობლემები

საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების მიზნით, 2015 წელს ინსპექტორის აპარატმა, როგორც საზედამხედველო ორგანომ, ჩაატარა 03 შემოწმება - სსიპ ,,ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიუროში“ (განცხადების ფარგლებში), სსიპ ქალაქ წალკის №1 და №2 საჯარო სკოლებში. ამასთან, ამავე საკითხზე განიხილა მოქალაქეთა 07 განცხადება. აპარატიდან მოწოდებული ინსპექტორის 05 გადაწყვეტილებიდან, ერთ შემთხვევაში, განმცხადებელი დავობდა ნასამართლობის მონაცემებზე არაკანონიერად წვდომის ფაქტს, თუმცა საკითხის შესწავლისას, გარემოება არ დადასტურდა. 02 შემთხვევაში - განმცხადებლების მიერ მითითებული სავარაუდო სამართალდარღვევის ჩადენის ფაქტი მომართვის დროისათვის უკვე ხანდაზმული იყო. აღსანიშნავია, რომ საკითხის პრიორიტეტულობის გათვალისწინებით, ხუთივე შემთხვევა ინსპექტორს განხილული აქვს 2015 წლის ანგარიშში.

[169] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

ამ პერიოდში, საჯარო სექტორში ერთ-ერთ ძირითად პრობლემად ინსპექტორი **მონაცემთა დამუშავებისათვის დადგენილი საფუძვლების დაუცველობას მიუთითებს**. „საჯარო თუ კერძო ორგანიზაციების მხრიდან 2015 წელსაც ჰქონდა ადგილი პერსონალური, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების კანონიერი საფუძვლის გარეშე დამუშავებას. ხშირად, მონაცემთა დამუშავების კანონიერების შემოწმების დროს, ორგანიზაციები ვერ ახდენენ შესაბამისი საფუძვლის იდენტიფიცირებას და ვერ წარადგენენ მონაცემთა ფლობისა თუ სხვაგვარი გამოყენების სათანადო სამართლებრივ არგუმენტაციას. საანგარიშო პერიოდში გამოვლინდა საჯარო უწყებებს შორის ზეპირი სახის შეთანხმებებსა თუ კონკრეტული სამართლებრივი საფუძვლის გარეშე გაფორმებულ მემორანდუმებზე დაყრდნობით, პერსონალური მონაცემების, როგორც ერთჯერადი, ასევე, მრავალჯერადი გაცემისა და მიღების ფაქტები, მაშინ, როდესაც მოქმედი კანონმდებლობით, ამგვარი შემთხვევებისთვის განსაზღვრულია ნორმატიული აქტით რეგულირების აუცილებლობა. მოქმედი კანონმდებლობა საჯარო უწყებებს ანიჭებს უფლებამოსილებას შექმნან, მართონ და მუდმივ რეჟიმში განაახლონ მონაცემთა ბაზები და კანონმდებლობით დაკისრებული ფუნქციების შესასრულებლად, სხვა საჯარო დაწესებულებებს მიანიჭონ წვდომა ინფორმაციაზე. ამის ერთ-ერთი თვალსაჩინო მაგალითია სახელმწიფო სერვისების განვითარების სააგენტო, რომლის ერთ-ერთი ძირითადი ფუნქცია არის მოსახლეობის ერთიანი რეესტრის წარმოება, სამოქალაქო აქტების რეგისტრაცია, საიდენტიფიკაციო დოკუმენტების გაცემა. სხვადასხვა საჯარო უწყებებს, კანონმდებლობით დაკისრებული ვალდებულებების შესასრულებლად, ესაჭიროებათ მუდმივ რეჟიმში ამ მონაცემებზე წვდომა და ამ მიზნით, შესაბამის ნორმატიულ აქტებზე დაყრდნობით, ხორციელდება ინფორმაციის ტექნიკური არხებით გამოთხოვა და მიღება. საკითხის ამგვარი რეგულირებით თავიდან არის აცილებული ბაზების დუბლირება, მოძველებული და არასწორი მონაცემების გამოყენება, მონაცემები მიზნობრივად მუშავდება და სხვა

ორგანიზაციები იღებენ მხოლოდ იმ მონაცემებს, რომლებიც ესაჭიროებათ დაკისრებული ფუნქციების შესასრულებლად.[170]

მონაცემთა დამუშავების პრინციპების დაცვის საკითხებზე საუბრობს ინსპექტორი 2015 წლის ანგარიშში და ხაზგასმით მიუთითებს, რომ 2015 წელსაც „ორგანიზაციებს (მონაცემთა დამმუშავებლებს) არ აქვთ განსაზღვრული მონაცემთა დამუშავების კონკრეტული და მკაფიო მიზანი, შესაბამისად, **ინფორმაცია მუშავდება მიზნის არაადეკვატური და არაპროპორციული მოცულობით, ამასთან, უმეტეს შემთხვევაში, კვლავ არ არის განსაზღვრული მონაცემთა შენახვის ვადები**.“[171] „დიდი მოცულობით პერსონალურ მონაცემებზე ან მოძველებულ, გასაახლებელ ინფორმაციაზე ორგანიზაციების ხელმისაწვდომობა მოქალაქეებს გარკვეულ დაბრკოლებას უქმნის სხვადასხვა მომსახურების მიღებისა და საკუთარი უფლებების რეალიზების დროს, **ზოგიერთ შემთხვევაში, წარსულში ნასამართლობის ფაქტის თუ ჯანმრთელობის მდგომარეობის გამჟღავნების გამო, რამდენიმე მოქალაქე გარკვეული დისკრიმინაციული მოპყრობის ობიექტადაც** კი იქცა“,-ნათქვამია ანგარიშში.

ერთ-ერთ მთავარ საკითხად გამოყოფილია **საჯარო სექტორში ინფორმაციაზე კანონიერი მიზნით წვდომის აუცილებლობა.** „კანონიერი პრინციპის დაცვისა და საზოგადოების ნდობის მოპოვების მიზნით, მნიშვნელოვანია, რომ შეგროვებულ ინფორმაციაზე წვდომა განხორციელდეს მხოლოდ კანონიერი მიზნით, აუცილებლობის შემთხვევებში და წინასწარ განსაზღვრული საჭიროებებისას. აღნიშნული საკითხი უფრო მეტ აქტუალობას იძენს მაშინ, როდესაც მონაცემთა დამმუშავებელ ორგანიზაციას წარმოადგენს სამართალდამცავი სტრუქტურა. საქართველოს შინაგან საქმეთა სამინისტრო ქვეყანაში ერთ-ერთი უმსხვილესი საჯარო უწყებაა, რომელიც კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად, პირთა შესახებ დიდი

[170] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

[171] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში,ხელმისაწვდომია: www.pdp.ge.

მოცულობით პერსონალურ მონაცემებს ამუშავებს. საქართველოს შინაგან საქმეთა სამინისტროს მონაცემთა ბაზებში თავს იყრის ინფორმაცია, რომელიც დაკავშირებულია: სისხლის სამართლის და ადმინისტრაციულ პასუხისმგებლობასთან, ავტოსატრანსპორტო საშუალებების საკუთრებასა და მართვის უფლებებთან, ფიზიკური პირების საზღვრის კვეთასთან, ნარკოლოგიურ შემოწმებასთან, უგზოუკვლოდ დაკარგულად და ძებნილად გამოცხადებასთან და სხვა.“[172]

2015 წლის ინსპექტორის ანგარიშში დადებითად არის შეფასებული საქართველოს შინაგან საქმეთა სამინისტროს საქმიანობა იმ მხრივ, რომ უწყებამ „მოაწესრიგა სამინისტროს ინფორმაციულ რესურსებთან თანამშრომელთა დაშვების საკითხები, განისაზღვრა სამინისტროს ფაილურ სისტემებში არსებული პერსონალური მონაცემების შენახვის, წაშლისა და დაარქივების ვადები, გამკაცრდა თანამშრომელთა მიერ მონაცემთა ბაზებზე წვდომის კანონიერების კონტროლი. დაარქივებულ ინფორმაციულ რესურსებთან წვდომა დაიშვება მხოლოდ დასაბუთებული წერილობითი მიმართვის საფუძველზე.“[173]

„2015 წელს ინსპექტორის მიერ მოქალაქეთა განცხადებების განხილვისა თუ შემოწმებების შედეგად, კვლავ გამოვლინდა ისეთი შემთხვევები, როდესაც **საჯარო ორგანიზაციების მიერ მონაცემთა დამუშავება, მათ შორის გამჟღავნება ხდებოდა მხოლოდ უწყებების ხელმძღვანელებს შორის ზეპირი შეთანხმებით, ყოველგვარი სამართლებრივი საფუძვლის არსებობის გარეშე.**

პერსონალური მონაცემების დამუშავების კანონიერების უზრუნველყოფის მიზნით, მონაცემთა დამმუშავებელ ორგანიზაციებს ეკისრებათ ვალდებულება, რომ მათ ბაზებში დაცული პერსონალური მონაცემების დამუშავება, მათ შორის მოპოვება, გადაცემა და ხელმისაწვდომობა მოახდინონ კანონმდებლობით, კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული მოთხოვნების დაცვით. მხოლოდ მხარეთა შორის ზეპირსიტყვიერი

[172] იხ. იგივე.
[173] იხ. იგივე.

შეთანხმება ან წერილობითი მემორანდუმი არ წარმოადგენს მონაცემთა დამუშავების სათანადო წინაპირობას. მკაფიო სამართლებრივი რეგულირების არსებობა განსაკუთრებით მნიშვნელოვანია მაშინ, როდესაც მონაცემების დამუშავების შედეგად, მოქალაქეებს ეზღუდებათ გარკვეული უფლებები, მაგალითად, დასაქმების უფლება.“[174]

2015 წლის ინსპექტორის ანგარიშში განხილულია კონკრეტული საქმეები, რომლებიც შეეხება **საჯარო უწყებებში განსაკუთრებული კატეგორიის პერსონალური მონაცემების კანონდარღვევით დამუშავებას.** „2015 წელს, პერსონალურ მონაცემთა დაცვის ინსპექტორს განცხადებით მომართა მოქალაქემ, რომელიც მიუთითებდა, რომ 2014 წელს, შინაგან საქმეთა სამინისტროს შესაბამის სტრუქტურულ ერთეულში ნარკოტესტზე ნებაყოფლობითი შემოწმების შედეგად, დაუდგინდა ნარკოტიკული საშუალების მიღების ფაქტი. აღნიშნულთან დაკავშირებით, კანონმდებლობით დადგენილი წესით, შედგა ადმინისტრაციული სამართალდარღვევის ოქმი, რომელიც გადაიგზავნა სასამართლოში. საქმის განხილვისას, მოქალაქემ წარადგინა მტკიცებულებები, რომლის შედეგადაც დადგინდა, რომ ნარკოტიკული ნივთიერების შემცველი პრეპარატი მიღებული ჰქონდა კანონიერად - ექიმის დანიშნულებით. სამართალდარღვევის ფაქტის არარსებობის გამო, სასამართლომ მიიღო გადაწყვეტილება საქმის შეწყვეტის შესახებ. მიუხედავად იმისა, რომ სასამართლო დადგენილების თანახმად, არ დადასტურდა მოქალაქის მიერ ადმინისტრაციული გადაცდომის ფაქტი, განმცხადებელი კვლავ იმყოფებოდა საქართველოს შინაგან საქმეთა სამინისტროს და სსიპ - ,,ლ. სამხარაულის სახელობის სასამართლო ექსპერტიზის'' ეროვნული ბიუროს შესაბამის ნარკოლოგიურ მონაცემთა ბაზებში ნარკოლოგიურ აღრიცხვაზე. განმცხადებელი აღნიშნავდა, რომ ამგვარ აღრიცხვაზე ყოფნით, საფრთხე შეექმნა მისი დასაქმების საკითხს და პერსონალურ მონაცემთა დაცვის ინსპექტორისგან ითხოვდა მის შესახებ არსებული არასწორი ინფორმაციის წაშლას.

[174] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში,ხელმისაწვდომია: www.pdp.ge.

განცხადების განხილვისას, დადგინდა, რომ მოქმედი კანონმდებლობა ითვალისწინებს მხოლოდ იმ პირთა აღრიცხვის ვალდებულებას, რომლებიც არიან ნარკომანიით დაავადებულნი ან ნარკოტიკული საშუალებების არასამედიცინო მიზნით მომხმარებლები. განმცხადებელი კი არ წარმოადგენდა არცერთ ზემოაღნიშნულ კატეგორიას. ამასთან, მოქმედი კანონმდებლობით, საქართველოს შინაგან საქმეთა სამინისტროს და სხვა საჯარო თუ კერძო დაწესებულების მიერ სსიპ - ,,ლევან სამხარაულის სახელობის სასამართლო ექსპერტიზის'' ეროვნული ბიუროს ნარკოლოგიური აღრიცხვის მონაცემთა საინფორმაციო ბაზისთვის ინფორმაციის მიწოდების შესაძლებლობა ან ვალდებულება დადგენილი არ არის. ასეთი ინფორმაციის აღრიცხვის ვალდებულება აქვს მხოლოდ საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს მიერ უფლებამოსილ დაწესებულებას, რომელსაც „ნარკოტიკული საშუალებების, ფსიქოტროპული ნივთიერებების, პრეკურსორებისა და ნარკოლოგიური დახმარების შესახებ“ საქართველოს კანონის 36-ე მუხლი უფლებამოსილებას ანიჭებს, შექმნას ნარკომანიით დაავადებული პირებისა და სპეციალურ კონტროლს დაქვემდებარებულ ნივთიერებათა მომხმარებლების ერთიანი საინფორმაციო ბანკი, თუმცა, დღეის მდგომარეობით, ამგვარი უფლებამოსილების მქონე პირი განსაზღვრული არ არის.

შემოწმების ფარგლებში, ასევე დადგინდა, რომ 2010 წელს საქართველოს შინაგან საქმეთა სამინისტროს ნარკოლოგიური მონაცემთა ბაზა და სასამართლო ექსპერტიზის ეროვნული ბიუროს ნარკოლოგიური აღრიცხვის მონაცემთა საინფორმაციო ბაზა, ამავე უწყებების ხელმძღვანელების ზეპირი შეთანხმების საფუძველზე, განთავსდა ერთიან სერვერზე და ბაზებში არსებული მონაცემები პირდაპირ რეჟიმში ხელმისაწვდომი იყო ორივე მხარისათვის, შესაბამისი საკანონმდებლო თუ კანონქვემდებარე ნორმატიული აქტით საკითხის დარეგულირების გარეშე.

ამდენად, საქართველოს შინაგან საქმეთა სამინისტროს მიერ განმცხადებლის შესახებ მონაცემების სსიპ - ,,ლ. სამხარაულის სახელობის

სასამართლო ექსპერტიზის ეროვნული ბიუროსთვის'' გამჟღავნება და ბიუროს მიერ განმცხადებლის აღრიცხვა ნარკოლოგიური აღრიცხვის მონაცემთა საინფორმაციო ბაზაში მოქმედი კანონმდებლობის დარღვევით, მონაცემთა დამუშავების საფუძვლის გარეშე მოხდა, რის გამოც, უწყებებს დაეკისრათ ადმინისტრაციული პასუხისმგებლობა ჯარიმის სახით. ასევე, სამინისტროს დაევალა ,,სსიპ - ლ. სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნული ბიუროსთვის" განმცხადებლის შესახებ ინფორმაციის მიწოდების შეწყვეტა, ხოლო სსიპ - ,,ლ. სამხარაულის სახელობის სასამართლო ექსპერტიზის ეროვნულ ბიუროს" დაევალა განმცხადებლის შესახებ არასწორი მონაცემების საინფორმაციო ბაზიდან წაშლა. აღსანიშნავია, რომ უწყებები არ დაეთანხმნენ ინსპექტორის გადაწყვეტილებას და სასამართლოში გაასაჩივრეს. თუმცა, სასამართლომ (საქმე №4/5047-15) სრულად გაიზიარა ინსპექტორის პოზიცია და მიღებული გადაწყვეტილება ძალაში დატოვა.[175]

2015 წლის ანგარიშში განხილულია სასამართლო სისტემაში პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები. „საქართველოს ზოგადი ადმინისტრაციული კოდექსის'' 28-ე მუხლის თანახმად, „საჯარო ინფორმაცია ღიაა, გარდა კანონით გათვალისწინებული შემთხვევებისა და დადგენილი წესით, პერსონალურ მონაცემებს, სახელმწიფო ან კომერციულ საიდუმლოებას მიკუთვნებული ინფორმაციისა."

საქართველოს საერთო სასამართლოების მიერ საქმის განხილვის წესი ამომწურავად არის რეგულირებული მოქმედი კანონმდებლობით. „საერთო სასამართლოების შესახებ" საქართველოს ორგანული კანონის მიხედვით, სასამართლოში საქმე განიხილება ღია სხდომაზე, გარდა კანონით გათვალისწინებული შემთხვევებისა და სასამართლო გადაწყვეტილება ყველა შემთხვევაში, ცხადდება საქვეყნოდ. ამასთან, სასამართლო პროცესზე

[175] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

კანონით გათვალისწინებული წესით, დაშვებულია პროცესის აუდიო და ვიდეო ჩაწერა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის თანახმად, სასამართლოს მიერ საბოლოო გადაწყვეტილების გამოტანამდე, კანონის მოქმედება არ ვრცელდება სამართალწარმოების მიზნებისათვის მონაცემთა დამუშავებაზე, რადგან ამან შეიძლება დააზიანოს სამართალწარმოება. გამომდინარე აღნიშნულიდან, ნათელია, რომ სასამართლო პროცესის მსვლელობისას, მონაცემთა დამუშავებაზე არ ვრცელდება პერსონალური მონაცემების დაცვის მარეგულირებელი ნორმები, თუმცა, მას შემდეგ, რაც საქმეზე საბოლოო გადაწყვეტილება იქნება გამოცხადებული, სამართალწარმოების მიზანი უკვე მიღწეულია და მონაცემთა დამმუშავებლებს, მათ შორის სასამართლოს, ეკისრებათ ვალდებულება, დაიცვან მონაცემთა დამუშავების შესაბამისი სტანდარტები.

სასამართლოს გადაწყვეტილება, რომელიც შეიცავს ფიზიკური პირის შესახებ მონაცემებს, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ პუნქტის თანახმად, წარმოადგენს პერსონალური მონაცემების შემცველ დოკუმენტს. ხოლო სასამართლოს ის გადაწყვეტილებები, რომლებიც შეიცავენ ინფორმაციას ფიზიკური პირის რასობრივი ან ეთნიკური კუთვნილების, პოლიტიკური შეხედულების, რელიგიური ან ფილოსოფიური მრწამსის, პროფესიულ კავშირში წევრობის, ჯანმრთელობის მდგომარეობის, სქესობრივი ცხოვრების, ნასამართლობის, ადმინისტრაციული პატიმრობის, პირისთვის აღკვეთის ღონისძიების შეფარდების, პირთან საპროცესო შეთანხმების დადების, განრიდების, დანაშაულის მსხვერპლად აღიარების ან დაზარალებულად ცნობის შესახებ, ასევე შეიცავენ განსაკუთრებული კატეგორიის მონაცემებს.

მოქმედი კანონმდებლობის თანახმად, მნიშვნელოვანი საჯარო ინტერესის, ასევე, მონაცემთა დამმუშავებელი ორგანიზაციის ან მესამე პირის კანონიერი ინტერესების დასაცავად (ასევე, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლით დადგენილ სხვა შემთხვევებში), სასამართლოს გადაწყვეტილების გასაჯაროება დასაშვებია

მხოლოდ იმ შემთხვევაში, თუ ის არ შეიცავს პირის შესახებ განსაკუთრებული კატეგორიის მონაცემებს. განსაკუთრებული კატეგორიის მონაცემების შემცველი სასამართლოს გადაწყვეტილების გასაჯაროება კი დასაშვებია მხოლოდ დეპერსონალიზებული ფორმით ან პირის თანხმობით.

ყურადღება უნდა გამახვილდეს ასევე პერსონალური მონაცემების დეპერსონალიზაციის ფორმაზე. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, მონაცემთა დეპერსონალიზაცია განმარტებულია, როგორც მონაცემთა იმგვარი მოდიფიკაცია, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა, არაპროპორციულად დიდ ძალისხმევას, ხარჯებსა და დროს საჭიროებდეს. იგივე მიდგომას ადგენს ევროპის მართლმსაჯულების სასამართლო საქმეში *Nikoaou v. Commission, 12.09.2007.* სასამართლო განმარტავს, რომ ინფორმაციის გამოქვეყნება, რომელშიც არ არის მითითებული პიროვნება, თუმცა მარტივად იძლევა მისი იდენტიფიცირების საშუალებას, უნდა ჩაითვალოს პერსონალური მონაცემების დამუშავებად“,- ნათქვამია ანგარიშში.

ამ მხრივ, ასევე საინტერესოა 2015 წელს ინსპექტორის მიერ მიღებული გადაწყვეტილება მოქალაქის განცხადებაზე, რომელიც მიუთითებდა, რომ სასამართლო დავის ფარგლებში, მისთვის ცნობილი გახდა, რომ მოწინააღმდეგე მხარე ფლობდა მისი ნასამართლობის შესახებ ინფორმაციას. მოქალაქე პერსონალურ მონაცემთა დაცვის ინსპექტორისგან ითხოვდა მისი ნასამართლობის შესახებ ინფორმაციის მოპოვების და დამუშავების კანონიერების შესწავლას. მსგავსი მოთხოვნით, ინსპექტორის აპარატს მომართა კიდევ ერთმა მოქალაქემ, რომელიც აღნიშნავდა, რომ ერთ-ერთი არასამთავრობო ორგანიზაციის მიერ გავრცელდა ინფორმაცია, თითქოს იგი ნასამართლევი იყო განსაკუთრებით მძიმე დანაშაულის ჩადენისათვის. აღნიშნული ინფორმაციის დასტურად კი მითითებული იყო სასამართლოს განაჩენის ასლი. მიუხედავად იმისა, რომ განაჩენში პერსონალური მონაცემები დაშტრიხული სახით იყო მოცემული, არასამთავრობო ორგანიზაციის მტკიცებით, განაჩენი სწორედ

განმცხადებლის მიერ დანაშაულის ჩადენას უკავშირდებოდა. განმცხადებელი მიუთითებდა, რომ ის არ ყოფილა ნასამართლევი და თბილისის საქალაქო სასამართლოს გასაჯაროებული განაჩენი ეხება სხვა ადამიანს, ორგანიზაციის მიერ მითითებული ფაქტები არ შეესაბამებოდა სინამდვილეს და ემსახურებოდა მისი სახელის დისკრედიტაციას.

საკითხის შესწავლის შედეგად, გამოვლინდა, რომ ორივე შემთხვევაში, სასამართლოს მხრიდან განაჩენის ასლი გაიცა საჯარო ინფორმაციის სახით, პერსონალური მონაცემების გარეშე, დაშტრიხული ფორმით, მხოლოდ ინიციალების მითითებით. მიუხედავად დაშტრიხული ფორმით ინფორმაციის გაცემისა, მნიშვნელოვანია ის გარემოება, რომ განსახილველ შემთხვევებში, სასამართლოსგან მოითხოვეს კონკრეტული ფიზიკური პირების (სახელისა და გვარის მითითებით) შესახებ განაჩენების ასლები და სასამართლომ გასცა ინფორმაცია განცხადებაში მითითებული პირების შესახებ. ამდენად, მხოლოდ ის ფაქტი, რომ სასამართლოს განაჩენის ასლში დაშტრიხული იყო მონაცემთა სუბიექტის ვინაობა, არ იქნა მიჩნეული დეპერსონალიზებული ფორმით ინფორმაციის გაცემის შემთხვევად. აღწერილ შემთხვევებში, ინფორმაციის მიმღებს შეეძლო, მარტივად, ყოველგვარი ძალისხმევის გარეშე, განაჩენში მითითებული ინიციალის ფიზიკურ პირთან დაკავშირება და მისი ამგვარად იდენტიფიცირება.

სასამართლოს არ შეუფასებია ის გარემოება, თუ რამდენად იძლეოდა მის მიერ შერჩეული ფორმით ინფორმაციის გაცემა პირის იდენტიფიცირების საშუალებას. ამდენად, ინსპექტორის გადაწყვეტილებით, დადგინდა, რომ ადგილი ჰქონდა განსაკუთრებული კატეგორიის პერსონალური მონაცემების გამჟღავნებას კანონის დარღვევით.[176]

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების ერთ-ერთ მნიშვნელოვან საქმედ, პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიშში გამოყოფილია ერთ-ერთი არასამეწარმეო არაკომერციული იურიდიული პირის მიერ, მათი მიმართვის

[176] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge

საფუძველზე, შეზღუდული შესაძლებლობების მქონე პირების უფლებების დაცვის, მათი გარემოსდაცვითი განათლების ხელშეწყობის უზრუნველყოფისა და აღნიშნულ ღონისძიებებში შშმ პირთა საგანმანათლებლო საჭიროებების შეფასების ღონისძიებების ინდიკატორული განსაზღვრების მიზნით, ერთ-ერთ საჯარო სკოლიდან საჯარო ინფორმაციის გამოთხოვის საკითხის შესწავლა. „მიუხედავად იმისა, რომ მოთხოვნილი არ ყოფილა პერსონალური მონაცემების შემცველი ინფორმაციის მიწოდება, სკოლისგან მიღებული ინფორმაცია შეიცავდა მოსწავლეთა პერსონალურ მონაცემებს, კერძოდ, შშმ მოსწავლეების ინდივიდუალურ სასწავლო გეგმებს, სადაც სასწავლო პროცესთან დაკავშირებულ ინფორმაციასთან ერთად, ფიქსირდებოდა ინფორმაცია მოსწავლეების ჯანმრთელობასთან დაკავშირებული პრობლემის შესახებ, ასევე, მათი სახელი, გვარი, კლასი, მშობლებისა და პედაგოგების სახელი და გვარი.

მიღებული ინფორმაციის საფუძველზე, ჩატარდა საჯარო სკოლის შემოწმება. შემოწმების შედეგად დადგინდა, რომ სკოლის ადმინისტრაციამ მოსწავლეთა შესახებ ინფორმაციის გაცემამდე, მოახდინა მშობელთა ინფორმირება მოსწავლეთა ინდივიდუალური სასწავლო გეგმების გამოთხოვის შესახებ და დაისვა შეკითხვა, თანახმა იყვნენ თუ არა ისინი მოსწავლეთა ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციის გაცემაზე. ინფორმაციის გადაცემასთან დაკავშირებით მშობლებმა განაცხადეს წერილობითი თანხმობა.

მიუხედავად მონაცემთა დამუშავების საფუძვლის არსებობისა, შემოწმების დროს, გამოიკვეთა, რომ სკოლამ საკმარისად არ გამოიკვლია ის კანონიერი მიზანი, რომლის მისაღწევადაც ინფორმაციის მიმღებს ესაჭიროებოდა მოსწავლეთა მაიდენტიფიცირებელი მონაცემების შემცველი ინფორმაციის მიღება. სკოლისაგან საჯარო ინფორმაციის მოთხოვნა მიზნად ისახავდა გარემოსდაცვითი განათლების ხელშეწყობის უზრუნველყოფისა და შშმ პირთა საგანმანათლებლო საჭიროებების შეფასების ღონისძიებების განსაზღვრას, რისთვისაც საკმარისი იქნებოდა შშმ მოსწავლეთა

იდენტიფიცირების გამომრიცხავი ფორმით ინფორმაციის წარდგენა. ჯანმრთელობის მდგომარეობის შემცველი ინფორმაციის, როგორც განსაკუთრებული კატეგორიის მონაცემის მიმართ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს დაცვის მაღალ სტანდარტს და უთითებს, რომ ამგვარი მონაცემების დამუშავება აკრძალულია, გარდა ამავე კანონით პირდაპირ დადგენილი გამონაკლისი შემთხვევებისა.

რადგანაც მაღალია პირისათვის მორალური ზიანის მიყენების რისკი, ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციის დამუშავება, განსაკუთრებით კი მისი გაცემისა თუ სხვაგვარად ხელმისაწვდომად გახდომის გზით, საჭიროებს როგორც კანონიერ საფუძვლის, ასევე, კანონიერი მიზნის არსებობას. იმ შემთხვევაში, როდესაც არასრულწლოვანთა ჯანმრთელობასთან დაკავშირებული მონაცემების გაცემას ეხება საკითხი, განსაკუთრებული ყურადღება უნდა დაეთმოს ინფორმაციის შემდგომი გამოყენების რისკების შეფასებას. ამგვარი ინფორმაციის გაცემის თითოეული შემთხვევისათვის. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „გ“ ქვეპუნქტის შესაბამისად, უნდა შეფასდეს იმ კანონიერი მიზნის არსებობა, რომლის მისაღწევადაც გაიცემა მონაცემი. ასევე, მონაცემები შეიძლება გაიცეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი მიზნის მისაღწევად. ამდენად, სკოლას უნდა მოეხდინა მონაცემთა დეპერსონალიზაცია და მისი გაცემა მოსწავლეთა იდენტიფიცირების გამომრიცხავი ფორმით. ვინაიდან, მოსწავლეთა შესახებ პერსონალური მონაცემების შემცველი ინფორმაციის გაცემით, დაირღვა „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „გ“ ქვეპუნქტის მოთხოვნა, საჯარო სკოლას დაეკისრა პასუხისმგებლობა გაფრთხილების სახით.[177]

პერსონალურ მონაცემთა დაცვის ინსპექტორი 2015 წლის ანგარიშში ხაზგასმით აღნიშნავს, რომ მონაცემთა დამმუშავებელი ორგანიზაციები განსაკუთრებული სიფრთხილით უნდა მოეკიდონ პირის შესახებ

[177] პერსონალურ მონაცემთა დაცვის ინპექტორის 2015 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge

განსაკუთრებული კატეგორიის მონაცემების გასაჯაროებას, რომლებიც ჩვეულებრივი პერსონალური მონაცემებისაგან განსხვავებული სამართლებრივი რეგულირების ქვეშ ექცევიან. განსაკუთრებული კატეგორიის პერსონალური მონაცემების გასაჯაროება საჭიროებს პირის წერილობით თანხმობას და ადმინისტრაციული ორგანო ვალდებულია დაიცვას ეს ინფორმაცია გამხელისაგან, სანამ თავად ეს პირი არ გამოავლენს ინფორმაციის გაცემის ნებას. მაღალი საზოგადოებრივი ინტერესის არსებობის მიუხედავად, მოქმედი კანონმდებლობა არ ითვალისწინებს თანამდებობის პირთა შესახებ განსაკუთრებული კატეგორიის მონაცემების, მაგალითად, ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციის, მათი თანხმობის გარეშე გასაჯაროების შესაძლებლობას.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-3 პუნქტის თანახმად, განსაკუთრებული კატეგორიის მონაცემთა დამუშავების შემთხვევაში, დაუშვებელია სუბიექტის თანხმობის გარეშე მონაცემთა გასაჯაროება და მესამე პირისათვის მათი გამჟღავნება. თუმცა, კანონმდებლობა პერსონალური მონაცემების შემცველი ინფორმაციის დეპერსონალიზებული ფორმით გამჟღავნების შესაძლებლობას იძლევა. აუცილებელია, მონაცემთა დეპერსონალიზაცია მოხდეს იმგვარად, რომ შეუძლებელი იყოს მათი დაკავშირება მონაცემთა სუბიექტთან ან ასეთი კავშირის დადგენა არაპროპორციულად დიდ ძალისხმევას, ხარჯებსა და დროს საჭიროებდეს.

4.3. 2016 წელს გამოვლენილი პრობლემები

საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების მიზნით, 2016 წელს ინსპექტორის აპარატის მიერ ჩატარდა 06 შემოწმება - სსიპ თბილისის №114 საჯარო სკოლაში, სსიპ - ადიგენის მუნიციპალიტეტის სოფელ აბასთუმნის საჯარო სკოლაში, საქართველოს შინაგან საქმეთა სამინისტროში (2-ჯერ), სსიპ ქაქუცა ჩოლოყაშვილის სახელობის ქალაქ თბილისის №178-ე საჯარო სკოლას და საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტროში (ინფორმაციის მოწოდების დროისთვის შემოწმება არ იყო

დასრულებული). ამასთან, ამავე საკითხზე, ინსპექტორმა განიხილა მოქალაქეთა 12 განცხადება. აპარატიდან მოგვეწოდა ინსპექტორის მიერ გამოტანილი 15 გადაწყვეტილება. 2016 წელს ინსპექტორის მიერ ამ განხილული 15 შემთხვევიდან, აღსანიშნავია, რომ 05 შემთხვევაში, კონკრეტული უწყებების (შინაგან საქმეთა სამინისტრო, შპს ვენერიულ სნეულებათა სამეცნიერო-კვლევითი ეროვნული ცენტრი, საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო, შპს „ფსიქიკური ჯანმრთელობის და ნარკომანიის პრევენციის ცენტრი“) მხრიდან განცხადებაში მითითებული სამართალდარღვევის ჩადენის ფაქტი არ დადასტურდა, 03 შემთხვევაში, განმცხადებლების მიერ მითითებული სავარაუდო სამართალდარღვევის ჩადენის ფაქტი ინსპექტორის მიმართვის დროისათვის უკვე ხანდაზმული იყო, ხოლო დარჩენილ 07 შემთხვევაში, ინსპექტორმა გაატარა შემდეგი ღონისძიებები:

- საქართველოს ფინანსთა სამინისტრო ცნო სამართალდამრღვევად საგამოძიებო სამსახურის მიერ ვებგვერდის მეშვეობით, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის გათვალისწინებული სამართლებრივი საფუძვლის გარეშე გამჟღავნებისათვის და შეუფარდა ჯარიმა 1000 ლარის ოდენობით;
- საქართველოს შინაგან საქმეთა სამინისტრო ცნო სამართალდამრღვევად ოფიციალურ ვებგვერდზე პირის პირდაპირ იდენტიფიცირებადი ფორმით ამსახველი ვიდეოკადრების ხელმისაწვდომად გახდომის გზით გამჟღავნებისათვის, მონაცემთა დამუშავების საფუძვლებისა და პრინციპების დარღვევით დამუშავებაში და შეუფარდა ჯარიმა 2000 ლარის ოდენობით;
- საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო ცნო სამართალდამრღვევად ა(ა)იპ „სამედიცინო, სოციალურ-ეკონომიკურ და კულტურულ საკითხთა ცენტრ ,,ურანტის“ ბაზაზე არსებული ნარკომანიის ჩანაცვლებითი თერაპიის სახელმწიფო პროგრამაში ჩართული განმცხადებლების პერსონალური, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების საფუძვლის

გარეშე დამუშავებაში და ადმინისტრაციული სახდელის სახით, შეუფარდა ჯარიმა 1000 ლარის ოდენობით.

➢ სსიპ ქალაქ ჩოლოყაშვილის სახელობის ქ. თბილისის №178-ე საჯარო სკოლას შეუფარდა გაფრთხილებაა, იმისთვის რომ სკოლამ ა(ა)იპ „ინვალიდთა და შეზღუდული შესაძლებლობების მქონე პირთა ასოციაციას“ გადაუგზავნა სკოლის მოსწავლეთა შესახებ პერსონალური ინფორმაცია იმგვარად, რომ მიმღებს შეეძლო მონაცემების დაფარვის მიუხედავად, დაფარული ნაწილის მოხსნა და დოკუმენტის სრული სახით ხილვა. შესაბამისად, დაარღვია მონაცემთა უსაფრთხოების დაცვისათვის დადგენილი ნორმები.

➢ სსიპ ქალაქ თბილისის 114-ე სკოლას შეუფარდა გაფრთხილება, ვინაიდან სპეციალური საგანმანათლებლო საჭიროების მქონე მოსწავლეთა პერსონალური მონაცემები ა(ა)იპ გარემოს დაცვისა და ბუნებრივი რესურსების სააგენტოს გადასცა, მონაცემთა დამუშავებისათვის დადგენილი პრინციპების დარღვევით, ისე, რომ არ შეაფასა მონაცემთა გაცემის კანონიერი მიზანი და ამ მიზნის შესასრულებლად გადასაცემი მონაცემების საჭირო მოცულობა.

➢ საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო სამართალდამრღვევად ცნო მონაცემთა სუბიექტის ინფორმირების წესების დარღვევაში და შეუფარდა გაფრთხილება;

➢ თბილისის საქალაქო სასამართლოს და სსიპ - აღსრულების ეროვნულ ბიუროს დაავალა, განესაზღვრათ კანონიერი მიზნის მისაღწევად, რა ვადით და მოცულობით იყო საჭირო მათ ვებგვერდებზე პერსონალური მონაცემების შემცველი შეტყობინებების/წინადადებების საჯაროდ განთავსება. რათა, აღნიშნული ვადის გასვლის შემდგომ, უწყებებს უზრუნველეყოთ გასაჯაროებული მონაცემების წაშლა, განადგურება ან პირის იდენტიფიცირების გამომრიცხავი ფორმით დამუშავება. აღსანიშნავია ის გარემოებაც, რომ ზემოაღნიშნული გადაწყვეტილებების უმეტესი ნაწილი განხილულია ინსპექტორის 2016 წლის ანგარიშში.

აღნიშნული გადაწყვეტილებებისა და ინსპექტორის ანგარიშზე დაყრდნობით, 2016 წლის ერთ-ერთ უმთავრეს პრობლემატურ საკითხს საჯარო სექტორში კვლავ **მონაცემთა დამუშავების პრინციპებისა და საფუძვლების დაუცველობა წარმოადგენდა.** „2016 წელს ინსპექტორის მიერ განხილული 216 განცხადებიდან 121 მოქალაქის განცხადება სწორედ მონაცემთა დამუშავების საფუძვლებისა და პრინციპების საკითხს უკავშირდებოდა. აქედან, განცხადებების დიდი ნაწილი ეხებოდა მათ ფინანსურ მონაცემებზე წვდომისა და სასესხო ვალდებულებების შესახებ მონაცემების მესამე პირებისთვის გამჟღავნებას, ასევე, ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის ხელმისაწვდომობას.“[178] რაც შეეხება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების მიმართულებით საჯარო სექტორში არსებულ ვითარებას, 2016 წელის ანგარიშში ინსპექტორი ერთ-ერთ მთავარ პრობლემად მიუთითებს საჯარო უწყებების მიერ პერსონალური მონაცემების, მათ შორის განსაკუთრებული კატეგორიის პერსონალური მონაცემების გამჟღავნებასა და ხელმისაწვდომობას ინტერნეტსივრცეში.

ანგარიშში აღნიშნულია, რომ „პერსონალურ მონაცემთა დაცვის ინსპექტორს განცხადებით მომართა მოქალაქის წარმომადგენელმა, რომელმაც მიუთითა, რომ საქართველოს შინაგან საქმეთა სამინისტრომ თავის ოფიციალურ ვებგვერდზე და სხვადასხვა საინფორმაციო საშუალებებით გაავრცელა პირის დაკავების ვიდეოკადრები, რომლითაც შესაძლებელი იყო დაკავებულის პირდაპირი იდენტიფიცირება. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა შეისწავლა ეს შემთხვევა და არ გაიზიარა საქართველოს შინაგან საქმეთა სამინისტროს დასაბუთება, რომ დაკავების კადრების გავრცელება ემსახურებოდა საზოგადოებრივი უსაფრთხოების დაცვის, საფრთხის შემცველი გარემოებებისა და პიროვნებების ვინაობის გასაჯაროების გზით მოსალოდნელი უარყოფითი შედეგების თავიდან აცილების მიზანს. ინსპექტორმა გადაწყვეტილებაში განმარტა, რომ აღნიშნულ საქმეზე პირის

[178] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge

დაკავებისას, მოსალოდნელი უარყოფითი შედეგები უკვე განეიტრალებული იყო და ამ დროისათვის აღარ არსებობდა საზოგადოებრივი უსაფრთხოების დაცვის, საფრთხის შემცველი გარემოებებისა და პიროვნებების გასაჯაროების სახელმწიფო ინტერესი. ამასთან, მხედველობაში იქნა მიღებული ის ფაქტიც, რომ მსგავს შემთხვევებში, სამინისტრო, როგორც წესი, დაკავების ვიდეოკადრებს ავრცელებდა პირთა იდენტიფიცირების გამომრიცხავი ფორმით, რაც აღიარებული საერთაშორისო პრაქტიკაა. წარმოდგენილი და საქმის სხვა ფაქტობრივი გარემოებების გათვალისწინებით, საქართველოს შინაგან საქმეთა სამინისტროს დაუდგინდა მონაცემების საფუძვლის გარეშე და პრინციპების დარღვევით დამუშავების ფაქტი.

კიდევ ერთი ინსპექტირების ფარგლებში, გამოვლინდა, რომ საქართველოს შინაგან საქმეთა სამინისტრომ ოფიციალური ვებგვერდის მეშვეობით, გაასაჯაროვა პირის წარსულში რამდენჯერმე ნასამართლობის შესახებ ინფორმაცია, თუმცა შემოწმების შედეგად გაირკვა, რომ აღნიშნულ პირს წარსულში ჩადენილი დანაშაულების მსჯავრდების ფაქტებზე ნასამართლობა გაქარწყლებული ჰქონდა. შესაბამისად, სამინისტროს მიერ გავრცელებული ინფორმაცია არ იყო ნამდვილი და ზუსტი. მოქმედი კანონმდებლობის თანახმად, ნასამართლობაგაქარწყლებული პირი წარმოადგენს ნასამართლობის არმქონე პირს. ამდენად, როდესაც საკითხი ეხება ისეთი სენსიტიური, განსაკუთრებული კატეგორიის პერსონალური მონაცემის გასაჯაროებას, როგორიცაა პირის ნასამართლობის შესახებ ინფორმაცია, საჯარო უწყება ვალდებულია, კონკრეტული პირის მიმართ დაადგინოს არა მხოლოდ მსჯავრდების, არამედ ნასამართლობის გაქარწყლების საკითხიც და განსაკუთრებული კატეგორიის მონაცემების დამუშავება მხოლოდ კანონით პირდაპირ გათვალისწინებულ შემთხვევებში განახორციელოს.“[179]

2016 წლის ინსპექტორის ანგარიშში საუბარია ასევე, საქართველოს ფინანსთა სამინისტროს საგამოძიებო სამსახურის მიერ ოფიციალური

[179] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge

ვებგვერდის (www.is.ge) საშუალებით, პერსონალური მონაცემების დამუშავების კანონიერებაზე. კერძოდ, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლით გათვალისწინებული სამართლებრივი საფუძვლის გარეშე განსაკუთრებული კატეგორიის მონაცემის გამჟღავნებაზე (ყალბი ფულის დამზადება-გასაღების გამოვლენისა და ამ ფაქტზე წარსულში ანალოგიური დანაშაულისთვის ნასამართლევი პირის დაკავების შესახებ ინფორმაცია). სამინისტროს განმარტებით, აღნიშნული ქმედების სამართლებრივ საფუძველს წარმოადგენდა მათ მიერ დანაშაულის პრევენციის მიზნით, საზოგადოებისათვის ინფორმაციის მიწოდება, საგამოძიებო სამსახურის მიერ დანაშაულის წინააღმდეგ ბრძოლაში მიღწეული წარმატებების თაობაზე, კონკრეტულად, გამოვლენილი და აღკვეთილი დანაშაულების შესახებ, ასევე, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ზ“ და „ე“ პუნქტებით გათვალისწინებული საფუძვლები, დანაშაულის პრევენცია, მაღალი საჯარო ინტერესის არსებობა და მესამე პირთა ინტერესების დაცვის მიზანი. მოცემულ შემთხვევაში, ინსპექტორმა გადაწყვეტილებაში განმარტა, რომ დანაშაულის პრევენციის მიზნის მისაღწევად, მნიშვნელოვანი იყო საზოგადოებისთვის მიეწოდებინათ ინფორმაცია, საგამოძიებო სამსახურის მიერ დანაშაულის წინააღმდეგ ბრძოლაში მიღწეული შედეგების თაობაზე, კონკრეტულად, გამოვლენილი და აღკვეთილი დანაშაულების შესახებ. თუმცა მოცემულ შემთხვევაში, თავად დანაშაულის სავარაუდოდ ჩამდენი პირების იდენტიფიცირება და მათ შესახებ ინფორმაციის გავრცელება არ წარმოადგენდა დანაშაულის პრევენციის აუცილებელ პირობას და მას არ შეეძლო გავლენა მოეხდინა საზოგადოების აზრის ფორმირებაზე, ასევე, ვერ უზრუნველყოფდა დანაშაულებრივი ხელყოფის თავიდან აცილებასა და მართლწესრიგის დაცვას. შესაბამისად, მნიშვნელოვანი საჯარო ინტერესის დაცვის მიზანი ამ შემთხვევაში, მიიღწეოდა საგამოძიებო სამსახურის ოფიციალურ ვებგვერდზე ინფორმაციის ისეთი ფორმით განთავსებითაც, რომლითაც არ იქნებოდა შესაძლებელი მონაცემთა სუბიექტების სრული

იდენტიფიცირება. ადმინისტრაციული სახდელის გარდა, სამინისტროს ასევე დაევალა საგამოძიებო სამსახურის ოფიციალურ ვებგვერდზე გამოქვეყნებული და ინსპექტირების ფარგლებში განხილული პერსონალური მონაცემების შემცველი ინფორმაციის წაშლა ან დეპერსონალიზებული ფორმით განთავსება.“[180]

2016 წელის ერთ-ერთ მთავარ გამოწვევად ინპექტორი **არასრულწლოვანთა ჯანმრთელობის მდგომარეობის შესახებ მონაცემების დამუშავებასაც** მიუთითებს. „საქართველოს განათლებისა და მეცნიერების სამინისტროსგან მიღებული მომართვის საფუძველზე, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა შეისწავლა ერთ-ერთ რეგიონში მოქმედი საჯარო სკოლის მიერ ორი მოსწავლის განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერება. საქმის გარემოებების შესწავლის შედეგად, დადგინდა, რომ მოსწავლეები რამდენიმე წლის წინ მკურნალობდნენ ჰაერწვეთოვანი გზით გადამდები ინფექციის დიაგნოზით და მკურნალობის შემდეგ, მობილობის წესით, გადავიდნენ ერთ-ერთი რაიონის საჯარო სკოლაში. საგულისხმოა, რომ მათ ჰქონდათ დაავადების დახურული ფორმა, რომელიც გარშემომყოფთათვის საფრთხეს არ წარმოადგენდა. სასწავლო პროცესში სკოლის დირექციისა და თანაკლასელების მშობლებისთვის თავად მოსწავლეებისგან ცნობილი გახდა ინფორმაცია მათი ჯანმრთელობის მდგომარეობის შესახებ, რასაც მოჰყვა პროტესტი ერთ-ერთი მასწავლებლისა და მოსწავლეების მშობლების მხრიდან. სკოლის დირექტორი დაუკავშირდა მოსწავლეების მშობელს და სთხოვა, ბავშვები გამოჯანმრთელებამდე არ მიეყვანა სკოლაში. ერთ-ერთმა მასწავლებელმა, რომლის შვილიც სწავლობდა ამავე სკოლაში, დირექტორისგან გამოითხოვა მოსწავლეების ჯანმრთელობის მდგომარეობის შესახებ ცნობები და გავრცელებული ინფორმაციის ნამდვილობის გადასამოწმებლად, წარუდგინა ერთ-ერთი საავადმყოფოს მკურნალ ექიმს. საყურადღებოა, რომ ზემოაღნიშნულთან დაკავშირებით, ინფორმირებული არ ყოფილა მოსწავლეების მშობელი. ამ ფაქტიდან მოკლე

[180] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge

პერიოდში, ეს საკითხი განიხილეს მშობელთა კრებაზეც. სკოლამ მშობლებს მიაწოდა ინფორმაცია, რომ ჯანმრთელობის მდგომარეობის შესახებ არსებული ცნობების მიხედვით, მოსწავლეების სასწავლო პროცესში დაშვება შესაძლებელი იყო, რადგან მათი ჯანმრთელობის მდგომარეობა სხვებისთვის საშიშროებას არ წარმოადგენდა.

მოქმედი კანონმდებლობის თანახმად, სკოლა ვალდებულია, შექმნას ჯანმრთელობისათვის, სიცოცხლისა და საკუთრებისათვის უსაფრთხო გარემო სასკოლო დროს, აგრეთვე, სკოლის ან/და მის მიმდებარე ტერიტორიაზე. ამასთან, სკოლის დირექტორი პერსონალურად აგებს პასუხს სკოლაში მასწავლებლებისა და მოსწავლეებისათვის სიცოცხლისა და ჯანმრთელობისათვის უსაფრთხო გარემოს შექმნაზე. ამდენად, სკოლის დირექტორის ინტერესი, დაედგინა მოსწავლეთა დაავადების არსებობა, ფორმა და საჭიროების შემთხვევაში, შესაბამისი ზომების მიღების გზით, დაეცვა სკოლაში მყოფ პირთა ჯანმრთელობის მდგომარეობა, ამავდროულად, წარმოადგენს მის საკანონმდებლო ვალდებულებას და მონაცემთა მოპოვების კანონით გათვალისწინებულ სამართლებრივ საფუძველს.

თუმცა მონაცემების შემდგომი გავრცელება, კერძოდ, სკოლის მასწავლებლისთვის, კრებაზე სხვა მოსწავლეების მშობლებისა და ექიმისთვის ინფორმაციის მიწოდება, „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემთა მესამე პირებისათვის გამჟღავნებას წარმოადგენს. როცა საქმე განსაკუთრებული კატეგორიის მონაცემებს ეხება, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი დაცვის მაღალ სტანდარტს აწესებს, კერძოდ, მისი მე-6 მუხლის მე-3 პუნქტის თანახმად, მონაცემთა სუბიექტის წერილობითი თანხმობის გარეშე, დაუშვებელია განსაკუთრებული კატეგორიის მონაცემთა გასაჯაროება და მესამე პირისათვის გამჟღავნება. შემოწმების შედეგად, დადგინდა, რომ სკოლას ასეთი თანხმობა არ გააჩნდა. ის ფაქტი, რომ ინფორმაციის ადრესატებისთვის (მაგ. სკოლის მასწავლებლისთვის) ისედაც ცნობილი იყო მოსწავლეების დაავადების

შესახებ, არ ათავისუფლებდა სკოლას კანონით გათვალისწინებული ვალდებულებისგან, ამასთანავე, სკოლამ მოსწავლეთა დაავადების შესახებ ინფორმაცია (სრული დიაგნოზი) მასწავლებლის გარდა, ოფიციალურად ასევე, დაუდასტურა მესამე პირებს'', - ნათქვამია ანგარიშში.

2016 წელს ინსპექტორის აპარატმა განიხილა „17 მოქალაქის განცხადებაც, რომელიც მათ შესახებ ინფორმაციის მოპოვების კანონიერებას, ასევე, კანონით დადგენილ ვადაში და მოთხოვნილი ფორმით ინფორმაციის მიუწოდებლობას ეხებოდა. გამოვლინდა მოქალაქეთა ინფორმირების წესის დარღვევის 11 ფაქტი. განცხადებების უმრავლესობა კერძო ორგანიზაციების მხრიდან მათი ინფორმირების წესის დარღვევას ეხებოდა, თუმცა ერთ-ერთი განცხადებაში საუბარი იყო საჯარო დაწესებულებაზეც. ინსპექტორს განცხადებით მომართა ყოფილმა მსჯავრდებულმა, რომელმაც მიუთითა, რომ საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრომ არა მხოლოდ მისი პერსონალური მონაცემები დაამუშავა უკანონოდ, არამედ მისი ინფორმირების წესებიც დაარღვია.

განცხადების განხილვის ფარგლებში, მონაცემთა დამუშავების ნაწილში დადგინდა, რომ განმცხადებლის პერსონალური მონაცემების დამუშავება განხორციელდა კანონმდებლობის შესაბამისად, თუმცა გამოვლინდა მონაცემთა სუბიექტის ინფორმირების წესის დარღვევა, კერძოდ, ინფორმაციის მიწოდება მოხდა კანონმდებლობით დადგენილი 10-დღიანი ვადის დარღვევით.“[181]

ინსპექტორის ანგარიშებში წარმოდგენილი მასალის გაანალიზების საფუძველზე, თავისუფლად შეიძლება ითქვას, თუ რამდენად მნიშვნელოვანი შეიძლება იყოს ის სავარაუდო ზიანი, რაც განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების წესების დარღვევის შედეგად შეიძლება დადგეს. ამდენად, მნიშვნელოვანია ასეთი ხასიათის პრობლემის მიმართ საჯარო მმართველობის ორგანიზაციების მიერ სისტემური მიდგომის შემუშავება, პერსონალურ მონაცემთა დაცვის

[181] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის ანგარიში, ხელმისაწვდომია:www.pdp.ge

მნიშვნელობაზე ცნობიერების ამაღლებისა და მონაცემთა დაცვის მაღალი სტანდარტის დანერგვისთვის კონკრეტულ ნაბიჯების გადადგმა.

დასკვნა

წინამდებარე ნაშრომში წარმოდგენილია განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაცვის კუთხით საქართველოს საჯარო სექტორში არსებული რეალობა და გამოწვევები. ნაშრომიდან ცხადად ჩანს, თუ რაოდენ დიდი პასუხისმგებლობა აკისრიათ საჯარო უწყებებს განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვის პროცესში.

XXI საუკუნეში, როდესაც ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა, მსოფლიოში ტექნოლოგიების განვითარება წინ უსწრებს მიღებულ თუ მისაღებ საკანონმდებლო რეგულაციებს. როდესაც აქტიურად მიმდინარეობს სამყაროს ციფრული გარდაქმნა, მეტად მნიშვნელოვანია, საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის არსებობდეს სამართლებრივი და უსაფრთხო გარემო, რათა მონაცემთა სათანადო დაცვით, თავიდან იქნეს აცილებული მონაცემთა დანაშაულებრივი თუ სხვა მიზნებისთვის გამოყენების რისკები. ევროპის მონაცემთა დაცვის ზედამხედველის, პიტერ ჰუსტინქსის აზრით, „ციფრული ტექნოლოგიების ეპოქა, რომელშიც ჩვენ ვცხოვრობთ, გამოირჩევა კრეატიული და ინოვაციური მიდგომებით. შეუძლებელი და მიზანშეუწონელია კანონით „ინოვაციის“ რეგულირება, თუმცა კანონმა აუცილებლად უნდა შექმნას ადამიანის უფლებების რეალიზების საშუალებები და განსაზღვროს მონაცემთა დამმუშავებლების პასუხისმგებლობა.“

წარმოდგენილი მასალის ანალიზის საფუძველზე, საჯარო სექტორში განსაკუთრებული კატეგორიის მონაცემების დამუშავების კუთხით, იკვეთება შემდეგი ძირითადი პრობლემები:

1.პერსონალურ მონაცემთა დაცვის საკითხისადმი დაბალი ცნობადობა - აღსანიშნავია, რომ „ტექნოლოგიური პროგრესის პირობებში, პერსონალური მონაცემების მოპოვებამ და დამუშავებამ სწრაფი,

მასშტაბური და მოცულობითი ხასიათი შეიძინა. ადამიანები ყოველდღიურ ცხოვრებაში ხედავენ, რამდენად ხშირია მათი მონაცემების შეგროვება, შენახვა, გამჟღავნება ან გავრცელება. მოქალაქეთა გარკვეულ ნაწილს აქვს განცდა, რომ მუდმივი დაკვირვების ქვეშ არიან. შესაბამისად, აინტერესებთ, რა მიზნით და რა ვადით ხდება მათ შესახებ ინფორმაციის შეგროვება, არის თუ არა ეს კანონიერი, ვის მიუწვდება ხელი მათ მონაცემებზე, რა საშუალებები არსებობს მათი შელახული უფლებების დასაცავად. ინფორმირებულობის დაბალი მაჩვენებლის გამო, სამწუხაროდ, მოქალაქეები სოციალური ქსელებით თუ სხვა საშუალებებით, ხშირად ასაჯაროებენ საკუთარ პერსონალურ მონაცემებს და ვერ აცნობიერებენ, რა ზიანის მომტანი შეიძლება იყოს მათი ქმედება. ეს პრობლემა აქტუალურია არა მხოლოდ საქართველოში, არამედ სხვა, უფრო განვითარებულ ქვეყნებშიც. ევროპის კავშირის ფუნდამენტურ უფლებათა სააგენტოს მიერ 16 სახელმწიფოში ჩატარებული კვლევის საფუძველზე გამოქვეყნებულ ანგარიშში ხაზგასმულია მოქალაქეთა ცნობიერებისა და ინფორმირებულობის დაბალი დონე.[182]

2.განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის კანონში შესაბამისი ცვლილებისა და მონაცემთა დაცვის შიდა სახელმძღვანელო ინსტრუქციის არარსებობა - მნიშვნელოვანია ის გარემოება, რომ პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი საქართველოში 2012 წლის 01 მაისს შევიდა ძალაში და „შესაბამისად, ისეთ მნიშვნელოვანი სფეროების მარეგულირებელ სამართლებრივ აქტებში, როგორიცაა ჯანდაცვა, დაზღვევა, სოციალური უზრუნველყოფა, განათლება, კომუნიკაცია და სხვა, ცალსახად და მკაფიოდ არ არის ფორმულირებული მონაცემთა დამუშავების საკითხები, რაც პრაქტიკაში მონაცემთა არაერთ დამმუშავებელს უქმნის პრობლემას.“[183] პირადი ცხოვრების ხელშეუხებლობისა და მისი საჯარო ინტერესთან

[182] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

[183] პერსონალურ მონაცემთა დაცვის ინპექტორის 2014 წლის ანგარიში, ხელმისაწვდომია: www.pdp.ge.

შეუთავსებლობის საკითხი კვლავ რჩება გამოწვევად, თუმცა პერსონალური მონაცემების დაცვის კანონმდებლობის ჰარმონიზაცია საერთაშორისო სტანდარტებთან, წარმოადგენს საქართველო-ევროკავშირის ასოცირების ხელშეკრულების ვალდებულებასაც, რაც ამ მიმართულებით საჯარო უწყებებშიც სტრუქტურის სიღრმისეულ ცვლილებას გულისხმობს და სახელმწიფოსთვის ეს არ უნდა წარმოადგენდეს მხოლოდ ნაკისრ ვალდებულებას, რომელიც ფორმალურად უნდა შესრულდეს. ხშირია შემთხვევები, როდესაც საჯარო უწყებები, მიუხედავად მიზნობრიობისა, გასაკუთრებული კატეგორიის მონაცემებს ამუშავებენ კანონდარღვევით, მხოლოდ იმის გამო, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონში შესაბამისი ცვლილებები და საჯარო უწყების მარეგულირებელი სპეციალური კანონმდებლობის ჰარმონიზაცია არ განახორციელეს.

3.მონაცემთა დაცვაზე კონკრეტული პასუხსიმგებელი პირის/ სრტუქტურული რგოლისა და მონიტორინგის ეფექტიანი მექანიზმის არარსებობა - აღსანიშნავია, რომ ევროკავშირის პერსონალური მონაცემების დაცვის ახალი რეგულაცია ითვალისწინებს პერსონალური მონაცემების დაცვის ოფიცრის პოზიციის სავალდებულობას. აღნიშნული პოზიცია სავალდებულო უნდა იყოს საჯარო დაწესებულებებისათვის და იმ მონაცემთა დამმუშავებლებისათვის, რომლებიც დიდი ოდენობით პერსონალურ მონაცემებს ამუშავებენ, განსაკუთრებით იმ კომპანიებისათვის, რომლებიც ამუშავებენ განსაკუთრებული კატეგორიის მონაცემებს. მონაცემთა დაცვის ოფიცრის პოზიცია არ არის სიახლე ევროკავშირის ბევრი სახელმწიფოსათვის. თუმცა დღესდღეობით, ეს პოზიცია მეტად მნიშვნელოვანი გახდა ევროკავშირის ახალი რეგულაციის პრაქტიკაში, იმპლემენტაციის მიზნებიდან გამომდინარე. ექსპერტები მიიჩნევენ, რომ მონაცემთა დაცვის ოფიცერმა უნდა დააბალანსოს სიცარიელე და წინააღმდეგობა ინფორმაციული ტექნოლოგიების, იურიდიულ, ადამიანური რესურსების მართვისა და საზოგადოებასთან ურთიერთობის დეპარტამენტების საქმიანობას შორის. ამასთან, მან უნდა

ისარგებლოს დამოუკიდებლობით კომპანიის ან საჯარო დაწესებულების იერარქიაში. მონაცემთა დაცვის ოფიცერი მოიაზრება, როგორც შიდა პოლიციელი და მამხილებელი. მიუხედავად იმისა, რომ მონაცემთა დაცვის ოფიცრის პოზიცია არ არის სავალდებულო ყველა მონაცემთა დამმუშავებლისათვის, კომპანიაში აუცილებლად უნდა არსებობდეს პირი, რომელიც პასუხისმგებელი იქნება პერსონალური მონაცემების დაცვის საკითხებზე.

4. განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავების პრინციპების დარღვევითა და საფუძვლის გარეშე დამუშავება - ნაშრომში წარმოდგენილი მასალიდან ნათლად ჩანს, რომ საქართველოს მონაცემთა დაცვის კანონმდებლობა თითქმის სრულ ჰარმონიზაციაშია ევროპულ კანონმდებლობასთან, თუმცა ჯერ კიდევ პრობლემებია საჯარო უწყებებში, სტანდარტების შესაბამისად, პრაქტიკაში კანონის ინპლემენტაციასთან დაკავშირებით. საჯარო სექტორში მონაცემთა დამუშავების პროცესში, კვლავაც პრობლემას წარმოადგენს მონაცემთა დაცვისათვის კანონით გათვალისწინებული პრინციპების დარღვევა, რაც გამოიხატება მიზნის არაპროპორციულად, არაადეკვატურად, დიდი მოცულობითა და განუსაზღვრელი ვადით მონაცემთა შეგროვებასა და შენახვაში. ხშირია შემთხვევები, როდესაც დიდი მოცულობით პერსონალურ მონაცემებსა და მოძველებულ, გასაახლებელ ინფორმაციაზე ხელმისაწვდომობა აქვთ სახელმწიფო ორგანიზაციებს ან ამ კატეგორიის მონაცემებს ამუშავებენ შესაბამისი სამართლებრივი საფუძვლის გარეშე.

5. საჯარიმო სანქციების მცირე ოდენობა - „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა პრინციპების დარღვევითა და საფუძვლის გარეშე დამუშავებისათვის საჯარიმო სანქციებს ითვალისწინებს. თუმცა ნიშანდობლივია ის ფაქტიც, რომ სანქციების გაზრდის ინიციატივით გამოვიდა დიდი ბრიტანეთის პერსონალური მონაცემების დაცვაზე ზედამხედველობის განმახორციელებელი ორგანო (ICO), მას შემდეგ, რაც „ქალმა, რომელმაც უკანონოდ გაყიდა 28,000 ადამიანის პერსონალური მონაცემები, მიიღო

მოგება 5000 ფუნტი სტერლინგის ოდენობით, ხოლო სასამართლოს მიერ მასზე დაკისრებულმა ჯარიმამ მხოლოდ 1,000 ფუნტი სტერლინგი შეადგინა. დიდი ბრიტანეთის საზედამხედველო ორგანო მიზანშეწონილად მიიჩნევს, რომ პერსონალური მონაცემების დაცვის კანონმდებლობის ასეთი სახის დარღვევისათვის პასუხისმგებლობის ზომა უნდა იყოს არა მხოლოდ ჯარიმა, არამედ პატიმრობა.[184] [94]

ნაშრომში განხილულია საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს როლი განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების საკითხში. ამ მხრივ, წარმოდგენილი მასალის ანალიზის საფუძველზე, შეიძლება ითქვას, რომ პერსონალურ მონაცემთა დაცვის ინსპექტორისათვის მნიშვნელოვან გამოწვევას **(1) ცენტრალიზებული მმართველობა (2) ფაილური სისტემის ელექტრონული კატალოგის ეფექტიანი მექანიზმის არსებობა, (3) ინსპექტორის აპარატის ადამიანური რესურსის სიმცირე და (4) შესაბამისი საკანონმდებლო ცვლილებების საჭიროება წარმოადგენს.**

აღსანიშნავია, რომ დღეს მოქმედი კანონმდებლობით, ინსპექტორი საქმეს განიხილავს საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსით დადგენილი წესის შესაბამისად, რომლის 38-ე მუხლის პირველი პუნქტის თანახმად, ადმინისტრაციული სახდელი შეიძლება დაედოს არა უგვიანეს ორი თვისა სამართალდარღვევის ჩადენის დღიდან, ხოლო როცა სამართალდარღვევა დენადია – არა უგვიანეს ორი თვისა მისი გამოვლენის დღიდან, ხოლო ამავე კოდექსის 232-მუხლის მე-7 ნაწილის შესაბამისად, ადმინისტრაციული სამართალდარღვევის საქმის წარმოება არ უნდა დაიწყოს, ხოლო დაწყებული საქმე უნდა შეწყდეს, თუ საქმის განხილვის მომენტისათვის განვლო 38-ე მუხლით დადგენილმა ვადებმა.[185] [95] შესაბამისად, პერსონალურ მონაცემთა დაცვის ინსპექტორს

[184] Curtis J., „Information Commissioner calls for threat of prison sentences after rental car employee sells customer data“, see: http://www.itpro.co.uk/data-protection/25848/ico-data-thieves-must-face-tougher-punishments-than-fines [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

[185] საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 38-ე და 232-ე მუხლის მე-7 ნაწილი.

სამართალდარღვევაზე რეაგირება შეუძლია მხოლოდ იმ შემთხვევაში, თუ მისი ჩადენის დღიდან გასულია არაუმეტეს ორი თვისა, რაც როგორც მონაცემთა დამუშავების, ისე ინსპექტორის აპარატის საქმიანობის სპეციფიკის გათვალისწინებით, ვერ იძლევა დარღვევებზე ეფექტიანად რეაგირების საშუალებას და ამ მხრივ, მოდიფიცირებას საჭიროებს. ხაზგასასმელია ის გარემოებაც, რომ წარმოდგენილი 28 გადაწყვეტილებიდან 5 შემთხვევაში, აღნიშნული ნორმის მოთხოვნის მიუხედავად, ინსპექტორმა ხანდაზმული განცხადებები მიიღო წარმოებაში და განახორციელა მათი შესწავლა. ამასთან, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატს, დაარსების დღიდან, ოთხი წლის თავზე, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერების შემოწმების მიზნით, განხორციელებული აქვს 10 შემოწმება (ერთი შემოწმება, რომელიც 2016 წელს დაიწყო, ინფორმაციის გამოთხოვის მომენტისათვის კვლავ მიმდინარეობდა) და განხილული აქვს მოქალაქეთა 20 განცხადება (ერთი განცხადების განხილვა, რომელიც აპარატში 2016 წელს შევიდა, კვლავ მიმდინარეობდა). ტერიტორიული დაფარვის ფარგლებს თუ გადავხედავთ, შემოწმებები ჩატარებულია ძირითადად, ქ. თბილისის მასშტაბით, მხოლოდ 3 შემთხვევაში - რეგიონში, კერძოდ, წალკის ორ საჯარო სკოლაში თემატურად იდენტურ საკითხებზე და ადიგენის საჯარო სკოლაში.

დასკვნის სახით, შეიძლება ითქვას, რომ პერსონალურ მონაცემთა დაცვაზე სრულყოფილი სამართლებრივი სისტემის ამოქმედებისათვის აუცილებელია მოქმედი საზოგადოებრივი ღირებულებების კონცეპტუალური გადახედვა და მოდერნიზაცია. შესაბამისად, „საქართველოს მოუწევს, საკმაოდ სწრაფად გაიაროს სამართლებრივი ცნობიერების განვითარების ის გზა, რომელსაც ევროპული ქვეყნები ბოლო 30 წლის განმავლობაში გადიოდნენ.[186] ამასთან, „ევროკავშირსა და ევროპის საბჭოს განახლებულ სტანდარტებთან ჰარმონიზებისა და ევროკავშირის შესაბამისი უწყებების რეკომენდაციების შესრულების მიზნით, იკვეთება

[186] კორკელია კ., „ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო“, სტატიათა კრებული, 2011 წელი, თბილისი, გვ. 349.

საქართველოში პერსონალურ მონაცემთა დაცვის მარეგულირებელი კანონმდებლობის რეფორმის გაგრძელების საჭიროება.“[187]

რეკომენდაციები

ნაშრომში წარმოდგენილი მასალის ანალიზის საფუძველზე, შესაძლებელია, გავცეთ შემდეგი სახის რეკომენდაციები:

საქართველოს სახელმწიფოს საჯარო სექტორში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისა და დაცვისათვის აუცილებელია:

1. საჯარო მმართველობის ორგანიზაციებში, როგორც დასაქმებული პირების, ასევე, მონაცემთა დამმუშავებლების ინფორმირებულობა და საზოგადოებრივი ცნობიერების ამაღლება განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების, გამჟღავნებისა და დაუცველობის საფრთხეების შესახებ (შიდა ინსტრუქციების მომზადება, შესაბამისი ტრენინგკურსების განხორციელება, პერმანენტული გადამზადება);

2. პერსონალური მონაცემების დაცვის ოფიცრის პოზიციის ან პერსონალური მონაცემების დამუშავების კანონიერებაზე ზედამხედველი სტრუქტურული ერთეულის საკანონმდებლო დონეზე შექმნის სავალდებულოობა ყველა საჯარო დაწესებულებისთვის. ამასთან, სტრუქტურული ერთეულის შექმნის ვალდებულების დაკისრება იმ მონაცემთა დამმუშავებლებისათვის, რომლებიც დიდი ოდენობით პერსონალურ მონაცემებსა და/ან განსაკუთრებული კატეგორიის პერსონალურ მონაცემებს ამუშავებენ;

3. საჯარო მმართველობის ორგანიზაციების მარეგულირებელი სპეციალური ნორმატიული აქტების ჰარმონიზაცია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან. განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისათვის შესაბამისი

[187] ქალდანი თ., სარიშვილი ს., „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, 2016 წელი.

მიზნობრიობის არსებობის შემთხვევაში, საკანონმდებლო ცვლილებების განხორციელება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლში, რომლის საფუძველზეც, საჯარო ორგანიზაციას მიეცემა ამ კატეგორიის მონაცემების დამუშავების კანონისმიერი საფუძველი;

4. საჯარო მმართველობის ორგანიზაციებში განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების პროცედურის შიდაორგანიზაციული სტანდარტის შემუშავება, მათ შორის, ყოველ კონკრეტულ შემთხვევაში ამ კატეგორიის მონაცემების შენახვის ვადის განსაზღვრა დამოუკიდებლად;

5. საჯარო მმართველობის ორგანიზაციებში მონაცემთა დამმუშავებლების საქმიანობაზე შიდა მონიტორინგის ეფექტიანი მექანიზმის შექმნა. კერძოდ, მონაცემთა დამმუშავებელთა შემოწმება, მათ ხელთ არსებულ მონაცემების სისწორის, დამუშავებისა და შენახვის აუცილებლობის მიზნით. საჭიროების შემთხვევაში, ამ მიმართულებით, შესაბამისი პირის გამოყოფა და/ან სტრუქტურული ერთეულის შექმნა.

6. შიდა ორგანიზაციული დოკუმენტით საჯარო მმართველობის ორგანიზაციის მიერ განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაარქივების, ასევე არქივზე წვდომის უფლების შეზღუდვის, რეგულირების, მისი უსაფრთხოების სტანდარტის განსაზღვრა. ამასთან, ასეთი მონაცემების წაშლის შემთხვევაში, მონაცემების ამოშლის უზრუნველყოფა ყველა არსებული ბაზიდან, რომელთაც მონაცემები გადაეცათ გარკვეული მიზნებისათვის, რადგან მონაცემთა გადაცემა საჯარო უწყებას, როგორც მონაცემთა დამმუშავებელს, არ ათავისუფლებს და ტოვებს მონაცემზე პასუხისმგებელ პირად;

7. საჯარო მმართველობის ორგანიზაციებში განსაკუთრებული კატეგორიის მონაცემთა დაცვის მიზნით, უსაფრთხოების ეფექტიანი სისტემის შექმნა და უსაფრთხოების პოლიტიკის/მონაცემთა უსაფრთხოების წესების განსაზღვრა;

განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების კანონიერებაზე ეფექტიანი ზედამხედველობის განხორციელების მიზნით, პერსონალურ მონაცემთა დაცვის ინსპექტორს მიეცეს შემდეგი ხასიათის რეკომენდაციები:

1. საქართველოს მასშტაბით პერსონალურ მონაცემთა დაცვაზე ეფექტიანი ზედამხედველობის მიზნით, შექმნას რეგიონული მართვის ცენტრები;

2. გეგმიური ინსპექტირებების განსაზღვრისას, პრიორიტეტი მიანიჭოს და შეამოწმოს განსაკუთრებული კატეგორიის პერსონალურ მონაცემების დამუშავების კანონიერება იმ საჯარო მმართველობის ორგანიზაციებში, რომლებიც თავიანთი საქმიანობის პროცესში, ამუშავებენ ან დიდი მოცულობით ამუშავებენ ამ კატეგორიის პერსონალურ მონაცემებს;

3. საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 38-ე და 232-ე მუხლის მე-7 ნაწილის შესაბამისად, არ განიხილოს და შეწყვიტოს იმ მოქალაქეთა განცხადების წარმოება, რომელთა მომართვებიდანაც ნათლად დგინდება ჩადენილი სამართალდარღვევის ფაქტის ხანდაზმულობა. აღნიშნული შესაძლებლობას მისცემს აპარატს, პრიორიტეტულად და სწორად გაანაწილოს ინსპექტორის აპარატში დასაქმებული ადამიანური რესურსი;

4. განახორციელოს საკანონმდებლო ცვლილება, რითაც გაიზრდება განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა პრინციპების დარღვევითა და საფუძვლის გარეშე დამუშავებისათვის დაწესებული საჯარიმო სანქცია, ვინაიდან პასუხისმგებლობის მცირე ოდენობა ამცირებს კანონის აღსრულების მექანიზმის ეფექტურობას;

5. განახორციელოს ფაილური სისტემის ელექტრონული კატალოგის იმგვარად მოდიფიცირება, რომ ერთი მხრივ, მარტივად იყოს შესაძლებელი მონაცემთა დამმუშავებლების კონტროლი და მათზე არსებული ინფორმაციის ანალიზი (მათ შორის რაოდენობრივად თვლა), ხოლო მეორე მხრივ, შეიცვალოს საძიებო სისტემა იმგვარად, რომ მონაცემები არ მეორდებოდეს და მარტივად ხდებოდეს დიდი ოდენობის მონაცემების

დამმუშავებლების იდენტიფიცირება. აღნიშნული ხელს შეუწყობს კონკრეტულ უწყებაში არსებული რისკების სათანადო შეფასებასა და ინპექტორის აპარტის მიერ ინსპექტირებების პრიორიტეტულად დაგეგმვას.

ბიბლიოგრაფია:

1. „ადამიანის უფლებათა დაცვის ეროვნული და საერთაშორისო მექანიზმები (სტატიათა კრებული)“, ქალდანი თ., სარიშვილი ნ., სტატია, „პერსონალურ მონაცემთა დაცვის საერთაშორისო სტანდარტების დანერგვა საქართველოში 2016 წელი;

2. Tereza M.Payton and Theodore Claypoole „Privacy in the age of big data“;

3. „Analysis: Why an open and honest approach to personal data use could save you from losing a vital commodity“, see: http://www.cbronline.com/news/cybersecurity/data/data-protection-day-improve-your-privacy-policy-or-lose-your-data-4796165 [უკანასკნელად გადამოწმებულია 2017 წლის თებერვალში];

4. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში, გვ.25, ხელმისაწვდომია: www.pdp.ge;

5. კორკელია, კ., „ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო“, სტატიათა კრებული, ჯოხაძე გ., სტატია „პერსონალურ მონაცემთა დაცვა ადამიანის უფლებათა კონტექსტში: საქართველოს მაგალითი, გამოწვევები ტენდენციები, 2011 წელი, თბილისი, გვ. 327-329;

6. „The economic value of personal data for online platforms, firms and consumers“, by: Liem C., Petropoulos G., 2016 y, see: http://www.pieria.co.uk/articles/the_economic_value_of_personal_data_for_online_platforms_firms_and_consumers, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

7. ცაცანაშვილი მ., „ინფორმაციული სამართალი“, თბილისი, 2004 წ, გვ 100-110;

8. თამთა არჩუაძე, სამაგისტრო ნაშრომი „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას“, აღმოსავლეთ ევროპის უნივერსიტეტი, 2016 წელი, გვ.9-18;

9. Convention for the protection of Human Rights and fundamental freedoms. 1650;

10. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS. 180) adopted in Strasburg by the Council of Europe on 28 January 1981.

11. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS. No. 181, 2004;

12. 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.

13. Recommendation No. R(87)15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector, adopted by the Committee of Ministers on 17 September 1987.

14. Framework Decision of the Council of European Union 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

15. გოშაძე კ., მონაცემთა დაცვის ევროპული სამართალი, თბილისი, გამომცემლობა „იურისტების სამყარო“; 2015 წელი, გვ. 252;

16. Regulation 2016/679 of the European Parlament and of the Council 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), 27 April 2016;

17. ცერცვაძე მ., „პიროვნების დაცვის საერთოევროპული სამართლებრივი სტანდარტები პერსონალური მონაცემების ავტომატიზებული დამუშავებისას“,საქართველოს ელექტრონული სამეცნიერო ჟურნალი იურისპრუდენცია №1, 2002 წელი, გვ. 27-36;

18. Privacy law Fundamentals, Daniel J. Solove & Paul M. Schwartz, Edited by the International Association of Privacy Professionals (IAPP), 2015, p. 145-146;

19. „პერსონალურ მონაცმთა დაცვის შესახებ“ საქართველოს კანონი, ხელმისაწვდომია: www.matsne.gov.ge;

20. „პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.53;

21. „ადამიანის უფლებათა სტანდარტების გავლენა საქართველოს კანონმდებლობასა და პრაქტიკაზე“, სატიათა კრებული კორკელია კ. რედაქტორობით, საგინაშვილი ნ., „პესრონალური მონაცემების დაცვა და პირადი ცხოვრების ხელშეუხებლობა“, თბილისი, 2015 წ, გვ.166-191;

22. ინოვაციებისა და რეფორმების ცენტრი, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ინპლემენტაცია საქართველოს სამინისტროებში, მონიტორინგის ანგარიში, 2013 წელი, გვ.49, ხელმისაწვდომია ვებ-გვერდზე:www. irc.ge;

23. ინოვაციებისა და რეფორმების ცენტრი, „საქრათველოში მიგრაციის მართვის სფეროში პერსონალურ მონაცემთა დაცვის კვლევის ანგარიშის მოკლე მიმოხილვა“, 2015 წელი, გვ.42, ხელმისაწვდომია ვებ-გვერდზე:www. irc.ge;

24. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის ანგარიში, გვ.37, ხელმისაწვდომია: www.pdp.ge.

25. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში, გვ. 72, ხელმისაწვდომია : : www.pdp.ge;

26. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2016 წლის ანგარიში, გვ. 114, ხელმისაწვდომია:: www.pdp.ge;

27. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის 2017 წლის 16 მაისის №PDP 5 17 00001756 წერილი;

28. Hhe Right To Privacy, Samuel D. Warren & Luis D. Brandies, Published in the 2015 Hardcover Edition By Quid Pro Books, p…

29. Prof.dr. Lokke Moerel, Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof, 2014, see: http://www.debrauw.com/wp-content/uploads/NEWS%20%20PUBLICATIONS/Moerel_oratie.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

30. ბიჭია მ., „პირადი ცხოვრების დაცვა საქართველოს სამოქალაქო სამართლის მიხედვით“, გამომცემლობა „ბონა-კაუზა“ თბილისი, 2012 წელი, გვ. 60-76;

31. Иванский В., „Правовая зашита информации о частной жизни граждан“, 1999, ст. 141.

32. Karanja S., Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Netherlands, Martinus Nijhoff Publishers, 2008, p.123;

33. თემიდა, სამეცნიერო პრაქტიკული ჟურნალი, უგრეხელიძე ნ., სტატია „პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზა საქართველოში“, 2011 წელი, №5(7), გვ. 162-167;

34. Rawlinson K., „UK press accused of 'misinformed media storm' over email spying story“, 2016, see: http://www.theguardian.com/technology/2016/jan/16/uk-press-accused-of-misinformed-media-storm-over-email-spying-story, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

35. მუხლი 29 სამუშაო ჯგუფი (2013), მოსაზრება 03/2013 მიზნის ლიმიტირების შესახებ, WB 203, ბრიუსელი, 2 აპრილი, 2013 წელი;

36. ავსტრიის მონაცემთა დაცვის აქტი (Datenschutzgesetz), Fed. Law Gazette I No. 165/1999, პარაგრაფი 46, ხელმისაწვდომია ინგლისურ ენაზე: www.dsk.gv.at ;

37. ვროპის კომისიის სპეციალური ევრობარომეტრი 431, გვ. 15, ხელმისაწვდომია: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

38. 29-ე მუხლის სამუშაო ჯგუფის დამატებითი ინფორმაცია, ხემისაწვდომია: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Art29 [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

39. მუხლი 29 სამუშაო ჯგუფი (2007) სამუშაო დოკუმენტი ჯანმრთელობის ელექტრონულ რეესტრში (HER) ჯანმრთელობის შესახებ პერსონალურ მონაცემთა დამუშავების თაობაზე, WP131, ბრიუსელი, 15 თებერვალი 2007 წელი, ხელმისაწვდომია: https://secure.edps.europa.eu/

40. Association Agenda between the European Union and Georgia, see: www.eeas.europa.eu;

41. გაგნიძე ე., საიქოძე ნ., „პერსონალური მონაცემების დაცვასთან დაკავშირებული კერძო და საჯარო ინტერესის თანაფარდობა და უფლებაში ჩარევის საფუძვლიანობის კრიტერიუმები“, სტუდენტური სამართლებრივი ჟურნალი, 2016წ. გვ.64;

42. იზორია ლ., ბერიაია ი., და სხვები, „საპოლიციო სამართალი“, 2015 წელი, თბილისი, შსს აკადემიის გამომცემლობა, გვ.83;

43. საღარაძე ს., „ინფორმაციის თავისუფლება და პერსონალურ მონაცემთა დაცვა“, 2014 წელი, თბილისი, გვ. 5;

44. საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406.408 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“;

45. S.D. Warren & L.D. Brandeis, ‘The Right to Privacy’, Harvard Law Review, 1890, p. 193;

46. Sophie Stalla-Bourdillon, Joshua Phillips, Mark D. Ryan, Privacy vs. Security, 2010, p. 16;

47. ქვაკუთხედი, ეროვნულ-სარწმუნოებრივი ჟურნალი, თბილისი, 2011 წელი, №1(52), გვ. 8-10;

48. სამეცნიერო პრაქტიკული ჟურნალი თემიდა №6(8), მოსახლიშვილი ლ., სტატია - „პერსონალური მონაცემების დაცვის კანონდებლობა საქართველოში“, 2012 წელი, გვ. 77-84;

49. ჟურნალი „თბილისელები“, ხაჩიძე ნ., „როგორ გროვდება ადამიანის პერსონალური მონაცემები, სად ინახება ისინი და რა უნდა ვიცოდეთ იმისთვის, რომ თავიდან ავიცილოთ ჩვენივე მონაცემების ბოროტად გამოყენება“, 31.03.14-06.04.14., №13 (692);

50. Article 29, Data Protection Working Party, Advice paper on special categories of data („sensitive data”), 2011, p. 4, see: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

51. Handbook on European data protection law, Council of Europe, 2014, p. 81, see: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, [უკანასკნელად ნანახია 2017 წლის აპრილში];

52. Louise Wiseman, Jenny Gordon, Data protection: Guidelines for the use of personal data in system testing, Second edition, 2009, გვ. 2, გამოცემა ხელმისაწვდომია: http://shop.bsigroup.com/upload/Shop/Download/Books/BIP0002sample.pdf; [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

53. „ადმინისტრაციული სამართლის პრობლემები“, გიორგაძე ლ. საერთო რედაქტორობით, სტატიათა კრებული, ცანავა ლ., „პერსონალურ მონაცემთა დამუშავებისა და საჯაროობის სამართლებრივი მოწესრიგება“, დავით ბატონიშვილის სამართლის ინსტიტუტის გამომცემლობა, 2013 წელი, გვ.63.

54. „რეკომენდაციები ბიომეტრიულ მონაცემების დამუშავების შესახებ“, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, გვ. 13, ხელმისაწვდომია: www.pdp.ge;

55. Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective (2nd Edition), Offi ce of the Privacy Commissioner for Personal Data, Hong Kong, 2010, p. 44, see: https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

56. Article 29, Data Protection Working Party, Working Document on Genetic Data,WP 91, 2004, see: http://ec.europa.eu/ ;

57. „Who Owns Our Genes?": Proceedings of an international conference, by Nordic Committee on Bioethics, Tallin, October, 1999, p. 78;

58. Stefanick L., Controlling knowledge: Freedom of Information and Privacy Protection in a Networked World, Canada, AU Press, 2011. p. 101;

59. ბორნი ჰ., უილსი ა., „დაზვერვის სამსახურებზე ზედამხედველობის განხორციელება“, 2012 წელი, გვ.162;

60. ნორვეგიის პერსონალურ მონაცემთა დაცვის აქტი (2000 წლის 14 აპრლი), ხელმისაწვდომია: https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

61. დიდი ბრიტანეთის პერსონალურ მონაცემთა დაცვის აქტი (1988 წელი), ხელმისაწვდომია: http://www.legislation.gov.uk/ukpga/1998/29/section/2, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

62. იტალიის მონაცემთა დაცვის კოდექსი (2003 წელი), ხელმისაწვდომია: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code

+-+Legislat.+Decree+no.196+of+30+June+2003.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

63. თათია ცეცხლაძე, სამაგისტრო ნაშრომი „ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემის დაცვა სადაზღვევო სფეროში“, კავკასიის უნივერსიტეტი, 2017 წელი, გვ. 33-34;

64. Arthur J. Winfield, Judith Rees, Ian Smit, Pharmaceutical Practice, 2009, see: https://books.google.ge/books?id=G0lZEGZi9SMC&pg=PT489&lpg=PT489&dq=sensitive+personal+data+book&source=bl&ots=CXPbFwpXGu&sig=EMUJJJb6-NknQ3rVTSN7UB9H7ms&hl=en&sa=X&ved=0ahUKEwjSs8XOvMHTAhVD1BoKHW19Dcs4ChDoAQhAMAU#v=onepage&q=sensitive%20personal%20data%20book&f=false, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

65. Satellite Remote Sensing, A New Tool for Archaeology, Editors: Rosa Lasaponara and Nicola Masin, UK, 2012. p. 8;

66. Büllesbach A., Concise European IT Law, USA, Kluwer Law International, 2010, p. 94;

67. Allen & Overy, The EU General Data Protection Regulation, 2017, p. 4, see: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

68. „რეკომენდაცია ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემების დამუშავების შესახებ“, 2016 წელი, პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, გვ.12, ხელმისაწვდომია: www.pdp.ge;

69. Bridgit Dimond, Legal Aspects of Midwifery, third edition, 2006, p. 183, see: https://books.google.ge/books?id=pjsHBgAAQBAJ&pg=PA180&lpg=PA180&dq=sensitive+personal+data+book&source=bl&ots=kX5a8U1dpI&sig=QAi-AadIz2Ur_EDVtPijyNl8rl0&hl=en&sa=X&ved=0ahUKEwjpmbGxucHTAhXDtRQKHZrBDvw4ChDoAQg0MAM#v=onepage&q=sensitive%20personal%20data%20book&f=false, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

70. „არასაპატიმრო სასჯელთა აღსრულების წესისა და პრობაციის შესახებ“ საქართველოს კანონი, მუხლი 2, ხელმისაწვდომია: www.matsne.gov.ge;

71. „საერთაშორისო დაცვის შესახებ“ საქართველოს კანონი, მუხლი 2, ხელმისაწვდომია: www.matsne.gov.ge;

72. Acohido B., Swarts J., Zero Day Threat: The Shocking Truth of how Banks and Credit Bureaus Help Cyber Crooks Steal Your Monay and Identity, NY and London, Union Square Press an imprinted of Sterling Publishers Co., 2008. p. 101

73. Susanna Norelid and Emanuel Hollstrand, Data protection in Sweden: overview, 2017, see: https://uk.practicallaw.thomsonreuters.com/8-502-0348? lrTS=20170426060701848&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

74. Симонов Алексей., Предисловие, Волчинская Е.К., Защита персональных данных, Россия, 2001, ст. 6;

75. ახალი თაობა, ხურცილავა ნ., „რა ბედი ელის პერსონალურ მონაცემებს“ თბილისი, 2014 წლის 29 იანვარი, №23, გვ.7;

76. Петров М.И., Постатейный комментарий к Федеральному закону О персональных данных, Россия, Юстицинформ, 2007, ст. 28;

77. სამეცნიერო შრომების კრებული, რეფერატი და რეცენზირებული სამეცნიერო პრაქტიკული ჟურნალი, მოსახლიშვილი ლ., სტატია „პერსონალური მონაცემების დაცვა შრომით ურთიერთობებში“, თბილისის ღია სასწავლო უნივერსიტეტი, თბილისი, 2013 წელი, №4, გვ. 16-25;

78. წლიური ალმანახი, სტატიათა კრებული, ფალავანდიშვილი ბ., „პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი - ზოგადი მიმოხილვა, იურიდიული ფირმა „მგალობლიშვილი, ყიფიანი, ძიძიგური“, თბილისი, 2013 წელი, გვ.48-52

79. ევროპის კომისია, კვლევა „Study on the economic benefits of privacy- enhancing technologies (PETS)“, გვ. 17, ხელმისაწვდომია: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

80. Madsen, Wayne, Handbook of Personal Data Protection, 1992, p.16-62;

81. Winnie Chang, A Practical Guide to Singapore Data Protection Law, 2013, ხელმისაწვდომია: http://www.cnplaw.com/en/media/files/Brochure%20for%20A%20Practical%20Guide%20to%20Singapore%20Data%20Protection%20Law%20by%20Winnie%20Chang.pdf[უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

82. Shepher A., „Electronic Frontier Foundation gives messaging app one star out of five for security“, see: http://www.itpro.co.uk/security/24839/whatsapp-among-worst-rated-companies-in-privacy-study,[უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

83. Hart J., „New cyber security trends and new approaches to data protection“ December 2015y, see: http://www.itproportal.com/2015/12/17/2016-new-cyber-security-trends-new-approaches-data-protection/?, [უკანასკნელად ნანახია 2017 წლის მაისში];

84. Handbook on European data protection law, 2014, see: http://www.echr.coe.int/documents/handbook_data_protection_eng.pdf [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

85. საფრანგეთში მონაცემთა დაცვაზე საზედანხედველო ორგანოს ვებ-გვერდი: https://www.cnil.fr/en/node/287, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

86. ბულგარეთში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებ-გვერდი: https://www.cpdp.bg/en/index.php?p=element&aid=39, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

87. ბელგიის მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებ-გვერდი: https://www.privacycommission.be/en/in-a-nutshell [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

88. ჰოლანდიაში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებ-გვერდი: https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/commissioners-dutch-dpa, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

89. ესპანეთში მონაცემთა დაცვაზე საზედამხედველო ორგანოს ვებ-გვერდი: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/historia-iden-idphp.php [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

90. „Human error is the main cause of data breaches, according to the UK's data protection watchdog“ 2016, see: http://www.out-law.com/en/articles/2016/june/human-error-remains-main-cause-of-data-breaches-ico-data-shows/?, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში].

91. „Watchdog fines GP for data breach“, 2016, see: http://www.professionalsecurity.co.uk/news/case-studies/watchdog-fines-gp-for-data-breach/?, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

92. „Council fined £100,000 after social care files left in empty building“, 2016, see: https://www.theguardian.com/society/2016/aug/17/council-fined-100000-after-social-care-files-left-empty-building, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

93. „Ashley Madison hackers release vast database of 33m accounts“, 2015, see: http://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts, [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

94. Curtis J., „Information Commissioner calls for threat of prison sentences after rental car employee sells customer data“, see: http://www.itpro.co.uk/data-protection/25848/ico-data-thieves-must-face-tougher-punishments-than-fines [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

95. საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსი.

ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები:

1. ამანი შვეიცარიის წინააღმდეგ [Amann v. Switzerland [GC], ადამიანის უფლებათა ევროპული სასამართლო 2000 წლის 16 თებერვალი, No. 27798/95;
2. ტეილორ-საბორი გაერთიანებული სამეფოს წინააღმდეგ [Taylor-Sabori v. the United Kingdom], ადამიანის უფლებათა ევროპული სასამართლო, 2002 წლის 22 ოქტომბერი No. 47114/99;
3. კოპლანდი გაერთიანებული სამეფოს წინააღმდეგ [Copland v. The United Kingdom] 2007 წელის 03 ივლისი, No. 62617/00;
4. ბარბულეშკუ რუმინეთის წინააღმდეგ [Barbulescu v Romania] ადამიანის უფლებათა ევროპული სასამართლო, 2016 წლის 12 იანვარი No. 61496/08;
5. პეკი გაერთიანებული სამეფოს წინააღმდეგ [Peck v. the United Kingdom], ადამიანის უფლებათა ევროპული სასამართლო, 2003 წლის 28 იანვარი, No. 44647/98;
6. ხელილი შვეიცარიის წინააღმდეგ, Khelili v. Switzerland, ადამიანის უფლებათა დაცვის ევროპული სასამართლო, 2011 წლის 18 ოქტომბერი, No. 16188/07;
7. ს. და მარპერი გაერთიანებული სამეფოს წინააღმდეგ [S. and Marper v. the United Kingdom], ადამიანის უფლებათა ევროპული სასამართლო 2008 წლის 4 დეკემბერი, Nos. 30562/04 and 30566/04;
8. ჰარალამბი რუმინეთის წინააღმდეგ, Haralambie v. Romania, ადამიანის უფლებათა ევროპული სასამართლო, 2009 წლის 27 ოქტომბერი, No. 21737/03;
9. „კ. ჰ“ და სხვები სლოვაკეთის წინააღმდეგ, K.H. and Others v. Slovakia, ადამიანის უფლებათა ევროპული სასამართლო, 2009 წლის 28 აპრილი No. 32881/04;

ინტერნეტ-რესურსები:

www.pdp.ge
www.catalog.pdp.ge
www. matsne.gov.ge
www.echr.coe.int