პერსონალური მონაცემების დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში

მერი წერეთელი

2019 წელი

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
თბილისი

რეზიუმე

მეწარმე, რომელიც ახალ პროდუქტს ქმნის და ბაზარზე ადგილის დამკვიდრებას ცდილობს, შესაძლოა, რეგულაციების სიმრავლეს, დაბრკოლებად აღიქვამდეს. მით უფრო, თუ ჯერ არ აქვს საშუალება, იურიდიულ, ფინანსურ, თუ ტექნიკურ საკითხებში, ისარგებლოს შესაბამისი დარგის სპეციალისტების დახმარებით.

თუმცა, გონივრული კანონმდებლობა და რეგულაციები, ყოველთვის, ისეთი ღირებულების დასაცავად იქმნება, რომელიც სახელმწიფოსთვისაც მნიშვნელოვანია, მოქალაქისთვისაც და ბიზნესისთვისაც. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შემთხვევაში, ეს ღირებულება პირადი ცხოვრების ხელშეუხებლობა და მისი ერთ-ერთი მთავარი კომპონენტი - პერსონალური მონაცემების დაცვაა.

საქართველო ერთ-ერთია მსოფლიოს იმ 100-ზე მეტ ქვეყანას შორის, რომელშიც პერსონალურ მონაცემთა დაცვის კანონმდებლობა მოქმედებს და თანაბრად ვრცელდება, როგორც საჯარო, ისე კერძო ორგანიზაციებზე. ბიზნესს, ამ კანონმდებლობის მოთხოვნათა დაცვით, შექმნილი პროდუქტი, შესაძლოა, დაეხმაროს რესურსების დაზოგვაში, მომხმარებლების და საკუთარი გუნდის ნდობის მოპოვებაში და, შესაძლოა, იქცეს კონკურენტულ უპირატესობადაც. განსაკუთრებით მაშინ, თუ კომპანია გეგმავს საერთაშორისო ბაზარზე გასვლას.

წინამდებარე კვლევა, საკითხის სრულყოფილად შესწავლის მიზნით, მიმოიხილავს არამარტო ქართულ ნორმატიულ ბაზასა და პრაქტიკას, არამედ წარმოაჩენს პერსონალურ მონაცემთა დაცვის გარანტიების შექმნის კუთხით წარმატებული და გამოცდილი ქვეყნების იმ სამართალშემოქმედებით და პრაქტიკულ ასპექტებს, რომელთა განხორციელება, საქართველოშიც, მიზანშეწონილი და აუცილებელია.

ნაშრომში წარმოდგენილია, პერსონალურ მონაცემთა დამუშავებისას, ისეთი საშუალებების გამოყენების არსი და მნიშვნელობა, როგორებიცაა მონაცემთა ავტომატური დამუშავება, ნახევრად ავტომატური დამუშავება და არაავტომატური საშუალებით დამუშავება. განხილულია, პერსონალურ მონაცემთა დამუშავებისას, თითოეული მათგანით შესრულებული სამუშაოს დადებითი და უარყოფითი მხარეები და გამოვლენილია მონაცემთა

დამუშავების ისეთი სახე, რომელიც ყველაზე უკეთ უზრუნველყოფს პერსონალურ მონაცემთა გამჟღავნებისაგან დაცვას.

გამოკვლეულია, სამეწარმეო ბიზნეს სამართალში, პერსონალურ მონაცემთა დაცვის აუცილებლობა და წინაპირობები. ცალკეულ თემებად გამოყოფილია, საფინანსო სექტორში, პერსონალურ მონაცემთა დამუშავების პრობლემატიკა და ადგილობრივი კანონმდებლობის მაგალითები შედარებულია საერთაშორისო გამოცდილებასთან. ცალკე თავად არის განხილული შრომით სამართალში, დამსაქმებლის მიერ, დასაქმებულის პერსონალური მონაცემების დამუშავების სამართლებრივი წინაპირობები, საერთაშორისო და ადგილობრივი კანონმდებლობის გათვალისწინებით. თითოეული შემთხვევა განხილულია სხვადასხვა პრაქტიკული მაგალითის საფუძველზე.

და ბოლოს, ნაშრომი აანალიზებს, სამეწარმეო სამართალში, პერსონალურ მონაცემთა სუბიექტის კანონიერი უფლებების რღვევისას, ქართული კანონმდებლობით დაწესებულ პასუხისმგებლობის ზომებს და განსაზღვრავს, თუ განსაკუთრებით რომელი ზომა ემსახურება პერსონალური მონაცემების ხელშეუხებლობასა და უკანონო დამუშავებისგან დაცვას ბიზნეს ურთიერთობებისას, აგრეთვე რომელი ზომაა ყველაზე მისაღები მონაცემთა სუბიექტისთვის, რომელია ადეკვატური და სხვა.

ს ა რ ჩ ე ვ ი

შესავალი

ბოლო წლებში, მონაცემთა ავტომატური დამუშავება სულ უფრო ფართომასშტაბიან ხასიათს იძენს, ამ ყველაფერმა ხელი შეუწყო გარკვეული პროცესების ოპტიმიზაციას, მომსახურების გამარტივებას, ბიუროკრატიული საფეხურების შემცირებას. მონაცემთა ბაზების, ელექტრონული ტრანზაქციებისა და თანამედროვე კომუნიკაციის სისტემების განვითარების პარალელურად, გამარტივდა, საჯარო და კერძო ორგანიზაციების მიერ, მონაცემთა დამუშავება და მათზე წვდომის შესაძლებლობა, რამაც, თავის მხრივ, გაზარდა პერსონალური მონაცემების არამართლზომიერი გამოყენების საფრთხე. სტატისტიკის მიხედვით, ყოველდღიურად, მილიონ-ნახევრამდე 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]

საერთაშორისო ექსპერტების მოსაზრებით, მონაცემთა რაოდენობა 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 მსოფლიოში ერთ-ერთი კომპანიის, „IBM“-ის განმარტებით, აჟამად არსებული მონაცემების 90 პროცენტი შექმნილია 2011-2012 წლებში.[3]

საქართველოში, მე-20 საუკუნის ბოლოდან, დაიწყო და ყოველდღიურად იზრდება,კერძო კომპანიებში, ინფორმაციის დამუშავებისას კომპიუტერული ტექნოლოგიების გამოყენების პრაქტიკა. მონაცემების დამუშავება და

[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;

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

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, 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] პერსონალურ მონაცემთა ,,ხელშეუხებლობა არის ინდივიდის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობა“[5].

ნაშრომის მიზანია, მიმოიხილოს პერსონალურ მონაცემთა დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში. აგრეთვე იმ პრობლემებისა და ხარვეზების წარმოჩენა, რომელიც ჯერ კიდევ გააჩნია კანონმდებლობას და პრაქტიკას. შესაბამისად ნაშრომში შემოთავაზებული იქნება კონკრეტული რეკომენდაციები და წინადადებები, რომლებიც ,,პრობლემათა გადაწყვეტის რაციონალური, ლოგიკური, და სამართლებრივი გზისკენ იქნება მიპყობილი“[6].

წარმოდგენილ ნაშრომში კვლევის ობიექტი გამოხატულია შემდეგი საკვლევი ამოცანებით:

- პერსონალური მონაცემების განმარტება და განვითარების ისტორია;
- კერძო სექტორში, ბიზნეს ურთიერთობებში, პერსონალური მონაცემებისა დამუშავებისა და დაცვის ეროვნული სტანდარტები, ამ მხრივ არსებული საერთაშორისო გამოცდილება და შედარებითი ანალიზი;
- საქართველოს კერძო სექტორის სხვადასხვა სფეროში პერსონალური მონაცემების დამუშავებისა და დაცვის მხრივ არსებული პრობლემების ანალიზი/შეფასება;

[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-dayimprove-your-privacy-policy-or-lose-your-data-4796165 [უკანასკნელად გადამოწმებულია 2017 წლის თებერვალში];

[5] საქართველოს საკონსტიტუციო სასამართლოს 2009 წლის 10 ივნისის N1/2/458 განჩინება საქმეზე, ,,საქართველოს მოქალაქეები - დავით სართანია და ალექსანდრე მაჭარაშვილი საქართველოს პარლამენტისა და საქართველოს იუსტიციის სამინისტროს წინააღმდეგ“;

[6] გეგენავა დ., საკონსტიტუციო მართლმსაჯულება საქართველოში: სამართალწარმოების ძირითადი სისტემური პრობლემები, თბილისი, ,,დავით ბატონიშვილის სამართლის ინსტიტუტი“, 2012, გვ. 11;

- საქართველოს კერძო სექტორში, ბიზნეს ურთიერთობებში, პერსონალური მონაცემების დაცვისათვის კონკრეტული რეკომენდაციების შემუშავება;

დასმული ამოცანების გადაწყვეტისას, გამოიყენებოდა სამეცნიერო სფეროში გავრცელებული და კარგად აპრობირებული მეთოდები. ესენია: ისტორიულ-შედარებითი, ლოგიკური, სისტემურ-სტრუქტურული, ფუნქციური, კონტენტ-ანალიზი, სინთეზი, სიტუაციური ანალიზი, დოკუმენტების შესწავლა-შედარება და პროგნოზირება. შედარებით-სამართლებრივი კვლევის მეთოდი იძლევა სხვადასხვა ქვეყნის კანონმდებლობის დადებითი და უარყოფითი მხარეების შედარების საშუალებასა და შეჯერების მეშვეობით ლოგიკურ და თანამიმდევრულ დასკვნამდე იქნეს მსჯელობა წაყვანილი. ანალიტიკური კვლევის მეთოდი, თავისთავად, გულისხმობს პრობლემათა ანალიზს, რაც, კვლავ, მსჯელობის ლოგიკურ თანამიმდევრობას, განსაზღვრავს და იძლევა რაციონალური დასკვნის განხორციელების შესაძლებლობას. ისტორიული კვლევის მეთოდი კი პერსონალურ მონაცემთა დამცავი კანონმდებლობის განვითარების ეტაპებს წარმოაჩენს. რაც შეეხება სოციოლოგიური კვლევის მეთოდს, მისი გამოყენება აუცილებელიცაა, ვინაიდან პერსონალური მონაცემი თავისი არსით სოციუმს უკავშირდება და სოციუმში მყოფ თუთოეულ პიროვნებას გააჩნია ის.

მეწარმე, ბაზარზე ადგილის დამკვიდრებას ცდილობს, რეგულაციების სიმრავლეს, შესაძლოა, დაბრკოლებად აღიქვამდეს. მით უფრო, თუ ჯერ არ აქვს საშუალება, იურიდიულ, ფინანსურ, თუ ტექნიკურ საკითხებში ისარგებლოს შესაბამისი დარგის სპეციალისტების დახმარებით. თუმცა გონივრული კანონმდებლობა და რეგულაციები ყოველთვის ისეთი ღირებულების დასაცავად იქმნება, რომელიც სახელმწიფოსთვისაც მნიშვნელოვანია, მოქალაქისთვისაც და ბიზნესისთვისაც. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შემთხვევაში ეს ღირებულება პირადი ცხოვრების ხელშეუხებლობა და მისი ერთ-ერთი მთავარი კომპონენტი - პერსონალური მონაცემების დაცვაა. საქართველო ერთ-ერთია მსოფლიოს იმ 100-ზე მეტ ქვეყანას შორის, სადაც პერსონალურ მონაცემთა დაცვის კანონმდებლობა მოქმედებს და ის თანაბრად ვრცელდება, როგორც საჯარო, ისე კერძო ორგანიზაციებზე. ბიზნესს ამ კანონმდებლობის მოთხოვნათა დაცვით შექმნილი პროდუქტი შესაძლოა დაეხმაროს რესურსების დაზოგვაში, მომხმარებლების და საკუთარი გუნდის ნდობის მოპოვებაში და შესაძლოა, იქცეს კონკურენტულ უპირატესობადაც. განსაკუთრებით მაშინ, თუ კომპანია საერთაშორისო ბაზარზე გასვლას გეგმავს.

თავი I. პერსონალური მონაცემების არსი და ბიზნეს ურთიერთობებში მისი დამუშავების სამართლებრივი საფუძვლები

1.1. პერსონალურ მონაცემთა დაცვის ტერმინოლოგია და ისტორია

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“.[7]

ამერიკის უზენაესი სასამართლოს მოსამართლე ლუის ბრანდეისი პირადი ცხოვრების ხელშეუხებლობის გარანტირებასა და დაცვას ჯერ კიდევ 1928 წელს აღწერს როგორც ,,ყველაზე აღმატებულ და ღირებულ უფლებად ცივილიზებული ადამიანისთვის“[8], დღეს კი პერსონალურ მონაცემთა ხელშეუხებლობა, თანამედროვე ტექნოლოგიების ეპოქაში, კიდევ უფრო მნიშვნელოვანი და მეტად დაცვის ღირსია.

„მეორე მსოფლიო ომის შემდგომ, ნელ-ნელა დაიწყო რა ინფორმაციული ერა, სულ უფრო რთულდება პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვა“.[9] 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

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

[8] Solove D., Conceptualizing Privacy, ჯ. California Law Review, 2002, Issue 4, გვ. 1093 გადაწყვეტილებიდან: Olmstead V. United States, 277 U.S. 438 (1928), პარ. 478.

[9] 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/wpcontent/uploads/NEWS%20%20PUBLICATIONS/Moerel_oratie.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

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 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.“[10]

პერსონალური მონაცემთა დაცვასთან დაკავშირებით 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.[11] „2016 წლის მონაცემებით კი, „111 ქვეყანას აქვს შემუშავებული პერსონალური მონაცემების დაცვის მარეგულირებელი ეროვნული კანონმდებლობა, საიდანაც 54 ევროპული ქვეყანაა”.[12]

პერსონალურ მონაცემებთან დაკავშირებული საკითხების განხილვამდე, „მართებული იქნება ჩამოვაყალიბოთ, თუ რა არის პერსონალური მონაცემი“.[13] 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.

საქართველოში პერსონალურ მონაცემთა განმარტება და მისი მოცულობის განსაზღვრა სპეციალური კანონის მიღებამდე ხორციელდებოდა ,,საქართველოს

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

[11] Karanja S., Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Netherlands, Martinus Nijhoff Publishers, 2008. გვ. 123;

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

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

ზოგადი ადმინისტრაციული კოდექსის“ მეშვეობით, თუმცა ევროპისაკენ სწრაფვის პოლიტიკამ განაპირობა ცალკე საკანონმდებლო აქტით ამ საკითხის მოწესრიგების აუცილებლობა.

,,საქართველოს ზოგადი ადმინისტრაციული კოდექსის“ 1999 წლის რედაქცია, განმარტავდა პერსონალურ მონაცემს როგორც საჯარო ინფორმაციას, რომელიც პირის იდენტიფიკაციის საშუალებას იძლევა.[14] განმარტებიდან გამომდინარე, პერსონალური მონაცემი ყოველთვის უკავშირდებოდა საჯაროდ ხელმისაწვდომ ინფორმაციას, თუმცა თუკი გავითვალისწინებთ ხსენებული კანონის 44-ე მუხლის პირველი ნაწილის თავდაპირველ რედაქციას, რომლის შესაბამისად პერსონალური მონაცემები, თანამდებობის პირთა პერსონალური მონაცემების გარდა, არავისთვის არ უნდა ყოფილიყო ხელმისაწვდომი, თვით ამ პირის თანხმობის, ან კოდექსის 28-ე მუხლით გათვალისწინებულ შემთხვევებში, სასამართლოს დასაბუთებული გადაწყვეტილების გარეშე[15] პერსონალური მონაცემი კონფიდენციალურ და არა საჯარო სფეროს მიეკუთვნებოდა.

დღესდღეობით, ,,საქართველოს ზოგადი ადმინისტრაციული კოდექსი“ პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ სამართლებრივი ურთიერთობების მოწესრიგების ასპარეზს მთლიანად უთმობს ,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონს.[16]

1.2. პერსონალურ მონაცემთა დამუშავების ფორმები, პრინციპები და საფუძვლები საერთაშორისო და ადგილობრივი კანონმდებლობის მიხედვით

ადამიანის უფლებათა ევროპულ კონვენციას ბევრი მიიჩნევს ადამიანის უფლებათა დაცვის ყველაზე ეფექტიან საერთაშორისო ხელშეკრულებად, რომელმაც დაარსა განვითარებული საერთაშორისო საზედამხედველო მექანიზმი.[17] კონვენციის ასეთი შეფასება განპირობებულია არა იმ უფლებათა და თავისუფლებათა უნიკალურობით, რომლებიც გათვალისწინებულია კონვენციითა და მისი დამატებითი ოქმებით, არამედ მათი უზრუნველყოფის

[14] საქართველოს ზოგადი ადმინისტრაციული კოდექსის 27-ე მუხლის თ) ნაწილი, 25/06/1999 წლის მდგომარეობით;
[15] იქვე. 44-ე მუხლის 1-ლი ნაწილი;
[16] იხ. ზოგადი ადმინისტრაციული კოდექსის 271 მუხლი, 27.10.2015 წლის მდგომარეობით;
[17] A. Robertson & J. Merrills, Human Rights in Europe: A Study of the European Convention on Human Rights, 1993, 1;

საზედამხედველო მექანიზმით.[18] ევროპული კონვენცია პირველი საერთაშორისო ხელშეკრულებაა, რომელმაც გამატკიცა ადამიანის ძირითადი უფლებები და თავისუფლებები და შექმნა მათ შესრულებაზე საზედამხედველო მექანიზმი. სახელმწიფოებს გააჩნიათ საერთაშორისო ვალდებულება, კონვენციასთან შესაბამისობის მხრივ. ამჟამად, ევროპის საბჭოს ყველა წევრ ქვეყანას ინტეგრირებული ან ადაპტირებული აქვს კონვენციის დებულებები შიდასახელმწიფოებრივ კანონმდებლობაში, რომელიც ავალდებულებს მათ იმოქმედონ კონვენციით მოცემული დებულებების შესბაამისად. სწორედ, აღნიშნულის გამოხატულებაა, მსოფლიოს მასშტაბით, და, მათ შორის, საქართველოში, პერსონალური მონაცემების დაცვისათვის შექმნილი სპეციალური კანონი.

პერსონალური მონაცემების დაცვის უფლება წარმოადგენს იმ უფლებათა ნაწილს, რომელიც დაცულია ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლით, რის მიხედვითაც უზრუნველყოფილია პირადი და ოჯახური ცხოვრების, საცხოვრებლისა და მიმოწერის დაცვის უფლება და განსაზღვრულია პირობები, როდესაც დასაშვებია ამ უფლების შეზღუდვა.[19]

პერსონალურ მონაცემთა დამუშავება გულისხმობს ავტომატური, ნახევრად ავტომატური ან არაავტომატური საშუალებების გამოყენებით მონაცემთა მიმართ შესრულებულ ნებისმიერ მოქმედებას, კერძოდ, შეგროვებას, ჩაწერას, ფოტოზე აღბეჭდვას, აუდიოჩაწერას, ვიდეოჩაწერას, ორგანიზებას, შენახვას, შეცვლას, აღდგენას, გამოთხოვას, გამოყენებასა ან გამჟღავნებას მონაცემთა გადაცემის, გავრცელების ან სხვაგვარად ხელმისაწვდომად გახდომის გზით, დაჯგუფებას ან კომბინაციას, დაბლოკვას, წაშლასა ან განადგურებას[20].

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მე-2 თავი არეგულირებს მონაცემთა დამუშავების ზოგად წესებს. ხოლო ზოგიერთი მონაცემის სპეციფიური ბუნების გამო, კანონმდებელმა გადაწყვიტა ცალკე მუხლებად ჩამოეყალიბებინა მათი დამუშავების ნორმები, თუმცა რატომღაც მათ შორის არ გაითვალისწინა გენეტიკური მონაცემთა დამუშავების მოწესრიგება მიუხედავად თავისი მნიშვნელობისა.

---

[18] K. Vasak, The Council of Europe, in: The International Dimension of Human Rights, K. Vasak, (Ed.) vol.2, 1982, 673;

[19] ევროპის საბჭო, ადამიანის უ
ფლებათა ევროპული კონვენცია CETS No. 005, 1950 წელი;

[20] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 პუნქტის გ) ქვეპუნქტი;

,,პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი მონაცემთა ავტომატური დამუშავებას განმარტავს მონაცემთა ინფორმაციული ტექნოლოგიების მეშვეობით დამუშავებად[21]. კანონი არ აიდენტიფიცირებს, მონაცემთა ინფორმციული ტექნოლოგიების მეშვეობით დამუშავებას, თუმცა ჩამოთვლის გავრცელების სფეროებს, კერძოდ ესენია: დანაშაულის თავიდან აცილება და გამოძიება, ოპერატიულ-სამძებრო ღონისძიებებისა და მართლწესრიგის დაცვის მიზნებისათვის სახელმწიფო საიდუმლოებისათვის მიკუთვნებულ მონაცემთა ავტომატური დამუშავება[22].

მონაცემთა ავტომატური დამუშავება პრაქტიკულად ხორციელდება კომპიუტერებით ან კავშირგაბმულობის სხვა ქსელებით. შვედეთის მონაცემთა ინსპექციის საბჭოს მოსაზრებით ციფრული ფოტოაპარატით გადაღებული სურათების ვებ-საიტებზე განთავსება მათი შენახვის გარეშე, აგრეთვე მონაცემთა ავტომატური საშუალებით დამუშავებაა[23]. საქართველოში მონაცემთა ავტომატური დამუშავების პრობლემას წარმოადგენს სამართლებრივი საფუძვლის გარეშე უწყებებს შორის მონაცემთა გაცვლა ან/და წვდომა. აღნიშნული პრობლემა პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატისთვის დაფუძნების დღიდან გადაუჭრელია[24] და მასში მეტწილად ისეთი საჯარო უწყებები არიან ბრალდებულნი, როგორიცაა სახელმწიფო სერვისების განვითარების სააგენტო, შინაგან საქმეთა სამინისტრო და სხვანი.

თანამედროვე ტექნოლოგიების განვითარებასთან ერთად, იშვიათ მოვლენას წარმოადგენს პერსონალურ მონაცემთა დამუშავება არაავტომატური საშუალებებით, თუმცა ვინაიდან აღნიშნული მეთოდი რეალურად არსებობს, კანონმდებელმა ის მაინც დაარეგულირა, რათა მონაცემთა არაავტომატური საშუალებებით დამუშავება არ გამხდარიყო კანონის მოთხოვნების გვერდის ავლის საშუალება[25].

---

[21] იქვე, მე-2 მუხლის ე) პუნქტი;

[22] იქვე. მე-3 მუხლის 1-ლი პუნქტი;

[23] Decision by the Data Inspection Board from 20 sep. 2005. No 763-2005, წიგნიდან: Kirchberger K., Cyber Law in Sweden, By Christine, USA, Kluwer Law International, 2011,197;

[24] იხ. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“, გვ. 7, აგრეთვე პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში“ გვ. 14 და პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ", გვ. 70-71;

[25],,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის 11 პუნქტი;

არაავტომატური საშუალებებით მონაცემთა დამუშავება ხელით წერის მეშვეობით ,,ხელნაწერი ფაილების" შექმნას გულისხმობს და ხშირად გამოიყენება საავადმყოფოებში[26]. ზემოაღნიშნული მონაცემების დამუშავება უნდა მოხდეს მოქმედი კანონმდებლობით გათვალისწინებული წესით. ამასთან, „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი განსაკუთრებული კატეგორიის მონაცემთა დამუშავების საფუძვლად ითვალისწინებს ჯანმრთელობის დაცვის სისტემის მართვის ან ფუნქციონირების, საზოგადოებრივი ჯანმრთელობისა და ფიზიკური პირის ჯანმრთელობის დაცვის მიზნებს; თუმცა, ამავდროულად, მნიშვნელოვნად მიიჩნევს მონაცემთა დამუშავების ნებისმიერ ეტაპზე მონაცემთა კანონიერებასთან, ადეკვატურობასთან, პროპორციულობასთან, მოცულობასთან, შენახვის ვადებთან, ნამდვილობასა და სიზუსტესთან დაკავშირებული პრინციპების და მონაცემთა უსაფრთხოების დაცვას.

იმისათვის, რომ არაავტომატური საშუალებებით პერსონალურ მონაცემთა დამუშავება კონტროლს დაექვემდებაროს, აუცილებელია კანონმდებელმა გაითვალისწინოს, დაწესებულების მხრიდან მაკონტროლებელი ორგანოსთვის შეტყობინების ვალდებულება, იმის თაობაზე, რომ აწარმოებს მონაცემთა არაავტომატურ დამუშავებას, შემდგომ კი პერიოდულად უნდა ხდებოდეს აღნიშნულის განმახორციელებელი ორგანიზაციების ინსპექტირება.

შემაჯამებელი სახით შეიძლება ითქვას, რომ კონსტიტუციით გათვალისწინებული ლეგიტიმური მიზნების დაცვის რეალური საჭიროების დემონსტრირების შემდგომ, ასევე აუცილებელია, მონაცემთა დამმუშავებელმა ამ მიზნების მისაღწევად უფლებაში ჩარევის თანაზომიერი გზა აირჩიოს. ამისთვის კი, კანონმდებლის მიერ, შერჩეული რეგულაცია უნდა იყოს დასაშვები, აუცილებელი და პროპორციული. „ვინაიდან, ნებისმიერი სამართლებრივი წესრიგი მიზნისა და საშუალების მიმართზებაზეა აგებული, ეს ავალდებულებს სახელმწიფოს, მიზნის მისაღწევად გამოიყენოს ისეთი საშუალება, რომლითაც, როგორც მიზნის მიღწევა იქნება გარანტირებული, ასევე თანაზომიერების პრინციპი იქნება დაცული"[27].

[26] Büllesbach A., Concise European IT Law, USA, Kluwer Law International, 2010, გვ. 94;

[27] საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 19 დეკემბრის გადაწყვეტილება №1/2/411 საქმეზე შპს „რუსენერგოსერვისი", შპს „პატარა კახი", სს „გორგოტა", გივი აბალაკის ინდივიდუალური საწარმო „ფერმერი" და შპს „ენერგია" საქართველოს პარლამენტისა და ენერგეტიკის სამინისტროს წინააღმდეგ;

1.3. პერსონალურ მონაცემთა სუბიექტები

პერსონალურ მონაცემთა სუბიექტი არის ნებისმიერი ფიზიკური პირი, რომლის შესახებ მონაცემები მუშავდება[28]. აღსანიშნავია, რომ აღნიშნული ჩანაწერი აწესრიგებს მხოლოდ ფიზიკური პირების პერსონალური მონაცემების დაცვას, ხოლო იურიდიული პირების მსგავს ინფორმაციას კანონმდებელი პერსონალურ მონაცემებად არ მიიჩნევს[29]. კანონის ჩანაწერის მხოლოდ ფიზიკურ პირზე გავრცელების ტენდენცია განაპირობა ,,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ ევროპული კონვენციის“ რეგულირების სფერომ, რომელიც ეხება მხოლოდ პიროვნების უფლებათა და ძირითად თავისუფლებათა დაცვის გარანტიების გავრცელებას, განსაკუთრებით თითოეული ადამიანის უფლებას კონფიდენციალურობის დაცვის შესახებ[30].

მონაცემთა სუბიექტს, უფლება აქვს მოითხოვოს დამმუშავებლისგან ინფორმაციის მიწოდება მონაცემთა დამუშავების მიზნების, ობიექტის, შეგროვების გზების, სამართლებრივი საფუძვლების, კონკრეტულ პირზე ან ორგანიზაციაზე გაცემული ინფორმაციის და სხვათა თაობაზე[31], ხოლო საჭიროების შემთხვევაში მის შესახებ არსებულ მონაცემთა გასწორების, განახლების, დამატების ან სხვა ოპერაციის მოთხოვნის უფლებაც აქვს[32].

კანონით დადგენილ შემთხვევებში, როდესაც მონაცემთა დამუშავება მოითხოვს მონაცემთა სუბიექტის თანხმობას, სუბიექტს უფლება აქვს გასცეს ის, ან გაცემულ თანხმობაზე უარი განაცხადოს[33]. მსგავს შემთხვევაში მონაცემთა სუბიექტი არამარტო მიღებულ გადაწყვეტილებაზე იღებს პასუხისმგებლობას, არამედ მის შედეგებზეც[34]. შესაბამისად მნიშვნელოვანია, რომ აღნიშნული პირი სრულად აცნობიერებდეს გადაწყვეტილების მართებულობას, სპეციალური

[28]„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის ვ) პუნქტი;

[29] ბეჟაშვილი ზ., პერსონლურ მონაცემთა დამუშავებისა და საჯაროობის სამართლებრივი მოწესრიგება საავტორო სამართლებრივ დაცვასთან მიმართებით, ჟ. ,,ადმინისტრაციული სამართლის პრობლემები“, 2013, გვ. 40;

[30],,პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენცია, CETS No.108, (მიღებულია 1981 წლის 28 იანვარს, ძალაში შევიდა 1985 წლის 1 ოქტომბერს), პრეამბულა;

[31],,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 21-ე მუხლი;

[32] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 22-ე მუხლი;

[33] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 25-ე მუხლი;

[34] ПЕТРОВ М.И., Постатейный комментарий к Федеральному закону О персональных данных, Россия, Юстицинформ, 2007, გვ. 28;

კანონი კი არ ითვალისწინებს მონაცემთა სუბიექტის ასაკს, ქმედუნარიანობას და სხვა კრიტერიუმებს თანხმობის ან თანხმობაზე უარის თქმისას, შესაბამისად საჭიროა კანონში გაკეთდეს მითითება, თუ რა შემთხვევაში ჩაითვლება მონაცემთა სუბიექტის მიერ გამოხატული ნება ნამდვილად და რეალურად.

1.4. კერძო სექტორი, როგორც პერსონალურ მონაცემთა ერთ-ერთი ძირითადი დამმუშავებელი

პრაქტიკულად არ არსებობს ბიზნესი, რომელიც არ ამუშავებს პერსონალურ მონაცემებს. 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“[35], ხოლო მეორე მხრივ, მონაცემთა დამუშავების პროცესში მონაცემთა დამმუშავებელი/უფლებამოსილი პირის მიერ კანონით განსაზღვრული ვალდებულებების შესრულება. ვინაიდან, იქ, სადაც „მოქალაქე დაუცველია, სახელმწიფო ვერ იტყვის, რომ დემოკრატიული სისტემა შექმნა“[36]. რასაც უნდა აწარმოებდეს, ყიდდეს თუ ქმნიდეს კომპანია, საქმიანობის პროცესში, იგი აგროვებს, ინახავს და იყენებს ინფორმაციას მომხმარებლების, თანამშრომლებისა და პარტნიორების შესახებ. ეს ამ კომპანიებს მონაცემთა დამმუშავებლის სტატუსსა და, შესაბამისად, გარკვეულ პასუხისმგებლობებს აკისრებს - როგორც კანონის, ისე ყველა იმ ადამიანის წინაშე, რომლის მონაცემებიც მუშავდება მათ მიერ.

ძნელად წარმოსადგენია თანამედროვე ბიზნესი, რომელიც მომხმარებლის გემოვნებაზე ორიენტირებული პროდუქტის შექმნას არ ცდილობდეს. თუმცა, შესაძლოა, გაუჩნდეთ ცდუნება, განსაკუთრებით დიდი მოცულობით ინფორმაცია შეაგროვონ მომხმარებლების შესახებ, ან ახალი მომსახურების, თუ პროდუქტის შექმნისას წინასწარ არ გაითვალისწინონ კანონმდებლობის მოთხოვნები. ასეთ შემთხვევაში, მათთვის, წინასწარი თანხმობის არსებობის შემთხვევაშიც კი, პირს უფლება აქვს მოსთხოვოს მისი ფოტოს, ვიდეო ან აუდიო

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

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

მასალის წაშლა, სახის დაფარვა და ა.შ. კომპანიები ვალდებულნი არიან, ეს მოთხოვნა უნდა შეასრულონ. კომპანიას შესაძლოა დაეკისროს ჯარიმა, მიადგეს რეპუტაციული ზიანი, ან მოუწიოს დამატებითი ხარჯების გაღება დაშვებული შეცდომის გამოსასწორებლად.

კერძო 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“[37].

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 პოლიტიკა და ასაჯაროებენ თუ არა ინფორმაციას მთავრობის მხრიდან ინფორმაციის წაშლის მოთხოვნებთან დაკავშირებით. Apple-ი აღმოჩნდა იმ მცირერიცხოვან კომპანიებს შორის, რომლებმაც სრული ხუთი ვარსკვლავი

[37]„პერსონალური მონაცემების დამუშავებისა და დაცვის სახელმძღვანელო“, პერსონალურ მოანცემთა დაცვის ინსპექტორის აპარატი, 2013 წელი, გვ.43;

მიიღეს. ხუთი ვარსკვლავი მიიღეს ისეთმა კომპანიებმა, როგორებიც არიან Wordpress-ი, Dropbox-ი, Yahoo, CREDO, Sonic-ი, Wickr-ი და Wikimedia.[38]

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.

თავი II. პერსონალური მონაცემი და პირდაპირი მარკეტინგი

2.1. პირდაპირი მარკეტინგის ცნება და მისი გამოყენების ფარგლები

სიტყვა მარკეტინგი, საბაზრო საქამინაობას ნიშნავს და, ბუნებრივია, რომ ადამიანებმა მარკეტინგული საქმიანობა ბიზნესის გაჩენასთან ერთად დაიწყეს. ადამიანები ქმნიდნენ პროდუქტს, ადებდნენ ფასს, ირჩევდნენ გასაყიდ ადგილს და ცდილობდნენ მომხმარებლების ყურადღების მიპყრობას. იმისათვის, რომ ბიზნესის წინ მდგომი ამოცანები წარმატებით გადაიჭრას მენეჯმენტის, მარკეტინგის, აღრიცხვისა და ფინანსების გამოყენებით, აუცილებელია, შესაბამისი ინფორმაციის ფლობა.

ჯუდიტ დონოვანის (2000) განმარტებით პირდაპირი მარკეტინგი არის ,,მეცნიერება, რომელსაც შეუძლია ადამიანის გონების გამოჭერა, ფულის საკეთებლად“[39]. დღესდღეობით, ტერმინი ,,პირდაპირი მარკეტინგი“ აღარ არის მოდური, მის ნაცვლად გამოიყენება ტერმინი ,,კლიენტებთან ურთიერთობის მარკეტინგი“. პირდაპირი მარკეტინგი (DM) სამიზნე აუდიტორიასთან უშუალო კონტაქტის ყველაზე ეფექტიანი საშუალებაა. DM ერთერთი ყველაზე იაფი საკომუნიკაციო არხია თუმცა მას ფართო გამოყენება გააჩნია, როგორც მცირე ასევე საშუალო და დიდ კომპანიებში, რადგან ეს ის ინსტრუმენტია რომლის მეშვეობითაც ინფორმაციას ვაწვდით სწორედ იმ ადამიანს ვინც ჩვენი პოტენციური მომხმარებელია, სწორედ მაშინ როცა ყველაზე სასურველი მომენტია, იმ ფორმით რაც ყველაზე მიმზიდველია. მიუხედავად იმისა, რომ

[38] 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-ratedcompanies-in-privacy-study, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];

[39] Mullin R., Direct Marketing: A Step-by-step Guide to Effective Planning and Targeting, Great Britain, Kogan Page, 2002, გვ. 1;

ტერმინოლოგია იცვლება თითქმის ყოველ დღე, მისი მნიშვნელობა სულაც არ შეცვლილა[40].

კომპანიებში გროვდება დიდი რაოდენობით ინფორმაცია ბაზარსა თუ მომხმარებლებზე. ბიზნესის მიერ, განხორციელებული თითოეული გარიგება გარკვეული ინფორმაციის მატარებელია. კომპანიისა და მომხმარებლების ურთიერთობისას თანამშრომლები (გამყიდველები, კონსულტანტები და ა. შ.) ძალიან ბევრ რამეს იგებენ მიზნობრივი ჯგუფების, მათი დამოკიდებულებებისა და პრეფერენციების შესახებ. თანამედროვე მონაცემთა ბაზები ფირმებს ეხმარება, სასურველი ინფორმაციის ორგანიზებული სახით დალაგებასა და მარტივად მოძიებაში.

მომხმარებელთა ელექტრონულ მონაცემთა ბაზების გამოყენების ერთ-ერთი წარმატებული მაგალითი „მერიოტი“-ს სასტუმროების ქსელში გვხვდება. „მერიოტს“ აქვს გლობალური მონაცემთა ბაზა, სადაც აისახება ებისმიერი ტრანსაქვია თითოეულ სტუმართან (მაგალითად, როგორ ოთახს ირჩევს ხოლმე, რა დამატებით მომსახურეობებს უკვეთავს, რა საკვებსა თუ სასმელს მიირთმევს და ა. შ.). მსოფლიოს რომელ კუთხეშც არ უნდა იყოს „მერიოტი“, ეს ინფორმაცია მისი პერსონალისთვის ხელმისაწვდომი იქნება. აღნიშნულით ნათელია, თუ როგორ იყენებენ კომპანიები პირთა პერსონალურ ინფორმაციას, პირდაპირი მარკეტინგის მიზნით.

,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შესაბამისად პირდაპირი მარკეტინგი არის ფოსტის, სატელეფონო ზარების, ელექტრონული ფოსტის ან სხვა სატელეკომუნიკაციო საშუალებით საქონლის, მომსახურების, დასაქმების ან დროებითი სამუშაოს შეთავაზება[41]. მისი მიზნები, მხოლოდ მითითებული შეთავაზებებით არ ამოიწურება, არამედ შესაძლებელია გამოყენებულ იქნეს იმისათვის, რომ ამომრჩეველზე ზეგავლენა მოახდინოს არჩევნების წინარე პერიოდში. ჯერ კიდევ ეიზენჰაუერის საპრეზდნეტო კამპანიის დროს, პირდაპირი ფოსტა გამოიყენებოდა მასშტაბურად და 1992 წლის ამერიკის არჩევნებში პირდაპირი მარკეტინგის განმახორციელებელი აქტივიტსტები მრავლად იყვნენ ჩართულები. აღნიშნული პრაქტიკა იმდენად

[40] Housden M., Thomas B., Direct Marketing in Practice, London and NY, Routledge, Taylor and Francis Group, 2002, გვ. 3;

[41] ,, პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-2 მუხლის უ) პუნქტი;

წარმატებით გამოიყენა სამმა საპრეზიდენტო კანდიდატმაც: ბუშმა, კლინტონმა და პეროტმა[42].

პირდაპირი მარკეტინგის განმახორციელებელი არის საჯარო დაწესებულება, ფიზიკური ან იურიდიული პირი, რომელიც განსაზღვრავს პირდაპირი მარკეტინგის მიზნებისთვის მონაცემთა დამუშავების საშუალებებს, უშუალოდ ან უფლებამოსილი პირის მეშვეობით[43]. პირდაპირი მარკეტინგის წარმატება დამოკიდებულია ინფორმაციის შეგროვებასა და გამოყენებაზე[44]. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი უშვებს იმ მონაცემთა დამუშავებას, რომლებიც საჯაროდ ხელმისაწვდომი წყაროებიდან არის მოპოვებული[45] ან თავად მომხმარებლისგან იქნა მიწოდებული.[46] კერძოდ, ესეთი მონაცემი შეიძლება იყოს: ,,სახელი (სახელები), მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი, ფაქსის ნომერი[47]. პირდაპირი მარკეტინგი მიმართულია ფიზიკურ პირებზე, რომლებიც მათი პერსონალური მონაცემების დამუშავების შემდეგ იღებენ მომსახურებას ან საქონლის შეთავაზებას. ამ მიზნებისთვის მონაცემები შეიძლება შეგროვდეს უშუალოდ მომხმარებლისგან ან საჯაროდ ხელმისაწვდომი წყაროებიდან. ამ უკანასკნელისგან შეიძლება შეგროვდეს მხოლოდ შემდეგი მონაცემები: სახელი, გვარი, მისამართი, ტელეფონის ნომერი, ელექტრონული ფოსტის მისამართი და ფაქსის ნომერი[48]. პირის შესახებ ინფორმაცია საჯაროა თუ სუბიექტი უშუალოდ თვითონ ასაჯაროებს ინფორმაციას, მისი თანხმობით გახდა საჯარო ან იმ შემთხვევაში, როდესაც ცალკეული მონაცემების საჯაროობა განსაზღვრულია კანონით.

თუმცა, კანონის მოთხოვნათა დარღვევით განსაჯაროებული პერსონალური მონაცემების გამოყენება პირდაპირი მარკეტინგის მიზნებისათვის დაუშვებელია[49]. მონაცემთა დამმუშავებელი, რომლის მთავარი მიზანი პირდაპირი მარკეტინგის განსახორციელებლად საჭირო მონაცემების მოპოვებაა,

---

[42] Bird B., Commonsense Direct and Digital Marketing, London and Philadelphia, Kogan Page, 2007, 5th edition, გვ. 8;

[43] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების შესახებ, გვ. 1;

[44] Housden M., Thomas B., Direct Marketing in Practice, London and NY, Routledge, Taylor and Francis Group, 2002, გვ. 57;

[45] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-8 მუხლის 1-ლი პუნქტი;

[46] იქვე, მე-8 მუხლის მე-3 პუნქტი;

[47] იქვე, მე-8 მუხლის მე-2 პუნქტი;

[48] იქვე, მე-8 მუხლის მე-2 პუნქტი;

[49] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების შესახებ, გვ. 3;

არ არის ვალდებული იკვლიოს საჯაროდ ხელმისაწვდომი მონაცემთა ბაზების კანონიერება, მაგრამ, თუკი მისთვის აღნიშნული ცნობილი გახდა, კანონი უნდა ავალდებულებდეს შესაბამისი სტრუქტურებისათვის დარღვევის შეტყობინების სავალდებულოობას.

პირდაპირი მარკეტინგის მიზნებისათვის პესონალური მონაცემების შეგროვება ხშირად ხორციელდება უშუალოდ სუბიექტისაგან (მომხმარებლისგან). მაგალითად, მაღაზიაში ნივთის შეძენისას პირმა დატოვა საკონტაქტო მონაცემები და სურს, მიიღოს შეტყობინება ახალი პროდუქციის შესახებ[50]. ხშირია შემთხვევები, როდესაც მონაცემთა სუბიექტი მხოლოდ ერთ კონკრეტულ ორგანიზაციას ან პიროვნებას აწვდის საკუთარ პერსონალურ მონაცემებს დასამუშავებლად, თუმცა აღმოჩნდება, რომ სხვა კონტრატორი ორგანიზაციებისთვის და ფიზიკური პირებისთვისაც არის ის ხელმისაწვდომი.

2.2. პირდაპირ მარკეტინგზე უარის თქმის სამართლებრივი მექანიზმი როგორც პერსონალური მონაცემების სუბიექტის უფლებათა დაცვის კანონიერი საფუძველი

მონაცემთა სუბიექტს აქვს უფლება, რომ ,,მონაცემთა დამმუშავებელს, ნებისმიერ დროს, მოსთხოვოს მის შესახებ მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის გამოყენების შეწყვეტა[51]. ხოლო, მონაცემთა დამმუშავებელი ვალდებულია, პირდაპირი მარკეტინგის მიზნებისთვის, მონაცემთა დამუშავება შეწყვიტოს, სუბიექტისაგან მოთხოვნის მიღებიდან, არაუგვიანეს 10 სამუშაო დღისა[52]. ასეთ შემთხვევაში, სუბიექტის მონაცემები გადაიგზავნება იმ პირთა სიაში, რომლებსაც აღარ უნდა მიუვიდეთ სარეკლამო შეტყობინება. მსგავსი თვითკონტროლი კარგია, როგორც სუბიექტებისათვის, რომლებსაც უნდათ რომ აღარ მიიღონ შეტყობინებები, აგრეთვე ორგანიზაციებისთვის, რომ მათ ფული აღარ დახარჯონ არარეაგირებადი ადრესატებისთვის შეტყობინების გაგზავნაზე[53].

---

[50] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების შესახებ, გვ. 3;

[51] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-8 მუხლის მე-4 პუნქტი.

[52] იქვე, მე-8 მუხლის მე-5 პუნქტი;

[53] Rich P., Hines D., Membership Development: An Action Plan for Results, USA, Jones and Bartlett Publishers, 2006, გვ. 116;

კანონმდებლობით, ასევე, დადგენილია იმ ფიზიკური პირების (პირდაპირი მარკეტინგის სუბიექტები) უფლებები, რომელთა მონაცემები მუშავდება პირდაპირი მარკეტინგის მიზნით. კერძოდ,

- იცოდეს, მონაცემთა შეგროვების წყარო, მარკეტინგის განმახორციელებლის ვინაობა, მონაცემთა დამუშავების მიზანი და კანონიერი საფუძველი;
- იცოდეს, რა მონაცემები მუშავდება მის შესახებ და, ნებისმიერ დროს, მოითხოვოს მათი გასწორება, განახლება, დამატება, დაბლოკვა, წაშლა ან განადგურება;
- მოითხოვოს მისი მონაცემების, პირდაპირი მარკეტინგის მიზნებისთვის, გამოყენების შეწყვეტა, ნებისმიერ დროს, (მიუხედავად იმისა, აქვს თუ არა თანხმობა გაცემული) იმავე ფორმით, რა ფორმითაც ხორციელება მარკეტინგი ან გამოიყენოს სხვა ხელმისაწვდომი და ადეკვატური საშუალება;
- უარი განაცხადოს მისი მონაცემების მესამე პირთათვის გადაცემაზე;

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[54]. შესაბამისად, თუ, პირდაპირი მარკეტინგის სუბიექტი მიიჩნევს, რომ მის პერსონალურ მონაცემებს ამუშავებენ უკანონოდ, შეუძლია, მიმართოს პერსონალური მონაცემების დაცვის ინსპექტორს ან სასამართლოს.

სახელმწიფო ინსპექტორის სამსახურის (სახელმწიფო ინსპექტორის სამსახური დამოუკიდებელი სახელმწიფო ორგანოა, რომელიც როგორც პერსონალურ მონაცემთა დაცვის ინსპექტორის უფლებამონაცვლე, საქართველოში 2019 წლის 10 მაისიდან ამოქმედდა.) ერთ-ერთი ძირითადი ფუნქცია, სწორედ, პერსონალურ მონაცემთა დაცვის მარეგულირებელი

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

კანონმდებლობის შესრულებაზე ზედამხედველობა და მონაცემთა დამუშავების კანონიერებაზე კონტროლია.

პერსონალურ მონაცემთა დაცვის კანონმდებლობის სიახლიდან გამომდინარე, საკონსტიტუციო სასამართლოს უმნიშვნელოვანესი როლი გააჩნია ამ უფლების დაცვის მიმართულებით, ვინაიდან მისი მიდგომით კონსტიტუციასთან შესაბამისობის კუთხით მოწმდება არამხოლოდ ნორმა, არამედ ნორმის გამოყენების პრაქტიკაც[55]. საქართველოში პერსონალურ მონაცემთა დამცავი ნორმები მიმოფანტულია სხვადასხვა საკანონმდებლო აქტში, რომელთა გასაჩივრების შემდგომ საკონსტიტუციო სასამართლომ გადაწყვეტილებებსა თუ განჩინებებში, საკმაოდ მრავალფეროვანი პრაქტიკა ჩამოაყალიბა.

ბოლოდროინდელი გადაწყვეტილებებიდან აღსანიშნავია 2016 წლის 14 აპრილის გადაწყვეტილება, რომლის შესაბამისად დავის საგანს წარმოადგენდა ,,ელექტრონული კომუნიკაციის შესახებ“ კანონის ნორმები, რომლებიც სახელმწიფო უსაფრთხოების სამსახურს ანიჭებდა უფლებამოსილებას, ჰქონოდა კავშირგაბმულობის და კომუნიკაციის ფიზიკური ხაზებიდან ინფორმაციის რეალურ დროში მოპოვების და ამ მიზნით სათანადო აპარატურის და პროგრამული უზრუნველყოფის საშუალებების განთავსების შესაძლებლობა. ასევე სამსახური აღჭურვილი იყო უფლებამოსილებით, განეხორციელებინა კავშირგაბმულობის არხში არსებული მაიდენტიფიცირებელი მონაცემების კოპირება და მათი 2 წლის ვადით შენახვა. სასამართლომ აღნიშნული ნორმები მიიჩნია არაკონსტიტუციურად და ცნო ისინი არაპროპრციუად და ზედმეტად შემზღუდველ ნორმებად. აგრეთვე ინფორმაციის შენახვა 2 წლის ვადით ჩათვალა არაგონივრულად ხანგრძლივ პერიოდად[56].

საკონსტიტუციო სასამართლოს პრაქტიკაში საკმაოდ მნიშვნელოვანია 2008 წლის 30 ოქტომბრის გადაწყვეტილება, რომელიც შეეხებოდა საქართველოს საგადასახადო კოდექსიდან გამომდინარე საგადასახადო საიდუმლოებასთან დაკავშირებულ რეგულაციებს. მოსარჩელე მხარის განმარტებით საგადასახადო

[55] ზოიძე ბ., საკონსტიტუციო კონტროლი და ღირებულებათა წესრიგი საქართველოში, თბილისი, (GTZ), 2007, გვ. 63;

[56] საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება საქმეზე ,,საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები - გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა - საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“,საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ";

საიდუმლოების მარეგულირებელი ნორმები შეუსაბამო იყო საქართველოს კონსტიტუციის 41-ე მუხლის პირველ პუნქტთან. საკონსტიტუციო სასამართლომ აღნიშნულ გადაწყვეტილებასთან მიმართებით განაცხადა, რომ საგადასახადო საიდუმლოებას მიკუთვნებული ინფორმაცია არის იმ მონაცემების ერთობლიობა, რაც გადასახადის გადამხდელის იდენტიფიცირების საშუალებას წარმოადგენს, მათ შორის იგულისხმება მის ფინანსებთან დაკავშირებული ინფორმაციაც, რაც დაცულია საქართველოს კონსტიტუციის 41-ე მუხლის მე-2 პუნქტით. სასამართლომ განმარტა, რომ მსგავსი ინფორმაციის გასაიდუმლოება ნორმატიულად დამკვიდრებულ წესს წარმოადგენდა ისეთ ქვეყნებშიც, როგორიცაა აშშ, გერმანიის ფედერაციული რესპუბლიკა, შვეიცარია და სხვა. საკონსტიტუციო სასამართლომ ყურადღება გაამახვილა გადასახადების გადახდის სახელმწიფოსათვის სასიცოცხლო მნიშვნელობაზე და გადასახადის გადამხდელსა და სახელმწიფოს შორის ურთიერთნდობის ფაქტორზე მსჯელობისას აღნიშნა, რომ საგადასახადო ორგანოსთვის მიწოდებული ინფორმაცია არ უნდა იქნეს გამოყენებული არაპროგნოზირებადი, არასაგადასახადო მიზნებისთვის, რათა საფრთხის ქვეშ არ დადგეს გადასახადის გადამხდელის მხრიდან მისი მოვალეობების შესრულების ხარისხი, რაც ესოდენ მნიშნველოვანია სახელმწიფოს არსებობისთვის. საგადასახადო კოდექსის აღნიშნული ნორმები ქმედითად შენარჩუნდა[57].

თავი III. პერსონალური მონაცემების დამუშავება საფინანსო სექტორის მიერ

3.1. ხელშეკრულებით გათვალისწინებული თანხმობა, როგორც პერსონალურ მონაცემთა დამუშავების ძირითადი საფუძველი

კანონი უთითებს პერსონალურ მონაცემთა დამუშავების რვა საფუძველს[58]. მითითებული საფუძვლებიდან, მხოლოდ რამდენიმე შეიძლება იყოს რელევანტური საფინანსო საქმიანობისათვის. ესენია:

- მონაცემთა სუბიექტის თანხმობა;

[57] იხ. საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406,408 გადაწყვეტილება საქმეზე, ,,საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“;

[58] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-5 მუხლი;

- მონაცემთა დამუშავების კანონით გათვალისწინებული შემთხვევა;
- მონაცემთა დამუშავება კანონმდებლობით დაკისრებული ვალდებულების შესასრულებლად;
- მონაცემთა დამუშავება მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად;
- მონაცემთა სუბიექტის განცხადების განხილვა და მისთვის მომსახურების გაწევა.

თანხმობა ნიშნავს „მონაცემთა სუბიექტის სურვილების თაობაზე, ნებისმიერ ნებაყოფლობით კონკრეტულ და ინფორმირებულ გამოხატულებას[59].“ რიგი პროცესებისას, იგი არის მონაცემთა კანონიერი დამუშავების სამართლებრივი საფუძველი. ნებაყოფლობით თანხმობას კანონიერი ძალა გააჩნია მხოლოდ მაშინ, თუ მონაცემთა სუბიექტს აქვს შესაძლებლობა თავად განახორციელოს არჩევანი და არ არსებობს შეცდომაშ შეყვანის, დაშინების, იძულებისა ან აშკარა ნეგატიური შედეგის დადგომის შესაძლებლობა იმ შემთხვევაში, თუ იგი არ განაცხადებს თანხმობას[60].

ინფორმირებული თანხმობის შემთხვევაში, მონაცემთა სუბიექტს უნდა ჰქონდეს საკმარისი ინფორმაცია გადაწყვეტილების მიღებამდე. არის, თუ არა მიწოდებული ინფორმაცია საკმარისი, შსაძლებელია, განისაზღვროს ყოველ კონკრეტულ შემთხვევაში. ძირითადად, ინფორმირებული თანხმობა მოიცავს საკითხის ზუსტად და ადვილად გასაგებ აღწერას, რაზეც მოიპოვება თანხმობა და, ამასთან, ნათელს ხდის თანხმობის გაცემის ან არ გაცემის შედეგებს. ინფორმირებისთვის გამოყენებული ენა უნდა იყოს ადაპტირებული ინფორმაციის შესაძლო ადრესატებისთვის. ინფორმაცია, ასევე, უნდა იყოს ადვილად ხელმისაწვდომი მონაცემთა სუბიექტისთვის. ინფორმაციის ხელმისაწვდომობა და გამჭვირვალობა არის მნიშვნელოვანი ელემენტი. ინტერნეტ-სივრცეში, ინფორმირების თანმიმდევრული შეტყობინებები შესაძლოა სწორი მიდგომა აღმოჩნდეს, რამდენადაც, ინფორმაციის არსებულ ვერსიასთან ერთად, მონაცემთა სუბიექტისთვის ხელმისაწვდომი იქნება მეტად განვრცობილი ვარიანტიც.

კანონიერი ძალის არსებობისთვის, თანხმობა, ასევე უნდა იყოს კონკრეტული. ეს აუცილებელი პირობაა, თანხმობის საგნის შესახებ მიწოდებული

[59] მონაცემთა დაცვის დირექტივა, მე-2 მუხლის „ჰ“ ქვეპუნქტი;
[60] იხ. ასევე, მუხლი 29, სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის ცნების შესახებ, WP 187, ბრიუსელი,13 ივლისი 2011 წელი, გვ. 12. 100 იქვე, გვ. 15;

ინფორმაციის ხარისხთან ერთობლიობაში. ამ კონტექსტში, მონაცემთა სუბიექტის გონივრული მოლოდინი რელევანტური იქნება. მონაცემთა სუბიექტს, შესაძლოა, ხელმეორედ ეთხოვოს თანხმობის გაცემა, თუ დამუშავების ოპერაციები უნდა იქნეს დამატებული ან შეცვლილი იმგვარად, რომ ამის განჭვრეტა, გონივრულობის ფარგლებში, შეუძლებელი იყო, თავდაპირველი თანხმობის გაცემის დროს. აღნიშნულთან დაკავშირებით, გასათვალისწინებელია შემდეგი საქმე: საქმეზე Deutsche Telekom AG[61], მართლმსაჯულების ევროპული კავშირის სასამართლოს წინაშე დგას საკითხი, თუ რამდენად სჭირდებოდა ტელეკომ-პროვაიდერს, პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების შესახებ დირექტივის[62] მე-12 მუხლის საფუძველზე, მისი აბონენტების პერსონალური მონაცემების გადაცემისათვის განახლებული თანხმობის მიღება მონაცემთა სუბიექტისგან, რამდენადაც, თავდაპირველად თანხმობის გაცემისას, მიმღებები არ იყვნენ დასახელებულნი.

სასამართლომ დაადგინა, რომ, ამ მუხლის თანახმად, მონაცემთა გადაცემამდე განახლებული თანხმობის მიღება არ იყო აუცილებელი, ვინაიდან მონაცემთა სუბიექტებს, მოცემული პირობის საფუძველზე, შესაძლებლობა ჰქონდათ, თანხმობა განეცხადებინათ მხოლოდ დამუშავების მიზნისთვის, რაც გულისხმობს მათი მონაცემების გამოქვეყნებას, და არ შეეძლოთ, აერჩიათ ის მიმართულებები, სადაც, შესაძლოა, ყოფილიყო მათი მონაცემები გამოქვეყნებული.

როგორც სასამართლომ აღნიშნა, „ეს გამომდინარეობს პირადი ცხოვრებისა და ელექტრონული კომუნიკაცების დირექტივის მე-12 მუხლის კონტექსტუალური და სისტემური განმარტებიდან, სადაც მე-12 მუხლის მე-2 პუნქტის საფუძველზე, არსებული თანხმობა ეხება პერსონალურ მონაცემთა საჯარო წყაროში გამოქვეყნების მიზანს და არა კონკრეტული წყაროს პროვაიდერის ვინაობას.[63] გარდა ამისა, „ეს არის საჯარო წყაროში პერსონალური მონაცემების გამოქვეყნება სპეციალური მიზნისთვის, რომელიც შესაძლებელია, აღმოჩნდეს

[61] მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG v. Germany, 5 მაისი 2011 წელი; იხ. ძირითადად პარაგ. 53 და 54;

[62] ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დამუშავების შესახებ OJ 2002 L 201 (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივა);

[63] მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG. V. Germany, 5 მაისი 2011 წელი; იხ. ძირითადად, პარაგ. 61;

ზიანის მომტანი აბონენტისთვის“[64] და არა მოცემული პუბლიკაციის ავტორისათვის.

ხშირ შემთხვევაში, ბანკს, როგორც საფინანსო სექტორის წარმომადგენელს, რამდენიმე საფუძველი გააჩნია პერსონალური მონაცემების დასამუშავებლად, თუმცა, უმეტესწილად, კომერციული ბანკის მიერ პირის პერსონალური მონაცემების დამუშავება კანონითაა მოთხოვნილი ან ბანკს აღნიშნული ესაჭიროება კანონმდებლობით გათვალისწინებული ვალდებულებების შესასრულებლად. ასეთ შემთხვევებს განეკუთვნება, მათ შორის იდენტიფიკაცია საბანკო მომსახურების ხელშეკრულების გაფორმებამდე (მათ შორის - იმის დასადგენად, განეკუთვნება თუ არა პირი პოლიტიკურად აქტიური პირების კატეგორიას, ასევე FATCA-ს სტატუსი)[65], საბანკო ანგარიშის გახსნა, გარკვეული საბანკო სერვისები ანგარიშის გახსნის გარეშე, რომლებიც საჭიროებენ იდენტიფიკაციას, საბანკო ტრანზაქციების განხორციელება და ა.შ. ამავდროულად, როგორც წესი, ბანკსა და კლიენტს შორის გაფორმებული საბანკო მომსახურების ხელშეკრულების პირობებზე დათანხმებით, ან, გარკვეულ შემთხვევაში - მატერიალური თუ ელექტრონული ფორმით საგადახდო დავალებაზე დათანხმებით, კლიენტი გამოხატავს თანხმობას მისი პერსონალური მონაცემების დამუშავებაზე.

„კომერციული ბანკების საქმიანობის შესახებ“ საქართველოს კანონის 17(1) მუხლის თანახმად, სახელმწიფო სერვისების განვითარების სააგენტოს (შემდგომში - სსგს) მონაცემთა ელექტრონული ბაზაში არსებული კლიენტის მონაცემების გადასამოწმებლად, საჭიროა მის მიერ კანონმდებლობის შესაბამისად გაცემული თანხმობის არსებობა. სავარაუდოა, რომ ასეთი მაღალი ტიპის დაცვა კანონმდებელმა შემოიღო სწორედ სსგს მონაცემთა ელექტრონულ ბაზაში დაცული მომხმარებლების პერსონალური მონაცემების მნიშვნელობიდან და მოცულობიდან გამომდინარე. აღსანიშნავია, რომ კომერციული ბანკების კანონის მითითებული მუხლი მიუთითებს მონაცემთა დამუშავების მიზანზე. კერძოდ, ამ მუხლზე დაყრდნობით ბანკი სსგს მონაცემთა ბაზას იყენებს კლიენტის იდენტიფიკაციისა და ვერიფიკაციისათვის. შესაბამისად, ბანკის

[64] იქვე. იხ. ძირითადად, პარაგ. 62;

[65] Foreign Account Tax Compliance Act (FATCA) აქტი უცხოური ანგარიშის საგადასახადო შესაბამისობის შესახებ და მის შესაბამისად 2015 წლის 10 ივლისს გაფორმებული „შეთანხმება ამერიკის შეერთებული შტატების მთავრობასა და საქართველოს მთავრობას შორის საერთაშორისო საგადასახადო ვალდებულებების შესრულების გაუმჯობესების და უცხოური ანგარიშის საგადასახადო შესაბამისობის აქტის (FATCA) შესრულების მიზნით“ (რატიფიცირებულია საქართველოს მთავრობის მიერ 2015 წლის 18 სექტემბერი);

კანონისმიერი ვალდებულებაა მოახდინოს კლიენტის იდენტიფიკაცია და ვერიფიკაცია კანონის შესაბამისად, ხოლო სსგს მონაცემთა ბაზის გამოყენება, არის უფლება, რომელსაც ბანკი იყენებს კლიენტის შესაბამისი თანხმობის არსებობის შემთხვევაში[66].

საკანონმდებლო მოთხოვნის საფუძველზე, ბანკის მიერ, მომხმარებლის, მონაცემთა სუბიექტის, თანხმობით ,კლიენტის განცხადების განხილვისას, პერსონალური მონაცემების დამუშავების შემთხვევაში (მაგ. საკრედიტო, სადეპოზიტო და საგადახდო პროდუქტები), მხოლოდ ფორმალური მოთხოვნის - თანხმობის ან შესაბამისი განცხადების არსებობა არ არის საკმარისი მონაცემთა, კანონის შესაბამისად, დამუშავების უზრუნველსაყოფად. თანხმობის არსებობა არ ნიშნავს, რომ ბანკს უფლება აქვს მოიპოვოს ნებისმიერი ინფორმაცია მომხმარებლის შესახებ, არამედ, მონაცემთა დამუშავების საფუძვლის არსებობასთან ერთად, დაცული უნდა იქნეს მონაცემთა დამუშავების პრინციპებიც[67].

კერძოდ, ბანკის მიერ, მომხმარებლის თანხმობით, მისი განცხადების დამუშავების/მომსახურების გაწევის პროცესში, ინფორმაციის მოპოვება უნდა შეესაბამებოდეს კანონიერების, სამართლიანობის პრინციპებს, არ უნდა ლახავდეს მონაცემთა სუბიექტის ღირსებას; უნდა იყოს ზუსტი, უნდა შეესაბამებოდეს სამართალურთიერთობის მიზანს და უნდა იყოს მისი პროპორციული, ანუ არ უნდა მოხდეს ისეთი ინფორმაციის მოპოვება, რაც არარელევანტური ან გადაჭარბებულია ურთიერთობის მიზანთან მიმართებაში. მნიშვნელოვანია აღინიშნოს, რომ ბანკმა ზემოჩამოთვლილი პრინციპების გამოყენება უნდა უზრუნველყოს არა მარტო მომხმარებლის თანხმობით მოპოვებული ინფორმაციის შინაარსთან მიმართებაში, არამედ ინფორმაციის მოპოვების ფორმასა და წყაროებთან მიმართებაშიც.

3.2. საფინანსო სექტორის მიერ, მონაცემთა დამუშავების სამართლებრივი ფარგლები

რაც შეეხება შენახვის ვადას, მიუხედავად იმისა, რომ ამ საფუძვლებით მოპოვებული ინფორმაციის დამუშავების საფუძველს არ წარმოადგენს „უკანონო შემოსავლის ლეგალიზაციის აღკვეთის ხელშეწყობის შესახებ საქართველოს

[66] ევროკავშირისა (EU) და გაეროს განვითარების პროგრამის (UNDP) მხარდაჭერით შექმნილი რეკომენდაცია კომერციული ბანკის მიერ პერსონალური მონაცემების დამუშავების შესახებ, გვ. 18, 2019 წელი;

[67] იქვე. გვ. 19;

კანონით“ მონიტორინგის განმხორციელებელი პირისათვის განსაზღვრული ვალდებულება, შენახვის შემთხვევაში, ამგვარად მოპოვებული ინფორმაციის დიდი ნაწილი მოექცევა იმ კატეგორიის ინფორმაციაში, რაც განსაზღვრულია ხსენებული კანონით და „კომერციული ბანკების კატეგორიით კანონით განსაზღვრული ვადებით შესანახ ინფორმაციაში“.

პერსონალური მონაცემია ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ სხვა მახასიათებლებთან ერთად ერთობლიობაში, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.

თანამედროვე ტექნოლოგიებით გაჯერებულ სამყაროში, პერსონალური მონაცემების დაცვის აუცილებლობა კიდევ უფრო დიდ მნიშვნელობას იძენს. დღევანდელ რეალობაში არა მხოლოდ საბანკო - საფინანსო, არამედ სხვა მრავალი სერვისის მისაღებად, პერსონალური მონაცემების დამუშავება აუცილებელი პირობაა. საბანკო მომსახურების გაწევის პროცესში პერსონალური მონაცემების დამუშავება, ფაქტობრივად მუდმივ რეჟიმში მიმდინარეობს. თუმცა, ხშირ შემთხვევაში, თავად მონაცემთა სუბიექტი შესაძლოა ვერ აცნობიერებდეს ამ პროცესის მასშტაბებს და შესაძლო შედეგების სავარაუდო გავლენას მის ცხოვრებაზე.

ბანკში მონაცემები ძირითადად მუშავდება: მომსახურების გაწევის, განცხადებების განხილვის, სახელშეკრულებო ურთიერთობების შესრულების, დასაქმების მიზნით; ასევე, როდესაც არსებობს მონაცემთა სუბიექტის თანხმობა, მონაცემთა დამუშავება გათვალისწინებულია კანონით, მონაცემთა დამუშავება საჭიროა ბანკის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად.

გასათვალისწინებელია, მონაცემთა დამუშავების პრინციპების გამოყენებისას, ბანკი ეყრდნობა შეფასებით კატეგორიებს, როგორიცაა, მაგალითად “მონაცემთა სუბიექტის ღირსება”, “სამართლიანობა”, “ადეკვატურობა და პროპორციულობა”. კლიენტის შესახებ დამატებითი ინფორმაციის მოპოვების მიზანი, ბანკის წინაშე

არსებული რისკების[68] დაზღვევაა. მიუხედავად იმისა, რომ ბანკის მიერ ამ კონტექსტში მოსაპოვებელი დამატებითი ინფორმაციის კონკრეტული და ამომწურავი ჩამონათვალი არ არსებობს, მონიტორინგის განმხორციელებელი პირის (ამ შემთხვევაში - ბანკის) უფლებამოსილებას ამ მიმართულებით შემოფარგლავს როგორც პერსონალურ მონაცემთა დაცვის კანონი, ასევე - უკანონო შემოსავლის ლეგალიზაციის აღკვეთის შესახებ საქართველოს კანონი. ეს ორი საკანონმდებლო აქტი ითვალისწინებს, რომ მოპოვებული ინფორმაცია უნდა შეესაბამებოდეს მონაცემთა დამუშავების მიზანს[69] და ბანკი უფლებამოსილია მოიპოვოს დამატებითი ინფორმაცია, რომელიც რელევანტურია გარიგებასთან ან გარიგების მხარეებთან მიმართებაში[70]. თავის მხრივ, თუ რა უნდა იგულისხმოს ბანკმა გარიგებასთან და გარიგების მხარეებთან დაკავშირებულ ინფორმაციაში, უნდა განიმარტოს „უკანონო შემოსავლის ლეგალიზაციის აღკვეთის შესახებ“ საქართველოს კანონის მიზნებიდან გამომდინარე.

ამასთანავე, არსებობს საერთაშორისო პრაქტიკა, სახელმძღვანელო დოკუმენტები და კითხვარების ნიმუშები, რომელიც მნიშვნელოვნად ეხმარება ბანკს მოსაპოვებელი ინფორმაციის შინაარსისა და ფარგლების დადგენაში[71]. ბაზელის კომიტეტის სახელმძღვანელო[72] განსაზღვრავს, რომ ანგარიშის გახსნისას და კლიენტის რისკის პროფილის მინიჭებისას, ბანკმა უნდა გაითვალისწინოს, სულ მცირე, ისეთი მნიშვნელოვანი ფაქტორები, როგორებიცაა, კლიენტის საქმიანობა, შემოსავლის/ფულადი სახსრების წყარო, წარმოშობის ქვეყანა, იმ საბანკო პროდუქტების ხასიათი, რომლებითაც სარგებლობს ან ისარგებლებს, დაკავშირებული ანგარიშები, დამსაქმებლის

[68] მაგ. ფულის გათეთრების კანონმდებლობით განსაზღვრული რეგულაციების დარღვევის შედეგად სანქცირების რისკი, რეპუტაციული რისკი, და ა. შ.;

[69] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონი, მუხლი 4, „ბ“ ქვეპუნქტი;

[70] უკანონო შემოსავლის ლეგალიზაციის აღკვეთის ხელშეწყობის შესახებ საქართველოს კანონი, მუხლი 6, პუნქტი 7;

[71] მაგ. ფინანსური ქმედების სამოქმედო ჯგუფის (Financial Action Task Force – FATF) საუკეთესო პრაქტიკის სახელმძღვანელოების და მითითებები, ხელმისაწვდომია http:// www.fatf-gafi.org/documents/guidance/?hf=10&b=20&s=desc(fatf_releasedate); საბანკო ზედამხედველობის ბაზელის კომიტეტის „სახელმძღვანელო ფულის გათეთრების და ტერორიზმის დაფინანსების რისკის ჯანსაღი მენეჯმენტის შესახებ,“ ხელმისაწვდომია https://www.bis.org/bcbs/publ/d405.htm და ა.შ.;

[72] საბანკო ზედამხედველობის ბაზელის კომიტეტის „სახელმძღვანელო ფულის გათეთრების და ტერორიზმის დაფინანსების რისკის ჯანსაღი მენეჯმენტის შესახებ,“ ხელმისაწვდომია https://www.bis.org/bcbs/publ/d405.htm, გვ. 7.;

ვინაობა და საქმიანობის შინაარსი და ა.შ. ამავე დოკუმენტის დანართი N4[73], რომელიც ანგარიშის გახსნას ეხება, კონკრეტულად განსაზღვრავს, თუ რა მინიმალური ინფორმაცია/დოკუმენტაცია უნდა მოიპოვოს ბანკმა და რა ინფორმაციის მოპოვებაა სასურველი კლიენტის რისკის პროფილიდან გამომდინარე. ამასთან, თავად დოკუმენტი უთითებს, რომ ჩამონათვალი ამომწურავი არ არის. მაგალითად, ფულადი სახსრების წარმომავლობის დადგენისას, ბანკმა შეიძლება შეიტყოს, რომ ფულადი სახსრები, რაც უნდა განთავსდეს ანგარიშზე, აზარტული თამაშების შედეგადაა მოპოვებული. ამ ინფორმაციაზე დაყრდნობით, ბანკმა უნდა განსაზღვროს მომხმარებლის რისკის პროფილი და აღნიშნულიდან გამომდინარე იმსჯელოს თუ რა სერვისები იქნება მომხმარებლისთვის ხელმისაწვდომი, ასევე, მოიპოვოს თუ არა სხვა დამატებითი ინფორმაცია მომხმარებელთან დაკავშირებით და ა.შ.

შესაბამისად, თავად ბანკმა უნდა განსაზღვროს, თუ რა დამატებითი ინფორმაცია სჭირდება მას მიზნის მისაღწევად. თუმცა, მიზნის მიღწევის საშუალება არ უნდა ეწინააღმდეგებოდეს და არღვევდეს კანონს და ეფუძვნეოდეს შემდეგ სამართლებრივ პრინციპებს:

- კანონიერება და სამართლიანობა- მონაცემთა დამუშავების პირველი პრინციპის გამოყენებისას, პროცესი ერთდროულად სამი კრიტერიუმით უნდა იყოს გამყარებული, ესენია: კანონიერება, სამართლიანობა და მონაცემთა სუბიექტის ღირსების შეულახავობა. ლახავს თუ არა რაიმე კონკრეტული პერსონალური მონაცემის დამუშავება ბანკის მიერ მონაცემთა სუბიექტის ღირსებას, სუბიექტური შეფასების საგანია. თუმცა, საზოგადოებაში დაშვებული ეთიკის ნორმების საფუძველზე, შესაძლოა თავად ბანკმა, ხოლო სუბიექტის მხრიდან გასაჩივრების შემთხვევაში - პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა ან სასამართლომ დაადგინოს, თუ რამდენად შეიძლება პერსონალურ მონაცემთა დამუშავების ესა თუ ის კონკრეტული შემთხვევა არღვევდეს პირის ღირსებას. ამასთან, პერსონალურ მონაცემთა დამუშავებისას, მონაცემთა სუბიექტის ღირსების დაცვა განსაკუთრებით აქტუალურია ისეთ შემთხვევებში, როდესაც ბანკი პერსონალურ მონაცემებს არ აგროვებს უშუალოდ მონაცემთა სუბიექტებისგან (მაგ. მონაცემების დამოუკიდებელ მესამე წყაროებზე დაყრდნობით გადამოწმების შემთხვევაში);

[73] იქვე, გვ. 35;

- მიზნის შესაბამისობა- მოპოვებული ინფორმაცია უნდა შეესაბამებოდეს ინფორმაციის მოპოვების მიზანს და არ უნდა იქნეს გამოყენებული სხვა თავდაპირველ მიზანთან შეუთავსებელი მიზნით. მაგ. თუ ბანკი ანგარიშის გახსნისას დამატებითი ინფორმაციის სახით მოიპოვებს ინფორმაციას პირის ჯანმრთელობის შესახებ (განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავების თავისებურებების გათვალისწინებით), უპირველეს ყოვლისა, უნდა დადგინდეს, თუ რამდენად შეესაბამება ასეთი მონაცემების მოპოვება ანგარიშის გახსნის მიზანს. ხოლო, თუ დადგინდა, რომ შეესაბამება, მოპოვებული დამატებითი ინფორმაცია არ უნდა იქნეს გამოყენებული ამავე პირისათვის საკრედიტო პროდუქტის შეთავაზების შემთხვევაში;
- ადეკვატურობა და პროპორციულობა- ბანკი განსაზღვრავს თუ რა მოცულობის ინფორმაციაა ადეკვატური და პროპორციული დასახული მიზნის მისაღწევად. ამ პრინციპის მიზანია ეს პროცესი მოაქციოს ლოგიკურ ჩარჩოებში და მოთხოვნილი ინფორმაციის ადეკვატურობის და პროპორციულობის ბანკის მიერ გამოყენებული სტანდარტი მისაღები და გასაგები იყოს როგორც მონაცემთა სუბიექტისთვის, ისე ყველა ზედამხედველი ორგანოსათვის, რომელსაც შესაძლოა შეხება ჰქონდეს კონკრეტულ შემთხვევასთან. მაგალითისთვის, მეორე პრინციპთან მიმართებაში განხილული პირის ჯანმრთელობის შესახებ ინფორმაციის მოპოვების შემთხვევა საბანკო ანგარიშის გახსნის თვალსაზრისით, დიდი ალბათობით, ვერ დააკმაყოფილებს პროპორციულობის და ადეკვატურობის სტანდარტებს;
- მონაცემთა სიზუსტე- პასუხისმგებლობას ანაწილებს როგორც ინფორმაციის დამმუშავებელზე, ასევე მონაცემთა სუბიექტზე: სუბიექტი ვალდებულია დამმუშავებელს მიაწოდოს ზუსტი ინფორმაცია, ხოლო დამმუშავებელი ვალდებულია უზრუნველყოს ინფორმაციის სიზუსტე, უცვლელობა და, აუცილებლობის შემთხვევაში - განახლება. მაგალითად, მონაცემთა სიზუსტის პრინციპს ეხმიანება ფულის გათეთრებასთან ბრძოლის კანონმდებლობით განსაზღვრული ბანკის ვალდებულება აწარმოოს მუდმივი მონიტორინგი[74]. როგორც წესი, ბანკები კლიენტების ინფორმაციის განახლების პერიოდულობას თავიანთი შიდა პოლიტიკით განსაზღვრავენ, კლიენტის რისკის პროფილიდან გამომდინარე. ეს

[74] უკანონო შემოსავლის ლეგალიზაციის აღკვეთის ხელშეწყობის შესახებ საქართველოს კანონი, მუხლი 6, პუნქტი 15;

კანონით განსაზღვრული ვალდებულებაა და მონაცემთა სუბიექტისგან ამის შესახებ დამატებითი თანხმობის მოპოვების ვალდებულება არ არსებობს. ამასთან, გასათვალისწინებელია, რომ მუდმივი მონიტორინგის ვალდებულება არ გულისხმობს ბანკის მიერ მხოლოდ იმ ინფორმაციის განახლებას, რაც მასთან უკვე დაცულია. ეს დებულება ბანკს უფლებას ანიჭებს მოიპოვოს ისეთი ინფორმაციაც, რაც მას შესაძლოა თავდაპირველად არ დაუმუშავებია, თუმცა, მომხმარებლის რისკის პროფილის ცვლილებიდან ან სხვა საფუძვლიდან გამომდინარე აუცილებლად მიიჩნია მისი მოპოვებაც. ამ პროცესში, მნიშვნელოვანია ზედმიწევნით იყოს დაცული მონაცემთა დამუშავების პრინციპები, მათ შორის - მიზანთან შესაბამისობის, პროპორციულობის და კანონიერების, ვინაიდან სწორედ ამ პრინციპებთან შესაბამისობაა ბანკის მიერ კანონის მოთხოვნების დაცვის ტესტი

- შენახვის ვადა- ითვალისწინებს პერსონალური მონაცემების მხოლოდ იმ ვადით შენახვას, რაც საკმარისია მონაცემთა დამუშავების მიზნის მისაღწევად ან კანონით დადგენილი ვადით. ამ პრინციპის ცალმხრივი წაკითხვის შემთხვევაში, პირველი დასკვნა იქნებოდა, რომ დამატებითი ინფორმაცია, რომელიც ბანკმა მოიპოვა ანგარიშის გახსნის მიზნით, "უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს ..." ანგარიშის გახსნის შემდეგ. თუმცაღა, თავად ეს პრინციპი უთითებს კანონით გათვალისწინებულ სხვა შემთხვევებზე. შესაძლოა, კანონმდებლობა ადგენდეს კონკრეტული მონაცემების შენახვის სპეციალურ ვადას. მაგალითად, მონაცემთა შენახვის ვადას განსაზღვრავს „უკანონო შემოსავლის ლეგალიზაციის აღკვეთის ხელშეწყობის შესახებ" საქართველოს კანონის მე-7 მუხლი და ამავე კანონის საფუძველზე გამოცემული საქართველოს ფინანსური მონიტორინგის სამსახურის უფროსის 2012 წლის 18 იანვრის N4 ბრძანებით დამტკიცებული „კომერციული ბანკების მიერ ინფორმაციის მიღების, სისტემატიზაციის, დამუშავებისა და საქართველოს ფინანსური მონიტორინგის სამსახურისათვის გადაცემის წესის შესახებ" დებულების 11-ე მუხლი, რომლის თანახმად კლიენტის შესახებ იდენტიფიკაციის პროცესში მოპოვებული ინფორმაცია უნდა იქნას შენახული 6 წლის ვადით, ასევე, „კომერციული ბანკების საქმიანობის შესახებ" საქართველოს კანონის 23-ე მუხლის მე-2 პუნქტით დადგენილია, რომ კომერციული ბანკი ვალდებულია კლიენტების, მათ მიერ და მათ ანგარიშებზე განხორციელებული ნებისმიერი ოპერაციის შესახებ

ინფორმაცია ელექტრონული ფორმით შეინახოს არანაკლებ 15 წლის განმავლობაში.

3.3. პერსონალურ მონაცემთა გადაცემა მესამე პირთათვის და მონაცემთა სუბიექტის თავდაცვის სამართლებრივი ბერკეტები, პერსონალური მონაცემების გასაჯაროვების ხელშეშლის უზრუნველსაყოფად

ევროპული კავშირის კანონმდებლობით, მონაცემთა უსაფრთხო დამუშავების ვალდებულება ეკისრება ყველა პირს, კერძოდ, დამმუშავებელსა და უფლებამოსილ პირებს, დაიცვან მონაცემთა კოფიდენციალურობა.

კონფიდენციალურობის ვალდებულება არ ვრცელდება იმ შემთვევებზე, როდესაც მონაცემები ცნობილი გახდაპირისათვის პირადად, და არა, როგორც დამმუშავებლის ან უფლებამოსილი პირის სტატუსით. ამ მხრივ, მონაცემთა დაცვის დირექტივის მე-16 მუხლი არ ვრცელდება იმდენად, რამდენადაც, ფიზიკური პირების მიერ, პერსონალურ მონაცემთა გამოყენება, კერძო პირებს შორის, სრულიად თავისუფალია დირექტივის რეგულირებისგან. ამგვარი გამოყენება ექცევა ე.წ. პირადი მიზნებისათვის გამოყენების ფარგლებში[75]. ეს გამონაკლისი წარმოადგენს პერსონალური მონაცემების გამოყენებას „ფიზიკური პირების მიერ, აშკარად, პირადი ან საშინაო საქმიანობის მიზნებისათვის“[76]. მართლმსაჯულების ევროპული კავშირის სასამართლოს გადაწყვეტილებებიდან გამომდინარე, საქმეზე Bodil Lindqvist[77], ეს გამონაკლისი უნდ აგანიმარტოს ვიწროდ, განსაკუთრებით, მონაცემთა გამჟღავნების მხრივ. კერძოდ, პირადი მიზნებისთვის არსებული გამონაკლისი არ უნდა გავრცელდეს, ინტერნეტში, პერსონალურ მონაცემთა პუბლიკაციაზე, მიმღებთა შეუზღუდავი წრისათვის (მეტად დაწვრილებით, იხ. პარაგრაფები 2.1.2, 2.2, 2.3.1 და 6.1).

მონაცემთა დაცვის დირექტივა განასხვავებს პეროსნალურ მონაცემთა გადაცემას „მესამე პირებსა“ და „მიმღებებს“ შორის. კერძოდ, „მესამე პირი“ არის ის, ვინც სამართლებრივად განცალკევებულია დამმუშავებლისაგან. შესაბამისად, მონაცემთა გამჟღავნება მესამე პირისთვის, ყოველთვის, მოითხოვს სპეციალურ სამართლებრივ საფუძველს. მონაცემთა აცვის დირექტივის მე-2

[75] მონაცემთა დაცვის დირექტივა, მე-3 მუხლის მე-2 პუნქტი, მეორე აბზაცი;
[76] Ibid;
[77] მართლმსაჯულების ევროპული კავშირის სასამართლო,C-101/01, Lindqvist, 6 ნოემბერი 2003 წელი;

მუხლის -f- ქვეპუნქტის თანახმად, მესამე პირი არის „ნებისმიერი ფიზიკური ან იურიდიული პირი, სახელმწიფო დაწესებულება, სააგენტო ან სხვა, ნებისმიერი ორგანო, რომელიც არ არის მონაცემთა სუბიექტი, დამმუშავებელი, უფლებამოსილი პირის უშუალო დაქვემდებარებაში მყოფი პირი, გააჩნიათ მონაცემთა დამუშავების უფლებამოსილება.“ ეს ნიშნავს, პირები, რომლებიც მუშაობენ ორგანიზაციისათვის, რომელიც, სამართლებრივად, დამოუკიდებელია დამმუშავებლისაგან, იმ შემთხვევაშიც კი, თუ იგი მიეკუთვნება კომპანიების გარკვეულ ჯგუფს ან ჰოლდინგს, მიიჩნევიან „მესამე პირებად“. მეორეს მხრივ, ბანკის ფილიალები, რომლებიც ამუშავებენ მომხმარებლის ანგარიშებს, მათი ხელმძღვანელობის პირდაპირი მოთხოვნით, არ მიიჩნევიან „მესამე პირებად“[78].

„მიმღები“, შედარებით, ფართო ცნებაა, ვიდრე „მესამე პირი“. მონაცემთა დაცვის დირექტივის მე-2 მუხის -გ- ქვეპუნქტის თანახმად, „მიმღები“ ნიშნავს „ნებისმიერ ფიზიკურ ან იურიდიულ პირს, სახელმწიფო დაწესებულებას, სააგენტოს, ან ნებისმიერ სხვა ორგანოს, რომელსაც გადაეცემა მონაცემები, როგორც მესამე პირს ანს ხვა პირს“. „მიმღები“, შესაძლებელია, იყოს დამმუშავებლისაგან ან უფლებამოსილი პირისაგან დამოუკიდებელი, რომელიც, ამ შემთხვევაში, იქნება „მესამე პირი“, ან რომელიმე პირი დამმუშავებლის ან უფლებამოსილი პირის შიდა სტრუქტურაში, როგორიცაა დასაქმებული ან იმავე კომპანიის ან დაწესებულების სხვა განყოფილება.

განსხვავება „მიმღებსა“ და „მესამე პირებს“ შორის საყურადღებოა, მხოლოდ, მონაცემთა კანონიერი გადაცემიდან გამომდინარე. დამმუშავებლისა ან/და უფლებამოსილი პირის დასაქმებულებს, დამატებითი სამართლებრივი საფუძვლის გარეშე, შეუძლიათ, იყვნენ პერსონალური მონამების მიმღებნი, თუ ისინი ჩართულნი არიან, დამმუშავებლისა ან/და უფლებამოსილი პირის მიერ, წარმოებულ დამუშავების პროცესებში. მეორეს მხრივ, მესამე პირი, რომელიც არის იურიდიულად დამოუკიდებელი, დამმუშავებლისა და უფლებამოსილი პირისაგან, არ არის უფლებამოსილი, გამოიყენოს, დამმუშავბელის მიერ, დამუშავებული პერსონალური მონაცემები, გარდა, კანონით დადგენილი, სპეციალური გამონაკლისებისა. მომაცემთა „მიმღები მესამე პირები“, შესაბამისად, ყოველთვის, საჭიროებენ სამართლებრივი საფუძვლის არსებობას, პერსონალურ მონაცემთა კანონიერი მიღებისათვის.

[78] მუხლი 29 სამუშაო ჯგუფი (2010), მოსაზრება 1/2010 „დამმუშავებლისა“ და „უფლებამოსილი პირის“ ცნებების შესახებ, WP 169, 16 თებერვალი 2010 წელი, გვ.31;

სხვა შემთხვევებში, მონაცემთა დამმუშავებლები და უფლებამოსილი პირები შებოჭილნი არიან კოფიდენციალურობის ვალდებულებით. უფლებამოსილი პირებისათვის კონფიდენციალურობა გულისხმობს, რომ მათ უნდა გამოიყენონ დამმუშავებლისაგან გადაცემული პერსონალური მონაცემები მხოლოდ იმ ინსტრუქციების შესაბამისად, რომლებიც განსაზღვრულია მათი ზემდგომების მიერ. კონფიდენციალურობის პირობა, ასევე, გათვალისიწნებულ უნდა იქნეს დამმუშავებელსა და უფლებამოსილ პირს შორის არსებულ ყველა ხელშეკრულებაშიც. ამასთანავე, დამმუშავებლებსა და უფლებამოსილ პირებს ექნებათ ვალდებულება, მიიღონ სპეციალური ზომები მათი, დასაქმებულების მიერ, კონფიდენციალურობის სამართლებრივი მოთხოვნის უზრუნველსაყოფად. ძირითადად, დამსაქმებელსა და დასაქმებულს შორის, არსებულ ხელშეკრულებაში კონფიდენციალურობის განმსაზღვრელი პირობების ჩართვით.

მონაცემთა გადაცემა ხორციელდება საერთაშორისო მასშტაბითაც. მონაცემთა საერთაშორისო გადაცემა წარმოადგენს პერსონალურ მონაცემთა, სხვა ქვეყნის კანონმდებლობაზე დაქვემდებარებული, მიმღებისათვის გადაცემას.

108-ე კონვენციის დამატებითი ოქმის მე-2 მუხლის პირველი პუნქტი განმარტავს მონაცემთა საერთაშორისო გადაცემას. როგორც პერსონალურ მონაცემთა, უცხო ქვეყნის კანონმდებლობას დაქვემდებარებული, მიმღებისათვის გადაცემას. მონაცემთა დაცვის დირექტივის 25-ე მუხლის 1-ლი პუნქტით დარეგულირებულია „დამუშავების პროცესში არსებულ, ან გადაცემის შემდეგ, დამუშავებისათვის გამიზნულ, პერსონალურ მონაცემთა გადაცემას მესამე ქვეყნისათვის“. მონაცემთა ამგვარი გადაცემა ნებადართულია, მხოლოდ, 108-ე კონვენციის მე-2 მუხლით დადგენილი წესების თანახმად. ხოლო ევროპული კავშირის ქვეყნებისათვის მონაცემთა დაცვის 25-ე და 26-ე მუხლებით გათვალისწინებულ შემთხვევებშიც.

აღნიშნულთან დაკავშირებით, გასათვალისიწნებელია შემდეგი საქმე: საქმეზე Bodil Lindqvist[79], მართლმსაჯულების ევროპული კავშირის სასამართლომ აღნიშნა, რომ „ვებ-გვერდის მეშვეობით სხვადასხვა პირების იდენტიფიცირება და მათთვის მიმართვა სახელით ან სხვა საშუალებით, მაგალითად, მათ სამუშაო პირობების, მათი ტელეფონის ნომრის ან/და ჰობის შესახებ ინფორმაციით, წარმოადგენს პერწონალური მონაცემების სრულად ან ნაწილობრივ

[79] მართლმსაჯულების ევროპული კავშირის სასამართლო,C-101/01, Lindqvist, 6 ნოემბერი 2003 წელი, პარაგ. 27, 68 და 69;

დამუშავებას ავტომატური საშუალებით 95/46 დირექტივის მე-3 მუხლის 1-ლი ნაწილის თანახმად“.

სასამართლომ ასევე აღნიშნა, რომ დირექტივით განსაზღვრულია სპეციალური წესებიც, რომლებიც წევრ ქვეყნებს უფლებას აძლევს მონიტორინგი გაუწიონ მესამე პირებისათვის მონაცემთა გადაცემას.

თუმცა, უპირველესად, დირექტივის შედგენისას, ინტერნეტის დონის გათვალისწინებით, და, ასევე, გამომდინარე იქედან, რომ ინტერნეტის გამოყენებაზე მოქმედი კრიტერიუმი არ არის მოცემული დირექტივით, „ნაკლებად სავარაუდოა, რომ- „მონაცემთა გადაცემა მესამე ქვეყნისთვის“- შემთხვევაში, კანონმდებლობამ განიზრახა, მოეცვა მონაცემთა ჩატვირთვაც ინერნეტ-გვერდზე. ასევე, იმ შემთხვევაშიც, თუ მონაცემები ხელმისაწვდომია პირებისატის მესამე ქვეყნებში, წვდომის ტექნიკური საშუალებების გამოყენებით“.

წინააღმდეგ შემთხვევაში, დირექტივა განიმარტებოდა შემდეგნაირად „მონაცემთა გადაცემა მესამე ქვეყნისათვის სახეზე იქნებოდა ყველა შემთხვევაში, როდესაც პერსონალური მონაცემები ჩატვირთულია ვებ-გვერდზე, ხოლო მოქმედებები ჩაითვლებოდა გადაცემად ყველა იმ მესამე ქვეყანაში, სადაც არსებობს ინტერნეტთან წვდომის ტექნიკური საშუალებები. დირექტივის მიერ დადგენილი სპეციალური რეჟიმი მოგვევლინებოდა, შესაბამისად, ინტერნეტ-ოპერაციებთან დაკავშირებული ზოგადი რეგულირების წესად. აქედან გამომდინარე, თუ კომისია დაადგენდა, რომ რომელიმე ქვეყანა არ აკმაყოფილებს ადეკვატური დაცვის დონეს, წევრი ქვეყნები ვალდებულნი იქნებოდნენ არ განეთავსებინათ რაიმე სახის პერსონალური მონაცემი ინტერნეტში“.

ევროპის საბჭოს კანონმდებლობით, კერძოდ, 108-ე კონვენციის მე-12 მუხლის მე-2 პუნქტით, შესაძლებელია პერსონალურ მონაცემთა თავისუფალი გადაადგილება კონვენციის ხელმომწერ სახელმწიფოებს შორის. შიდასახელმწიფოებრივი კანონმდებლობა არ უნდა კრძალავდეს ხელშემკვრელ სახელმწიფოებთან პეროსნალურ მონაცემთა ექსპორტს, გარდა იმ შემთხვევისა, თუ

- ეს საჭიროა მონაცემთა განსაკუთრებული ბუნებიდან გამომდინარე[80];

[80] 108-ე კონვენცია, მე-12 მუხლის მე-3 პუნქტის -ა- ქვეპუნქტი;

- შეზღუდვა აუცილებელია, რათა თავიდან იქნეს აცილებული ადგილობრივი კანონმდებლობისათვის გვერდის ავლა, მონაცემთა საერთაშორისო მასშტაბით, მესამე ქვეყნებისთვის გადაცემისას[81].

ევროპის საბჭოს კანონმდებლობა ნებას რთავს შიდასახელმწიფოებრივ კანონმდბელობას, დაადგინოს მონაცემთა თავისუფალი გადაადგილება არაწევრ სახელმწიფოებში, თუ მიმღები სახელმწიფო ან ორგანიზაცია უზრუნველყოფს დაცვისათვის ადეკვატურ დონეს, მონაცემთა დაგეგმილი გადაცემისას[82]. შიდასახელმწიფოებრივი კნონმდებლობით წყდება, თუ როგორ და ვის მიერ იქნება მონაცემთა დაცვის დონე შეფასებული უცხო ქვეყანაში.

მონაცემთა დაცვის დირექტივა არ მოიცავს გაცემული თანხმობის, ნებისმიერ დროს, უკან გამოთხოვის ზოგად უფლებას. თუმცა, ფართოდ აღიარებულია, რომ ამგვარი უფლება არსებობს და მონაცემთა სუბიექტს შეუძლია, ამ უფლების რეალიზაცია, შეხედულებისამებრ. გაცემული თანხმობის გამოთხოვის შესახებ, მონაცემთა სუბიექტს, არ უნდა მოეთხოვებოდეს ახსნა-განმარტებები და თანხმობის გაუქმებას არ უნდა სდევდეს ნეგატიური შედეგები, ასევე არც რაიმე თვადპირველი, მონაცემთა გამოყენების შედეგად მიღებული, სარგებლის გაუქმება.

თავი IV. პერსონალური მონაცემების დაცვა შრომის სამართალში.

4.1. დამსაქმებლის მიერ, შრომით ურთიერთობებში, დამუშავებული პერსონალური მონაცემების შეგროვება/შენახვა

შრომით ურთიერთობებში, მონაცემთა დაცვისათვის სპეციალური წესები მოცემულია ევროპის საბჭოს რეკომენდაციაში[83], დასაქმების მონაცემთა შესახებ. მონაცემთა დაცვის დირექტივაში, შრომითი ურთიერთობები კონკრეტულად მოხსენიებულია მხოლოდ განსაკუთრებული მონაცემების დამუშავების

[81] იქვე, მე-12 მუხლის მე-3 პუნქტის -ბ- ქვეპუნქტი;

[82] 108-ე კონვენცია, დამატებითი ოქმი, მე-2 მუხლის 1-ლი პუნქტი;

[83] ევროპის საბჭო, მინისტრთა კომიტეტი (1989), რეკომენდაცია Rec89(2), წევრი ქვეყნებისთვის პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე, 18 იანვარი 1989 წელი. იხ. შემდგომ, 108-ე კონვენციის საკონსულტაციო კომიტეტი, პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე რეკომენდაციის No. R (89) 2 კვლევა და პროექტის შეთავაზება მოცემული რეკომენდაციის გადასინჯვის თაობაზე, 9 სექტემბერი 2011 წელი;

კონტექსტში. დასაქმების კონტექსტთან დაკავშირებული მონაცემთა დაცვის ყველაზე გავრცელებული პრობლემატიის განხილვა მოცემულია მუხლი 29 სამუშაო ჯგუფის სამუშაო დოკუმენტში[84].

პერსონალურ მონაცემთა დაცვა ემსახურება ბალანსის უზრუნველყოფას დამსაქმებლის ლეგიტიმურ ინტერესსა და დასაქმებულის უფლებებს შორის. შრომით ურთიერთობებში პერსონალური მონაცემების დაცვა არ გულისხმობს დამსაქმებლის მიერ დასაქმების პროცესში საჭირო ინფორმაციის შეგროვებისა და დამუშავების აკრძალვას. პერსონალურ მონაცემებს შეიცავს დამსაქმებლის მიერ დასაქმებულის შესახებ დამუშავებული ნებისმიერი სახის დოკუმენტი, მაგალითად, პირადობის მოწმობის ასლი, განათლების ან კვალიფიკაციის დამადასტურებელი დოკუმენტის ასლი, ბიოგრაფია, სარეკომენდაციო წერილები, სამედიცინო-ნარკოლოგიური შემოწმების ცნობა, ტესტირების შედეგი, ფოტოსურათი, ელ-ფოსტა და ა.შ. შრომითი ურთიერთობების პროცესში დასაქმებულის მიერ სხვადასხვა სახის პერსონალური მონაცემების შემცველი დოკუმენტაციის წარდგენა დადგენილია კანონმდებლობით. გარკვეულ შემთხვევებში, მონაცემების დამუშავების საფუძველი არის მონაცემთა სუბიექტის (დასაქმებულის) თანხმობა, რომელიც მოპოვებული უნდა იქნეს კანონით დადგენილი ფორმით.

დასაქმებისა და შრომითი ურთიერთობების პროცესში პერსონალური მონაცემები შესაძლებელია დამუშავდეს სხვადასხვა მიზნით, მაგალითად: კვალიფიციური კადრების შერჩევა, შრომითი ხელშეკრულების დადება, თანამშრომელთა კვალიფიკაციის ამაღლება, ორგანიზაციის უსაფრთხოებისა და საკუთრების დაცვა, თანამშრომელთა ჯანმრთელობის დაზღვევა და სხვა. შრომითი ურთიერთობების პროცესში მონაცემთა დამმუშავებლის (დამსაქმებლის) მიერ მნიშვნელოვანია შემდეგი პრინციპების დაცვა:

- ადამიანის კონსტიტუციური უფლებების პატივისცემა - დამსაქმებელმა პერსონალური მონაცემების დამუშავებისას პატივი უნდა სცეს დასაქმებულთა კონსტიტუციით გარანტირებულ უფლებებსა და თავისუფლებებს, მათ შორის, ადამიანის პატივისა და ღირსების, პირადი და ოჯახური ცხოვრების ხელშეუხებლობისა და პიროვნების თავისუფალი განვითარების უფლებებს. დასაქმებულებს სამუშაო ადგილზე უნდა ჰქონდეთ სოციალური და პირადი ურთიერთობების

[84] მუხლი 29 სამუშაო ჯგუფი (2001), მოსაზრება 8/2001 პერსონალურ მონაცემთა დამუშავების შესახებ დასაქმების კონტექსტში, WP 48, ბრიუსელი, 13 სექტემბერი 2001 წელი;

დამყარების შესაძლებლობა. ისეთი ინფორმაცია, რომელიც არ არის დაკავშირებული პროფესიულ საქმიანობასთან, მაგალითად, ჰობი, მეგობრების წრე, უპირატესობის მინიჭება სპორტის სახეობისა თუ ხელოვნების დარგისთვის, დამსაქმებელმა შეიძლება დაამუშაოს მხოლოდ დასაქმებულის თანხმობის საფუძველზე, თუმცა, ამგვარი მონაცემები არ უნდა გახდეს სამსახურში აყვანის, კარიერული საფეხურისა და ანაზღაურების ოდენობის განმსაზღვრელი ფაქტორი;

- დისკრიმინაციის დაუშვებლობა - პერსონალური მონაცემების დამუშავება მიზნად არ უნდა ისახავდეს და არ უნდა იწვევდეს დასაქმების, შრომითი ურთიერთობებისა და კარიერული წინსვლის პროცესში რაიმე სახის დისკრიმინაციას;
- დასაქმებულთა ინფორმირებულობა - დასაქმებულს უნდა ჰქონდეს ინფორმაცია მისი პერსონალური მონაცემების დამუშავების (თუ რა მიზნით, რა საფუძვლით მუშავდება მონაცემები, ხომ არ ხდება მათი მესამე მხარისათვის გადაცემა და ა.შ.) კანონიერებისა და უფლებების შესახებ;
- ადეკვატურობა და პროპორციულობა - ყველა ტიპის მონაცემების დამუშავებას (შეგროვებას, შენახვას, გამჟღავნებას და ა.შ.) უნდა ჰქონდეს დამოუკიდებელი, კანონიერი და მკაფიოდ განსაზღვრული მიზანი. დამსაქმებელმა შრომითი ურთიერთობის პროცესში უნდა დაამუშაოს მხოლოდ ის პერსონალური მონაცემები, რომლებიც აუცილებელია აღნიშნული მიზნის მისაღწევად.

დასაქმებულის შესახებ პერსონალური მონაცემების შეგროვება უნდა ხდებოდეს უშუალოდ მისგან, ხოლო იმ შემთხვევაში, თუ აუცილებელია პერსონალური მონაცემების შეგროვება მესამე პირისგან, დასაქმებულს უნდა ეცნობოს ამის შესახებ - განემარტოს პერსონალური მონაცემების მესამე პირისგან მოპოვების მიზეზი და მიზანი, ინფორმაციის სავარაუდო წყარო და მისი მოპოვების საშუალება. თუ კანონით სხვა რამ არ არის დადგენილი, მესამე პირისგან ინფორმაციის მოპოვება შესაძლებელია მხოლოდ დასაქმებულის წინასწარი და ინფორმირებული თანხმობით. სამუშაო ჯგუფმა გააანალიზა თანხმობის მნიშვნელობა, როგორც დასაქმების შესახებ მონაცემთა დამუშავების სამართლებრივი საფუძველი[85]. აღსანიშნავია, რომ ეკონომიკური დისბალანსი

[85] მუხლი 29 სამუშაო ჯგუფი (2005), სამუშაო დოკუმენტი 1995 წლის 24 ოქტომბრის 95/46/EC დირექტივის 26-ე მუხლის პირველი პუნქტის ერთგვაროვანი განმარტების თაობაზე, WP 114, ბრიუსელი, 25 ნოემბერი 2005 წელი;

თანხმობის მომთხოვნს დამსაქმებელსა და, თანხმობის გამცემ, დასაქმებულს შორის, ხშირად, წარმოშობს ეჭვებს, თანხმობის ნებაყოფლობით გაცემის თაობაზე. თანხმობის მოთხოვის საფუძვლად განსაზღვრული პირობები ყურადღებით უნდა იქნეს განხილული, რათა შეფასდეს თანხმობის კანონიერება.

პროპორციულობისა და ადეკვატურობის პრინციპიდან გამომდინარე, დამსაქმებელმა უნდა შეაგროვოს მხოლოდ ის პერსონალური მონაცემები, რომლებიც, სამუშაოს სპეციფიკის გათვალისწინებით, აუცილებელია კანდიდატის შესარჩევად და შრომითი ურთიერთობის წარმოშობისთვის. დასაქმების პროცესში უნდა შეგროვდეს მხოლოდ ის მონაცემები, რომლებიც აუცილებელია სასურველი კვალიფიკაციის მქონე კანდიდატის შესარჩევად. გასაუბრებისას დასმული შეკითხვები და მიღებული პირადი ხასიათის ინფორმაცია უნდა იყოს კონკრეტულ პოზიციაზე კვლიფიციური კადრის შერჩევის მიზნის ადეკვატური.

დასაქმებულის მიერ დამსაქმებლისთვის იმ ინფორმაციის მიწოდების შემთხვევაში, რომელიც არ არის საჭირო შრომითი ურთიერთობის მიზნებისთვის, დოკუმენტები უნდა დაუბრუნდეს მონაცემთა სუბიექტს ან განადგურდეს დადგენილი წესის შესაბამისად.

თუ ვაკანსიაზე განმცხადებელს/კანდიდატს მოეთხოვება კითხვარის შევსება, სასურველია, კითხვარში აღინიშნოს, რომელი ველის შევსებაა სავალდებულო. არასავალდებულო ველების შეუვსებლობა არ უნდა გახდეს პირის შემდგომ ეტაპზე გადაყვანის შეზღუდვის საფუძველი.

ტესტირების შედეგად მიღებული ინფორმაცია არის პერსონალური მონაცემი და მათი დამუშავება უნდა მოხდეს კანონით განსაზღვრული საფუძვლებით და პრინციპების დაცვით.

პერსონალური მონაცემების შენახვისას, ისევე როგორც პერსონალური მონაცემების დამუშავების სხვა შემთხვევებში, აუცილებელია კანონით გათვალისწინებული პრინციპების დაცვა. დამსაქმებლის მიერ შენახული უნდა იქნეს მხოლოდ ის ინფორმაცია, რომელიც აუცილებელია მონაცემთა დამუშავების კონკრეტული მიზნის მისაღწევად.

პერსონალური მონაცემები შენახული უნდა იყოს მხოლოდ იმ ვადით, რაც საჭიროა შრომითი ურთიერთობების მიზნიდან გამომდინარე, რომლისთვისაც ისინი შეგროვდა/დამუშავდა, გარდა იმ შემთხვევებისა თუ:

- საქმე ეხება ვაკანსიაზე განმცხადებლის/კანდიდატის პერსონალური მონაცემების შენახვას მონაცემთა სუბიექტის თანხმობით. მაგალითად, პირი თანახმაა მისი მონაცემები ინახებოდეს რეზერვში;
- მონაცემების კონკრეტული ვადით შენახვის ვალდებულება დადგენილია კანონმდებლობით;
- მონაცემები საჭიროა შრომითი ურთიერთობის არსებობის ფაქტის დასადგენად.

თანამშრომლის პირად საქმეში დამსაქმებელს გადააქვს მისი შერჩევისას დამუშავებული პერსონალური ინფორმაციის მხოლოდ ის ნაწილი, რომელიც საჭიროა შრომითი ურთიერთობის დასამყარებლად. ინფორმაცია, რომლის შენახვის საჭიროებაც აღარ არსებობს, უნდა წაიშალოს ან განადგურდეს. დასაქმებული ინფორმირებული უნდა იყოს მის პირად საქმეში განხორციელებული ცვლილებისა ან/და მონაცემთა გასწორების შესახებ.

4.2. განსაკუთრებული კატეგორიისა და ბიომეტრიული მონაცემთა დამუშავება შრომით ურთიერთობებში

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემებს განეკუთვნება ინფორმაცია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული ორგანიზაციის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან ან ნასამართლობასთან, ასევე ბიომეტრული მონაცემი, რომლითაც შესაძლებელია პირის იდენტიფიცირება ზემოაღნიშნული ნიშნებით. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, განსაკუთრებული კატეგორიის მონაცემების დამუშავება აკრძალულია, გარდა კანონის მე-6 მუხლით განსაზღვრული გამონაკლისებისა. ერთ-ერთ გამონაკლისს წარმოადგენს მონაცემთა დამმუშავებლის მიერ შრომითი ვალდებულების შესრულებისათვის ან მასთან დაკავშირებული უფლების განხორციელებისათვის მონაცემთა დამუშავების აუცილებელობა. აღნიშნული საფუძველი არ უნდა განიმარტოს ფართოდ, განსაკუთრებული კატეგორიის მონაცემები უნდა დამუშავდეს მხოლოდ ლეგიტიმური მიზნის ადეკვატური მოცულობით.მონაცემთა დაცვის დირექტივაში, მე-8 მუხლის მე-2 პუნქტით,

განსაზღვრულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავების შემთხვევები.

მაგალითად, დამსაქმებელი დასაქმებულებს სთხოვს სისხლის ჯგუფის შესახებ ინფორმაციის მიწოდებას, რადგან ზოგიერთი მათგანი აყვანილია ჯანმრთელობის დაზიანების რისკის შემცველ სამუშაოზე. ამ შემთხვევაში სისხლის ჯგუფის შესახებ ინფორმაციის მოთხოვნა ლეგიტიმურია. თუმცა, სხვა თანამშრომლების მიმართ, რომლებიც მხოლოდ საოფისე სამუშაოს ასრულებენ, იგივე მოთხოვნის დაწესება შეიძლება ჩაითვალის არაადეკვატური მოცულობის ინფორმაციის მოთხოვნად.

განსაკუთრებული კატეგორიის მონაცემთა პრიორიტეტული ბუნების გამო, კანონმდებელმა საერთოდ აკრძალა ამ ინფორმაციათა დამუშავება, მონაცემთა სუბიექტის წერილობითი თანხმობის გარეშე, ამავდროულად დამუშავების ლეგიტიმურ საფუძვლებში მოიხსენია მონაცემთა სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესების დაცვა, ბრალდებულთა და მსჯავრდებულთა პირადი საქმეებისა და რეესტრების წარმოება, როგორც საზოგადოებრივი, ასევე ფიზიკური პირის ჯანმრთელობის დაცვა და სხვა[86]. კანონმდებლის წინდახედული სვლა იყო, რომ მან მონაცემთა სუბიექტის წერილობითი თანხმობის ადრესატად განსაზღვრა უშუალოდ ის მონაცემთა დამმუშავებელი, რომელსაც სუბიექტმა საკუთარი ინფორმაციის დამუშავებასთან დაკავშირებით ნდობა გამოუცხადა[87].

საქართველოს კანონი „საჯარო სამსახურის შესახებ“ ითვალისწინებს საჯარო სამსახურში მუშაობის დამწყებთათვის სამედიცინო-ნარკოლოგიური ცნობის წარდგენის ვალდებულებას. ეს მოთხოვნა საჯარო დაწესებულებებისათვის წარმოადგენს მონაცემთა დამუშავების საფუძველს. კერძო სექტორში ანალოგიური მოთხოვნა შესაძლოა ეფუძნებოდეს ორგანიზაციის შინაგანაწესს ან სხვა რეგულაციას.

ასევე გასათვალისწინებელია, რომ ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია დასაქმების პროცესში შეიძლება მოთხოვნილ იქნეს მხოლოდ შესასრულებელ სამუშაოსთან დასაქმებულის შესაბამისობის დადგენის, პრევენციული მედიცინის მოთხოვნების, შრომისუუნარობის დადგენის და სოციალური უზრუნველყოფის მიზნებისათვის.

[86] ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლი;
[87] იქვე, მე-6 მუხლის მე-3 პუნქტი;

განსაკუთრებული კატეგორიის მონაცემების დამუშავების შესაძლებლობა შრომითი ვალდებულების შესრულების მიზნებისათვის არ ნიშნავს, რომ ამ საფუძვლით უნდა გამართლდეს დასაქმებულის პირად ცხოვრებაში ჩარევა. მაგალითად, თუ პირი ექიმთან მიდის ვიზიტზე სამუშაო საათების განმავლობაში, დამსაქმებელს არ აქვს უფლება მოითხოვოს დიაგნოზი. ეს წესი მოქმედებს მაშინაც კი, როდესაც დამსაქმებელს აქვს საფუძვლიანი ეჭვი, რომ პირმა სამუშაო საათები სხვა მიზნით გამოიყენა.

გარკვეულ შემთხვევებში დამსაქმებელი უფლებამოსილია, დაამუშაოს პერსონალური მონაცემები, თუ აქვს ეჭვი რომ დასაქმებული სამუშაოზე გამოცხადდა ალკოჰოლის ან ნარკოტიკული ნივთიერების ზემოქმედების ქვეშ. ასეთ დროს მნიშვნელოვანია ბალანსის დაცვა დამსაქმებლის ლეგიტიმურ ინტერესსა და დასაქმებულის უფლებას შორის.

იმ შემთხვევაში, თუ დასაქმებულს სთხოვენ, ხელი მოაწეროს მისი განსაკუთრებული კატეგორიის მონაცემების დამუშავებაზე თანხმობას, თანხმობის ტექსტი შედგენილი უნდა იყოს მარტივ და გასაგებ ენაზე, ასევე მასში აღნიშნული უნდა იყოს, რა ფორმითა და ვადით დამუშავდება მონაცემები.

დამსაქმებელმა არ უნდა შეაგროვოს პერსონალური მონაცემები, რომლებიც შეეხება პირის პოლიტიკურ შეხედულებას, რელიგიურ ან ფილოსოფიურ მრწამსს, სქესობრივ ცხოვრებას, აღნიშნული მონაცემების შეგროვება დასაშვებია მხოლოდ გამონაკლის შემთხვევებში, საქართველოს კანონმდებლობით დადგენილი წესით.

კონკურსის საწყის ეტაპზე დამსაქმებელმა თავი უნდა შეიკავოს განსაკუთრებული კატეგორიის მონაცემების შეგროვებისაგან. კითხვები, რომლებიც უკავშირდება განსაკუთრებული კატეგორიის მონაცემებს, ამოღებული უნდა იქნეს სამუშაოზე განაცხადის ფორმიდან. საჭიროების შემთხვევაში, ამ კატეგორიის მონაცემები უნდა შეგროვდეს უკვე შერჩეული კანდიდატებისგან.

ორგანიზაციები ხშირად ახდენენ ბიომეტრული მონაცემების დამუშავებას დასაქმებულთა შენობაში შესვლის/გადაადგილების, ელექტრონულ სისტემებსა და ტექნოლოგიებზე წვდომის პროცესში. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად, ბიომეტრული მონაცემების დამუშავება შესაძლებელია მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნით, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან

ასაცილებლად. კერძო დაწესებულებათა მიერ ბიომეტრული მონაცემების გამოყენება დასაშვებია საქმიანობის განხორციელების მიზნითაც, თუ ამ მიზნების მიღწევა სხვა საშუალებებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. ბიომეტრული მონაცემების დამუშავება უნდა ხდებოდეს შრომითი ხელშეკრულების ან სპეციალური რეგულაციის საფუძველზე, სადაც დეტალურად იქნება გაწერილი ამ სახის მონაცემების დამუშვების პირობები.

მაგალითად, დაუშვებელია დაწესებულების მიერ თითის ანაბეჭდების გამოყენება დასაქმებულთათვის შრომითი ანაზღაურების განსაზღვრისა და სამსახურში მათი გამოცხადების აღრიცხვის მიზნით, აღნიშნულ შემთხვევაში შესაძლებელია ანაზღაურების ან სამსახურში გამოცხადების კონტროლი სხვა საშუალებით, მაგალითად ტაბელით, აღრიცხვის ჟურნალით ან ბარათით.

ბიომეტრიული მონაცემების დამუშავება არ საჭიროებს მონაცემთა სუბიექტის თანხმობას და არის შანსი, რომ ეს მონაცემი, რომელიც ერთ დროს რაღაც კონკრეტული, სუბიექტისათვის ცნობილი მიზნით, გამოიყენეს, შემდგომშიც გამოყენებულ იქნეს არასანქცირებულად, კანონით გაუთვალისწინებელი მიზნებისთვის. ბიომეტრიულ მონაცემთა აღნიშნული წესით გამოყენება ,,მცოცავი ფუნქციის“ სახელითაა ცნობილი, და მან შეიძლება გამოიწვიოს სავალალო შედეგი საზოგადოებრივი ნდობის დაკარგვის კუთხით, დაარღვიოს ,,პროპორციულობის პრინციპი“ და მონაცემთა სუბიექტს ბევრად ნაკლები ღირებულების სარგებელი მისცეს, ვიდრე საკუთარი ბიომეტრიული მონაცემებია[88].

ბიომეტრული მონაცემების გამოყენებამდე კერძო ორგანიზაციამ პერსონალურ მონაცემთა დაცვის ინსპექტორს უნდა მიაწოდოს დეტალური ინფორმაცია ბიომეტრული მონაცემების დამუშავების შესახებ, მათ შორის, მონაცემთა დამუშავების მიზეზი, დაცვის გარანტიები და ის ინფორმაცია, რომელიც მიეწოდება მონაცემთა სუბიექტს.

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.

[88] Campisi P., Security and Privacy in Biometrics, UK, Springer, 2013, გვ. 6;

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.

4.3. დამსაქმებლის მიერ, სამსახურეობრივი ელფოსტის კონტროლი

დღევანდელ, ჩვეულ, სამუშაო გარემოში, მონაცემთა დაცვის გავრცელებული პრობლემაა, სამუშაო ადგილზე დასაქმებულთა ელექტრონული კომუნიკაციების მონიტორინგის განხორციელების დასაშვები ფარგლები. გარკვეულ შემთხვევებში დამსაქმებელს უფლება აქვს გააკონტროლოს დასაქმებულის სამსახურებრივი ელექტრონული ფოსტა. ასეთი კონტროლის შემთხვევაში, აუცილებელია დასაქმებული იყოს ინფორმირებული. ზოგჯერ სამსახურებრივი ელ-ფოსტის გამოყენება ხდება პირადი ხასიათის მიმოწერისათვისაც.

დამსაქმებელმა მიმოწერის კონტროლის დროს შეძლებისდაგვარად უნდა მოახდინოს სამსახურებრივი და პირადი კორესპონდენციის გამიჯვნა და კონტროლი განახორციელოს მხოლოდ სამსახურებრივ მიმოწერაზე.

საუკეთესო შემთხვევაში, დამსაქმებელმა უნდა შეიმუშაოს კორპორაციული ელ-ფოსტის გამოყენების წესები, სადაც იქნება ინფორმაცია დამსაქმებლის მიერ ელექტრონული ფოსტის კონტროლის შესაძლებლობის შესახებ. თუ კი დასაქმებულები სამსახურებრივ ფოსტას იყენებენ პირადი კორესპონდენციისთვის, მიზანშეწონილია პირადი ხასიათის მეილები განთავსდეს ცალკე საქაღალდეში სათანადო მითითებით (მაგალითად, „private”). დასაქმებული ინფორმირებული უნდა იყოს სარეზერვო კოპირებისა („back-up”) და მისი მიმოწერის შენახვის ვადის შესახებ.

მიჩნეულია, რომ აღნიშნული პრობლემა, შესაძლებელია, მარტივად იქნეს გადაწყვეტილი სამსახურში კომუნიკაციების საშუალებების პირადი მიზნებისთვის გამოყენების აკრძალვით. თუმცა, ამგვარი აკრძალვა, შესაძლებელია, იყოს არაპროპორციული და არარეალური. ამ მხრივ, საყურადღებოა ადამიანის უფლებათა ევროპული სასამართლოს მოცემული

გადაწყვეტილება: საქმეზე Copland v. UK[89], კოლეჯში დასაქმებულის მიმართ ხორციელდებოდა ტელეფონის, ელ-ფოსტისა და ინტერნეტის გამოყენების ფარული მონიტორინგი, დასაქმებულის მიერ, კოლეჯის საშუალებების პირადი მიზნებისთვის გამოყენების განხორციელების დასამტკიცებლად. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ სამსახურის შენობიდან განხორციელებული სატელეფონო ზარები ექცეოდა პირადი ცხოვრებისა და მიმოწერის ცნებათა ფარგლებში. შესაბამისად, სამსახურიდან განხორციელებული ზარები, გაგზავნილი ელ-ფოსტები, როგორც მიღებული ინფორმაცია, ინტერნეტის პირადი გამოყენების მონიტორინგის შესახებ, დაცულია კონვენციის მე-8 მუხლით. მოცემულ საქმეზე არ არსებობდა კონკრეტული დებულებები, რომლითაც დარეგულირდებოდა მონიტორინგის პირობები, დამსაქმებლის მიერ, დასაქმებულების მხრიდან, ტელეფონების, ელ-ფოსტისა და ინტერნეტის გამოყენებისას. შესაბამისად, ჩარევა არ შეესაბამებოდა კანონს და სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

4.4. დამსაქმებლის მიერ, ვიდეოთვალთვალის განხორციელების სამართლებრივი საფუძვლები სამუშაო ადგილზე

ვიდეოთვალთვალის სისტემა განიმარტება, როგორც სივრცის, მოვლენის, საქმიანობის ან პირის ვიზუალური/აუდიო მონიტორინგი ელექტრონული მოწყობილობის მეშვეობით[90]. ვიდეოთვალთვალის სისტემებს თავდაპირველად შეიარაღებული ძალები და ქვეყნის სხვა უსაფრთხოების საქმიანობებში მოღვაწე ორგანიზაციები იყენებდნენ. მალე მათ გზა გაიკვალეს ყოველდღიური ცხოვრების ყველა ასპექტში. მათ შორის პრევენციული ვიდეოთვალთვალის კუთხით საჯარო ადგილებში, აეროპორტებში, მაგისტრალების, საზღვრების, სანაპირო გარემოს, საწარმოო, სახლისა და პირადი უსაფრთხოების სფეროში[91].

[89] ადამიანის უფლებათა ევროპული სასამართლო, Copland v. the United Kingdom, No. 62617/00, 3 აპრილი 2000 წელი;

[90] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ, გვ. 1;

[91] Al Najjar M., Ghantous M., Bayoumi M., Video Surveillance for Sensor Platforms: Algorithms and Architectures, USA, Springer, 2013, გვ. 1-2;

ვიდეოთვალთვალი უნდა გამოიყენებოდეს მხოლოდ აუცილებელ შემთხვევებში, მონაცემთა დამმუშავებლის მხრიდან შესაბამისი გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილას განთავსებით[92].

2002 წლის სექტემბერში, მილიონობით ადამიანმა საინფორმაციო პროგრამების მეშვეობით ნახა ,,კოლის" უნივერიმაღის ავტოსადგომის ვიდეოჩანაწერი, თუ როგორ სცემდა მადელინ თაგუდი, 25 წლის დედა, საკუთარ ქალიშვილის ავტომობილის უკანა სავარძელზე. აღსანიშვნავია, რომ დედამ ქმედების განხორციელებამდე დაათვალიერა პერიმეტრი, რათა დარწმუნებულიყო, რომ ის სათვალთვალო კამერების მიერ არ დაფიქსირდებოდა. კადრები საჯაროდ გავრცელდა პოლიციის მიერ[93], რაც ვიდეოთვალთვალის განხორციელების აუცილებლობაზე მიუთითებს.

კერძო და საჯარო დაწესებულებებს შეუძლიათ მონიტორინგის მიზნით განახორციელონ შენობების ვიდეოთვალთვალი, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების, არასრულწლოვანის მავნე ზეგავლენისაგან დაცვისა და საიდუმლო ინფორმაციის დაცვის მიზნებისათვის. დასაშვებია მხოლოდ შენობის გარე პერიმეტრისა და შესასვლელის მონიტორინგი.

საჯარო და კერძო დაწესებულებებში ვიდეოთვალთვალის სისტემის გამოყენება ყველაზე პოპულარულია და მას მთელს მსოფლიოში აქტიურად იყენებენ დამსაქმებლები. კერძოდ, ავსტრალიამ დახარჯა ყველაზე ბევრი თანხა ერთ სულ მოსახლეზე, ვიდრე სხვა ინდუსტრიულმა ქვეყნებმა, ვიდეოთვალთვალის აღჭურვილობაზე, აღნიშნული კი დაარეგულირა ,,სამუშაო ადგილებზე ვიდეოთვალთვალის 1998 წლის აქტით". ვიდეოთვალთვალის გამოყენება სამუშაო პირობებში ფართოდ არის გავრცელებული ახალ ზელანდიაშიც და ხშირად ხდება პერსონალურ მონაცემთა კომისრის აპარატის ანგარიშების ყურადღების ცენტრში[94].

სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის დაყენება შეიძლება მხოლოდ გამონაკლის შემთხვევაში, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, ასევე საიდუმლო ინფორმაციის დაცვის მიზნებისათვის და თუ ამ მიზნების სხვა საშუალებით მიღწევა

[92] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ", გვ. 45;
[93] Yesil B., Video Surveillance: Power and Privacy in Everyday Life, El Paso, LFB Scholarly Publishing, 2009, გვ. 1;
[94] Privacy-Law of Civil Liberties, Edited by: Sally Ramage, NY, iUniverse inc., 2007. გვ. 122;

შეუძლებელია. საჯარო და კერძო დაწესებულებებში ვიდეოთვალთვალი ხორციელდება მხოლოდ შენობის გარე პერიმეტრსა და შესასვლელში, მონაცემთა დამმუშავებლის მიერ შესაბამისი გამაფრთხილებელი ნიშნის განთავსებით[95]. თუმცა პრაქტიკულად, სამუშაო ადგილებზე დამსაქმებელთა მიერ ვიდეოთვალთვალის სისტემის დამონტაჟების ძირითადი მიზანია ის, რომ აკონტროლონ დასაქმებულთა საქმიანობა, მათი ვიზუალური მხარე, მოქმედებები. აღნიშნულს ამტკიცებს პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ 2015 წლის საანგარიშო პერიოდში ორი მსხვილი პროდუქციის რეალიზატორი კომპანიის 500-500 ლარით დაჯარიმების ფაქტი. კერძოდ, კომპანიების მიზანს, ვიდეოკონტროლისას საკუთრების დაცვასა და პირის უსაფრთხოებასთან ერთად, წარმოადგნედა დასაქმებულ პირთა მიერ გაწეული მომსახურების კონტროლის ხარისხი, რაც არაკანონიერი მიზანია[96]

მაგალითად, ბანკში მოლარის სამუშაო მაგიდასთან ვიდეოთვალთვალის განხორციელება საჭიროა მოლარის და ბანკის უსაფრთხოების დასაცავად, რათა თავდასხმის შემთხვევაში უსაფრთხოების სამსახურმა მოახდინოს სწრაფი რეაგირება.

გასათვალისწინებელია, რომ ვიდეოთვალთვალი ავტომატურად არ გულისხმობს აუდიო მონიტორინგს (ხმის ჩაწერას). შესაბამისად, ვიდეოთვალთვალის განხორციელებისას არ უნდა იყოს შესაძლებელი დასაქმებულთა საუბრის მოსმენა, გარდა გამონაკლისი შემთხვევებისა (როგორიცაა უსაფრთხოების ზომები და სხვა), რის შესახებაც უნდა ეცნობოს დასაქმებულს.

შესაბამის კერძო ან საჯარო დაწესებულებაში დასაქმებული ყველა პირი წერილობითი ფორმით უნდა იყოს ინფორმირებული სამუშაო ადგილზე ვიდეოთვალთვალის განხორციელებისა და სუბიექტის უფლებების შესახებ. დაწესებულებებმა უნდა უზრუნველყონ ვიდეო კონტროლის ზონაში შესაბამისი გამაფრთხილებელი ნიშნების თვალსაჩინო ადგილას განთავსება.

ვიდეოთვალთვალის განხორციელება დაუშვებელია გამოსაცვლელ ოთახებსა და ჰიგიენისათვის განკუთვნილ ადგილებში. შშ-ის ფედერალურმა სასამართლომ თითქმის ერთსულოვნად დაადასტურა, რომ ხმის ჩაწერის გარეშე

[95] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-12-ე მუხლის მე-2 პუნქტი;

[96] იხ. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ", გვ. 47-48;

განხორციელებული ვიდეოთვალთვალი არ არის აკრძალული შესაბამისი კანონით (ECPA), თუმცა ვიდეოთვალთვალი, რომელიც შესაძლებლობას იძლევა, რომ ჩაწერილ იქნეს საუბრები არაკანონიერია[97]. პერსონალურ მონაცემთა დაცვის ინსპექტორმა საკუთარ ანგარიშებში მოიხსენია სამი ფარმაცევტული კომპანიის მიერ ვიდეოკონტროლისა და აუდიოჩაწერის განხორციელებით მომხმარებელთა პირადი ცხოვრების უფლების დარღვევის ფაქტი და აღნიშნა, რომ მიუხედავად სააფთიაქო ქსელის კანონიერი მიზნისა - გაეკონტროლებინათ საკუთარი მომსახურეობის ხარისხი, მომხმარებლის პირად ცხოვრებაში უხეშ და არაპროპორციულ ჩარევად აღიქმებოდა აუდიოჩაწერის მეშვეობით ფარმაცევტსა და მომხმარებელს შორის არსებული კომუნიკაცია[98].

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი, საჯარო და კერძო დაწესებულებაში ვიდეომონიტორინგთან ერთად, აუდიოჩაწერის განხორციელების შესაძლებლობას არ ითვალისწინებს, თუმცა კანონმა აღნიშნული აუცილებლად პირდაპირ უნდა განსაზღვროს, რათა ყოველი კონკრეტული შემთხვევა მიზნის მიღწევის პროპორციულ და ადეკვატურ პრინციპთან არ იქნეს შესაფასებელი[99].

[97] Privacy-Law of Civil Liberties, Edited by: Sally Ramage, NY, iUniverse inc., 2007. გვ. 122;

[98] პერსონალურ მონაცემთა დაცვის ინსპექტორის 2015 წლის ანგარიში ,,პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ", გვ. 48-49;

[99] ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მე-4 მუხლის გ) პუნქტი;

დასკვნა

ნაშრომში წამოჭრილმა პრობლემებმა გამოავლინა, რომ მონაცემთა დამუშავებასთან დაკავშირებული ხშირი და განმეორებითი დარღვევები განპირობებულია მათი გადაჭრის არსებული გზების არასრულფასოვნებით და, ხშირ შემთხვევაში, დამმუშავებლისათვის, პასუხისმგებლობის ზომების ნაკლები სიმკაცრით. ფაქტია, რომ, მონაცემთა დამმუშავებლისთვის, მოცემულ შემთხვევაში კი ბიზნეს სამართლის სუბიექტისათვის, პერსონალურ მონაცემთა კანონის დარღვევისას, ნაკლებად ,,მტკივნეულია" გაფრთხილება ან ჯარიმა, იმ მიზანთან შედარებით, რასაც ის მონაცემთა არაკანონიერად დამუშავებით აღწევს. 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[100]“.

ნაშრომში დასმული ისეთი პრობლემები, როგორიცაა მონაცემთა ნახევრად ავტომატური ან არაავტომარი საშუალებებით დამუშავებისას, მონაცემთა დამმუშავებლის უკონტროლო მდგომარეობა, უნდა მოგვარდეს საკანონმდებლო დონეზე და ისე უნდა იქნეს დარეგულირებული, რომ დამმუშავებელი ვალდებული იყოს მსგავსი დამუშავების მეთოდების გამოყენების დროს დაექვემდებაროს კონტროლს. პრობლემატურია აგრეთვე ვიდეომონიტორინგის განხორციელების რეალური მიზნების გაუთვითცნობიერებელი სიტუაცია. ვიდეომონიტორინგი თავისთავად ემსახურება დადებით მიზნებს, თუმცა დამსაქმებელი ვერ ავლებს ზღვარს საჭიროებასა და პირად სივრცეში შეჭრას შორის. შესაბამისად, ხშირია, დამსაქმებლის მიერ, დასაქმებული პირადი მონაცემების უხეში დარღვევა, განისაზღვრელი ვადით დამუშავება/შენახვა და ა.შ.

[100] 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-facetougher-punishments-than-fines [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];

ნაშრომში დასმული პრობლემა ეხება აგრეთვე გენეტიკური მონაცემების დამუშავებასთან დაკავშირებული მცირემასშტაბიან რეგულირებას, თუმცა აღნიშნული ინფორმაცია რეალურად ძალიან მნიშვნელოვანია და კანონმა ის უფრო ფართოდ უნდა დაარეგულიროს. აღსანიშნავია აგრეთვე, რომ აუცილებელია სამეწარმეო სმაართალში არსებული აქტების მოდერნიზაცია და ,,პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონთან ჰარმონიზაცია. გარდა ამისა, უშუალოდ ბიზნეს სამართლის წარმომადგენელთა მხრიდან, მოხდეს პერსონალურ მონაცემთა დაცვის გარანტიების შექმნა და მხარდაჭერა, რათა მონაცემთა სუბიექტს გააჩნდეს ნდობა მათ მიმართ.

მნიშვნელოვანია სასამართლოთა როლი ნორმის სწორად და ადეკვატურად განმარტების კუთხით, ვინაიდან მათი გადაწყვეტილებები სავალდებულოა საქართველოს მთელს ტერიტორიაზე და სამოქმედო მიმართულებას წარმოადგენს მონაცემთა დამმუშავებლისათვის. აუცილებელია აგრეთვე, პერსონალურ მონაცემთა დაცვის პროპაგანდა, რაც უნდა განხორციელდეს მასობრივი საშუალებების მეშვეობით დარღვევებისა და შეფარდებული პასუხისმგებლობის ზომების გაშუქებით, რათა თავად მონაცემთა სუბიექტის როლიც გააქტიურდეს კანონმდებლობის ცოდნისა და საკუთარი უფლებების პრაქტიკულად დაცვის მოთხოვნის კუთხით.

საბოლოოდ შეიძლება ითქვას, რომ ქართულ კანონმდებლობასა და პრაქტიკას მონაცემთა დამუშავებისა და მონაცემთა სუბიექტისთვის დაცვის გარანტიების სრულყოფის კუთხით, ჯერ კიდევ ბევრი ხარვეზი გააჩნია, თუმცა ყველაფერი გამოსწორებადია, თუკი გათვალისწინებულ იქნება ამ მიმართულებით გამოცდილი ქვეყნების რეგულირება და პრაქტიკა.

ბიბლიოგრაფია

ქართულენოვანი ლიტერატურა

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. საკონსტიტუციო მართლმსაჯულება საქართველოში: სამართალწარმოების ძირითადი სისტემური პრობლემები, გეგენავა დ., თბილისი, ,,დავით ბატონიშვილის სამართლის ინსტიტუტი“, 2012;
3. პერსონალური მონაცემების დაცვა, საზღვარგარეთის ქვეყნების კანონმდებლობის ანალიზი, ხათუნა ყვირალაშვილის რედაქტორობით, თბილისი, 2007;
4. ადამიანის უფლებები და საქართველოს საკონსტიტუციო სასამართლოს სამართალწარმოების პრაქტიკა, ტუღუში თ., ბურჯანაძე გ., მშვენიერაძე გ., გოცირიძე გ., მენაბდე ვ., თბილისი, საქართველოს ახალგაზრდა იურისტთა ასოციაციის გამომცემლობა, 2013;
5. საკონსტიტუციო კონტროლი და ღირებულებათა წესრიგი საქართველოში, ზოიძე ბ., თბილისი, (GTZ), 2007;
6. პერსონალურ მონაცემთა დაცვის ინსპექტორის 2013-2014 წლის ანგარიში, გვ. 25, ხელმისაწვდომია: www.pdp.ge;
7. „ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო“, კორკელია, კ., სტატიათა კრებული, ჯოხაძე გ., სტატია „პერსონალურ მონაცემთა დაცვა ადამიანის უფლებათა კონტექსტში: საქართველოს მაგალითი, გამოწვევები ტენდენციები, 2011 წელი, თბილისი, გვ. 327-329;
8. სამაგისტრო ნაშრომი „პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას“, თამთა არჩუაძე, აღმოსავლეთ ევროპის უნივერსიტეტი, 2016 წელი, გვ.9-18;
9. მონაცემთა დაცვის ევროპული სამართალი, გოშაძე კ., თბილისი, გამომცემლობა „იურისტების სამყარო“; 2015 წელი, გვ. 252;
10. თემიდა, სამეცნიერო პრაქტიკული ჟურნალი, უგრეხელიძე ნ., სტატია „პერსონალურ მონაცემთა დაცვის საკანონმდებლო ბაზა საქართველოში“, 2011 წელი, №5(7), გვ. 162;

11. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები პირდაპირი მარკეტინგის მიზნებისათვის პერსონალურ მონაცემთა დამუშავების შესახებ, გვ. 1;
12. მუხლი 29, სამუშაო ჯგუფი (2011), მოსაზრება 15/2011 თანხმობის ცნების შესახებ, WP 187, ბრიუსელი,13 ივლისი 2011 წელი, გვ. 12. 100 იქვე, გვ. 15;
13. ევროპული პარლამენტისა და საბჭოს 2002 წლის 12 ივლისის დირექტივა 2002/58/EC ელექტრონული კომუნიკაციების სექტორში პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა დამუშავების შესახებ OJ 2002 L 201 (პირადი ცხოვრებისა და ელექტრონული კომუნიკაციების დირექტივა);
14. ევროკავშირისა (EU) და გაეროს განვითარების პროგრამის (UNDP) მხარდაჭერით შექმნილი რეკომენდაცია კომერციული ბანკის მიერ პერსონალური მონაცემების დამუშავების შესახებ, გვ. 18, 2019 წელი;
15. საბანკო ზედამხედველობის ბაზელის კომიტეტის „სახელმძღვანელო ფულის გათეთრების და ტერორიზმის დაფინანსების რისკის ჯანსაღი მენეჯმენტის შესახებ," ხელმისაწვდომია https://www.bis.org/bcbs/publ/d405.htm გვ. 7;
16. ევროპის საბჭო, მინისტრთა კომიტეტი (1989), რეკომენდაცია Rec89(2), წევრი ქვეყნებისთვის პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე, 18 იანვარი 1989 წელი. იხ. შემდგომ, 108-ე კონვენციის საკონსულტაციო კომიტეტი, პერსონალურ მონაცემთა დასაქმების მიზნებისთვის გამოყენების თაობაზე რეკომენდაციის No. R (89) 2 კვლევა და პროექტის შეთავაზება მოცემული რეკომენდაციის გადასინჯვის თაობაზე, 9 სექტემბერი 2011 წელი;
17. პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატის რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ, გვ. 1;
18. პერსონლურ მონაცემთა დამუშავებისა და საჯაროობის სამართლებრივი მოწესრიგება საავტორო სამართლებრივ დაცვასთან მიმართებით, ბეჟაშვილი ზ., ჟ. ,,ადმინისტრაციული სამართლის პრობლემები", 2013, გვ. 40;
19. ახალი თაობა, ხურცილავა ნ., „რა ბედი ელის პერსონალურ მონაცემებს" თბილისი, 2014 წლის 29 იანვარი, №23, გვ.7;

უცხოენოვანი ლიტერატურა

1. Tereza M.Payton and Theodore Claypoole „Privacy in the age of big data“;
2. 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-improveyour-privacy-policy-or-lose-your-data-4796165 [უკანასკნელად გადამოწმებულია 2017 წლის თებერვალში];
3. Conceptualizing Privacy, Solove D., California Law Review, 2002, Issue 4;
4. „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];
5. The Right To Privacy, Samuel D. Warren & Luis D. Brandies, Published in the 2015 Hardcover Edition By Quid Pro Books;
6. Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof, Prof.dr. Lokke Moerel, 2014,ხელმისაწვდომია: http://www.debrauw.com/wpcontent/uploads/NEWS%20%20PUBLICATIONS/Moerel_oratie.pdf [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];
7. Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Karanja S., Netherlands, Martinus Nijhoff Publishers, 2008. გვ. 123;
8. Human Rights in Europe: A Study of the European Convention on Human Rights, A. Robertson & J. Merrills, 1993, 1;
9. Постатейный комментарий к Федеральному закону О персональных данных, ПЕТРОВ М.И., Россия, Юстицинформ, 2007, გვ. 28;
10. „Electronic Frontier Foundation gives messaging app one star out of five for security“, Shepher A., ხელმისაწვდომია: http://www.itpro.co.uk/security/24839/whatsapp-among-worst-ratedcompanies-in-privacy-study, [უკანასკნელად გადამოწმებულია 2017 წლის აპრილში];
11. Direct Marketing: A Step-by-step Guide to Effective Planning and Targeting, Mullin R., Great Britain, Kogan Page, 2002, გვ. 1;
12. Commonsense Direct and Digital Marketing, London and Philadelphia, Bird B., Kogan Page, 2007, 5th edition, გვ. 8;

13. Direct Marketing in Practice, Housden M., Thomas B., London and NY, Routledge, Taylor and Francis Group, 2002, გვ. 3;
14. Membership Development: An Action Plan for Results, Rich P., Hines D., USA, Jones and Bartlett Publishers, 2006, გვ. 116;
15. Security and Privacy in Biometrics, Campisi P., UK, Springer, 2013, გვ. 6;
16. Video Surveillance for Sensor Platforms: Algorithms and Architectures, Al Najjar M., Ghantous M., Bayoumi M., USA, Springer, 2013, გვ. 1-2;
17. Video Surveillance: Power and Privacy in Everyday Life, Yesil B., El Paso, LFB Scholarly Publishing, 2009, გვ. 1;
18. „Information Commissioner calls for threat of prison sentences after rental car employee sells customer data“, Curtis J., see: http://www.itpro.co.uk/data-protection/25848/ico-data-thieves-must-facetougher-punishments-than-fines [უკანასკნელად გადამოწმებულია 2017 წლის მაისში];
19. Privacy-Law of Civil Liberties, Edited by: Sally Ramage, NY, iUniverse inc., 2007. გვ. 122.

გამოყენებული სასამართლო გადაწყვეტილებები

1. Decision by the Data Inspection Board from 20 sep. 2005. No 763-2005, წიგნიდან: Kirchberger K., Cyber Law in Sweden, By Christine, USA, Kluwer Law International, 2011,197;
2. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის N1/1/625, 640 გადაწყვეტილება საქმეზე ,,საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები - გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა - საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ";
3. საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის №2/3/406,408 გადაწყვეტილება საქმეზე, ,,საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“;

4. მართლმსაჯულების ევროპული კავშირის სასამართლო,C-101/01, Lindqvist, 6 ნოემბერი 2003 წელი;
5. მართლმსაჯულების ევროპული კავშირის სასამართლო, C-543/09, Deutsche Telekom AG v. Germany, 5 მაისი 2011 წელი; იხ. ძირითადად პარაგ. 53 და 54;

გამოყენებული ნორმატიული მასალა

1. Convention for the protection of Human Rights and fundamental freedoms. 1650;
2. 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;
3. 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;
4. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, ხელმისაწვდომია: www.matsne.gov.ge;
5. საქართველოს ზოგადი ადმინისტრაციული კოდექსი, 25/06/1999 წლის მდგომარეობით;
6. ევროპის საბჭო, ადამიანის უფლებათა ევროპული კონვენცია CETS No. 005, 1950 წელი;
20. Foreign Account Tax Compliance Act (FATCA) აქტი უცხოური ანგარიშის საგადასახადო შესაბამისობის შესახებ და მის შესაბამისად 2015 წლის 10 ივლისს გაფორმებული „შეთანხმება ამერიკის შეერთებული შტატების მთავრობასა და საქართველოს მთავრობას შორის საერთაშორისო საგადასახადო ვალდებულებების შესრულების გაუმჯობესების და უცხოური ანგარიშის საგადასახადო შესაბამისობის აქტის (FATCA) შესრულების მიზნით“ (რატიფიცირებულია საქართველოს მთავრობის მიერ 2015 წლის 18 სექტემბერი);
21. უკანონო შემოსავლის ლეგალიზაციის აღკვეთის ხელშეწყობის შესახებ საქართველოს კანონი, მუხლი 6, პუნქტი 7;

ინტერნეტ-რესურსები:

1. www.pdp.ge
2. www.catalog.pdp.ge
3. www.matsne.gov.ge
4. www.echr.goe.int