პერსონალურ მონაცემთა დაცვის აქტუალური საკითხები

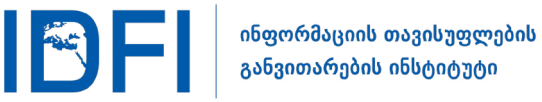
ესეების კრებული

თბილისი | 2021

პერსონალურ მონაცემთა დაცვის აქტუალური საკითხები

ესეების კრებული

თბილისი ● 2021



ესეების კრებული მომზადდა პროექტის „პერსონალური მონაცემების დაცვის მხარდაჭერა საქართველოში“ ფარგლებში. პროექტი დაფინანსებულია საქართველოში ნიდერლანდების საელჩოს მიერ. ესეების შინაარსზე სრულად არიან პასუხისმგებელი მათი ავტორები. კრებულში გამოხატული მოსაზრებები შეიძლება არ ასახავდეს ნიდერლანდების საელჩოს, „ინფორმაციის თავისუფლების განვითარების ინსტიტუტისა“ და სახელმწიფო ინსპექტორის სამსახურის პოზიციას.

ესეების მომზადებაში გაწეული დახმარებისთვის მადლობას ვუხდით სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩებს: ნინო ჯავახიშვილს, ნინო ბოქოლიძეს, გიორგი აბულაძეს, ნათია ეგუტიძეს, დონარი დონდარიძეს, ზეინაბ შავაძეს, გვანცა სოფრომაძეს, გიორგი ღარიბაშვილს და ნინო მაჭარაშვილს.

სარჩევი

წინასიტყვაობა 4

პერსონალურ მონაცემთა დაცვა და საჯარო ინფორმაციის ხელმისაწვდომობა 6

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა 14

პერსონალური მონაცემების დაცვა და საჯარო ინფორმაციის ხელმისაწვდომობა 20

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება 29

კონფლიქტი პერსონალურ მონაცემთა დაცვის უფლებასა და საჯარო ინფორმაციის ხელმისაწვდომობის უფლებას შორის და მისი დაძლევის კონსტიტუციურ-სამართლებრივი პერსპექტივები 39

პერსონალური მონაცემების დაცვა შრომის სამართალში 46

მონაცემთა უსაფრთხოების თანამედროვე გამოწვევები 60

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა (პანდემიის პერიოდში დაწესებული ცალკეული შეზღუდვის განხილვის მაგალითზე) 67

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა 82

სახის ამომცნობი სისტემების მიერ პერსონალური მონაცემების დამუშავება 90

პერსონალური მონაცემების დამუშავება მედია საშუალებების მიერ 102

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება TIK-TOK-ის მაგალითზე 118

სახის ამომცნობი სისტემის მიერ პერსონალურ მონაცემთა დამუშავება 128

შრომით ურთიერთობებში პერსონალური მონაცემების დაცვა ეროვნული კანონმდებლობისა და საერთაშორისო პრაქტიკის ანალიზზე 143

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება 152

წინასიტყვაობა

თანამედროვე ტექნოლოგიები ჩვენი პროფესიული, პირადი და სოციალური ცხოვრების განუყოფელი ნაწილია. ციფრული განვითარება და ტექნოლოგიური პროგრესი ადამიანთა ყოველდღიური ცხოვრების ფაქტობრივად ყველა ასპექტზე აისახება, ასევე გავლენას ახდენს ხელისუფლებასა და მოქალაქეებს შორის ურთიერთობაზე.

მიუხედავად არაერთი სარგებლისა, ციფრული ეპოქა გარკვეულ გამოწვევებს ქმნის პირადი ცხოვრებისა და მონაცემების დაცვის კუთხით, რადგან გროვდება დიდი მოცულობის პერსონალური ინფორმაცია, რომელიც სულ უფრო კომპლექსური გზებით მუშავდება. შესაბამისად, სამართლებრივი ჩარჩოსა და პრაქტიკის ადაპტირება ახალ გამოწვევებსა და რისკებთან განსაკუთრებულ მნიშვნელობას იძენს.

პირადი ცხოვრების ხელშეუხებლობის უფლება ადამიანებს თავიანთი პიროვნების, შეხედულებებისა და ურთიერთობების თავისუფლად განვითარების შესაძლებლობას ანიჭებს. პერსონალურ მონაცემთა დაცვა მჭიდროდ არის დაკავშირებული ადამიანის ავტონომიურობასთან. ნებისმიერ პირს უნდა შეეძლოს განკარგოს და გააკონტროლოს საკუთარი ინფორმაციის დამუშავების ფარგლები. ამავე დროს, ხშირად წარმოიშობა კონფლიქტი სხვადასხვა სამართლებრივ სიკეთეს შორის და მათი სამართლიანი და ეფექტიანი დაბალანსების საკითხი განსაკუთრებულ მნიშვნელობას იძენს.

ჩვენი მიზანია ხელი შევუწყოთ სტუდენტების ცოდნის ამაღლებას პერსონალური მონაცემების დაცვის თაობაზე, ასევე წავახალისოთ აკადემიური მსჯელობა და დისკუსიები პრობლემურ ასპექტებზე.

დიდი მადლობა მინდა გადავუხადო საქართველოში ნიდერლანდების საელჩოს პროექტის მხარდაჭერისთვის, ასევე სახელმწიფო ინსპექტორის სამსახურს ნაყოფიერი თანამშრომლობისთვის. განსაკუთრებული მადლობა ნაშრომების ავტორებს, რომლებმაც შეძლეს პერსონალურ მონაცემთა დაცვის აქტუალური და პრობლემური საკითხები საინტერესო და ორიგინალური სახით მიეწოდებინათ მკითხველისთვის.

ქეთევან კუკავა

კანონის უზენაესობისა და ადამიანის უფლებების მიმახთულების ხელმძღვანელი
ინფოხმაციის თავისუფლების განვითახების ინსტიტუტი (IDFI)

ბოლო ათწლეულის მანძილზე, ევროკავშირთან დაახლოების პროცესის პარალელურად, პერსონალურ მონაცემთა დაცვის კანონმდებლობამ მნიშვნელოვანი პროგრესი განიცადა საქართველოში: დაიხვეწა მონაცემთა დაცვის სტანდარტები, გაძლიერდა საზედამხედველო ორგანოს ინსტიტუციური დამოუკიდებლობა და გაიზარდა მისი უფლებამოსილება. მიუხედავად ამისა, მსოფლიოში მიმდინარე რეფორმების, გლობალური და ადგილობრივი გამოწვევების ფონზე, მონაცემების დაცვის თანამედროვე, მაღალი სტანდარტის დასამკვიდრებლად ჯერ კიდევ ბევრი ნაბიჯია გადასადგმელი.

დღევანდელ სამყაროში, როცა, მონაცემების შეგროვებისა და დამუშავების მასშტაბი იზრდება, ტექნოლოგიები კი ვითარდება, განსაკუთრებულ ყურადღებას საჭიროებს მოქალაქეების ინფორმირებულობა. ტექნოლოგიური პროგრესის პარალელურად, ადამიანებმა უფრო ნაკლები იციან თუ ვინ და რა მოცულობით ამუშავებს მათ შესახებ ინფორმაციას, რაც მათ უკარგავს შესაძლებლობას, აკონტროლონ ამ ინფორმაციის გავრცელების ფარგლები.

სახელმწიფო ინსპექტორის სამსახური 2013 წლიდან საზოგადოების ცნობიერების ასამაღლებლად არაერთ აქტივობას ატარებს. ესეების კონკურსის მიზანიც სწორედ პერსონალური მონაცემების დაცვის მნიშვნელობის შესახებ საზოგადოების, განსაკუთრებით კი, სტუდენტების ცნობიერების ამაღლებაა. ესეები ეხმაურება ისეთ აქტუალურ საკითხებს როგორიცაა პერსონალური მონაცემების დაცვა და საჯარო ინფორმაციის ხელმისაწვდომობა, პერსონალური მონაცემების დაცვა თანამედროვე ტექნოლოგიების გამოყენებისას, შრომით ურთიერთობებში, ვიდეოთვალთვალის განხორციელებისას. ვიმედოვნებთ, რომ წარმოდგენილი ნაშრომები საინტერესო იქნება მკითხველისთვის და წაახალისებს სამომავლო დისკუსიებს ამ სფეროებში.

დიდ მადლობას ვუხდით საქართველოში ნიდერლანდების სამეფოს საელჩოსა და ინფორმაციის თავისუფლების განვითარების ინსტიტუტს (IDFI), რომელთა მხარდაჭერითა და თანამშრომლობით გახდა შესაძლებელი ამ პროექტის განხორციელება. ნაშრომების ავტორებს კი წარმატებებს ვუსურვებ სამომავლო საქმიანობაში.

საღომე ბახსოღიანი

სახელმწიფო ინსპექტორის მოადგილე

პერსონალურ მონაცემთა დაცვა და საჯარო ინფორმაციის ხელმისაწვდომობა

ავტორი: ანა არუთუნიანი[1]
სამცხე-ჯავახეთის სახელმწიფო უნივერსიტეტი

1. შესავალი

პერსონალური მონაცემები და საჯარო ინფორმაცია ერთმანეთის მიმართ კონკურირებადი ცნებებია. მათი შეპირისპირების თუ თანაარსებობის უკეთ წარმოსაჩენად, ნაშრომში განხილული იქნება პერსონალური მონაცემების დაცვასთან დაკავშირებული თანამედროვეობის გამოწვევები, ასევე, საჯარო ინფორმაციის ხელმისაწვდომობის როლი ქვეყნის დემოკრატიული განვითარებისთვის. აღნიშნულის პარალელურად კი გაანალიზდება დასახელებული ორი მნიშვნელოვანი ინსტიტუტის ძირითადი მახასიათებლები.

2. რა არის პერსონალური მონაცემები და თანამედროვე ეპოქაში რა გამოწვევებთან არის დაკავშირებული მათი დაცვა?

ვთანხმდებით იმაზე, რომ ინტერნეტ სივრცე ძალიან ბევრ შესაძლებლობას გვაძლევს და ეს შეგვიძლია სასარგებლოდ გამოვიყენოთ. თუმცა, გარდა დადებითისა, აქვს უარყოფითი მხარეებიც, რომლებიც ხშირ შემთხვევაში ადვილად შესამჩნევია. თანამედროვე ეპოქაში ინტერნეტი გლობალურ საკომუნიკაციო და საინფორმაციო საშუალებად იქცა, რაც დიდი მოცულობით პერსონალური მონაცემების ინტერნეტში დაგროვებას განაპირობებს. აღნიშნულ პროცესებში, პერსონალურ მონაცემთა არასათანადო დაცვა ზრდის მონაცემთა კანონსაწინააღმდეგო მიზნით გამოყენების რისკებს და საფრთხის ქვეშ აყენებს ინტერნეტის მომხმარებელთა პირადი ცხოვრების ხელშეუხებლობას. შესაბამისად, მნიშვნელოვანია, რომ მოქალაქეებს ჰქონდეთ ინფორმაცია ინტერნეტ სივრცის გამოყენებასთან დაკავშირებული რისკებისა და მათი უფლებების დაცვის შესახებ.

დღეს ადამიანებს ნაკლებად გვაქვს გამიჯნული ონლაინ და რეალურ სივრცეში არსებული სანაცნობო წრე. ჩვენ ხშირ შემთხვევაში ინტერნეტის მეშვეობით ვურთიერთობთ იმ ადამიანებთან, ვისთანაც რეალურ სამყაროში კომუნიკაცია არ გვაქვს. თუ გიფიქრიათ, რა რაოდენობის მონაცემები ვრცელდება ინტერნეტ სივრცეში – რამდენი ვიდეო იტვირთება, რამდენი მოთხოვნა იგზავნება გუგლის საძიებო სისტემაში? თითოეული გაზიარება, თითოეული დაწერილი პოსტი თუ ატვირთული სურათი სამუდამოდ ციფრულ მონაცემთა ნაწილი ხდება და მნიშვნელოვნად ზრდის მის საერთო მოცულობას. ბმულზე ჩვენი ყოველი გადასვლაც კვალს ტოვებს ციფრულ სამყაროში და ჩვენ შესახებ გარკვეული სახის ინფორმაციას იძლევა.

[1] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნინო ჯავახიშვილი.

ბოლო პერიოდში საკმაოდ აქტუალურია პერსონალური მონაცემების დაცვასთან დაკავშირებული საკითხები. საქართველოში პერსონალური მონაცემები დაცულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, რომლის მიზანია პერსონალური მონაცემის დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა. საქართველოში მონაცემთა დამუშავების კანონიერებას სახელმწიფო ინსპექტორი აკონტროლებს. პერსონალური მონაცემები არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.[2]

ციფრულმა ტექნოლოგიებმა შეცვალა და გარკვეულწილად გააიოლა ადამიანთა შორის კომუნიკაცია. ჩვენი მონაცემების ინტერნეტში ყველასთვის ხელმისაწვდომი ფორმით გასაჯაროებამ შესაძლოა არასასურველი ზეგავლენა მოახდინოს ჩვენზე (გავხდეთ ბულინგის ან სხვა სახის არასასურველი მოპყრობის ობიექტი). როგორც რეალურ, ისე ონლაინ სამყაროში არსებული ურთიერთობები, მხოლოდ პოზიტიურ კომუნიკაციას არ შეიცავს და ორივე ტიპის ურთიერთობებში ვხვდებით ბულინგის[3] შემთხვევებს. აშშ-ს, კანადისა და ევროპული ქვეყნების მონაცემების თანახმად, მოსახლეობის 20% გამხდარა კიბერბულინგის მსხვერპლი. კიბერბულინგიც, ტრადიციული ბულინგის მსგავსად, აგრესიის, ჩაგვრის და სისტემატური ხასიათის მქონე ძალადობის გავრცელებას უწყობს ხელს. თუმცა, მას ფსიქოლოგიური ძალადობის კიდევ უფრო მეტი გამოხატვის საშუალება აქვს. ამ შემთხვევაში მაღალია ანონიმურობა, ანუ უფრო მეტია იმის საშუალება, რომ კიბერაგრესორმა გამოხატოს ის, რასაც პირისპირ არ ან ვერ გამოხატავს. კიბერბულინგს არ სჭირდება ფიზიკური ძალის გამოყენება ან ფსიქოლოგიური ზეწოლის გამოყენებისათვის პირისპირ შეხვედრა. კიბერბულინგის და ზოგადად კიბერდანაშაულის განმახორციელებელს ანუ კიბერაგრესორს შეუძლია ზემოთ ხსენებული ქმედებათაგან, განახორციელოს ნებისმიერი, ნებისმიერ დროს და ნებისმიერი პირის მიმართ. აქედან გამომდინარე, მოძალადის ტიპი ონლაინ და ოფლაინ სივრცეში ერთმანეთისაგან განსხვავდება, რადგან ონლაინ სივრცეში რთულია მოძალადე პიროვნების იდენტიფიკაცია და კიბერბულინგის შედეგებიც ვირტუალურ სივრცეში შეიძლება მეტად მძიმე აღმოჩნდეს, ვიდრე რეალურ სივრცეში.

სათანადო უსაფრთხოების ზომების გატარებითა და დაცული ტექნოლოგიური საშუალებებით შესაძლებელია პერსონალური მონაცემების უკანონო გამოყენებასთან დაკავშირებული რისკების შემცირება. ამასთან დაკავშირებით, აღსანიშნავია სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები მოსახლეობის მიმართ იმასთან დაკავშრებით, რომ არ განათავსონ ინტერნეტში ისეთი მონაცემები, როგორიც არის სახლის მისამართი, ტელეფონის ნომერი, პაროლი და სხვა.

მომხმარებელი უნდა დაინტერესდეს შემდეგი ინფორმაციით: ვინ ამუშავებს (აგროვებს, ინახავს, ცვლის და ა. შ.) მის შესახებ მონაცემებს? რამდენად აუცილებელია კონკრეტული მონაცემის მიწო-

[2] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ ქვეპუნქტი.

[3] ბულინგი განიმარტება, როგორც აგრესიის ხშირი გამოვლენა ადამიანის ან ადამიანთა ჯგუფის მხრიდან სხვა ადამიანის ან ადამიანთა ჯგუფის მიმართ.

დება? როგორ მოხდება ამ მონაცემების გამოყენება და რა შედეგი მოჰყვება მას? მონაცემთა დამმუშავებელი კი ვალდებულია სუბიექტს ეს ინფორმაცია მიაწოდოს.

გაციფრულების პროცესი, რომელიც ისედაც სწრაფად მიმდინარეობდა, დააჩქარა მსოფლიოში არსებულმა ეპიდემიურმა ვითარებამ. დისტანციურ სწავლებაზე გადავიდნენ საგანმანათლებლო დაწესებულებებიც (სკოლები, უნივერსიტეტები). ონლაინ შეხვედრების, ონლაინ-სწავლების ამსახველი მასალა (ფოტო, ვიდეო გამოსახულება) წარმოადგენს პირის პერსონალურ მონაცემებს, რაც გათვალისწინებული უნდა იქნას მათი გასაჯაროებისას. თანამედროვე ტექნოლოგიებმა დისტანციურად მუშაობა მარტივი გახადა, თუმცა ასეთ დროს დღის წესრიგში დგება სამსახურებრივი ინფორმაციის კონფიდენციალობის დაცვისა და უსაფრთხოების საკითხი. ორგანიზაციათა უმეტესობამ უკვე მიმართა დისტანციურად მუშაობის რეჟიმს.

COVID-19-ის (ახალი კორონავირუსი) გავრცელების მასშტაბის ზრდასთან ერთად, საზოგადოებაში ჩნდება კითხვები ვირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით. შექმნილ ვითარებაში, პერსონალურ მონაცემთა დამუშავების საკითხებზე, რეკომენდაციები გაიცა სხვადასხვა ქვეყნის მონაცემთა დაცვის საზედამხედველო უწყებების მხრიდან. სახელმწიფო ინსპექტორის სამსახურმა შეიმუშავა რეკომენდაციები, რომლებიც ვიდეო თუ წერილობითი სახით გაავრცელა საზოგადოებაში. ამ პერიოდის განმავლობაში გაიზარდა მოქალაქეთა ცნობიერების დონე „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიმართ, რომელიც პერსონალურ მონაცემთა დაცვის ზოგად წესებსა და მოთხოვნებს ადგენს.

3. რა არის საჯარო ინფორმაცია და რატომ უნდა იყოს ის ხელმისაწვდომი?

მიუხედავად სხვადასხვა ქვეყნის მიერ საჯარო ინფორმაციის განსხვავებული რეგულირებისა, მისი არსი უნივერსალურია. თითქმის ყველა მათგანს: ინფორმაციის თავისუფლების შესახებ კანონებს, ინფორმაციის ხელმისაწვდომობის შესახებ რეგულაციებს, გამჭვირვალობის სტრატეგიებს, ინფორმაციის ღიაობის შესახებ შესაბამის აქტებს, ერთი საერთო აქვს და ეს არის საზოგადოებისთვის ინფორმაციის ხელმისაწვდომობის უზრუნველყოფა, რაც ორ ძირითად პრინციპს მოიცავს:

- ინფორმაციის გაცემა მოთხოვნის შესაბამისად, რაც გულისხმობს ინფორმაციის მოთხოვნის პროცედურას, ღიაობის წესების დაცვის გადამოწმებას, შიდა ბიუროკრატიულ დადასტურებას, იდენტიფიცირებას და დოკუმენტების მომზადებას (შესაძლებლობის ფარგლებში მოდიფიცირებას, მაგალითისთვის, რედაქტირებას) საფასურის გადახდას და სხვა;
- ინფორმაციის პროაქტიული გამოქვეყნება, რაც ასევე გულისხმობს ისეთ სახელმძღვანელო პროცედურებს ან, სულ მცირე, შესაბამისი კანონების, კანონქვემდებარე აქტებისა და რეგულაციების აღწერილობას, ძირითად „გამოქვეყნების სტანდარტს,“ რომელიც განსაზღვრავს საჯარო სექტორის მიერ გამოსაქვეყნებელი დოკუმენტების ინდიკატორებს, ასევე, ადგენს მათ პერიოდულობასა და წყაროებს.

ინფორმაციის თავისუფლების შესახებ მხოლოდ კანონი, ნებისმიერი მოქალაქის მიერ საჯარო ინფორმაციის მიღების უფლება ან პროაქტიულად ინფორმაციის გამოქვეყნების ვალდებულება არ განსაზღვრავს მთავრობის ღიაობასა და „გამჭვირვალობას“, როგორც ყურადსაღებ/მნიშვნელოვან ელემენტს კარგ მმართველობაში, რადგან ყველაზე გამჭვირვალე კანონსაც კი აქვს შეზღუდვები, როგორიც არის: „საჯარო ინფორმაცია ხელმისაწვდომია ყველასთვის, თუ რაიმე მნიშვნელოვანი ფაქტორი არ ზღუდავს ინფორმაციის გაცემას“.[4]

ინფორმაციის თავისუფლება დემოკრატიული საზოგადოების ერთ-ერთი უმნიშვნელოვანესი პოსტულატი და ფასეულობაა. 2008 წლის 26 ნოემბერს ევროპის საბჭოს მიერ მიღებული კონვენციით „ოფიციალურ დოკუმენტებზე ხელმისაწვდომობის თაობაზე,“ რომელსაც ხელი საქართველომაც მოაწერა, ინფორმაციის თავისუფლება ერთ-ერთ ფუნდამენტურ უფლებად იქნა აღიარებული, რაც, ხაზს უსვამს ხელისუფლების ღიად და გამჭვირვალედ საქმიანობის ვალდებულებას და საზოგადოების წინაშე არსებული ანგარიშვალდებულების ამგვარად შესრულების აუცილებლობას.[5] საქართველოს კანონმდებლობით გარანტირებულია ყველა ადამიანის უფლება, მიიღოს მის შესახებ არსებული ინფორმაცია, ასევე, საჯარო დაწესებულებებში დაცული დოკუმენტები, თუკი ისინი საიდუმლო ინფორმაციას არ შეიცავენ.

საჯარო ინფორმაციისა და პერსონალური მონაცემების დაცვის კუთხით საქართველოში არსებული ვითარების გაანალიზებისას, აღსანიშნავია საქართველოს კონსტიტუციის კონკრეტული ჩანაწერები, რომლებიც მთლიანობაში ინფორმაციის თავისუფლების მაღალ სტანდარტს აწესებს. კონსტიტუციის თანახმად, ყველას აქვს უფლება კანონით დადგენილი წესით გაეცნოს საჯარო დაწესებულებაში მასზე არსებულ ან სხვა ინფორმაციას ან ოფიციალურ დოკუმენტს, გარდა იმ შემთხვევისა, როდესაც იგი შეიცავს კომერციულ ან პროფესიულ საიდუმლოებას ან დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების ან სამართალწარმოების ინტერესების დასაცავად კანონით ან კანონით დადგენილი წესით აღიარებულია სახელმწიფო საიდუმლოებად.[6]

საჯარო დაწესებულებაში დაცული ინფორმაციის ხელმისაწვდომობას საქართველოს ასევე ავალდებულებს ევროპის ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის მე-10 მუხლი, რომლის თანახმადაც, გამოხატვის თავისუფლება მოიცავს ადამიანის უფლებას, მიიღოს და გაავრცელოს ინფორმაცია და მოსაზრებები საჯარო ხელისუფლების ჩარევის გარეშე.

საჯარო ინფორმაციის ხელმისაწვდომობის კუთხით საქართველოს კანონმდებლობის დახასიათებისას აღსანიშნავია 1999 წელს, საქართველოს პარლამენტის მიერ ადმინისტრაციულ სამართალში განხორციელებული მნიშვნელოვანი და პროგრესული რეფორმა, რომლის შედეგად დამტკიცდა ახალი კოდექსი ადმინისტრაციულ სამართალში, რომელიც ჰოლანდიური, გერმანული და ამერიკული ადმინისტრაციული სამართლის კონცეფციებს ეყრდნობოდა.[7] კოდექსმა, რომელიც ძალაში 2000

[4] თომას ჰარტი, „საჯარო ინფორმაციის ხელმისაწვდომობა“, გვ. 3, ხელმისაწვდომია: https://bit.ly/2Wk9yws წვდომის თარიღი: 23.08.2021.

[5] IDFI, საჯარო ინფორმაციის ხელმისაწვდომობა საქართველოში - საინფორმაციო ბიულეტენი №2, 2011 , გვ. 4.

[6] საქართველოს კონსტიტუციის მე-18 მუხლის მე-2 პუნქტი.

[7] IDFI, საჯარო ინფორმაციის ხელმისაწვდომობა საქართველოში - საინფორმაციო ბიულეტენი №2, 2011 , გვ. 4.

წლის დასაწყისში შევიდა, გამჭვირვალობისა და ანგარიშვალდებულების სრულიად ახალი ფუნდამენტური პრინციპები დაამკვიდრა საქართველოში.

კოდექსით გათვალისწინებული ახალი დებულებებიდან ერთ-ერთი ძირითადი საკითხია საჯარო ინფორმაციის გაცემის წესები. ინფორმაციის ხელმისაწვდომობის მარეგულირებელი ნორმები და მექანიზმები მასში ყველაზე ვრცლად და დეტალურად არის მოცემული. ზოგადი ადმინისტრაციული კოდექსის მიხედვით, საჯარო ინფორმაცია უნდა იყოს ღია და მისი მიღება უნდა შეეძლოს ნებისმიერ იურიდიულ და ფიზიკურ პირს, მისი მოქალაქეობის მიუხედავად. საქართველოს ზოგადი ადმინისტრაციული კოდექსის (შემდგომ - „სზაკ“) თანახმად, „ყველას აქვს უფლება, მოითხოვოს საჯარო ინფორმაცია მისი ფიზიკური ფორმისა და შენახვის მდგომარეობის მიუხედავად და აირჩიოს საჯარო ინფორმაციის მიღების ფორმა“.[8] სზაკ-ის თანახმად, საჯარო ინფორმაცია განმარტებულია, როგორც „ოფიციალური დოკუმენტი (მათ შორის, ნახაზი, მაკეტი, გეგმა, სქემა, ფოტოსურათი, ელექტრონული ინფორმაცია, ვიდეო და აუდიო ჩანაწერები) ანუ საჯარო დაწესებულებაში დაცული, აგრეთვე საჯარო დაწესებულების ან მოსამსახურის მიერ სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია“.[9] კოდექსი, განსაზღვრავს ინფორმაციის იმ სახეობებსაც, რომლის გასაიდუმლოებაც დაუშვებელია. ასეთია:

- ინფორმაცია გარემოს შესახებ, აგრეთვე მონაცემები იმ საშიშროების თაობაზე, რომელიც ემუქრება მათ სიცოცხლეს ან ჯანმრთელობას;
- საჯარო დაწესებულების საქმიანობის ძირითადი პრინციპები და მიმართულებები;
- საჯარო დაწესებულების სტრუქტურის აღწერა, მოსამსახურეთა ფუნქციების განსაზღვრისა და განაწილების, აგრეთვე გადაწყვეტილებათა მიღების წესი;
- საჯარო დაწესებულების იმ საჯარო მოსამსახურეთა ვინაობა და სამსახურებრივი მისამართი, რომელთაც უკავიათ თანამდებობა ან ევალებათ საჯარო ინფორმაციის გასაიდუმლოება ან საზოგადოებასთან ურთიერთობა და მოქალაქეთათვის ინფორმაციის მიწოდება;
- კოლეგიურ საჯარო დაწესებულებაში გადაწყვეტილების მისაღებად გამართული ღია კენჭისყრის შედეგები;
- არჩევით თანამდებობაზე პირის არჩევასთან დაკავშირებული ყველა ინფორმაცია;
- საჯარო დაწესებულების საქმიანობის შესახებ აუდიტორული დასკვნებისა და რევიზიების შედეგები, აგრეთვე სასამართლოს მასალები იმ საქმეებზე, რომელშიც საჯარო დაწესებულება მხარეს წარმოადგენს;
- საჯარო დაწესებულების გამგებლობაში არსებული საჯარო მონაცემთა ბაზის სახელწოდება და ადგილსამყოფელი, აგრეთვე საჯარო მონაცემთა ბაზისათვის პასუხისმგებელი პირის ვინაობა და სამსახურებრივი მისამართი;

[8] სზაკ-ის 37-ე მუხლის პირველი ნაწილი.
[9] სზაკ-ის მე-2 მუხლის პირველი ნაწილის „მ“ ქვეპუნქტი.

- საჯარო დაწესებულების მიერ მონაცემთა შეგროვების, დამუშავების, შენახვისა და გავრცელების მიზნები, გამოყენების სფეროები და სამართლებრივი საფუძველი;
- საჯარო მონაცემთა ბაზაში მისი პერსონალური მონაცემების არსებობა ან არარსებობა, აგრეთვე მათი გაცნობის წესი, მათ შორის, იმ პროცედურისა, რომლითაც მოხდება პირის იდენტიფიკაცია, თუ პირმა (მისმა წარმომადგენელმა) შეიტანა მოთხოვნა თავის შესახებ მონაცემების გაცნობის ან მათში ცვლილების თაობაზე;
- იმ პირთა კატეგორია, რომელთაც კანონით უფლება აქვთ გაეცნონ საჯარო მონაცემთა ბაზაში არსებულ პერსონალურ მონაცემებს;
- საჯარო მონაცემთა ბაზაში არსებულ მონაცემთა შემადგენლობა, წყაროები და იმ პირთა კატეგორია, რომელთა შესახებ გროვდება, მუშავდება და ინახება ინფორმაცია;
- ყველა სხვა ინფორმაცია, რომელიც კანონით გათვალისწინებულ შემთხვევებში და დადგენილი წესით არ არის მიჩნეული სახელმწიფო, კომერციულ ან პირად საიდუმლოებად.

4. საჯარო ინფორმაციის ხელმისაწვდომობის შეზღუდვა და მისი გამართლება

აღსანიშნავია, რომ ინფორმაციის ღიაობა ორ შემთხვევაშია შეზღუდული:

- როდესაც ეს კანონითაა გათვალისწინებული;
- როცა დადგენილი წესით ინფორმაცია მიეკუთვნება სახელმწიფო, კომერციულ და პირად საიდუმლოებას.

სახელმწიფო საიდუმლოებისადმი ინფორმაციის მიკუთვნების წესი შესაბამისი კანონმდებლობით რეგულირდება, მაგალითად, საქართველოს კანონით „სახელმწიფო საიდუმლოების შესახებ“. რაც შეეხება კომერციული და პირადი ინფორმაციის საიდუმლოების დეფინიციას, ისინი კოდექსში ზოგადად არის მოცემული, კერძოდ: კომერციული საიდუმლოება არის ის ინფორმაცია, რომლის გამჟღავნებამ შესაძლოა, ზიანი მიაყენოს პირის კონკურენტუნარიანობას. ადმინისტრაციულ ორგანოს არ შეიძლება გააჩნდეს საკუთარი კომერციული საიდუმლოება. ინფორმაციის კომერციულ საიდუმლოებად მიჩნევის შესახებ ინიციატივა მისი მესაკუთრისგან უნდა მოდიოდეს, თუმცა მისი გასაიდუმლოების შესახებ საბოლოო გადაწყვეტილებას ის საჯარო დაწესებულება იღებს, რომელშიც ეს ინფორმაცია ინახება; პირადი საიდუმლოება არის ის ინფორმაცია, რომელიც პირის იდენტიფიცირების საშუალებას იძლევა (პერსონალური მონაცემი) და რომლის პირად საიდუმლოებად მიჩნევის საკითხს წყვეტს თავად ის პირი, ვის შესახებაც არსებობს ეს ინფორმაცია. თუმცა, ამავდროულად, აღსანიშნავია კოდექსის 44-ე მუხლით გათვალისწინებული დებულება, რომელიც ერთმნიშვნელოვნად აცხადებს თანამდებობის პირთა (თანამდებობაზე წარდგენილ კანდიდატთა) პერსონალური მონაცემების ღიაობას: „საჯარო დაწესებულება ვალდებულია არ გაახმაუროს პირის პერსონალური მონაცემები თვით ამ პირის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის

ან სხვათა უფლებების დასაცავად. თანამდებობის პირის, აგრეთვე თანამდებობაზე წარდგენილი კანდიდატის პერსონალური მონაცემები საჯაროა“. მაშასადამე, როცა საქმე გვაქვს „თანამდებობის პირის პერსონალურ მონაცემებთან“, ზოგადი ადმინისტრაციული კოდექსის მიხედვით ინფორმაცია ღიაა და არ საჭიროებს ამ პირის თანხმობას ინფორმაციის გაცემისას.

საქართველოში ინფორმაციის გამოთხოვისთვის წერილობითი პროცედურაა დადგენილი, ხოლო საჯარო დაწესებულება ვალდებულია უზრუნველყოს ამ ინფორმაციის გაცნობის შესაძლებლობა დაუყოვნებლივ ან არა უგვიანეს 10 დღისა. ინფორმაციის გაცემაზე უარის თქმის გადაწყვეტილების მიღებისას საჯარო დაწესებულება ვალდებულია 3 დღის ვადაში აცნობოს ამის შესახებ განმცხადებელს და განუმარტოს მისი უფლებები და გასაჩივრების წესი.

საქართველოს კანონმდებლობაში არის რიგი სხვა ნორმატიული აქტებიც, სადაც აგრეთვე საუბარია ინფორმაციის თავისუფლების შესახებ: მაგალითად, საქართველოს კანონი „სიტყვისა და გამოხატვის თავისუფლების შესახებ“, საქართველოს სისხლის სამართლის კოდექსი და სხვა. თუმცა, საჯარო ინფორმაციის შესახებ ძირითადი დებულებები მაინც სზაკ-შია მოცემული, ხოლო ინფორმაციის ღიაობის შეზღუდვის შესახებ ნორმატიული ჩანაწერები კი სხვადასხვა სპეციალურ სამართლებრივ აქტში გვხვდება. აღნიშნულთა რიცხვს მიეკუთვნება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონიც, რომელიც პერსონალური მონაცემების შემცველი დოკუმენტების გავრცელებისა და გამჟღავნებისთვის მკაფიო და საყურადღებო რეგულაციებს აწესებს.

5. პერსონალურ მონაცემთა დაცვა საჯარო ინფორმაციის ხელმისაწვდომობის პირისპირ

როგორც ზემოთ აღინიშნა, პერსონალური მონაცემების დაცვის საკითხს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი აწესრიგებს, რომელიც ძალაშია 2012 წლიდან. კანონი ეყრდნობა კონვენციას „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“, რომელიც რატიფიცირებულია საქართველოს პარლამენტის 2005 წლის დადგენილებით. აღნიშნული კანონის მიზანია, პერსონალური მონაცემის დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა. პირადი ცხოვრების ხელშეუხებლობის პრინციპი გამომდინარეობს ადამიანის თავისუფლების ზოგადი კონსტიტუციური პრინციპიდან, რომელიც საქართველოს სამართლებრივი სისტემის მნიშვნელოვანი ელემენტია. პირადი ცხოვრების ხელშეუხებლობის დაცვის მიზანია სუბიექტისთვის თავისუფლების მინიჭება, თავად გადაწყვიტოს, არის თუ არა თანახმა მის პიროვნებასთან დაკავშირებული ინფორმაცია სხვას გააცნოს, რაც მისი თავისუფალი სფეროს განსაზღვრის მნიშვნელოვანი ელემენტია.

პერსონალური მონაცემების (კერძო სფეროს) დაცვა არ გულისხმობს მისი დამუშავების სრულ აკრძალვას. რიგ შემთხვევებში ფიზიკური პირი ვალდებულია, ითმინოს მისი პერსონალური მონაცემების დამუშავება. განსაკუთრებით, როდესაც საჯარო ინტერესები ამას მოითხოვს ან მისი დამუშავების ინტერესები აღემატება პერსონალური მონაცემების ხელშეუხებლობის ინტერესს.

პერსონალური მონაცემების დამუშავების დასაშვებობა არ გულისხმობს დამმუშავებლის განუსაზღვრელ უფლებას. ამ შემთხვევაშიც ძალაში რჩება კერძო სფეროს დაცვის ვალდებულება. პერსონალური ინფორმაციის დამუშავება გულისხმობს სწორი ინფორმაციის დამუშავებას და არასწორი ინფორმაციის დამუშავების აკრძალვას. ფიზიკურ პირს უფლება აქვს მოითხოვოს მასზე სწორი ინფორმაციის დამუშავება.[10]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მონაცემთა დამუშავების ერთ-ერთ საფუძვლად ითვალისწინებს იმ შემთხვევას, როდესაც ეს აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად.[11] აღნიშნული ჩანაწერით, კანონმდებელი მონაცემთა ყველა დამმუშავებელს უდგენს სპეციალურ ტესტს, რომლითაც მნიშვნელოვან განაცხადს აკეთებს ინფორმაციის ღიაობის, გამჭვირვალობის და კარგი მმართველობის პრაქტიკის დანერგვის კუთხით.

შესაბამისად, დასკვნის სახით უნდა აღინიშნოს, რომ საქართველოს კანონმდებლობა საკმარისად მკაფიოდ არეგულირებს ერთდროულად როგორც ადამიანების პირადი ცხოვრების და პერსონალური მონაცემების, ასევე, საჯარო მმართველობის გამჭვირვალობისა და ინფორმაციის ღიაობის იმ ძირითადი მოთხოვნების დაცვის შესაძლებლობას, რომლებიც ქვეყნის დემოკრატიული განვითარებისთვის აუცილებელ წინაპირობებს ქმნიან. პერსონალური მონაცემების და შესაბამისად, ადამიანების პირადი ცხოვრების ხელშეუხებლობის უფლება, აბსოლუტურ უფლებათა კატეგორიას არ განეკუთვნება, რაც იმას ნიშნავს, რომ ამ უფლების შეზღუდვა, მათ შორის საჯარო ინფორმაციის ხელმისაწვდომის უზრუნველსაყოფად, დასაშვებია. ამასთან, ჩარევის ლეგიტიმაციისთვის ყოველი ამგვარი შეზღუდვა, უნდა ეყრდნობოდეს საქმის ყოველმხრივ გაანალიზებას, ყველა ინტერესის შეპირისპირებას და ადამიანის უფლებაში ჩარევის თანაზომიერ საშუალებებს.

[10] პაატა ტურავა, ლევან ავალიშვილი, სერგი ჯორბენაძე, ინფორმაციის თავისუფლება - გზამკვლევი საჯარო დაწესებულებებისთვის (მეორე გამოცემა), 2016, გვ. 10, ხელმისაწვდომია: https://bit.ly/386zUVu წვდომის თარიღი: 23.08.2021.

[11] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლის „ზ“ ქვეპუნქტი.

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა

ავტორი: ანა ნიჟარაძე[12]
ვიადრინას ევროპული უნივერსიტეტი

1. შესავალი

ვიდეოთვალთვალის მიმდინარეობას ადამიანები უკვე ყოველდღიური ცხოვრების ყოველ ნაბიჯზე ვხვდებით. ამის მაგალითია: ქუჩები, მაღაზიები, აფთიაქები, სხვადასხვა შენობები, აეროპორტები, სახელმწიფო საზღვრები და ადამიანთა თავშეყრის სხვა ადგილები, სადაც ვიდეოკონტროლი ყოველდღიურ რეჟიმში და განუწყვეტლივ ხორციელდება.[13] ამასთან, თითოეული ინდივიდის პირადი ცხოვრების ხელშეუხებლობის დაცვა თანამედროვე მსოფლიოს ერთ-ერთი ძირითადი გამოწვევაა. თითოეული სახელმწიფო ვალდებულია მოქალაქეთათვის შექმნას პიროვნული განვითარებისა და ღირსების უფლების რეალიზების ინსტრუმენტები და მექანიზმები, რომლებიც საჯარო და კერძო სექტორს მათი საქმიანობის განხორციელებისას მკაცრ მოთხოვნებს დაუწესებს.

ვიდეოთვალთვალის გამოყენება მხოლოდ აუცილებელ შემთხვევებშია დასაშვები, თუმცა პრაქტიკა გვიჩვენებს, რომ ხშირია ვიდეოთვალთვალის განხორციელებისას კანონით დადგენილი მოთხოვნების გაუთვალისწინებლობა და შესაბამისად, ადამიანთა პერსონალური მონაცემების უკანონო მოპოვება.

2. ვიდეოთვალთვალის განხორციელების სამართლებრივი ჩარჩო და ფარგლები

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-2 მუხლის „დ“ ქვეპუნქტის მიხედვით, ვიდეოჩაწერა პერსონალურ მონაცემთა დამუშავების ერთ-ერთი გამოხატულებაა. ვიდეოთვალთვალის განხორციელების შედეგად მიღებული ჩანაწერი წარმოადგენს პირის პერსონალურ მონაცემს, თუ მასში შესაძლებელია ადამიანის სახის გამოსახულების გარჩევა ან ადამიანის სხვაგვარი იდენტიფიცირება. ადამიანის უფლებათა ევროპულმა სასამართლომ საქმეში „ლოპეზ რიბალდა და სხვები ესპანეთის წინააღმდეგ“ აღნიშნა, რომ „ადამიანის გამოსახულება მისი პიროვნულობის ერთ-ერთი მთავარი ატრიბუტია, ვინაიდან ის ამჟღავნებს პიროვნების უნიკალურ მახასიათებლებს და გამოარჩევს მას სხვებისგან. შესაბამისად, საკუთარი გამოსახულების დაცვის უფლება პირის განვითარების აუცილებელი კომპონენტია“. [14]

[12] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნინო ბოჭოიძე.

[13] მარი წერეთელი, პერსონალური მონაცემების დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში, ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი, 2019, გვ. 46-47.

[14] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 88.

იმდენად, რამდენადაც ვიდეოთვალთვალი ადამიანთა ყოველდღიურობის ნაწილია, ვიდეთვალთვალის სისტემების განთავსება სხვადასხვა მიზანს ემსახურება.[15] საჯარო და კერძო დაწესებულებები ვიდეოთვალთვალის სისტემის განთავსებას სხვადასხვა მიზანს უკავშირებენ, რის სამართლებრივ ჩარჩოს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-11-14 მუხლები წარმოადგენს. აღსანიშნავია, რომ ვიდეოთვალთვალის განხორციელება წარმოადგენს კონფლიქტს საჯარო ინტერესსა და პერსონალურ მონაცემთა დაცვას შორის, რომლის მოგვარება ზემოთ აღნიშნული კანონის მეშვეობით არის შესაძლებელი.

როგორც აღინიშნა, ვიდეოთვალთვალის განხორციელება დასაშვებია მხოლოდ კანონით გათვალისწინებული მიზნების მისაღწევად. ასეთ მიზნებს კი წარმოადგენს დანაშაულის პრევენცია, პირის უსაფრთხოების, საკუთრების, საზოგადოებრივი წესრიგის და არასრულწლოვანთა მავნე ზეგავლენისგან დაცვა. სწორედ ვიდეოთვალთვალის სისტემა არის ის ერთ-ერთი ტექნიკური საშუალება, რომლითაც შესაძლებელია ამ მიზნების მიღწევა. უნდა აღინიშნოს ისიც, რომ დაუშვებელია ვიდეოთვალთვალის განხორციელება, თუ ის ზემოთ ჩამოთვლილი მიზნების მიღწევის საშუალებას არ წარმოადგენს, არამედ გამოიყენება როგორც მოქალაქეთა ქცევის კონტროლის მექანიზმი ან სხვა.[16]

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-11 მუხლის პირველი პუნქტი ითვალისწინებს ვიდეოთვალთვალის განხორციელებას ნებისმიერი თავშეყრის ადგილას, როგორიც არის ქუჩა, პარკი, სკვერი, სათამაშო მოედანი და სხვა, ასევე საზოგადოებრივი ტრანსპორტის გაჩერებასთან და თავად ტრანსპორტშიც. მსგავს ადგილებში ვიდეოთვალთვალის განხორციელება ემსახურება მხოლოდ იმ მიზნებს, რომლებიც ზემოთ არის ჩამოთვლილი. ამავე მუხლის მეორე პუნქტის თანახმად, ვიდეოთვალთვალის განხორციელებისთვის საჯარო და კერძო დაწესებულებები ვალდებულნი არიან შესაბამის პერიმეტრზე და ადამიანის თვალისთვის შესამჩნევ ადგილას განათავსონ ვიდეოთვალთვალის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი. აღნიშნული წესი სხვა შემთხვევებშიც მოქმედებს, სადაც კანონით დასაშვებია ვიდეომონიტორინგის განხორციელება. უნდა აღინიშნოს ისიც, რომ გამაფრთხილებელი ნიშნის ამგვარი განთავსებით მონაცემთა სუბიექტი მისი პერსონალური მონაცემის შესაძლო დამუშავებაზე ინფორმირებულად ითვლება და ამასთან, ეს წარმოადგენს ინდივიდთა უფლებების პატივისცემისა და დაცვის გამოხატულებას.[17] მე-11 მუხლის მესამე პუნქტის მიხედვით, დაუშვებელია ვიდეოთვალთვალის შედეგად მოპოვებული მონაცემების არამართლზომიერი გამოყენება. მაგალითისთვის, სამართალდამცავი ორგანოს წარმომადგენელთა მიერ კერძო კომპანიის კომპიუტერულ სისტემაში არსებული ვიდეოჩანაწერის მოპოვება კანონდარღვევად იქნა მიჩნეული, რადგან საგამოძიებო მიზნით კომპიუტერული მონაცემების მოპოვებისთვის საქართველოს სისხლის სამართლის საპროცესო კოდექსი მოითხოვს მოსამარ-

[15] ეკატერინე ნანდოშვილი, ვიდეოთვალთვალი და პერსონალური მონაცემების დამუშავება, ხელმისაწვდომია: https://bit.ly/3sCXSkP წვდომის თარიღი: 23.06.2021.

[16] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 88.

[17] იქვე.

თლის განჩინებას ან გადაუდებელი აუცილებლობისას პროკურორის დადგენილების არსებობას, რაც მოცემულ შემთხვევაში არ არსებობდა.[18]

საქართველოში ვიდეოთვალთვალის განხორციელება ყველაზე ხშირი და სისტემატურია ქუჩებსა და გზებზე, რომლითაც ფიქსირდება ავტომობილთა მძღოლების მიერ სამართალდარღვევის ჩადენა, რაც იწვევს მათ ადმინისტრაციულ თუ სისხლისსამართლებრივ პასუხისმგებლობას. საბოლოო ჯამში, ეს ადამიანთა ჯანმრთელობისა და საზოგადოებრივი წესრიგის დაცვას ემსახურება.

ნებისმიერ დაწესებულებას კანონის მოთხოვნების გათვალისწინებით და საკუთრების დაცვის მიზნით შეუძლია მისი შენობის ვიდეოთვალთვალის განხორციელება, რომლის სამართლებრივ რეგულირებას „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-12 მუხლი ახდენს და ამ შემთხვევაშიც ის ზემოთ ჩამოთვლილი მიზნების მიღწევის საშუალებაა.

ვიდეომონიტორინგის სისტემა დღეს უკვე ხშირად მონტაჟდება საცხოვრებელი სახლების თუ კორპუსების შიდა და გარე პერიმეტრზე, რომლებიც გამიზნულია პირის და მისი ქონების უსაფრთხოების დასაცავად.[19] ამ შემთხვევაშიც უმნიშვნელოვანესია მისი იმგვარი განთავსება, რომელიც უკანონოდ არ მოახდენს ადამიანთა შესახებ პერსონალური მონაცემების მოპოვებას. კანონმდებელი საცხოვრებელი შენობის მხოლოდ გარე პერიმეტრის და შესასვლელის ვიდეოკონტროლის განხორციელებას ხდის დასაშვებად, რათა დაცულ იქნეს პირთა პერსონალური მონაცემები.[20] მე-13 მუხლის პირველი პუნქტით, საცხოვრებელი შენობის რამდენიმე მესაკუთრის არსებობის შემთხვევაში ვიდეოთვალთვალის განხორციელებისთვის აუცილებელია მესაკუთრეთა ნახევარზე მეტის წერილობითი თანხმობა. ასევე საყურადღებოა კერძო საკუთრების შემთხვევაში ვიდეოსათვალთვალო სისტემის დამონტაჟების კანონიერებაც, რადგან შესაძლებელია იგი ხელყოფდეს სხვა ადამიანების, მაგალითად, მეზობლების პირადი ცხოვრების უფლებას.[21] მაგალითად, ვიდეოთვალთვალის სისტემა შესაძლებელია იმგვარად იქნეს დამონტაჟებული, რომლის ხედვის არეალშიც ექცეოდეს მეზობლის სახლის შესასვლელი კარ-ფანჯარა, თანასაკუთრებაში არსებული დერეფანი და სხვა. ამდენად, ფიზიკური პირის მიერ საკუთრების ვიდეომონიტორინგის შემთხვევაში მნიშვნელოვანია ხედვის არეალში არ ექცეოდეს სხვათა საკუთრება. ძირითად შემთხვევებში მესაკუთრეები საკუთრების ვიდეომონიტორინგს მათი დაცვის მიზნით ახდენენ.[22] ასეთ შემთხვევებში, ვიდეოთვალთვალი დანაშაულის გახსნის მნიშვნელოვან საშუალებას შეიძლება წარმოადგენდეს.

[18] ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის დასკვნა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ წარმოდგენილ 2018 წლის ანგარიშზე პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ (№1-3942/19; 01.03.2019), გვ. 9.

[19] საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, მუხლი 13, პუნქტი 2.

[20] იქვე, მუხლი12, ნაწილი 2 და მუხლი 13, ნაწილი 3.

[21] ეკატერინე ნანდოშვილი, ვიდეოთვალთვალი და პერსონალური მონაცემების დამუშავება, ხელმისაწვდომია: https://bit.ly/3sCXSkP წვდომის თარიღი: 23.06.2021.

[22] ამ საკითხთან დაკავშირებულია ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება: CJEU, C-212/13, František Ryneš v. Úřad pro ochranu osobnich udajů, 2014 წლის 11 დეკემბერი. ამ საქმეში განმცხადებელი ახდენდა საკუთარი სახლის ვიდეომონიტორინგს უსაფრთხოების დაცვის მიზნით და მართლაც, ვიდეოჩანაწერები საქმეში მნიშვნელოვან მტკიცებულებებად იქნა მიჩნეული, როდესაც ორმა პირმა დააზიანა მისი საკუთრება.

პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის ანგარიშში აღინიშნა, რომ მოცემულ პერიოდში ფიქსირდებოდა მოქალაქეთა ხშირი მიმართვიანობა საცხოვრებელ შენობებში ვიდეოთვალთვალის მიმდინარეობის კანონიერების ეჭვქვეშ დაყენებასთან დაკავშირებით. განაცხადზე რეაგირების შედეგად დადგინდა, რომ ვიდეოთვალთვალი, რომლის ხედვის არეალშიც ექცეოდა ის პირები და ობიექტები, არ იყო კანონთან შესაბამისი. ასევე არაკანონიერად მიმდინარეობდა აუდიომონიტორინგიც.[23]

რაც შეეხება სამუშაო ადგილას ვიდეოთვალთვალის განხორციელებას, მე-12 მუხლის მე-3 პუნქტით აღნიშნული დასაშვებია მხოლოდ გამონაკლის შემთხვევებში: პირის უსაფრთხოების, საკუთრებისა და საიდუმლო ინფორმაციის დასაცავად. ასეთ შემთხვევებში, ამავე მუხლის მე-5 პუნქტის თანახმად, დასაქმებულ პირებს აუცილებლად წერილობით უნდა ეცნობოთ ვიდეომონიტორინგის განხორციელების შესახებ. სამუშაო ადგილას ვიდეოთვალთვალის განხორციელებასთან დაკავშირებით ადამიანის უფლებათა ევროპულმა სასამართლომ განიხილა საქმე,[24] სადაც დადგინდა განმცხადებლის ბრალეულობა სამსახურში ჩადენილი ქურდობისთვის. განმცხადებელი კი დაობდა მის მიმართ პირად ცხოვრებაში უკანონო ჩარევას, თუმცა სასამართლომ მის მიმართ არ დაადგინა ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის მე-8 მუხლის დარღვევა, რომელიც პირადი და ოჯახური ცხოვრების დაცულობის უფლებას განამტკიცებს.

დასაქმების სფეროში უკანონო ვიდეომონიტორინგის განხორციელების მაგალითი შეიძლება იყოს თანამშრომელთა ჩაცმულობის, ქცევის, კომუნიკაციის კონტროლის შემოწმება და სხვა. მაგალითად, კანონის დარღვევა არ იქნება, თუ ვიდეომონიტორინგის შედეგად კონტროლდება თანამშრომელთა სამსახურებრივი ფორმის ტარების შემოწმება. პრაქტიკის მიხედვით, მსგავს შემთხვევებში თანამშრომლებს დისციპლინური სახდელის სახით სასტიკი საყვედური გამოეცხადათ.[25] „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-12 მუხლის მე-3 პუნქტით ვიდეომონიტორინგის განხორციელება ასევე დასაშვებია საგამოცდო ცენტრებსა თუ აუდიტორიებშიც.

ვიდეოთვალთვალის განხორციელების ნებისმიერ შემთხვევაში აუცილებელია შეიქმნას ვიდეოჩანაწერების შენახვისთვის განკუთვნილი ფაილური სისტემა პირის პერსონალურ მონაცემთა დამუშავების თარიღის, ადგილის და დროის მითითებით. მე-14 მუხლის პირველი პუნქტის თანახმად, ამა თუ იმ დაწესებულებებს პირთა შენობაში შესვლისა და გასვლისას შეუძლიათ შეაგროვონ ისეთი ინფორმაცია, როგორიც არის: სახელი და გვარი, შესვლის და გასვლის პერიოდი, მიზეზები, საიდენტიფიკაციო ნომერი და სახე, მისამართი. კანონმდებელი ასევე ითვალისწინებს ამგვარი ინფორმაციის შენახვის მაქსიმალურ ვადას. პირთა პერსონალური მონაცემების შენახვა დასაშვებია მხოლოდ 3 წლის განმავლობაში, თუ კონკრეტულ შემთხვევაში კანონი განსხვავებულ ვადას არ ადგენს. ამ ვადის გასვლის შემდეგ კი აუცილებელია მათი განადგურება.[26]

[23] ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის დასკვნა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ წარმოდგენილ 2018 წლის ანგარიშზე პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ (№1-3942/19; 01.03.2019), გვ. 14.

[24] ადამიანის უფლებათა ევროპულმა სასამართლო, კოპკე გერმანიის წინააღმდეგ, No. 420/07, 2010 წლის 5 ოქტომბერი.

[25] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 93.

[26] პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-14 მუხლის მეორე ნაწილი.

ფაილური სისტემის არარსებობაზე და შესაბამისად, კანონის მოთხოვნის დარღვევაზე საუბარია ინსპექტორის 2018 წლის ანგარიშში. არაერთი ორგანიზაციის შემოწმების შედეგად დადგინდა, რომ მათ ვიდეოთვალთვალის სისტემასთან ერთად არ გააჩნდათ ვიდეოჩანაწერთა ელექტრონული ჟურნალი.[27] 2017 წლის ანგარიშის მიხედვით კი გამომჟღავნდა ორგანიზაციების მიერ ვიდეოჩანაწერების განუსაზღვრელი ვადით შენახვა, რომლის აუცილებლობა და შესაბამისი კანონიერი მიზანი არ არსებობდა.[28] ინსპექტორის მიერ 2017 წლის შესწავლის შედეგად კანონის ისეთ დარღვევებს ჰქონდა ადგილი, როგორებიც არის: ვიდეოთვალთვალის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშნების განუთავსებლობა, სამუშაო გარემოში დასაქმებულთა არაინფორმირებულობა, ვიდეოჩანაწერების შენახვის ვადის დარღვევა, არაუფლებამოსილი მესამე პირებისთვის ჩანაწერების გამჟღავნება და სხვა, რისთვისაც შესაბამის დაწესებულებებს პასუხისმგებლობის სახით ჯარიმა და გაფრთხილება დაეკისრათ.[29]

რაც შეეხება იმას, თუ სად არის აკრძალული ვიდეოთვალთვალის სისტემის დამონტაჟება, მე-12 მუხლის მე-4 პუნქტით, აღნიშნული დაუშვებელია ჰიგიენისთვის განკუთვნილ ადგილებსა და გამოსაცვლელ ოთახებში, რადგან მიიჩნევა, რომ ისინი წარმოადგენს ადგილებს, სადაც თითოეული ადამიანი სარგებლობს პირადი ცხოვრების უფლებით და აქვს მოლოდინი, რომ მას არ უთვალთვალებენ.[30]

ინსპექტორის 2018 წლის ანგარიშის მიხედვით, დაჯარიმდა ერთ-ერთი სპორტულ-გამაჯანსაღებელი კომპლექსი, რომელიც კანონის დარღვევით ახდენდა გასახდელი ოთახის ვიდეოთვალთვალს. ასევე 2017 წლის ანგარიშის თანახმად, ინსპექტორის სამსახურმა არაერთი შემთხვევა შეისწავლა. მაგალითისთვის, მედიასაშუალებებით გავრცელებული ინფორმაციის საფუძველზე, სამსახურმა ერთ-ერთი კომპანიის გამოსაცვლელ ოთახებსა და ჰიგიენისთვის განკუთვნილ ადგილებში ვიდეოთვალთვალის განხორციელების ფაქტის შესწავლა დაიწყო და დაადგინა, რომ კომპანია მართლაც კანონის დარღვევით ახდენდა ქალებისთვის განკუთვნილი გამოსაცვლელი ოთახების ვიდეომონიტორინგს. კომპანიის პასუხი, რომ ის ვიდეომონიტორინგს დასაქმებულთა უსაფრთხოების და საკუთრების დაცვის მიზნით ახდენდა, არ იქნა გამართლებული. კომპანია ადმინისტრაციული სახდელით დაჯარიმდა, დაევალა ვიდეომონიტორინგის სისტემის დემონტაჟი და მოპოვებული ვიდეოჩანაწერების განადგურება. ასევე, კანონის დარღვევად იქნა მიჩნეული სასტუმროს მართვის პროცესში და ბავშვთა ჰიგიენისთვის განკუთვნილი სივრცეების ვიდეოთვალთვალი. შესაბამისად, როგორც ვხედავთ, ჰიგიენისთვის განკუთვნილ ადგილებსა და გამოსაცვლელ ოთახებში ყოველთვის გაუმართლებელია ვიდეომონიტორინგის სისტემების განთავსება.[31]

[27] ადამიანის უფლებათა დაცვისა და სამოქალაქო ინტეგრაციის კომიტეტის დასკვნა პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ წარმოდგენილ 2018 წლის ანგარიშზე პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ (№1-3942/19; 01.03.2019), გვ. 14.

[28] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 100.

[29] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 89;

[30] პაატა ტურავა, ლევან ავალიშვილი, სერგი ჯორბენაძე, ინფორმაციის თავისუფლება - გზამკვლევი საჯარო დაწესებულებებისთვის (მეორე გამოცემა), 2016, გვ. 10, ხელმისაწვდომია: https://bit.ly/386zUVu წვდომის თარიღი: 23.08.2021; პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 91.

[31] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, ანგარიში პერსონალურ მონაცემთა დაცვის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2017, გვ. 91.

3. დასკვნა

ყოველივე ზემოთ აღნიშნულიდან გამომდინარე, ვიდეოთვალთვალის გზით პერსონალურ მონაცემთა მოპოვებისას გათვალისწინებულ უნდა იქნეს შემდეგი გარემოებები: აუცილებელია ვიდეოთვალთვალი განხორციელდეს მხოლოდ დანაშაულის პრევენციის, პირის უსაფრთხოების, საკუთრების, საზოგადოებრივი წესრიგის და არასრულწლოვანთა მავნე ზეგავლენისგან დაცვის მიზნების მისაღწევად. ასევე, მისი მიმდინარეობის შესახებ შესაბამისი ნიშნის განთავსებით და წერილობითი შეტყობინებით უნდა ეცნობოთ ვიდეოთვალის ხედვის არეალში მოხვედრილ სავარაუდო პირებს. ამასთან, ვიდეოთვალის მონტაჟი უნდა განხორციელდეს კანონით გათვალისწინებულ ადგილას. ამდენად, უმნიშვნელოვანესია ვიდეოთვალთვალის განხორციელების მიზნობრიობის დადგენა და კანონის მოთხოვნების დაცვა.

მნიშვნელოვანია იმის ხაზგასმა, რომ საჯარო და კერძო დაწესებულებებმა მკაცრად უნდა დაიცვან ვიდეოთვალთვალის სისტემის დამონტაჟების კანონიერების ფარგლები, ასევე აუცილებელია თავად ფიზიკურმა პირებმაც იცოდნენ მათი უფლებების შესახებ, თუ სად და რა დროს შეიძლება იქნას მათი პერსონალური მონაცემები უკანონოდ მოპოვებული, რასაც ხელს შეუწყობს ცნობიერების ამაღლების კამპანიები.

პერსონალური მონაცემების დაცვა და საჯარო ინფორმაციის ხელმისაწვდომობა

ავტორი: არტურ ჩობანიანი [32]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

პერსონალური მონაცემი პიროვნების პროფილის ჩამოყალიბების საშუალებას წარმოადგენს და როგორც მაიდენტიფიცირებელი ფენომენი, ადამიანის ვინაობის დადგენას ემსახურება. პერსონალურ ინფორმაციაზე საუბრისას პირველი, რაც გვახსენდება, არის ადამიანის ინდივიდუალიზაცია. ოცდამეერთე საუკუნეში, ტექნოლოგიების აღორძინების ეპოქაში, ნებისმიერ საჯარო/კერძო სექტორში, სხვადასხვა დაწესებულებაში, ყოველი ფეხის ნაბიჯზე, იქაც კი, სადაც ადამიანი ვერც წარმოიდგენდა, თუნდაც მცირე ინფორმაცია თითქმის ყველა ჩვენგანის შესახებ არსებობს.

მოგეხსენებათ, რომ პირადი ცხოვრების უფლება არის ინდივიდის და არ ექვემდებარება ჩამორთმევას, თუმცა პიროვნების ცხოვრებაზე სხვადასხვა ინფორმაციის მოძიებითა და მიღებით ხდება ჩარევა ამ უფლებით დაცულ სფეროში და შესაძლოა მნიშვნელოვანი ზიანი მიადგეს ადამიანს. მართებული იქნება იმის აღნიშვნა, რომ პერსონალური მონაცემების გამჟღავნებისგან თავის დაცვაში უმნიშვნელოვანესი როლი თითოეულ ადამიანს აკისრია. არ იქნება გადამეტებული თუ ვიტყვით, რომ პერსონალური მონაცემების დაცვა თანამედროვე მსოფლიოს უდიდესი გამოწვევაა.

აქვე უნდა აღინიშნოს, რომ კარგი მმართველობის და დემოკრატიული განვითარების ქვეყნები მეტი გამჭვირვალობისკენ, საჯარო ინფორმაციის მეტი ხელმისაწვდომობისკენ და ამ საშუალებებით ხალხის მიერ ხელისუფლების განხორციელებაში მონაწილეობის მეტი შესაძლებლობისკენ მიისწრაფვიან. პერსონალურ მონაცემთა დაცვის და ინფორმაციის ხელმისაწვდომობის ინტერესები ხშირად იკვეთება ერთმანეთთან და მათთან დაკავშირებული საკითხები მრავალმხრივ გაანალიზებას საჭიროებს, სწორი გადაწყვეტილებების მისაღებად. გადაწყვეტილებების სისწორე მრავალ ფაქტორზეა დამოკიდებული. თითოეული მათგანი კი, ყოველ კონკრეტულ შემთხვევებში, ერთმანეთისგან განსხვავებულ გარემოებებს ეყრდნობა.

ნაშრომში მნიშვნელოვანი ადგილი დაეთმობა პერსონალური მონაცემების არსს, ამასთან, გაანალიზდება საჯარო ინფორმაციის ხელმისაწვდომობის უზრუნველსაყოფად, პერსონალური მონაცემების დამუშავების კანონიერებისთვის საჭირო გარემოებები.

[32] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - გიორგი აბულაძე.

2. პერსონალურ მონაცემთა არსი და კლასიფიკაცია

როგორც ევროპული კავშირის, ისე ევროპის საბჭოს კანონმდებლობის თანახმად, „პერსონალური მონაცემი“ განმარტებულია, როგორც ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს[33]. ეს ნიშნავს ინფორმაციას პირის შესახებ, რომლის ვინაობა ცნობილია ან შეიძლება დადგინდეს დამატებითი ინფორმაციის მოძიების შედეგად. თუ აღნიშნული პირის შესახებ მუშავდება მონაცემები, ეს პირი იწოდება როგორც მონაცემთა სუბიექტი. „პერსონალური მონაცემი“ მოიცავს კონკრეტული ფიზიკური პირის შესახებ ინფორმაციას დაწყებული სახელი-გვარიდან, დამთავრებული ისეთი სენსიტიური მონაცემებით, როგორიც არის ინფორმაცია პირის ჯანმრთელობის, პოლიტიკური შეხედულების, ოჯახური მდგომარეობის, საქმიანობის სფეროების შესახებ და სხვა. იგი იძლევა ადამიანთა იდენტიფიცირების შესაძლებლობას პირდაპირ ან ირიბად.

დღესდღეობით, პერსონალურ მონაცემთა დაცვასთან დაკავშირებული სამართლებრივი ურთიერთობები ეროვნულ დონეზე მოწესრიგებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით, რომელიც ფიზიკური პირის იდენტიფიცირებისთვის „გამოსადეგ“ ძირითადად ყველა სახის ინფორმაციას ეხება. ევროპული კონვენცია კი პერსონალური მონაცემების დეფინიციას ნაკლები კონკრეტიზაციით გვთავაზობს და განმარტავს, რომ „პერსონალური მონაცემები“ აღნიშნავს ნებისმიერ ინფორმაციას, რომელიც შეეხება განსაზღვრულ ან განმსაზღვრელ პირს (ანუ ინფორმაციის სუბიექტს).[34]

საქართველოს კონსტიტუცია არ შეიცავს პერსონალური ინფორმაციის ცნებას, თუმცა მე-18 მუხლში წარმოდგენილია ინფორმაციათა ჩამონათვალი, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, მის ფინანსებთან ან სხვა კერძო საკითხებთან და პერსონალურ მონაცემთა სფეროს მიეკუთვნება. უზენაეს კანონში რეგულირებული საკითხები მხოლოდ ყველაზე მნიშვნელოვანს ეხება, მაგალითად, პირის ჯანმრთელობასთან დაკავშირებული ინფორმაცია უკავშირდება ადამიანის ფიზიკური არსებობის საკითხს, ხოლო ფინანსებთან დაკავშირებული ინფორმაცია მისი განვითარების, ღირსების და საქმიანობის მატერიალურ საფუძვლებს.[35] ადამიანის ინტიმური ცხოვრების სფეროს მიკუთვნებული ურთიერთობები ადამიანის პირად ცხოვრებას ქმნის, მაშასადამე, პერსონალური მონაცემი პრივატულ ინფორმაციას წარმოადგენს.

პერსონალური მონაცემების შინაარსის უკეთ გასაანალიზებლად, რამდენიმე კონკრეტულ ინფორმაციას შეეხება წინამდებარე ნაშრომი, მათ შორის აღსანიშნავია, რომ:

- **განასხვავებენ ე. წ. ანონიმირებულ და ფსევდონიმირებულ მონაცემებს**. მონაცემი არის ანონიმირებული, თუ ის აღარ შეიცავს რაიმე იდენტიფიკატორს, ხოლო მონაცემი არის ფსევდონიმირებული, თუ იდენტიფიკატორები დაშიფრულია. განსხვავებით ანონიმირებული მონაცემისგან, ფსევდონიმირებული მონაცემები წარმოადგენს პერსონალურ მონაცემებს.

[33] „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენციის მე-2 მუხლის „ა“ ქვეპუნქტი.

[34] „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპული კონვენციის მე-2 მუხლის „ა“ პუნქტი.

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

- **განსაკუთრებული კატეგორიის მონაცემებს** მიეკუთვნება ინფორმაცია, რომლებიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული კავშირის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, აღკვეთის ღონისძიების შეფარდებასთან, საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან. განსაკუთრებულ კატეგორიაში ასევე შედის ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა. განსაკუთრებული კატეგორიის მონაცემებს „ჩვეულებრივი“ მონაცემებისგან ის განასხვავებს, რომ კანონით მათი დაცვის განსაკუთრებით მაღალი სტანდარტია დაწესებული და წესების დარღვევის შემთხვევაში სანქციაც უფრო მკაცრია.

- **ბიომეტრიული მონაცემია** თითის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი ანუ ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის. ბიომეტრიული მონაცემების დამუშავება დასაშვებია მხოლოდ მაშინ, თუ ეს აუცილებელია ორგანიზაციის საქმიანობის განხორციელების, უსაფრთხოებისა და საკუთრების დაცვის, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით, თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს. ბიომეტრიული მონაცემების დამუშავების შესახებ წინასწარ უნდა ეცნობოს სახელმწიფო ინსპექტორის სამსახურს.[36]

- **გენეტიკა ორგანიზმის „მოკვლევის“ საშუალებაა.** მისი მეშვეობით შესაძლებელია იმ უნიკალური და მუდმივი ინფორმაციის მოძიება, რომელიც მხოლოდ კონკრეტული სუბიექტისთვის და მისი ოჯახის სისხლით ნათესავი წევრებისთვის არის დამახასიათებელი. გენეტიკური მონაცემების ცოდნამ შესაძლოა ინდივიდს თავიდან ააცილებინოს ან მნიშვნელოვნად შეუმციროს მემკვიდრეობითი დაავადებები, ან მოხდეს მათი პროგნოზირება, თუმცა მისმა შემთხვევითმა გაჟღერებამ შესაძლებელია კონკრეტული პიროვნების მასიდან გარიყვაც გამოიწვიოს. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი გენეტიკურ მონაცემს განმარტავს როგორც „მონაცემთა სუბიექტის უნიკალურ და მუდმივ მონაცემს გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება“, იგი ამავდროულად განსაკუთრებული კატეგორიის მონაცემთა კატეგორიაა.

ზემოაღნიშნული დასახელების და შინაარსის მონაცემებისთვის, საქართველოს კანონმდებლობა განსხვავებულ, მათზე მორგებულ დაცვის მექანიზმებს გვთავაზობს. მთლიანობაში კი, მონაცემთა დაცვაში ძირითად როლს მათი კონკრეტული საფუძვლით და კანონმდებლობით დადგენილი პრინციპების შესაბამისად დამუშავება თამაშობს, იმგვარი ორგანიზაციულ-ტექნიკური ზომების მიღებით, რომლებიც მონაცემთა უსაფრთხოების უზრუნველყოფის მაქსიმალურ შესაძლებლობას ქმნის.

[36] დამატებით იხ. „ბიომეტრული და გენეტიკური მონაცემების დამუშავება“, ხელმისაწვდომია ბმულზე: https://bit.ly/384YWV1 წვდომის თარიღი: 23.08.2021.

3. პერსონალურ მონაცემთა დაცვა საერთაშორისო დონეზე

გერმანიამ, საფრანგეთმა და შვედეთმა პირველებმა მიიღეს საკანონმდებლო აქტები ევროპის ფარგლებში, რომლებიც ეხებოდა ინდივიდების შესახებ არსებულ ე.წ. პერსონალურ და კონფიდენციალურ ინფორმაციას. შეიძლება ითქვას, რომ მათი რეგულაციები მიიჩნევა ნორმატიულ დონეზე პერსონალური მონაცემების დამცველ პირველ მექანიზმად. რეგულაციების დაწესებაზე მუშაობა 1970-იან წლებში დაიწყო და დასრულდა 1981 წელს, ევროპის საბჭოს 108-ე კონვენციის მიღებით.

ნიშანდობლივია, რომ საერთაშორისო დონეზე პერსონალურ მონაცემთა მიმართ ყურადღების გამოხატულების მაგალითია ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის (OECD) მიერ 1980 წელს შემუშავებული პირადი ცხოვრების დაცვისა და პერსონალურ მონაცემთა საერთაშორისო გადაცემის თაობაზე მიღებული სარეკომენდაციო დებულებები (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). მის უპირატესობას წარმოადგენს ერთგვარი საერთაშორისო „კონსენსუსი"[37] იმის შესახებ, თუ როგორ უნდა დაბალანსდეს პირადი ცხოვრების დაცვა პერსონალური მონაცემების თავისუფალ გადაადგილებასთან მიმართებით. აღნიშნული სარეკომენდაციო დებულება ამკვიდრებს პერსონალურ მონაცემთა დაცვის 8 პრინციპს, ესენია:

- სამართლიანობა, კანონიერება და პერსონალურ მონაცემთა მოპოვება სუბიექტის თანხმობის ან მისი ინფორმირების საფუძველზე.
- პერსონალურ მონაცემთა მიზნობრივი დამუშავების პრინციპი.
- პერსონალურ მონაცემთა მიზნის პროპორციულად დამუშავების პრინციპი.
- თავდაპირველ მიზანთან შეუთავსებელი მიზნით დამუშავების დაუშვებლობა.
- პერსონალურ მონაცემთა უსაფრთხოდ შენახვა.
- ინდივიდის მონაწილეობა პროცესში, რაც გულისხმობს მისი უფლებების რეალიზაციას დამმუშავებლის წინაშე.
- წესების საჯაროობა, რაც ეხება ინფორმაციის ხელმისაწვდომობას პერსონალურ მონაცემთა დამუშავების წესების შესახებ.
- ანგარიშვალდებულება, რომელიც უზრუნველყოფს დამმუშავებლის მიერ ზემოხსენებული პრინციპების დაცვას.

პერსონალურ მონაცემთა დაცვის სფეროში მნიშვნელოვან მოვლენად ითვლება 1981 წლის 28 იანვარს ევროპის საბჭოს მიერ პერსონალურ მონაცემთა დაცვის თაობაზე საერთაშორისო აქტის მიღება. ევროპის საბჭოს კონვენცია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ" წარმოადგენს პირველ საერთაშორისო სამართლებრივ დოკუმენტს. ზემოაღნიშნული კონვენცია, რომელსაც ხშირად მოიხსენიებენ, როგორც 108-ე კონვენციას,

[37] კახაბერ გოშაძე, „პერსონალურ მონაცემთა დაცვისა და დამუშავების კონსტიტუციურ-სამართლებრივი გარანტიები", სადისერტაციო ნაშრომი, 2017, გვ. 94.

შეიცავს წესებს პერსონალურ მონაცემთა დამუშავებისთვის საჯარო და კერძო ორგანიზაციების ფარგლებში, ასევე იცავს ფიზიკურ პირებს უფლების დარღვევისგან, მაგალითად, მონაცემთა უნებართვო შეგროვებისა და შემდგომი დამუშავებისგან, გარდა ამისა, მოიცავს ნორმებს მონაცემთა საერთაშორისო გადაცემის შესახებ. მნიშვნელოვანია ის, რომ მასში განმტკიცებულია მონაცემთა დაცვის მთავარი პრინციპები, კერძოდ, მიზნობრიობა, კანონიერება, სამართლიანობა, პროპორციულობა და დამუშავებისას შესაბამისი ვადების დაცვა. 108-ე კონვენცია გამორჩეულია ასევე იმითაც, რომ იგი არის ერთადერთი საერთაშორისო სამართლებრივი ინსტრუმენტი პერსონალურ მონაცემთა დაცვის ასპექტში, რომელიც ღიაა რატიფიცირებისთვის არაევროპული სახელმწიფოებისთვისაც. კონვენცია რატიფიცირებულ იქნა საქართველოს უმაღლესი წარმომადგენლობითი ორგანოს მიერ 2005 წლის 28 ოქტომბერს.

პერსონალურ მონაცემთა დაცვის ქართული მოდელი ევროპული ანალოგის მსგავსია, სადაც შიდასახელმწიფოებრივი და საერთაშორისო რეგულაციები ითვალისწინებენ ე. წ. „ქოლგის“ ტიპის, ყველა სექტორზე გავრცელებად კანონთა ფუნქციონირებას.[38] სწორედ ამით განსხვავდება პერსონალურ მონაცემთა დაცვის ევროპული და ამერიკული მოწესრიგება, სადაც ეს უკანასკნელი არ იცნობს ერთიან აქტს და აღნიშნული სფერო სხვადასხვა სპეციალური კანონით არის მოწესრიგებული. ზემოხსენებული გარემოებების გათვალისწინებით, არ იქნება გადაჭარბებული თუ ვიტყვით, რომ პერსონალურ მონაცემთა დაცვის მარეგულირებელი ქართული კანონმდებლობა ითვალისწინებს ამ სფეროში დღეს არსებულ მიდგომებს და პერსონალური მონაცემების დაცვის მძლავრ სამართლებრივ ბაზისს ქმნის.

4. პერსონალური მონაცემების დაცვა ავტორის შეხედულებით

პერსონალური მონაცემების დაცვა ადამიანის ერთ-ერთი უმნიშვნელოვანესი უფლებაა. მისი აქტუალობა საზოგადოებრივი ურთიერთობებისა და ტექნოლოგიური საშუალებების განვითარების პარალელურად მატულობს. საერთაშორისო კვლევების თანახმად, ერთი ადამიანის პერსონალური მონაცემები საშუალოდ 250-დან 1000-მდე ბაზაშია რეგისტრირებული,[39] თანამედროვე ტექნოლოგიების მეშვეობით კი მილიონობით ადამიანის შესახებ ინფორმაციის დამუშავება სულ რამდენიმე წუთშია შესაძლებელი. დღესდღეობით, ადამიანის მიერ განხორციელებული აქტივობების მნიშვნელოვანი ნაწილი დაკავშირებულია პერსონალური მონაცემების გაზიარებასა და დამუშავებასთან. პერსონალურ მონაცემთა გაზიარება აადვილებს კომუნიკაციას, თუმცა მისი გადაცემა შესაძლებელია საფრთხის შემცველი აღმოჩნდეს. მოქალაქეებმა, ისევე როგორც კომპანიებმა კრიტიკულად უნდა შეხედონ ამა თუ იმ მონაცემის შეგროვების, გავრცელების და სხვადასხვა ფორმებით დამუშავების აუცილებლობას. სასურველია, შიდასახელმწიფოებრივ დონეზე უზრუნველყოფილი იყოს პირთა ცნობიერების ამაღლება პერსონალურ მონაცემთა დაცვის კუთხით, რადგან მათ შეძლონ დაიცვან კანონით გათვალისწინებული უფლება.

---

[38] იქვე, გვ. 98.

[39] დამატებით ინფორმაცია იხ.: http://www.loialte.com.ge/ka/blogs/20 წვდომის თარიღი:23.08.2021.

ამ თემაზე მსჯელობისას ყოველთვის მახსენდება სწრაფი გადახდის აპარატებით სარგებლობის შემთხვევა, როდესაც ადამიანი ყურადღებით არ ეკიდება ქვითარს, რომელზეც წერია მისი პერსონალური ინფორმაცია, რაც ბევრჯერ გამხდარა პერსონალური მონაცემების უკანონო დამუშავების მიზეზი. ცხადია, საკუთარი მონაცემების ბოროტი მიზნებით გამოყენებაში მონაცემთა სუბიექტის დაუდევრობის წილი დიდია. არ იქნება გადამეტებული თუ ვიტყვით, რომ პერსონალური მონაცემების დაცვა თანამედროვე მსოფლიოს უდიდესი გამოწვევაა.

5. პერსონალურ მონაცემთა დამუშავება საჯარო ინფორმაციის ხელმისაწვდომობის ასპექტში

საქართველოს კონსტიტუციის მე-18 მუხლი პერსონალური მონაცემების შემცველი დოკუმენტების ხელმისაწვდომობის გარანტირებასთან ერთად, საჯარო დაწესებულებებში დაცული იმ ინფორმაციის თუ ოფიციალური დოკუმენტების ღიაობის დეკლარირებას ახდენს, რომლებიც საიდუმლო ინფორმაციას არ მოიცავს. საჯარო დაწესებულებაში არსებული და დაცული ნებისმიერი სახის ინფორმაციას და საზოგადოებისათვის მის ხელმისაწვდომობას არ აქვს თანაბარი მნიშვნელობა. საჯარო ინფორმაციის გარკვეული კატეგორიის მიმართ შესაძლოა, არსებობდეს ღიაობის მომეტებული ინტერესი. ამგვარ განსაკუთრებულ ინტერესზე უპირველესად მიუთითებს ინფორმაციის არსი, დანიშნულება და ის სიკეთე, რომლის დაცვასაც უზრუნველყოფს ამგვარი ინფორმაციის საჯაროობა. აღსანიშნავია, რომ საჯარო დაწესებულებაში არსებულ ინფორმაციაზე ხელმისაწვდომობის უფლების „შეზღუდვის კონსტიტუციურობის შეფასებისას საქართველოს საკონსტიტუციო სასამართლო მხედველობაში მიიღებს სახელმწიფო დაწესებულებაში არსებული ინფორმაციის ხასიათს და მის მნიშვნელობას ხელისუფლების საზოგადოებრივი კონტროლის თვალსაზრისით.“[40]

„ჩვეულებრივი“ პერსონალური მონაცემების შემცველი ოფიციალური დოკუმენტაციის გასაჯაროებას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-5 მუხლი უშვებს მხოლოდ იმ შემთხვევაში, თუ ეს აუცილებელია ინფორმაციის მომთხოვნი პირის კანონიერი ინტერესის დასაცავად ან კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად. აშკარაა, რომ ხსენებული ნორმა მიემართება საგამონაკლისო შემთხვევებს და მასში მითითებული „კანონიერი ინტერესი“ უფრო ვიწროა, ვიდრე პირის ზოგადი ინტერესი, მოტივაციის ყოველგვარი წინასწარი დასაბუთების გარეშე მიიღოს საჯარო ინფორმაცია.

აღსანიშნავია, რომ საქართველოს ზოგადი ადმინისტრაციული კოდექსის 28-ე მუხლის პირველი ნაწილის თანახმად, საჯარო ინფორმაცია ღიაა, გარდა კანონით გათვალისწინებული შემთხვევებისა და დადგენილი წესით სახელმწიფო, კომერციული ან პროფესიული საიდუმლოებისთვის, ან პერსონალური მონაცემებისთვის მიკუთვნებული ინფორმაციისა. ამდენად, პერსონალურ მონაცემებს მიკუთვნებული ინფორმაციის ღიაობა არ არის დაცული ზოგადი ადმინისტრაციული კოდექსით. ამდენად, „ჩვეულებრივი“ მონაცემების შემცველი ოფიციალური დოკუმენტის მოთხოვნისას ინ-

[40] საქართველოს საკონსტიტუციო სასამართლოს 2018 წლის 14 დეკემბრის №3/1/752 გადაწყვეტილება საქმეზე „ა(ა)იპ „მწვანე ალტერნატივა“ საქართველოს პარლამენტის წინააღმდეგ“, II-30.

ფორმაციის მომთხოვნი მხარე ვალდებულია დაასაბუთოს, რომ მას ამა თუ იმ დოკუმენტზე ხელმისაწვდომობის არა ზოგადი, არამედ გამორჩეული ინტერესი გააჩნია. დასახელებული სადავო ნორმით დადგენილი ბალანსი არ შეესაბამება საქართველოს კონსტიტუციით დაცულ საჯარო ინფორმაციის ხელმისაწვდომობის უფლებას. საქართველოში მოქმედი პერსონალური მონაცემების დაცვის მარეგულირებელი სამართლებრივი აქტები იძლევა იმ დასკვნის გამოტანის შესაძლებლობას, რომ საჯარო ინფორმაციის ხელმისაწვდომობასთან მიმართებით პერსონალური მონაცემების სასარგებლოდ დადგენილია პირველადი ბალანსი, რაც შესაძლოა, რიგ შემთხვევებში არ იყოს თავსებადი საქართველოს კონსტიტუციით აღიარებულ ღირებულებათა წესრიგთან.[41] საჯარო ინფორმაციის მიღების უფლება არაეფექტური გახდება, თუ მისი მოთხოვნის შემდეგ, მასში არსებული პერსონალური მონაცემების გასაჯაროების საკითხის გადაწყვეტა არაგონივრულად გაჭიანურდება.

6. პერსონალური მონაცემების სამართლიანად და გამჭვირვალედ დამუშავება

მონაცემთა დამუშავება, თუნდაც ინფორმაციის ღიაობის უზრუნველსაყოფად, იმ აუცილებელ პრინციპებს უნდა ეყრდნობოდეს, რომლებსაც ეროვნული და საერთაშორისო კანონმდებლობა ადგენს მონაცემთა დამუშავების მიმართ. წინამდებარე ნაშრომში დასახელებული პრინციპებიდან განხილული იქნება სამართლიანობის და გამჭვირვალობის პრინციპი, როგორც მონაცემთა სუბიექტის პირადი ცხოვრების უფლებაში ჩარევისას - ინსტრუმენტი, მონაცემთა კანონიერად დამუშავების გასაკონტროლებლად. მოგეხსენებათ, რომ ე. წ. სამართლიანი დამუშავების პრინციპი, ძირითადად, აწესრიგებს ურთიერთობას მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტს შორის. დამმუშავებელმა მონაცემთა სუბიექტებსა და ფართო საზოგადოებას უნდა შეატყობინოს, რომ მონაცემებს ამუშავებს კანონიერად და გამჭვირვალედ. დამუშავება არ უნდა განხორციელდეს საიდუმლოდ, ხოლო მონაცემთა სუბიექტებს უნდა ჰქონდეთ ინფორმაცია რისკების შესახებ. ამასთან, მონაცემთა დამმუშავებელმა შეძლებისდაგვარად სწრაფად უნდა შეასრულოს მონაცემთა სუბიექტის სურვილები, განსაკუთრებით, თუ ამ უკანასკნელის თანხმობა ქმნის მონაცემთა დაცვის სამართლებრივ საფუძველს.

პერსონალურ მონაცემთა დამუშავების გამჭვირვალობა მონაცემთა დამმუშავებელს ავალდებულებს, რომ მიიღოს სათანადო ზომები მონაცემთა სუბიექტების (მომხმარებლისა თუ კლიენტების) ინფორმირებისთვის მათი მონაცემების გამოყენებაზე. ე.წ. გამჭვირვალობა გულისხმობს ინფორმაციას, რომელსაც მონაცემთა სუბიექტები იღებენ მონაცემთა დამუშავების დაწყებამდე. ეს ინფორმაცია მზა ფორმით უნდა იყოს ხელმისაწვდომი მონაცემთა სუბიექტებისათვის, დამუშავების პროცესში. გამჭვირვალობა შესაძლოა მოიცავდეს იმ ინფორმაციასაც, რომელსაც მონაცემთა სუბი-

[41] იხ. მაგ. „ა(ა)იპ „მედიის განვითარების ფონდი“ და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი“ საქართველოს პარლამენტის წინააღმდეგ“ - საქართველოს საკონსტიტუციო სასამართლოს 2019 წლის 7 ივნისის N1/4/693,857 გადაწყვეტილება, ხელმისაწვდომია: წვდომის თარიღი: https://bit.ly/3zdFPE2 23.08.2021.

ექტები იღებენ საკუთარ მონაცემებზე წვდომის მოთხოვნის საფუძველზე. დამუშავების ოპერაციები მონაცემთა სუბიექტს უნდა განემარტოს მარტივი ფორმით, რათა შეძლონ გაგება, თუ რა მოსდის მათ მონაცემებს. ეს ნიშნავს, რომ მონაცემთა სუბიექტმა პერსონალური მონაცემების შეგროვებისას უნდა იცოდეს მათი დამუშავების კონკრეტული მიზანი. დამუშავების გამჭვირვალობა საჭიროებს მარტივი და გასაგები ენის გამოყენებას. შესაბამის პირებს ნათელი წარმოდგენა უნდა ჰქონდეთ პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული რისკების, წესების, უსაფრთხოების ზომებისა და უფლებების შესახებ.

მინდა აღვნიშნო, რომ ევროპის საბჭოს კანონმდებლობა ასევე განმარტავს, რომ გარკვეული ინფორმაცია დამმუშავებელმა სავალდებულოდ და პროაქტიულად უნდა წარუდგინოს მონაცემთა სუბიექტებს. კერძოდ, შესაბამის ფორმატში უნდა იყოს მითითებული (ვებგვერდის ან პერსონალური მოწყობილობის ტექნოლოგიური ინსტრუმენტების საშუალებით) მონაცემთა დამმუშავებლის (ან თანადამმუშავებლების) სახელი და მისამართი, დამუშავების სამართლებრივი საფუძველი და მიზნები, დამუშავებული მონაცემების კატეგორიები, მიმღებები და უფლებებით სარგებლობის გზები. მთავარია, ეს ინფორმაცია მონაცემთა სუბიექტს სამართლიანად და ეფექტიანად წარედგინოს. წარდგენილი ინფორმაცია უნდა იყოს ადვილად ხელმისაწვდომი, გარკვევით შედგენილი, გასაგები და მონაცემთა სუბიექტის საჭიროებებზე მორგებული (მაგ.: საჭიროების შემთხვევაში, გამოიყენონ ბავშვისთვის გასაგები ენა). ასევე, წარმოდგენილი უნდა იყოს ნებისმიერი დამატებითი ინფორმაცია, რომელიც ესაჭიროება ან ეხმარება მონაცემთა სამართლიან დამუშავებას, მაგალითად: შენახვის ვადა, ინფორმაცია დამუშავების ლოგიკური საფუძვლის ან სხვა მხარისა თუ მესამე პირისათვის მონაცემთა გადაცემის შესახებ (მათ შორის, რამდენად იცავს მესამე პირი მონაცემებს), ან დამმუშავებლის მიერ განხორციელებული ღონისძიებები მონაცემთა სათანადოდ დაცვისთვის).[42]

მონაცემებზე წვდომის უფლების შესაბამისად, მონაცემთა სუბიექტს ენიჭება უფლება, დამმუშავებლისგან მოითხოვოს დასტური მისი მონაცემების დამუშავების შესახებ, ხოლო დადასტურების შემთხვევაში მიიღოს ინფორმაცია დამუშავებულ მონაცემთა კატეგორიებზე.

ამასთან, ინფორმაციის მიღების უფლების თანახმად, იმ პირებმა, ვისი მონაცემებიც მუშავდება, მონაცემთა დამმუშავებლისა თუ უფლებამოსილი პირისაგან დამუშავების დაწყებამდე და პროაქტიულად უნდა მიიღონ ინფორმაცია ამ პროცედურის მიზნების, ხანგრძლივობისა და საშუალებების შესახებ, სხვა დეტალებთან ერთად.[43]

[42] მოდერნიზებული 108-ე კონვენციის განმარტებითი ბარათი, პუნქტი 68.

[43] მონაცემთა დაცვის ზოგადი რეგულაცია, მე-13 და მე-14 მუხლები.

7. დასკვნა

2012 წელს, პერსონალურ მონაცემთა დაცვის ინსპექტორის ინსტიტუტის შემოღებით, რომლის უფლებამონაცვლეც 2019 წლიდან სახელმწიფო ინსპექტორის სამსახურია, საჯარო ინფორმაციის ხელმისაწვდომობის მზარდი სტანდარტის შესანარჩუნებლად/შესაქმნელად გარკვეული დამატებითი ნორმატიული რეგულაციების საჭიროება ბუნებრივად გაუჩნდა ქართულ საზოგადოებას. სხვადასხვა დროს საქართველოს იუსტიციის სამინისტროში თუ სხვა შესაბამის უწყებებში მიმდინარეობდა მუშაობა ინფორმაციის თავისუფლების მარეგულირებელ სპეციალურ აქტებზე.

საზოგადოებრივი ინტერესის საპასუხოდ, დემოკრატიული საწყისების შესანარჩუნებლად და სახელმწიფოებრივი მნიშვნელობის გადაწყვეტილებების მიღებაში ხალხის ჩასართავად, გამჭვირვალობას განსაკუთრებული მნიშვნელობა აქვს. საჯარო მმართველობის გამჭვირვალობის უზრუნველყოფის უმნიშვნელოვანესი ინსტრუმენტი კი საჯარო ინფორმაციის ხელმისაწვდომობაა. პერსონალური მონაცემების შემცველი დოკუმენტები ხშირად წარმოადგენს საზოგადოების განსაკუთრებული ინტერესის საგანს. განვითარებადი ქვეყნის მოსახლეობა ბუნებრივად მოწოდებულია ჩაერთოს, მაგალითად, ბიუჯეტის რაციონალური ხარჯვის გაკონტროლებაში, ინფრასტრუქტურული გადაწყვეტილებების თუ სოციალური პოლიტიკის განმსაზღვრელი გადაწყვეტილებების მიღებაში. ამისთვის კი მათ შესაბამისი ინფორმაცია სჭირდებათ, რომელიც ხშირად პერსონალურ მონაცემებსაც შეიცავს (მაგალითად პრემიების მიმღებ პირთა წრე, საჯარო მოსამსახურეები, რომელთა მფლობელობაშიც არის ავტომანქანები და სხვა). სახელმწიფოს ერთი მხრივ გამჭვირვალობის და საზოგადოების მიმართ ამ ფორმით ანგარიშვალდებულების მოვალეობა აკისრია, მეორე მხრივ კი ვალდებულია დაიცვას პერსონალური მონაცემები და ყოველ ჯერზე ერთმანეთს დაპირისპირებული ინტერესები გულისხმიერად აწონ-დაწონოს. სწორედ დაბალანსებული გადაწყვეტილებების მიღებით არის შესაძლებელი ერთდროულად ორივე ღირებული სამართლებრივი სიკეთის დაცვა და მათი არაკონსტიტუციური შეზღუდვის პრევენცია.

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება

ავტორი: გიორგი ჩუბინიძე[44]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

საზოგადოების განვითარებასთან ერთად ყალიბდება მრავალი მნიშვნელოვანი საკითხი, რომელთა შესრულება და პატივისცემა აუცილებელია დემოკრატიულ საზოგადოებაში. სწორედ ასეთია პერსონალური მონაცემების დაცვა, მისი კანონიერად მიღება და გამოყენება. თანამედროვე სამყაროში ფაქტობრივად ახალი რეალობა ჩამოყალიბდა, რომელსაც კიბერსივრცე ეწოდება. მისი დიდი ნაწილი სახელმწიფოთა სუვერენულ ტერიტორიაზე მდებარეობს,[45] მოცემული ჩანაწერის მიხედვით, სწორედ სახელმწიფოს მიწას, საზღვაო, საჰაერო და კოსმოსურ სივრცეს ემატება კიბერსივრცე, რომელშიც ადამიანები შეუფერხებლად და უპრობლემოდ „გადაადგილდებიან“.

მობილური ტელეფონი, რომელმაც „ჩაანაცვლა ბავშვის სათამაშო“ (მარგარეტ ჰეფერნანი), თანამედროვე სამყაროს განუყოფელი ნაწილია. თითოეული პროგრამა, იქნება ეს შემეცნებითი თუ გასართობი, ჩვენს პირად ინფორმაციას მოიხმარს, ზოგჯერ, ეს თვითნებურადაც კი ხდება, ისე, რომ გაურკვეველია რისი უფლება და მოვალეობა აქვს მომხმარებელს.

პირად მონაცემებს აპლიკაციები თავიანთი ფუნქციებისთვის მოიხმარს. ეს შესაძლოა იყოს წვდომა მომხმარებლის ფოტო-ვიდეო გალერეაზე, საკონტაქტო ინფორმაცია, პირადი ინფორმაცია, როგორიც არის პირადობის მოწმობა, რაც ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკით დადგენილია, როგორც აუცილებელი დოკუმენტი, რომელიც პიროვნებას აძლევს საშუალებას თავისი იდენტურობა დაამტკიცოს.[46]

მოცემული უპირველესად სწორედ სრულწლოვან პიროვნებებს უკავშირდება, თუმცა არასრულწლოვნები და განსაკუთრებით კი მცირეწლოვანები ფაქტობრივად უფრო ხშირად იყენებენ მობილურ ტელეფონს. ასე მაგალითად, დიდ ბრიტანეთში გამოკითხულთა 39% აცხადებს, რომ ტელეფონის გარეშე ვერ იარსებებდა.[47] ეს სტატისტიკა საჭიროა იმისთვის, რომ ბავშვთა აქტიურობა და მობილური ტელეფონის გამოყენების აქტუალურობა დადგინდეს. სწორედ ამიტომ აუცილებელია იმის აღნიშვნა, თუ როგორ უნდა მოხდეს ბავშვის მონაცემების დამუშავება და იმ

[44] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნათია ეგუტიძე.

[45] დ. ბეტცი და ტ. სტივენსი, Cyberspace and the State: Toward a Strategy for CyberPower, 2013 წელი, გვ.21.

ხელმისაწვდომია აქ: https://bit.ly/2Wmhb5B წვდომის თარიღი: 01.07.2021

[46] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე nos. 46133/99 და 48183/99 სმირნოვა რუსეთის წინააღმდეგ, 24 ივლისი 2003. პარაგრაფები 95-97.

[47] The guardian-ის ოფიციალური ვებ-გვერდი, ხელმისაწვდომია აქ: https://bit.ly/3mpKWNV წვდომის თარიღი: 07.07.2021.

შემთხვევაში, თუ არასრულწლოვანი იყენებს ისეთ აპლიკაციას, რომელიც განკუთვნილია სრულწლოვანებზე, როგორ უნდა მოხდეს ამის შეზღუდვა.

ნაშრომი დაყოფილია თავებად და ქვეთავებად, რათა მობილური ტელეფონის აპლიკაციების მიერ მონაცემთა დამუშავების მნიშვნელობა და კანონიერება დადგინდეს. იგი მოიცავს სამართლებრივ, შედარებით და კრიტიკულ ანალიზს, რათა სხვადასხვა შეხედულებით დამყარდეს ერთიანი პოზიცია მოცემული საკითხისადმი.

ნაშრომის მიზანია, რომ განსაზღვროს მობილური აპლიკაციების მიერ პერსონალურ მონაცემებზე წვდომის საკითხი, ასევე სამართლებრივად შეაფასოს და კონკრეტული ქმედითი ბერკეტები ჩამოაყალიბოს ამ საკითხის მიმართ.

მნიშვნელოვანია, რომ პერსონალური მონაცემები კანონიერი გზით იქნეს მოპოვებული. თუმცა, რამდენად ახორციელებენ ამას აპლიკაციები საეჭვოა. ასევე, აპლიკაციები იქმნება სხვადასხვა სახელმწიფოში, რომლებიც შემდეგ მსოფლიოს მასშტაბით ვრცელდება, სახელმწიფოს მხრიდან კი უნდა მოხდეს კონკრეტული აპლიკაციების შეზღუდვა, თუ ისინი მოითხოვენ ნებართვას ისეთ პერსონალურ მონაცემებზე, რომლებიც მათი ფუნქციების შესასრულებლად არ არის აუცილებელი.

2. მობილური აპლიკაციები

2.1. ისტორიული მიმოხილვა

მობილური აპლიკაცია (შემდგომ - „აპლიკაცია“) არის კომპიუტერული პროგრამა, რომელიც ტელეფონის ფუნქციონირებისთვის გამოიყენება. თანამედროვე ეტაპზე მისი მნიშვნელობა უფრო გაზრდილია, თუმცა თავდაპირველად, ის წარმოადგენდა მხოლოდ კონკრეტული მობილური ტელეფონის არსებით ნაწილს. ამის ნათელ მაგალითად პირველი სმარტფონი შეგვიძლია მივიჩნიოთ - IBM Simon,[48] რომელსაც სულ რაღაც 11 აპლიკაცია ჰქონდა.[49] საბოლოოდ, ის ჩაანაცვლა უფრო პრაქტიკულმა სმარტფონებმა, რომლებიც დღესაც აქტიურად გამოიყენება. თანამედროვე ეტაპზე კი ორი უმსხვილესი ოპერატიული სისტემა ჩამოყალიბდა „android” და “ios”, რომლებსაც თავიანთი წესები და პირობები გააჩნია, როგორც მომხმარებლების, ასევე აპლიკაციებისთვის. შესაბამისად, მონაცემთა დამუშავების რამდენიმე ძირეული ეტაპი შეიძლება გაიაროს მომხმარებელმა, როდესაც აპლიკაციას ან ზოგადად მობილურს გამოიყენებს.

ზემოთ აღნიშნულ ოპერატიულ სისტემებს საერთო ჯამში დაახლოებით 3 მილიარდი ადამიანი იყენებს, რაც ფაქტობრივად ბოლო ათი წლის განმავლობაში ყალიბდებოდა. მიუხედავად ამისა, ხშირია შემთხვევა, როდესაც აპლიკაციები დაუცველია კიბერ თავდასხმისგან ან კონკრეტული პერსონალური მონაცემების დამუშავება ფარულად და პიროვნების თანხმობის გარეშეც კი ხდება.

---

[48] დამატებით იხ. ინფორმაცია ბლუმბერგის ოფიციალურ ვებ-გვერდზე, ხელმისაწვდომია: https://bloom.bg/38d6N2I წვდომის თარიღი: 01.07.2021.

[49] Simon Personal Communicator, ხელმისაწვდომია: https://bit.ly/38bUCn3 წვდომის თარიღი: 01.07.2021.

სწორედ აპლიკაციების განვითარებასთან ერთად იზრდება პერსონალური მონაცემების დაცვის საკითხი. ასე მაგალითად, თუ თავდაპირველად, ინფორმაციის მიღება ფაქტობრივად შეუძლებელი იყო, თანამედროვე ეტაპზე პიროვნება ყოველგვარი წინააღმდეგობის გარეშე გასცემს თავის ინფორმაციას და გაუცნობიერებლად აძლევს ნებართვას აპლიკაციას, რომ დაამუშავოს მისი პირადი მონაცემები.

2.2. ინტერნეტით სარგებლობის უფლება

ინტერნეტის გარეშე ნებისმიერი პროგრამის არსებობა წარმოუდგენელი იქნებოდა. მართალია, ამ „სამყაროს“ დღესდღეობით აბსოლუტურად შესწავლა წარმოუდგენელია, თუმცა თითოეულ პიროვნებას გააჩნია უფლება, რომ ისარგებლოს ინტერნეტით.[50] მოცემულს ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკაც ადასტურებს და ცხადია, სახელმწიფო ვალდებულია, რომ შექმნას ამ უფლებით სარგებლობის შესაბამისი პირობები. საქართველოს კონსტიტუციის მე-17 მუხლის მიხედვით, ყველას აქვს ინტერნეტზე წვდომისა და ინტერნეტით თავისუფლად სარგებლობის უფლება.[51] ინტერნეტზე წვდომის გარეშე ინფორმაციის მიღების შესაძლებლობა, ინფორმაციის გავრცელება, გამოხატვის თავისუფლება და სხვა მრავალი უფლება შეიზღუდებოდა. სწორედ ამიტომ, თითოეული აპლიკაცია, რომელიც სწორედ ინტერნეტით სარგებლობას მოითხოვს, ასევე შეიძლება, რომ მოექცეს ინტერნეტით სარგებლობის ცნების ქვეშ. ევროპული ქვეყნების პრაქტიკის მიხედვით, ინტერნეტი დღესდღეობით საკანონმდებლო დონეზე არის ფუნდამენტურ უფლებად აღიარებული. კერძოდ, საფრანგეთის შემთხვევაში, ყველას აქვს ინტერნეტით სარგებლობის უფლება და შესაბამისად, მასზე მოქმედებს წესები, რომელთა დაცვაც ევალებათ მომხმარებლებს.[52]

რბილი სამართლის ყველაზე მნიშვნელოვანი ჩანაწერი კი გაეროს ადამიანის უფლებათა საბჭოს 2016 წლის 27 ივნისის რეზოლუციაა, რომელმაც ინტერნეტით სარგებლობის უფლება ფაქტობრივად ადამიანის ფუნდამენტურ უფლებად აღიარა.[53]

2.3. სოციალური მედია

სოციალურ მედიას საერთო ჯამში 4 მილიარდამდე ადამიანი მოიხმარს,[54] თითოეული პიროვნება კი გაუცნობიერებლად ერთვება სისტემაში, რომელსაც თავად ვერ მართავს. ასე მაგალითად, ყველა აპლიკაციას გააჩნია საკუთარი წესები და მოთხოვნები, რომელთა შესრულებაც მომხმარებლებს ევალებათ.

[50] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე nos. 48226/10 და 14027/11 „ჩენგიზი და სხვები თურქეთის წინააღმდეგ“, 2015 წლის 1 დეკემბერი, პარაგრაფები 49 და 52.

[51] „საქართველოს კონსტიტუცია“, მუხლი 17(4), 2020 წლის 29 ივნისის მდგომარეობით.

[52] დამატებით ინფორმაცია იხ. Bfmtv-ის ოფიციალურ ვებ-გვერდზე, ხელმისაწვდომია: https://bit.ly/3D9TheF წვდომის თარიღი: 02.07.2021.

[53] გაეროს ადამიანის უფლებათა საბჭოს რეზოლუცია, ხელმისაწვდომია: https://bit.ly/2Wk1z2w წვდომის თარიღი; 03.07.2021.

[54] Social Media Usage Statistics, ხელმისაწვდომია: https://bit.ly/3mIdzGe წვდომის თარიღი: 02.07.2021.

სოციალური მედია უპირველესად არის პიროვნებებს შორის კომუნიკაციის საშუალება.[55] მოცემული ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებიდან შეიძლება დავასკვნათ, რომელშიც სოციალური მედიის ერთ-ერთი ფუნქციაა გამოხატული. მიუხედავად ამისა, სოციალურ მედიაში ვერ გავრცელდება ყველა სახის ინფორმაცია ან აზრი. სიძულვილის ენა, რომელიც განმარტებულია ევროპის საბჭოს მინისტრთა კომიტეტის მიერ 1997 წელს,[56] ასევე ყალბი ინფორმაციის გავრცელება, რაც აუცილებელია, რომ შეიზღუდოს.[57]

ნაშრომის მიზნებიდან გამომდინარე, აუცილებელია რამდენიმე წამყვანი სოციალური მედიის აღნიშვნა, რომელთა აპლიკაციებიც პიროვნების პერსონალურ მონაცემებს იყენებს. “Facebook”, “Youtube”, “Facebook Messenger” და ბოლო წლების მონაცემებით განსაკუთრებულად გააქტიურდა ჩინური კომპანია, Bytedance-ის აპლიკაცია „TikTok“.[58] საერთო ჯამში კი საშუალოდ ადამიანი სოციალურ მედიაში 145 წუთს ატარებს,[59] რა დროშიც შესაძლოა, სრულიად გაუცნობიერებლად მოხდეს ნებართვის მინიჭება ისეთ პერსონალურ საკითხზე, რომლის გაცემაც პიროვნებას არ სურდა.

საბოლოოდ, მობილური აპლიკაციები ადამიანის განუყოფელი ნაწილია, რომლებიც ფაქტობრივად პიროვნების ყველა სურვილს აკმაყოფილებს, რაც მის ცხოვრებას ამარტივებს და სანაცვლოდ კი, მოითხოვს პიროვნების პერსონალურ ინფორმაციას.

3. პერსონალური მონაცემების დამუშავება

3.1. პერსონალური მონაცემი

პერსონალური მონაცემის ცნება 1995 წლის 24 ოქტომბრის ევროპის პარლამენტის დირექტივით განისაზღვრა.[60] მოცემულის მიხედვით, პერსონალური მონაცემი არის „ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (მონაცემთა სუბიექტი); ინდივიდი იდენტიფიცირებადია, რომლის ვინაობის დადგენა შესაძლებელია პირდაპირ ან არაპირდაპირ, მათ შორის, საიდენტიფიკაციო ნომრით ან ერთი ან მეტი ნიშნით, რომელიც ეხება მის ფიზიკურ, ფსიქოლოგიურ, მენტალურ, ეკონომიკურ, კულტურულ ან სოციალურ მახასიათებელს“.[61]

---

[55] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 24917/15 „ასადი და სხვები სლოვაკეთის წინააღმდეგ“, 2020 წლის 24 მარტი.

[56] ევროპის საბჭოს მინისტრთა კომიტეტი, რეკომენდაცია R(97) 20, ხელმისაწვდომია: https://rm.coe.int/1680505d5b წვდომის თარიღი; 03.07.2021.

[57] ს. ბრედშოუ, „Responding to Fake news through regulation and automation“, ხელმისაწვდომია: https://bit.ly/2XSWrmY წვდომის თარიღი; 03.07.2021.

[58] ჰ. ტანკოვსკა, „Global social networks ranked by number of users 2021“ Statista, 2021 წლის 29 ივნისი, ხელმისაწვდომია: https://bit.ly/3yaJ8La წვდომის თარიღი: 03.07.2021.

[59] ჰ. ტანკოვსკა, „Daily social media usage worldwide 2012-2020“ Statista, 2021 წლის 3 ივლისი ხელმისაწვდომია აქ: https://bit.ly/3BcDZ7j წვდომის თარიღი: 03.07.2021.

[60] ევროპის პარლამენტის დირექტივა 95/46/EC, 1995 წლის 24 ოქტომბერი, ხელმისაწვდომია: https://bit.ly/2UH6FWe წვდომის თარიღი: 03.07.2021..

[61] იქვე. მუხლი 1.

მოცემულის ჩანაწერის მიხედვით, პერსონალური მონაცემი მოიცავს პიროვნების როგორც ფიზიკურ მატერიას, ისე ფსიქოლოგიურ წარმოდგენას, შესაბამისად, თითოეული ასეთი ფაქტის შემცველი ინფორმაცია მნიშვნელოვნად განსაზღვრავს პიროვნებას.

ევროპული სტანდარტით პერსონალური ინფორმაცია სწორედ ასე განიმარტება, თუმცა უნდა აღინიშნოს ქართული კანონმდებლობა, რომელიც სწორედ ამ დირექტივის მიხედვით არის ჩამოყალიბებული. ამასთან „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-2 მუხლის „ბ“ ქვეპუნქტი ადგენს განსაკუთრებული კატეგორიის მონაცემს, რომელიც ფაქტობრივად, შემავსებელია ზემოთ მოცემული განმარტების და პიროვნების იდენტიფიცირების საშუალებას იძლევა.[62]

დირექტივის მიერ განსაზღვრული ჩანაწერი ევროპული სახელმწიფოებისთვის თითქმის საერთოა და ისინი პერსონალურ ინფორმაციას სწორედ ერთობლივად განსაზღვრავენ, თუმცა უნდა აღინიშნოს, რომ პერსონალური ინფორმაციის ცნება კიდევ უფრო ფართო მასშტაბებს შეიძენს, რადგან ახლა უკვე ყველაზე მარტივია სხვისი პირადი ინფორმაციის მოძიება, დამუშავება ისე, რომ ამას კანონიერი მოქმედების სახე ჰქონდეს.

პერსონალურ მონაცემებთან ერთად უნდა აღინიშნოს ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლი[63] და პირადი ცხოვრების დეფინიცია. ასე მაგალითად, სტრასბურგის სასამართლოს მიხედვით, პირადი ცხოვრება ფართო ცნებაა, რომელსაც არ აქვს ამომწურავი განმარტება,[64] ამასთან იგი მოიცავს ადამიანის ფიზიკურ და ფსიქოლოგიურ მთლიანობას[65] და შეიძლება მოიცავდეს პიროვნების ფიზიკური და სოციალური იდენტობის მრავალ ასპექტს.[66]

შესაბამისად, პირადი ცხოვრების დეტალების შემცველი ინფორმაციის დამუშავებას სჭირდება შესაბამისი სტანდარტი, რათა არ მოხდეს პიროვნების უფლების შეზღუდვა.

3.2. მონაცემების დამუშავება

პერსონალურ მონაცემთა დამუშავება ნიშნავს ნებისმიერ ქმედებას, როგორიც არის შეგროვება; აღრიცხვა/ჩაწერა; ორგანიზება; სტრუქტურირება; შენახვა; ადაპტაცია ან შეცვლა; ამოღება; გაცნობა; გამოყენება; გამჟღავნება გადაცემით, გავრცელებით ან სხვაგვარი ხელმისაწვდომობით; დაჯგუფება ან კომბინირება; შეზღუდვა; წაშლა ან განადგურება.[67] მონაცემთა დამუშავების და ზოგადად პერსონალურ მონაცემთა დაცვის სფეროში მთავარ დოკუმენტად მონაცემთა დაცვის ზოგადი რეგულაცია (შემდგომ - “GDPR”) გვევლინება.

---

[62] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 2.

[63] ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენცია, მე-8 მუხლი, 1950 წელი.

[64] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 13710/88 „ნიმიტცი გერმანიის წინააღმდეგ“, 1992 წლის 16 დეკემბერი. პარაგრაფი 29.

[65] ევროპის საბჭო, „Guide on Article 8 of the European Convention on Human Rights“, 2020. გვ.21. ხელმისაწვდომია: https://bit.ly/3BoYVbi წვდომის თარიღი: 03.07.2021.

[66] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 76639/11 „დენისოვი უკრაინის წინააღმდეგ, 2018 წლის 25 სექტემბერი, პარ. 95.

[67] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (2), 2016 წელი.

GDPR-ის მიხედვით მონაცემების დამუშავებას სჭირდება კონკრეტული პირობების შესრულება, ასეთად კი განსაზღვრულია დამუშავების კანონიერება, სამართლიანობა და გამჭვირვალობა.[68]

მონაცემთა დამუშავებისთვის სწორედ GDPR-ის მოთხოვნების გათვალისწინება არის აუცილებელი. ამასთან ევროკავშირთან ერთად ევროპის საბჭოს მოდერნიზებული 108-ე კონვენციაც განსაზღვრავს მოცემულ ჩანაწერებს.[69]

მონაცემთა დამუშავების ეს ზოგადი მოთხოვნები უნდა იქნეს დაკმაყოფილებული, თუმცა მობილური აპლიკაციების მიერ მონაცემთა დამუშავება შესაძლოა, გაუკონტროლებელი იყოს და პიროვნებას არ ჰქონდეს შესაძლებლობა, რომ თავისი უფლებები დაიცვას.

4. მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება

პერსონალურ მონაცემთა დაცვის ზემოთ აღნიშნული დებულებები სრულად ვრცელდება მობილურ აპლიკაციებზე და შესაბამისად, მათთვის წაყენებული მოთხოვნები შესასრულებლად სავალდებულოა. მობილურმა აპლიკაციამ უნდა შეაგროვოს მხოლოდ ისეთი სახის ინფორმაცია, რომელიც მკაცრად საჭიროა კანონიერი ფუნქციების შესასრულებლად, როგორც თავდაპირველად იყო განსაზღვრული და დაგეგმილი.[70] ამასთან ერთად, პერსონალური მონაცემების გამოყენებამდე, აპლიკაციებმა უნდა შეატყობინონ ამის თაობაზე მომხმარებლებს, რაც აშკარად გამოხატული ფორმით უნდა იქნეს მიწოდებული.[71]

მობილურმა აპლიკაციებმა სწორედ ლეგიტიმური მიზნის მისაღწევად უნდა გამოიყენონ პერსონალური ინფორმაცია და ამასთან, აუცილებელია, რომ ასეთი სახის ინფორმაციის ბოროტად გამოყენება არ მოხდეს.

4.1. „Facebook" და „Facebook Messenger"

Facebook-ის 533 მილიონი მომხმარებლის პერსონალური ინფორმაცია ინტერნეტ სივრცეში გავრცელდა.[72] ამ სათაურით ვრცელდებოდა სტატიები მსოფლიოში ყველაზე გავრცელებული სოციალური მედიის შესახებ. მიუხედავად იმისა, რომ მოცემული ქმედება Facebook-ის მიერ მონაცემთა დამუშავებას არ უკავშირდება და კიბერდანაშაულის ნიშნებს შეიცავს, ყოველი ასეთი ჩარევა მკვეთრად უარყოფით დამოკიდებულებას იწვევს საზოგადოებაში.

[68] იქვე. მუხლი 5 (1).

[69] ევროპის საბჭოს მოდერნიზებული 108-ე კონვენცია.

[70] ევროპის კავშირი, Guidelines on the protection of personal data processed by mobile applications, 2016 წლის ნოემბერი. გვ. 9.

[71] იქვე.

[72] ა. ჰოლმსი, "533 million Facebook users' phone numbers and personal data have been leaked online" insider, 2021 წლის 3 აპრილი, ხელმისაწვდომია: https://bit.ly/3B6pjpZ წვდომის თარიღი: 03.07.2021.

ინფორმაციის უკანონო მოპოვება და გავრცელება 2021 წელს მოხდა, მანამდე კი თავად Facebook-ის შემქმნელს მოუწია კითხვებზე პასუხი, რომლებიც ამ აპლიკაციის მიერ მონაცემების შეგროვებას ეხებოდა. ამასთან, აპლიკაციას აქვს წვდომა ისეთ პერსონალურ საკითხებზე, როგორიც არის კამერა, სატელეფონო კონტაქტები, ადგილმდებარეობა, მიკროფონი და ტელეფონის მეხსიერება, რაც მოიცავს ყველა სხვა აპლიკაციას. ამასთან, აპლიკაცია ამუშავებს და ინახავს ყველა სახის ინფორმაციას, თუ ვისთან აქვს ყველაზე ხშირად მომხმარებელს კონტაქტი, ასევე რომელ პროდუქტებსა თუ ვებ-გვერდებს სტუმრობს ის. ასევე ფინანსური სახის ინფორმაცია, საკრედიტო ბარათის ნომერი და ყველა ტრანზაქცია, რომელიც განხორციელდა ამ ბარათით.

მომხმარებლის მითითების შემთხვევაში, Facebook-ს შესაძლოა, ჰქონდეს წვდომა განსაკუთრებული კატეგორიის მონაცემებზე, როგორიც არის პიროვნების რელიგია ან ფილოსოფიური მრწამსი, პოლიტიკური შეხედულებები. აპლიკაციას ფაქტობრივად ყველა სახის ინფორმაციაზე აქვს წვდომა, რომელსაც არა მარტო მის ფარგლებში ავრცელებს, არამედ სხვა აპლიკაციებსაც აწვდის.

რაც შეეხება „Facebook Messenger"-ს, მას დამატებით წვდომა აქვს მიმოწერაზე. ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის მიხედვით, მიმოწერა მოიცავს არა მარტო კლასიკური სახით, წერილის ფორმით, არამედ ელექტრონულ მიმოწერას[73] ან მობილური ტელეფონის მეშვეობით.[74] ამის მიხედვით კი მასში ჩარევა, განსაკუთრებით თუ ის წარმოადგენს ადვოკატსა და კლიენტს შორის ურთიერთკავშირს, წარმოადგენს კონვენციის მე-8 მუხლით გათვალისწინებული უფლებების უხეშ დარღვევას.[75] აქედან გამომდინარე, შესაძლოა, რომ მოხდეს კონკრეტული მიმოწერის დამუშავება, რომლის შემოწმება და „გახსნა" ფაქტობრივად დაუშვებელია.

ამასთან, თუ ფარული საგამოძიებო მოქმედებების ჩატარებას შესაბამისი წესების შესრულება და კანონით გაწერილი პროცედურების გავლა სჭირდება, აპლიკაციების მიერ პერსონალურ მონაცემებზე განუსაზღვრელი წვდომის გამო, შესაძლებელია, სრულიად მარტივად იქნეს დამუშავებული ინფორმაცია და კონკრეტული პიროვნების ან პიროვნებების შესახებ სხვადასხვა სახის ინფორმაცია შეგროვდეს.

4.2. „Google"

1998 წელს შექმნილმა საძიებო პროგრამა Google-მა მთელი მსოფლიო სულ რაღაც რამდენიმე წელიწადში მოიცვა. დღესდღეობით, ის მართავს მრავალ აპლიკაციასა და პროგრამას, ეს კომპლექსური სისტემა კი ქმნის ერთიან სივრცეს. მილიარდობით ადამიანი კი ყოველდღიურად გასცემს თანხმობას მისი პირადი ინფორმაციის წვდომაზე.

---

[73] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 62617/00 „კოპლენდი გაერთიანებული სამეფოს წინააღმდეგ", 2007 წლის 3 აპრილი, პარ. 41.

[74] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 459/18 „საბერი ნორვეგიის წინააღმდეგ" 2020 წლის 17 დეკემბერი, პარ. 48.

[75] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე no. 28798/13 „ლორენტი საფრანგეთის წინააღმდეგ", 2018 წლის 24 მაისის გადაწყვეტილება, პარ. 36.

თუმცა, უშუალოდ google-ის განხილვამდე უნდა აღინიშნოს, მის მიერ შექმნილი „android". 2018 წელს ჩატარებული კვლევის მიხედვით, „android"-ის აპლიკაციები უფრო მეტ საეჭვო მოთხოვნას გასცემენ, ვიდრე მისი კონკურენტი ios-ის.[76] ამასთან, პერსონალურ ინფორმაციაზე წვდომის აუცილებლობის დასაბუთება ხშირ შემთხვევაში არ არის მოცემული.[77] „სარისკო ნებართვები", რომლებიც მოიცავს მომხმარებლის პერსონალურ ინფორმაციას, ხშირად შესაძლოა, რომ სრულიად შეესაბამებოდეს აპლიკაციის ფუნქციებს. მაგალითად, ტაქსის კომპანიის მიერ მომხმარებლის ადგილმდებარეობაზე წვდომა. თუმცა,, თუ ასეთი სახის კომპანია მოითხოვს შეტყობინებებზე, კამერაზე ან თუნდაც კალენდარზე წვდომას, მაშინ ამ აპლიკაციის მოთხოვნები გახდება საეჭვო.

დღესდღეობით, ერთ-ერთი გავრცელებული აპლიკაცია „Youtube", რომელიც პირდაპირ არის დაკავშირებული Gmail-თან. მოცემულის მიხედვით, საბოლოოდ, თითოეულ პერსონალურ ინფორმაციას „Google" ამუშავებს და შესაბამისად, აწვდის სხვადასხვა აპლიკაციას.

მთავარი პრობლემა შესაძლოა, რომ წარმოიშვას იმ შიდა აპლიკაციების მიერ, რომლებიც „Google Play Store"-ში არსებობს. ასე მაგალითად, ზოგიერთმა აპლიკაციამ, შესაძლოა, ისეთი ნებართვა მოითხოვოს, რომელიც მის ფუნქციონირებას არ სჭირდება.[78]

საბოლოოდ, მობილური აპლიკაციები იღებენ და ამუშავებენ ინფორმაციას მომხმარებლის აშკარა თანხმობის შემდგომ და ისინი მას იყენებენ თავიანთი ფუნქციების შესასრულებლად, ასევე სხვა აპლიკაციებთან წვდომისა და მათ შორის კავშირების დასამყარებლად.

4.3. ბავშვთა უფლებები მობილუს აპლიკაციებში

მობილური აპლიკაციების მთავარი პრობლემა არის პიროვნებების გადამოწმების შესაძლებლობა და ის, თუ ვინ იყენებს კონკრეტულ მობილურ ტელეფონს. ამის ნათელი მაგალითი კი „Facebook"-ის მოთხოვნაა, რომლის მიხედვით, 13 წლამდე ბავშვებს არ აქვთ უფლება, შექმნან ანგარიში. ამის მიუხედავად, 13 წლამდე ბავშვები მაინც იყენებენ აპლიკაციას[79] და შესაბამისად, მათზეც ჩვეულებრივ ვრცელდება პერსონალური მონაცემების შეგროვების ნორმები.

შესაძლოა, რომ ბავშვს აქვს უფლება ინტერნეტით სარგებლობაზე,[80] მაგრამ თითოეული მონაცემის შეგროვება, რაც ბავშვს შეეხება, უნდა იყოს აშკარად გამოხატული და კანონმდებლობის შესაბამისი. კერძოდ, ისეთი სახის აპლიკაციას, რომელიც არ მოითხოვს პიროვნების იდენტიფი-

[76] გ. კლერი, "Mobile Privacy: What Do Your Apps Know About You?" Broadcom, 2018 16 აგვისტო. ხელმისაწვდომია: https://bit.ly/3sH-dune წვდომის თარიღი: 03.07.2021.

[77] იქვე.

[78] იხ. სქოლიო 77, აპლიკაცია „rightest Flashlight LED - Super Bright Torch."

[79] Thorn, Benenson Strategy Group, Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking, research,2021 წელი, გვ. 42. ხელმისაწვდომია: https://bit.ly/3zcsw76 წვდომის თარიღი: 03.07.2021

[80] საქართველოს კონსტიტუცია, მუხლი 17, 2020 წლის 29 ივნისი. ასევე იხ. ბავშვის უფლებათა კოდექსი, მუხლი 14, 2019 წლის 27 სექტემბერი.

ცირებას, არ შეუძლია დააზუსტოს მომხმარებლის ასაკი. ამასთან, ასაკის ხელოვნური ბარიერის გადაკვეთა და პიროვნების გაყალბება ინტერნეტ სივრცეში ნებისმიერ პიროვნებას შეუძლია. შესაბამისად, მონაცემების დამუშავებისას აუცილებელია, რომ ბავშვის საუკეთესო ინტერესი იქნეს გათვალისწინებული და იგი მძიმე მდგომარეობაში არ ჩავარდეს, რათა არ დაირღვევს ერთი მხრივ, შიდა კანონმდებლობა და მეორე მხრივ, საერთაშორისო სამართლებრივი ნორმები.

სახელმწიფოს მხრიდან ყველა აპლიკაციისა თუ პროგრამის აკრძალვა ვერ მოხდება, შესაბამისად, ისეთი სახის მონაცემების დამუშავებისთვის, რომლებიც ბავშვთა უფლებებს პირდაპირ არღვევს, საჭიროა კონკრეტული ზომების მიღება. მაგალითად, მშობლებმა უნდა იცოდნენ ისეთი აპლიკაციების შესახებ, რომლებიც ბავშვის მობილური ტელეფონის ნომრებს აგროვებს, წვდომა აქვს პაროლებზე, განსაკუთრებით საჭიროა ისეთი აპლიკაციებისგან დაცვა, რომლებშიც ბავშვს უცხო პიროვნებებთან ექნება პირდაპირი კონტაქტი. ასეთ აპლიკაციებში არ არის გამორიცხული ბავშვის შესახებ ინფორმაციის დამუშავება არალეგიტიმური მიზნებისთვის მოხდეს. ამასთან, აპლიკაციები, რომლითაც ბავშვს კონკრეტული პროდუქტის შეძენა შეუძლია, ასევე წარმოადგენს მთავარ გამოწვევას, რადგან ასეთ შემთხვევაში ბავშვის საუკეთესო ინტერესი დაირღვევა და ამასთან, მასზე აპლიკაციას მეტი წვდომა ექნება.[81]

ერთ-ერთ გამოსავალს კი “parental control” წარმოადგენს. ამ აპლიკაციით ბავშვის კანონიერ წარმომადგენელს აქვს უფლება, რომ შეზღუდოს ან გააკონტროლოს ბავშვის ჩართულობა კონკრეტულ აპლიკაციაში და აპლიკაციის მიერ მონაცემთა დამუშავება ფაქტობრივად შეამციროს.

5. დასკვნა

პერსონალური მონაცემების მოპოვება და დამუშავება თანამედროვე საერთაშორისო სამართალში მნიშვნელოვან გამოწვევას წარმოადგენს სახელმწიფოებისთვის. ნაშრომში მოცემული მსჯელობები შეესაბამება საერთაშორისო სტანდარტებსა და კონკრეტული ქმედითი ბერკეტები განსაზღვრულია სხვადასხვა ავტორის მიერ.

მობილურ აპლიკაციებს ხშირად აქვთ წვდომა მომხმარებლის ყველა ფაილსა და შეტყობინებაზე. ამასთან, რამდენი ხნით გროვება ინფორმაცია და როდის განადგურდება ის შესაძლოა, მომხმარებელმა არ იცოდეს. ამის თავიდან ასაცილებლად, აპლიკაციებში ნათლად უნდა იყოს განსაზღვრული, თუ როგორ მოხდება კონკრეტული ინფორმაციის დამუშავება და შემდგომ მისი გამოყენება, ხოლო ამის შემდგომ მომხმარებელი თავად გადაწყვეტს, სურს თუ არა აპლიკაციის გადმოწერა.

მიუხედავად იმისა, რომ მრავალი საერთაშორისო სამართლებრივი შეთანხმება არსებობს, სახელმწიფოები შიდა სამართლებრივ სისტემებში აყალიბებენ მათთვის სასურველ კანონმდებლობას, რომლებიც საერთო ჯამში სრულიად შეესაბამება საერთაშორისო სამართალს. საქართველოს რეალობაში, მრავლად არსებობს აპლიკაციები და მათი ჩამოტვირთვის წყაროები, რომლებშიც

[81] “Do your kids’ mobile apps respect their privacy?“ webroot, ხელმისწავდომია: https://bit.ly/3zcF3Hu წვდომის თარიღი: 24.08.2021.

პიროვნების პერსონალური მონაცემების დამუშავება მისგან დამოუკიდებლად ხდება. ამის მთავარი გამოხატულება ის საეჭვო აპლიკაციებია, რომლებსაც არ გააჩნიათ „წარსული“ და მობილურ ტელეფონში არა დაცული წყაროებიდან, არამედ ე. წ. „browser”-დან მოხდა, რომელშიც ყველა სახის აპლიკაცია და პროგრამა არსებობს.

სრულწლოვანი პირისთვის, განსაკუთრებით, თუ მან უცხო ენა იცის, მარტივია აპლიკაციის შესახებ ინფორმაციების მოძიება. თუმცა, არასრულწლოვანი ან მცირეწლოვანი, რომელიც მისთვის მინიჭებული უფლებით სარგებლობის, ინტერნეტის მოხმარების დროს, შესაძლოა, სრულიად დაუცველი იყოს აპლიკაციების მიერ პერსონალური მონაცემების შეგროვებისას. საქართველოს კანონმდებლობის მიხედვით,[82] პირს არ შეიძლება უარი ეთქვას იმ ინფორმაციის გაცემაზე, რომელიც მოიცავს პერსონალურ მონაცემებს ან ჩანაწერებს მის შესახებ.[83] ბავშვის შემთხვევაში კი ერთვება კანონიერი წარმომადგენელი, რომელსაც თუ არ ექნება ინფორმაცია ბავშვის მიერ გამოყენებული აპლიკაციების შესახებ, მაშინ ვერ დაიცავს მის უფლებებს. ამიტომ ბავშვები მძიმე მდგომარეობაში ჩავარდებიან, თუ მათი კანონიერი წარმომადგენლები მათი უფლებების დასაცავად კონკრეტულ ნაბიჯებს არ გადადგამენ.

იმისთვის, რომ არ დაირღვეს პიროვნების პერსონალური მონაცემების დაცვის უფლება და მის შესახებ კონკრეტული კონფიდენციალური ინფორმაცია არ გადაეცეს სხვა პირებს, აუცილებელია, რომ აპლიკაციები დაცული წყაროდან იქნეს ჩამოტვირთული, რომელსაც მომხმარებელიც ენდობა და საერთაშორისო მასშტაბითაც ასეთად აღიარებულია. სწორედ ასეთ შემთხვევაში იქნება დაცული პიროვნების უფლებები და მას ექნება ინფორმაცია, თუ სად და როდის დამუშავდა მის შესახებ მონაცემები.

საბოლოოდ, მიმაჩნია, რომ უნდა მოხდეს პიროვნებების ინფორმირება და მათთვის კონკრეტული რჩევების თუ რეკომენდაციების მიწოდება, რათა მათი პერსონალური მონაცემები დაცული იყოს. რისკებისა და საეჭვო აპლიკაციების შემთხვევაში კი მომხმარებელს შეეძლება ამოიცნოს ასეთი აპლიკაცია და მას არ მიანიჭოს ნებართვა ცალკეულ საკითხებზე. ასევე დაცული წყაროების მითითების შემთხვევაში, მათ ეცოდინებათ, რომ პერსონალური ინფორმაცია დაცულია და იგი გამოიყენება ლეგიტიმური მიზნებისთვის.

ნაშრომის საერთო მიზანი დადგენილია და აპლიკაციებში პერსონალური მონაცემების დაცვის საკითხი აშკარად გამოხატულია. ამასთან მთავარია, რომ აპლიკაციებს არ მიენიჭოთ ყველა სახის პირად ინფორმაციაზე წვდომის უფლება, წინააღმდეგ შემთხვევაში, მათ შეეძლებათ ნებისმიერი სახის პერსონალური მონაცემის დამუშავება.

[82] საქართველოს სამოქალაქო კოდექსი, მუხლი 18[1], 2020 წლის 29 დეკემბერის მდგომარეობით.

[83] იქვე. მუხლი 18[1](2).

კონფლიქტი პერსონალურ მონაცემთა დაცვის უფლებასა და საჯარო ინფორმაციის ხელმისაწვდომობის უფლებას შორის და მისი დაძლევის კონსტიტუციურ-სამართლებრივი პერსპექტივები

ავტორი: ვასილ ჟიჟიაშვილი[84]
თავისუფალი უნივერსიტეტი

1. შესავალი

დემოკრატიული სახელმწიფოსთვის უჩვეულო არ არის ერთმანეთთან კონფლიქტში მყოფი უფლებების თანაარსებობა. ერთი უფლების ფარგლები და შინაარსი შესაძლოა წინააღმდეგობაში მოდიოდეს მეორე უფლების განხორციელებასთან, რა დროსაც წარმოიშობა საკითხი იმის შესახებ, თუ რომელს უნდა მიენიჭოს უპირატესობა. კანონმდებლის მიერ კონფლიქტში მყოფი უფლებების დაბალანსება ყოველთვის გულისხმობს ერთი უფლების სასიკეთოდ მეორე უფლების შეზღუდვას. ასეთ დროს კი არა უპირატეს მდგომარეობაში აღმოჩენილმა ადამიანებმა კანონმდებლის მიერ კონფლიქტში მყოფი უფლებების სამართლიანი დაბალანსების მცდელობა სადავო გახადონ საკონსტიტუციო სასამართლოში საკითხის კონსტიტუციურობის გარკვევის მიზნით. მაშინ როდესაც საპარლამენტო განხილვების დროს კანონში ასახული უფლებრივი ბალანსი შესაძლოა პოლიტიკური მიზანშეწონილობით იყოს განპირობებული, საკონსტიტუციო სასამართლოს მიერ კონფლიქტში მყოფი უფლებების დაბალანსება მოითხოვს სამართლებრივ არგუმენტაციას.

წინამდებარე ნაშრომი საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკის ანალიზის საფუძველზე მიზნად ისახავს იმ სახელმძღვანელო პრინციპების იდენტიფიცირებას, რომლითაც საკონსტიტუციო სასამართლო ხელმძღვანელობს საჯარო ინფორმაციის ხელმისაწვდომობისა და პერსონალური მონაცემებს შორის არსებული უფლებრივი კონფლიქტის დაბალანსებისას. საკითხი მნიშვნელოვანია იმდენად, რამდენადაც საზოგადოების მიერ ხელისუფლების კონტროლის ყველაზე ეფექტურ საშუალებას საჯარო ინფორმაციის ანალიზი წარმოადგენს, თუმცა ამავდროულად საჯარო დაწესებულებებში არსებულ ოფიციალურ დოკუმენტებში არსებული კერძო პირების პერსონალური მონაცემების გამჟღავნებით შესაძლოა დაზიანდნენ პერსონალურ მონაცემთა სუბიექტები. ნაშრომში წამოჭრილი საკითხის გამოკვლევა კი შესაძლებლობას მოგვცემს შევიქმნათ წარმოდგენა სად გადის ზღვარი საჯარო ინფორმაციის გამოთხოვის გზით საზოგადოების მიერ ხელისუფლების კონტროლის ინტერესსა და პერსონალური მონაცემების სუბიექტის პირადი ცხოვრების ხელშეუხებლობას შორის.

[84] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - დონარი ლონდარიძე.

2. საკონსტიტუციო სასამართლოს პრაქტიკა საჯარო ინფორმაციის თავისუფლებისა და პერონალური მონაცემების დაცვის დაბალანსების შესახებ

სანამ უშუალოდ განვიხილავთ საკონსტიტუციო სასამართლოს გადაწყვეტილებებს, რომელშიც სასამართლო ცდილობს თანაზომიერების ტესტის გამოყენებით დააბალანსოს საჯარო ინფორმაციის თავისუფლებისა და პერსონალური მონაცემების დაცვის უფლება, ასევე მნიშვნელოვანია მოკლედ მიმოვიხილოთ, თუ როგორია კონსტიტუციის მე-18 მუხლის ფარგლები და ფორმალური გარანტიები, რომელთა დაუცველობა შესაძლოა სადავო ნორმის არაკონსტიტუციურობის საფუძველი გახდეს.

2.1. კონსტიტუციის მე-18 მუხლის მე-2 ნაწილით დაცული უფლების ფარგლები

საკონსტიტუციო სასამართლოს პრაქტიკა საჯარო ინფორმაციის უფლებასთან დაკავშირებით უკავშირდება მისი ფორმალური და მატერიალური კონსტიტუციური გარანტიების შექმნასა და განმარტებას. კონსტიტუციის მე-18 მუხლის მე-2 პუნქტის მიხედვით, ყველას აქვს უფლება კანონით დადგენილი წესით გაეცნოს საჯარო დაწესებულებაში მასზე არსებულ ან სხვა ინფორმაციას ან ოფიციალურ დოკუმენტს გარდა იმ შემთხვევისა, როდესაც იგი შეიცავს კომერციულ ან პროფესიულ საიდუმლოებას ან დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების ან სამართალწარმოების ინტერესების დასაცავად კანონით ან კანონით დადგენილი წესით აღიარებულია სახელმწიფო საიდუმლოებად. ვინაიდან კონსტიტუციურ ტერმინებს აქვთ ავტონომიური სამართლებრივი მნიშვნელობა ის თუ რას გულისხმობს კონსტიტუციის მე-18 მუხლის მე-2 პუნქტით დაცული უფლების რეალური შინაარსი, უნდა განვიხილოთ საკონსტიტუციო სასამართლოს პრაქტიკის დეტალური ანალიზის გადმოსახედიდან.[85]

საზოგადოებას შესაძლოა ინტერესი გააჩნდეს ნებისმიერი დაწესებულებიდან საჯარო ინფორმაციის გამოთხოვასთან დაკავშირებით, თუმცა კონსტიტუციის მე-18 მუხლის მე-2 პუნქტით დაცულია პირის უფლება გაეცნოს მხოლოდ „საჯარო დაწესებულებაში“ არსებულ ოფიციალურ დოკუმენტებს. მაგალითად, ერთ-ერთ საქმეში მოსარჩელე ითხოვდა უფლება ჰქონოდა რელიგიური და პოლიტიკური დაწესებულებებიდან მიეღო საჯარო ინფორმაცია, რომელიც შეეხებოდა სახელმწიფო და ადგილობრივი თვითმმართველობის ბიუჯეტიდან მიღებული დაფინანსების ხარჯვას. საკონსტიტუციო სასამართლომ განმარტა, რომ იურიდიული პირები საჯარო დაწესებულებად შეიძლება ჩაითვალოს იმ შემთხვევაში, როდესაც ისინი კონსტიტუციით ან/და კანონით დელეგირებული უფლებამოსილების ფარგლებში ახორციელებენ საჯარო სამართლებრივ უფლებამოსილებას და ემსახურებიან სახელმწიფო ამოცანების შესრულებას. ამასთან, ვინაიდან არც

[85] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე №2/4/532,533 „საქართველოს მოქალაქეები - ირაკლი ქემოკლიძე და დავით ხარაძე საქართველოს პარლამენტის წინააღმდეგ“, 2014 წლის 8 ოქტომბერი, სამოტივაციო ნაწილის პარ. 63.

პოლიტიკური ორგანიზაციები და არც რელიგიური ორგანიზაციები არ ახორციელებდნენ საჯარო უფლებამოსილებებს ისინი ვერ განიხილებოდნენ როგორც საჯარო დაწესებულებები.[86]

აქვე აღსანიშნავია, რომ გარდა საჯარო ინფორმაციის სახელმწიფო დაწესებულებებში არსებული ოფიციალური ჩანაწერებიდან გაცნობისა, კონსტიტუცია ასევე იცავს სხვაგვარი ინფორმაციული წყაროების საშუალებით ინფორმაციის მიღებისა და გავრცელების უფლებასაც. კონსტიტუციის მე-17 მუხლის მე-2 პუნქტის მიხედვით, ყოველ ადამიანს აქვს უფლება თავისუფლად მიიღოს და გაავრცელოს ინფორმაცია. საკონსტიტუციო სასამართლოს პრაქტიკის მიხედვით, საქართველოს კონსტიტუციის მე-18 მუხლის მე-2 პუნქტით დაცული უფლებრივი ინფორმაციაზე ხელმისაწვდომობის კონსტიტუციურ-სამართლებრივი რეჟიმი განსხვავდება საყოველთაოდ ხელმისაწვდომი ინფორმაციის წყაროებიდან ინფორმაციის მიღების სამართლებრივი რეჟიმისაგან".[87]

2.2. კონსტიტუციის მე-18 მუხლის მე-2 ნაწილით დაცული ფორმალური კონსტიტუციური გარანტიები

კონსტიტუციის მიხედვით, საჯარო ინფორმაციისა და პერსონალურ მონაცემთა უფლებებს შორის ბალანსის გადაწყვეტა უნდა მოხდეს შესაბამისი ფორმალური პროცედურების დაცვით. როდესაც კანონმდებელს სურს პერონალური მონაცემების დაცვის მოტივით შეზღუდოს საჯარო ინფორმაციაზე ხელმისაწვდომობა, აღნიშნული უნდა განახორციელოს კანონის საფუძველზე, ვინაიდან კონსტიტუცია საჯარო ინფორმაციის ხელმისაწვდომობის უფლების შეზღუდვას მხოლოდ კანონის საფუძველზე ითვალისწინებს. საკონსტიტუციო სასამართლოს განმარტებით, კონსტიტუციის მე-18 მუხლის მე-2 პუნქტი განამტკიცებს სახელმწიფო დაწესებულებებში არსებული ოფიციალური დოკუმენტების „კანონით დადგენილი წესით" გაცნობის უფლებას. აღნიშნულიდან გამომდინარე, საქართველოს კონსტიტუცია ადგენს სახელმწიფო დაწესებულებების ოფიციალურ დოკუმენტებში არსებული ინფორმაციის ხელმისაწვდომობასთან დაკავშირებული საკითხების კანონით მოწესრიგების ფორმალურ მოთხოვნას".[88] ფორმალური კანონიერების მოთხოვნა კი დაკმაყოფილდება მაშინ, როდესაც საჯარო ინფორმაციის ხელმისაწვდომობის საკითხი: 1) უშუალოდ მოწესრიგებულია კანონით ან; 2) კანონმდებელი კანონით მოახდენს საკითხის მოწესრიგების უფლებამოსილების დელეგირებას შესაბამის ორგანოზე.[89] საქმეში სადაც ფუნდამენტური კვლევებისათვის სახელმწიფო სამეცნიერო გრანტების შეფასების კომისიის დამოუკიდებელ ექსპერტთა ვინაობა კონფიდენციალურად იყო მიჩნეული მთავრობის დადგენილების საფუძველზე, მაშინ როდესაც მთავრობას არ ჰქონდა დელეგირებული აღნიშნული საკითხის

[86] საქართველოს საკონსტიტუციო სასამართლოს განჩინება საქმეზე N1/1/618 „საქართველოს მოქალაქეები - გიორგი კეკენაძე, ნინი კვენეტაძე და ბესიკი გვენეტაძე საქართველოს პარლამენტის წინააღმდეგ, 2016 წელის 26 თებერვალი, სამოტივაციო ნაწილის პარ. 8-9.

[87] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N2/3/406,408 „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ", 2008 წლის 30 ოქტომბერი სამოტივაციო ნაწილის პარ. 11.

[88] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/4/757 „საქართველოს მოქალაქე გიორგი კრავეიშვილი საქართველოს მთავრობის წინააღმდეგ", 2017 წლის 27 მარტი, სამოტივაციო ნაწილის პარ. 19.

[89] იქვე.

გადაწყვეტის უფლებამოსილება, სასამართლომ მიიჩნია, რომ სადავო ნორმა ვერ აკმაყოფილებდა კონსტიტუციის მე-18 მუხლის მე-2 პუნქტით დადგენილ ფორმალურ კრიტერიუმს უფლების შეზღუდვის კანონით დადგენის აუცილებლობის თაობაზე.[90]

2.3. ბალანსი საჯარო ინფორმაციის ხელმისაწვდომობასა და პერსონალური მონაცემების დაცვის უფლებას შორის

საქართველოს საკონსტიტუციო სასამართლოს პრაქტიკაში არსებობს რამდენიმე გადაწყვეტილება სადაც სასამართლოს მოუწია დაებალანსებინა ერთი მხრივ, საჯარო ინფორმაციაზე ხელმისაწვდომობისა და, მეორე მხრივ, პერსონალურ მონაცემთა დაცვის ინტერესები. სასამართლოს მიერ ინტერესთა დაბალანსების პრაქტიკამ დროთა განმავლობაში პროგრესი განიცადა და სასამართლოს მოქმედი პრაქტიკა სათანადოდ უზრუნველყოფს საზოგადოებაში არსებულ აღნიშნული ინტერესების სამართლიან და გონივრულ დაბალანსებას.

სასამართლოს თავდაპირველ გადაწყვეტილებებზე დაკვირვებით შეგვიძლია ვთქვათ, რომ სასამართლო ოფიციალური დოკუმენტებისადმი საზოგადოებრივი ინტერესისა და პერსონალური მონაცემების დაცვის საკითხს სათანადო დასაბუთების გარეშე წყვეტდა. ასე მაგალითად, 2004 წლის ერთ-ერთ გადაწყვეტილებაში სასამართლომ არაკონსტიტუციურად არ მიიჩნია ის ნორმები, რომელიც მოსამართლეთა წინააღმდეგ დისციპლინური სამართალწარმოების დასრულების შედეგად მიღებული გადაწყვეტილების სამოტივაციო ნაწილზე ზღუდავდა საზოგადოების ხელმისაწვდომობას.[91] აღნიშნული გადაწყვეტილების მიღებისას სასამართლომ არ გაითვალისწინა ის კონტექსტი, თუ რა ხარისხის ინტერესი შეიძლება გააჩნდეს საზოგადოებას მოსამართლეთა დისციპლინური პასუხისმგებლობის საკითხთან დაკავშირებით. თუმცა, აღნიშნული პერიოდის სასამართლო გადაწყვეტილებებისადმი კრიტიკისას უნდა გავითვალისწინოთ ის გარემოება, რომ პირველი გადაწყვეტილებების მიღებისას საკონსტიტუციო სასამართლოს ჰქონდა მნიშვნელოვანი გამოწვევა საკონსტიტუციო მართლმსაჯულების ინსტიტუციური გამოცდილების არარსებობიდან გამომდინარე. თუმცა, განსხვავებით ძველი გადაწყვეტილებებისგან სასამართლოს გადაწყვეტილებების კრიტიკა უფრო მკაცრი შეიძლება იყოს იმ გადაწყვეტილებებზე, როდესაც სასამართლოს უკვე ჰქონდა საკმაო გამოცდილება საკონსტიტუციო მართლმსაჯულების პროცესში გამოეყენებინა ინტერესთა დაბალანსების მექანიზმი თანაზომიერების ტესტის სახით.

წინამდებარე ნაშრომის მიზნებისთვის, მნიშვნელოვანია, განვიხილოთ საკონსტიტუციო სასამართლოს N2/3/406,408 გადაწყვეტილება. საქმეში სადავოდ გამხდარი ნორმების მიხედვით საზოგადოებისთვის ხელმისაწვდომი არ იყო გადასახადის გადამხდელზე არსებული მთელი რიგი მონაცემები. შესაბამისად, სასამართლოს უნდა დაებალანსებინა ერთი მხრივ საზოგადოების

[90] იქვე, სამოტივაციო ნაწილის პარ. 26.

[91] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/3/209,276 „საქართველოს სახალხო დამცველი და საქართველოს მოქალაქე ქეთევან ბახტაძე საქართველოს პარლამენტის წინააღმდეგ“, 2004 წლის 28 ივნისი, სამოტივაციო ნაწილი.

ინტერესები გაცნობოდა გადასახადის გადამხდელთა მონაცემებს, ხოლო მეორე მხრივ გადასახადის გადამხდელთა ინტერესები არ გამჟღავნებულიყო მათ მიერ სახელმწიფოსათვის მიწოდებული ფინანსური ინფორმაცია. საკონსტიტუციო სასამართლომ აღნიშნული კონფლიქტის გადაწყვეტისთვის კონსტიტუციის მე-18 მუხლის მე-2 და მე-3 პუნქტების[92] სისტემური ანალიზი განახორციელა. კერძოდ, სასამართლომ ვერ დაინახა კოლიზია კონსტიტუციის მე-18 მუხლის მე-2 და მე-3 პუნქტებს შორის და განმარტა, რომ საჯარო დაწესებულებებში არსებული დოკუმენტების ხელმისაწვდომობა დაცულია კონსტიტუციის მე-18 მუხლის მე-2 პუნქტით, ხოლო კონსტიტუციის მე-18 მუხლის მე-3 პუნქტი იცავს არა პირის უფლებას მოიპოვოს საჯარო დაწესებულებებში არსებული ოფიციალური ჩანაწერები, არამედ იმ პირთა პერსონალური მონაცემების დაცვის უფლებას, რომელთა ჯანმრთელობასთან, ფინანსებთან ან სხვა პირად საკითხებთან დაკავშირებული ჩანაწერები დაცულია საჯარო დაწესებულებების ოფიციალურ დანაწერებში. საკონსტიტუციომ სასამართლომ მიიჩნია, რომ კონსტიტუცია არ იცავდა პირის უფლებას ოფიციალური წყაროებიდან მოეპოვებინა ინფორმაცია სხვა პირის ჯანმრთელობის, ფინანსებისა და სხვა კერძო საკითხებთან დაკავშირებით. უფლებებს შორის კონფლიქტის გადაჭრის ამგვარი გზა არ უნდა იქნეს მიჩნეული სამართლიან ბალანსად, რადგან აღნიშნულ გადაწყვეტილებაში სასამართლომ სათანადო ყურადღება არ მიაქცია მოსარჩელე მხარის არგუმენტს, რომ ოფიციალურ წყაროებში არსებული ინფორმაციის გასაჯაროებამ, რომელიც შეიცავს ცნობებს პირის ჯანმრთელობის, ფინანსების ან სხვა საკითხებთან დაკავშირებით შესაძლოა ყოველთვის არ დააზიანოს იმ პირის პირადი ცხოვრება, რომელსაც შეეხება საჯაროდ გამჟღავნებული ინფორმაცია. სასამართლომ მიიჩნია, რომ პირის ჯანმრთელობის მდგომარეობის, ფინანსებისა და სხვა სახის ინფორმაციის საზოგადოებისთვის გასაჯაროება ყოველთვის არღვევდა მის პირად ცხოვრების უფლებასა და პერსონალური მონაცემების დაცვის უფლებას.[93] სასამართლოს მიერ კონფლიქტში მყოფი უფლებების მსგავსი ბლანკეტური მოწესრიგებით გადაწყვეტა ნამდვილად არ უნდა მივიჩნიოთ ინტერესთა სამართლიანი დაბალანსების ნიმუშად.

აღსანიშნავია, რომ ზემოთ აღნიშნული პრაქტიკა, საკონსტიტუციო სასამართლომ თავადვე შეცვალა N3/1/752 გადაწყვეტილებაში. საკონსტიტუციო სასამართლოს პლენუმმა განმარტა, რომ კონსტიტუციის მე-18 მუხლის მე-2 პუნქტი არ მოითხოვდა ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებული იყო პირის ჯანმრთელობასთან, ფინანსებთან ან სხვა კერძო საკითხებთან, ყოფილიყო „ტაბუდადებული“ კონსტიტუციის მე-18 მუხლის მე-3 პუნქტიდან გამომდინარე. სასამართლომ დაადგინა ინტერესთა დაბალანსების ახალი სტანდარტი და აღნიშნა, რომ „როდესაც პირი ითხოვს სხვა პირის კერძო საკითხებთან დაკავშირებულ ოფიციალურ ჩანაწერებში არსებულ ინფორმაციაზე ხელმისაწვდომობას, ერთმანეთს უპირისპირდება

[92] საქართველოს კონსტიტუციის მე-18 მუხლის მე-3 პუნქტის მიხედვით: „ოფიციალურ ჩანაწერებში არსებული ინფორმაცია, რომელიც დაკავშირებულია ადამიანის ჯანმრთელობასთან, ფინანსებთან ან სხვა პირად საკითხებთან, არავისთვის უნდა იყოს ხელმისაწვდომი თვით ამ ადამიანის თანხმობის გარეშე, გარდა კანონით გათვალისწინებული შემთხვევებისა, როდესაც ეს აუცილებელია სახელმწიფო ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, საჯარო ინტერესების, ჯანმრთელობის ან სხვათა უფლებების დასაცავად“.

[93] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N2/3/406,408 „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“, 2008 წლის 30 ოქტომბერი სამოტივაციო ნაწილის პარ. 24.

საქართველოს კონსტიტუციის მე-18-ე მუხლის მე-2 და მე-3 პუნქტით დაცული უფლებები, რომელთა შორის კონფლიქტის საკითხი ყოველ ინდივიდუალურ შემთხვევაში, ამ უფლებების დაბალანსების გზით, თანაზომიერების პრინციპის შესაბამისად უნდა გადაწყდეს".[94] ინტერესთა დაბალანსების ინდივიდუალური მექანიზმი ნამდვილად უნდა მივიჩნიოთ საკონსტიტუციო სასამართლოს პროგრესულ გადაწყვეტილებად, რადგან ის შესაძლებლობას აძლევს სასამართლოს უფლებებს შორის კონფლიქტის გადაწყვეტისას ყურადღება გაამახვილოს კონკრეტულ საქმეში არსებულ გარემოებებზე, გამოთხოვილი ინფორმაციის ხასიათზე, იმ პირის სტატუსზე, რომლის მიმართაც არსებობს საზოგადოებრივი ინტერესი და სხვა გარემოებებზე. შემდეგი საქმეების ანალიზიც სწორედ ინტერესთა ინდივიდუალური დაბალანსების მექანიზმის პრაქტიკაში გამოყენებას დაეთმობა.

N1/4/693,857 გადაწყვეტილებაში სასამართლოს უნდა გადაეწყვიტა იმ ნორმების კონსტიტუციურობის საკითხი, რომელთა მიხედვითაც იზღუდებოდა ღია სასამართლო სხდომის ფარგლებში მიღებულ გადაწყვეტილებებში არსებული პირადი მონაცემების ხელმისაწვდომობა. სასამართლომ განმარტა, რომ საჯარო დაწესებულებაში არსებულ და დაცულ ნებისმიერი სახის ინფორმაციას და საზოგადოებისათვის მის ხელმისაწვდომობას არ გააჩნია თანაბარი მნიშვნელობა, რადგან საჯარო ინფორმაციის გარკვეული კატეგორიის მიმართ შესაძლოა არსებობდეს ღიაობის მომეტებული ინტერესი, ხოლო ზოგიერთი ინფორმაციისთვის ასეთი ინტერესი არ იყოს მომეტებული. სასამართლოს პოზიციით, ამგვარ განსაკუთრებულ ინტერესზე უპირველესად მიუთითებს ინფორმაციის არსი, დანიშნულება და ის სიკეთე, რომლის დაცვასაც უზრუნველყოფს ამგვარი ინფორმაციის საჯაროობა. გარდა ამისა, სასამართლომ აღნიშნა, რომ საკითხის შეფასებისას მნიშვნელოვანია ასევე იმის გათვალისწინებაც თუ ვის შეეხებოდა სასამართლოს აქტები - თუ საქმე შეეხება სახელმწიფო პოლიტიკურ თანამდებობის პირს, მის მიმართ მომეტებული/გაზრდილი საზოგადოებრივი ინტერესიდან გამომდინარე შესაძლოა გამოირიცხოს ინფორმაციის დახურვის საფუძველი.[95] საბოლოოდ, საჯარო დაწესებულებაში არსებულ ინფორმაციაზე ხელმისაწვდომობის უფლების შეზღუდვის კონსტიტუციურობის შეფასებისას საქართველოს საკონსტიტუციო სასამართლო მხედველობაში იღებს სახელმწიფო დაწესებულებაში არსებული ინფორმაციის ხასიათს და მის მნიშვნელობას ხელისუფლების საზოგადოებრივი კონტროლის თვალსაზრისით.[96] დემოკრატიულ, სამართლებრივ სახელმწიფოში სასამართლოს აქტების როლის და მათში გადმოცემული ინფორმაციის მნიშვნელობის გათვალისწინებით, სასამართლომ მიიჩნია, რომ სასამართლოს აქტები განეკუთვნებოდა საჯარო დაწესებულებაში არსებულ იმ ტიპის ინფორმაციას, რომლის ხელმისაწვდომობის მიმართაც თავისთავად არსებობს მომეტებული საზოგადოებრივი ინტერესი. თუმცა, ვინაიდან სადავო ნორმები არ იძლეოდა შესაძლებლობას ინდივიდუალური შეფასების პირობებში გადაწყვეტილიყო კონკრეტულ სასამართლო აქტში არსებული პერსონალური მონაცემების დაცვა უფრო აღმატებული ინტერესით სარგებლობდა თუ მათი საზოგადოებისთვის გასაჯაროება, სასამართლომ გასაჩივრებული ნორმები კონსტიტუციის საწინააღმდეგოდ მიიჩნია.

[94] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N3/1/752 „ა(ა)იპ „მწვანე ალტერნატივა" საქართველოს პარლამენტის წინააღმდეგ", 2018 წლის 14 დეკემბერი, სამოტივაციო ნაწილის პარ. 10.

[95] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/3/693, 857 „ა(ა)იპ „მედიის განვითარების ფონდი" და ა(ა)იპ „ინფორმაციის თავისუფლების განვითარების ინსტიტუტი" საქართველოს პარლამენტის წინააღმდეგ, 2019 წლის 7 ივნისი, სამოტივაციო ნაწილის პარ. 66.

[96] იქვე, პარ. 41.

აღნიშნულ უფლებათა კონფლიქტის გადაწყვეტა სასამართლოს ასევე მოუწია N2/1/877 გადაწყვეტილებაშიც. მოცემულ შემთხვევაში მოსარჩელე მიიჩნევდა, რომ სადავო ნორმების მიხედვით საავტორო უფლებების დაცვის კოლექტიურ ორგანიზაციებს შესაძლებლობა ჰქონდათ საჯარო დაწესებულებებისგან გამოეთხოვათ მათ ფინანსებთან ან სხვა პირად საკითხებთან დაკავშირებული ოფიციალური ჩანაწერები, რითაც ირღვეოდა მათი პერსონალური მონაცემების დაცვის უფლება. სასამართლომ სადავო ნორმების ანალიზის საფუძველზე დაადგინა, რომ კანონმდებლობით არ იყო განსაზღვრული ორგანიზაციების ვალდებულება მოსარჩელის ფინანსების ან სხვა საკითხების შესახებ ცნობების მოპოვების შემდეგ დაეცვა მათი კონფიდენციალობა. საბოლოოდ, სასამართლომ სადავო ნორმებით დადგენილი უფლების შეზღუდვა მიიჩნია არაკონსტიტუციურად, რადგან სადავო ნორმით დადგენილი ინტერესთა ბალანსი არასათანადოდ იცავდა პერსონალურ მონაცემთა დაცვის უფლებას.[97]

აღნიშნული გადაწყვეტილებების ანალიზი ნათლად აჩვენებს, რომ საკონსტიტუციო სასამართლოს პრაქტიკა ერთი მხრივ საჯარო ინფორმაციის ხელმისაწვდომობასა და, მეორე მხრივ, პერსონალური მონაცემების დაცვის უფლებას შორის კონფლიქტის დაბალანსებისას დროთა განმავლობაში მნიშვნელოვნად განვითარდა. სასამართლოს მოქმედი პრაქტიკა კი იძლევა შესაძლებლობას ყოველ ინდივიდუალურ შემთხვევაში ინტერესთა დაბალანსება გადაწყდეს სამართლიანი გადაწყვეტის პრინციპით.

3. დასკვნა

სამართლებრივ სახელმწიფოში ინტერესთა დაბალანსება უნდა ხდებოდეს ისეთი მექანიზმით, რომელიც შესაძლებელს გახდის მათ სამართლიან დაბალანსებას. საკონსტიტუციო სასამართლოს გადაწყვეტილებების ქრონოლოგიური ანალიზის მიხედვით გამოიკვეთა, რომ თავდაპირველ საქმეებში სასამართლო ვერ უზრუნველყოფდა საჯარო ინფორმაციის ხელმისაწვდომობისა და პერსონალურ მონაცემთა დაცვის უფლებას შორის სამართლებრივი ბალანსის დადგენას, რაც განპირობებული იყო სამართლიანი დაბალანსების მექანიზმის არ არსებობით. თუმცა, საკონსტიტუციო სასამართლომ თავადვე შეცვალა საკუთარი პრაქტიკა და ინტერესთა ინდივიდუალური დაბალანსების მექანიზმი შეიმუშავა, რა დროსაც საკითხის გადასაწყვეტად ყურადღებას უთმობს განმცხადებლის მიერ მოთხოვნილი ინფორმაციის არსს, დანიშნულებას, ინფორმაციის სუბიექტის სოციალურ სტატუსსა და იმ სიკეთეს, რომლის დაცვასაც უზრუნველყოფს გამოთხოვილი ინფორმაციის საჯაროობა. ზემოთ აღნიშნულ ინტერესთა ინდივიდუალური დაბალანსების მექანიზმი საკონსტიტუციო სასამართლოს შესაძლებლობას მისცემს საინფორმაციო ტექნოლოგიებისა და საჯარო ინფორმაციის რაოდენობრივ ზრდასთან ერთად სამომავლო პერსპექტივაში სამართლიანად დააბალანსოს საზოგადოებისა და კერძო პირთა ინტერესები.

[97] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე „„შპს ალტა“, „შპს ოქეი“, „შპს ზუმერი ჯორჯია“, „შპს ჯორჯიან მობაილ იმპორტი“ და „შპს სმაილი“ საქართველოს პარლამენტის წინააღმდეგ“, 2020 წლის 25 დეკემბერი, სამოტივაციო ნაწილის პარ. 155-156.

პერსონალური მონაცემების დაცვა შრომის სამართალში

ავტორი: ზურაბ კალაძე[98]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

შრომის სამართალი თანამედროვე (ქართული) სამართლის დინამიკური მიმართულებაა. შრომის სამართლით დარეგულირებული დასაქმებულის ზოგიერთი უფლება ადამიანის უფლებათა დაცვის სამართლის კატეგორიაა.[99] სამართლის ამ დარგს პირდაპირი გავლენა აქვს ინდივიდის სოციალურ თუ ეკონომიკურ მდგომარეობაზე. შრომით სტანდარტებსა და ეკონომიკურ განვითარებას შორის ურთიერთკავშირის შესახებ არსებული გლობალური დისკუსიის ფარგლებში ჩამოყალიბებული მიდგომით, შრომის სამართალს შესწევს უნარი, პოზიტიური თუ ნეგატიური ზემოქმედება მოახდინოს ქვეყნის ეკონომიკურ განვითარებაზე. მართებულია შეხედულება, რომ შრომის სამართალი სოციალური სამართლიანობის, დემოკრატიისა და ეკონომიკური განვითარების მიღწევის ერთ-ერთი ძირითადი კომპონენტია.[100]

სამართლებრივი ურთიერთობების ერთ-ერთი განუყოფელი ნაწილია ფიზიკური პირების პერსონალურ მონაცემთა დამუშავება, ხოლო შრომითი ურთიერთობები ის სფეროა, სადაც ამ მონაცემთა დამუშავება აქტიურად მიმდინარეობს. დამსაქმებლები და დასაქმებულები უნდა აცნობიერებდნენ, რომ შრომით კონტექსტში განხორციელებული ბევრი ქმედება მოიცავს დასაქმებულთა პერსონალური მონაცემების, ზოგჯერ კი ძალზე სენსიტიური ინფორმაციის დამუშავებას.[101]

საქართველოს ორგანული კანონის „საქართველოს შრომის კოდექსის“ (შემდგომში - „სშკ“) თანახმად, შრომითი ურთიერთობა არის შრომის ორგანიზაციული მოწესრიგების პირობებში დასაქმებულის მიერ დამსაქმებლისათვის სამუშაოს შესრულება ანაზღაურების სანაცვლოდ.

შრომითსამართლებრივ ურთიერთობაში დამსაქმებელი გვევლინება, როგორც „ძლიერი“ მხარე და დასაქმებული, როგორც „სუსტი“ მხარე. დამსაქმებელს გააჩნია უფრო მეტი ძალაუფლება დასაქმებულთან მიმართებით. ამ უკანასკნელს არ აქვს შესაძლებლობა გავლენა მოახდინოს რო-

[98] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - დონარი ლონდარიძე.

[99] ქ. ბოდონე, ნ. გუჯაბიძე, თ. თოდრია, ქ. მესხიშვილი, თ. ხაჟომია, ზ. შველიძე, „საქართველოს შრომის სამართალი და საერთაშორისო შრომის სტანდარტები“, შრომის საერთაშორისო ორგანიზაცია, თბილისი, 2017, გვ. 18-19.

[100] Javillier J.C., The Employer and the Worker: The Need for a Comparative and International Perspective, Boundaries and Frontiers of Labour Law, Goals and Means in the Regulation of Work, Davidov G., Langille B., (Ed.), Oxford and Portland, Oregon, 2006, გვ. 371.

[101] Article 29 – Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context (13.09.2001), გვ. 2.

გორც წინასახელშეკრულებო ურთიერთობაზე (რადგანაც იგი ვალდებულია დაემორჩილოს წინასწარ შედგენილ არსებით პირობებს), ასევე სამუშაო პროცესზე. „შრომითი ხელშეკრულებაში მხარეთა შორის თანასწორობის პრინციპი გარკვეულ სახეცვლილებას განიცდის, დასაქმებული დამოკიდებულია დამსაქმებელზე, ასრულებს მის მითითებებს და იმყოფება სუბორდინაციულ (დაქვემდებარებულ) მდგომარეობაში. ამ ურთიერთობებში აშკარად იკვეთება დამსაქმებლის დომინირებული მდგომარეობა დასაქმებულთან მიმართებით, რომელიც ქმნის საშიშროებას, რომ ამ უკანასკნელის მიმართ ძალაუფლება შესაძლოა არამართლზომიერად იქნეს გამოყენებული“.[102] საქართველოს კონსტიტუციით დაცულია შრომის თავისუფლება, რომელშიც, ასევე, მოიაზრება დამსაქმებლის მიერ დასაქმებულის პერსონალურ მონაცემთა დამუშავებაზე დასაქმებულის ხელმისაწვდომობა და ცნობიერება. შესაბამისად, მნიშვნელოვანია, რომ დასაქმებულთა უფლებები დაცული და გარანტირებული იქნეს პერსონალურ მონაცემთა კანონიერად დამუშავების ჭრილშიც, რაზედაც საქართველოში არსებული პრაქტიკის სიმწირე მნიშვნელოვან გავლენას ახდენს როგორც არსებულ, ასევე მომავალში შესაძლო დარღვეულ უფლებებზე.

2012 წლის 16 იანვარს მიღებულ იქნა ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომლის მიზანს წარმოადგენდა საქართველოს პერსონალური მონაცემების დამუშავების, გადაცემის, შენახვისა და დაცვის სრულყოფილი მოწესრიგება, დაცვის სათანადო მექანიზმის ჩამოყალიბება და საქართველოს მიერ საერთაშორისო დონეზე ნაკისრი ვალდებულებების შესრულება. მოგეხსენებათ, აღნიშნული კანონის შემოღებამდე პერსონალურ მონაცემების მომწესრიგებელ მატერიალურ საფუძველს წარმოადგენდა საქართველოს ზოგად ადმინისტრაციულ კოდექსში არსებული დებულებები, რომელიც მხოლოდ საჯარო დაწესებულებებზე ვრცელდება. შესაბამისად, საკანონმდებლო სიახლის ერთ-ერთ მნიშვნელოვან ასპექტს სწორედ ამ კანონის კერძო სექტორზე გავრცელება წარმოადგენს. შრომის თავისუფლება წარმოადგენს კონსტიტუციური რანგის უფლებას, რომლის განუხრელად დაცვა და გარანტირება სახელმწიფოს პოზიტიური ვალდებულებაა. შესაბამისად, იმისათვის რომ აღნიშნული უფლება სამართლიანად იქნეს რეალიზებული, მნიშვნელოვანია, რომ შრომითსამართლებრივ ურთიერთობებში პერსონალურ მონაცემთა დამუშავება განხორციელდეს კანონიერად, რაც გულისხმობს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლად დაცვას. შესაბამისად, სპეციალური კანონის სიახლემ განაპირობა კვლევებისა და პრაქტიკის სიმწირე შრომით ურთიერთობებში პერსონალურ მონაცემთა დაცვის კუთხით, რომელიც საჭიროებს აღნიშნული საკითხის ძირფესვიანად შესწავლის აუცილებლობას. შრომითსამართლებრივ ურთიერთობებში პერსონალურ მონაცემების დაცვა მნიშვნელოვანია, როგორც წინასახელშეკრულებო და შრომითი ურთიერთობის პერიოდში, ასევე შრომითი ურთიერთობის შეწყვეტის შემდეგაც.

[102] საქართველოს უზენაესი სასამართლოს გადაწყვეტილება, საქმე №ას 864 1150 09, 2010 წლის 28 აპრილი.

2. პერსონალური მონაცემები შრომის სამართალში

საქართველოს კონსტიტუციით აღიარებულია პირის უმნიშვნელოვანესი სოციალური უფლება – შრომის უფლება და დადგენილია, რომ შრომა თავისუფალია. შრომის კონსტიტუციური უფლება გარანტირებულს ხდის პირის თავისუფლებას შრომითი საქმიანობის არჩევანსა და მის განხორციელებაში, ამასთან, აწესებს სახელმწიფოს ვალდებულებას დაიცვას დასაქმებული მოქალაქის შრომითი უფლებები, რაც უზრუნველყოფილია სათანადო კანონით – შრომის კოდექსით.[103]

2013 წლის ზაფხულში ძალაში შევიდა საქართველოს შრომის კოდექსის ახალი ნორმები, რომლებიც, პრაქტიკული თვალსაზრისით, მრავალ მნიშვნელოვან სიახლეს შეიცავს. ახალი რეგულაციები, მათ შორის დასაქმებულთა მონაცემების დაცვა განაცხადების დამუშავების პროცესში, ეხება: შრომითი ხელშეკრულებების შედგენასა და შინაარსს, სამუშაო დროის ხანგრძლივობას, ზეგანაკვეთურ სამუშაოს, შვებულების მოთხოვნის უფლებას, ხელშეკრულების ვადის განსაზღვრას, შრომითი ხელშეკრულებების დასრულებას ხელშეკრულების შეწყვეტის გზით და გაფიცვის უფლებას, ანუ, სხვა სიტყვებით რომ გადმოვცეთ, ინდივიდუალური და შრომის სამართლის ყველა სფეროს. ახალი შრომის კოდექსით საქართველო უახლოვდება შრომის სამართლის იმ სტანდარტებს, რომლებიც მოქმედებს ევროკავშირის წევრ სახელმწიფოებში.

შრომით სამართლებრივ ურთიერთობაში პერსონალურ მონაცემთა დამმუშავებელი არის დამსაქმებელი ან უფლებამოსილი პირი დამსაქმებელთან დადებული ხელშეკრულების შესაბამისად, რომელიც აგროვებს და ამუშავებს მონაცემებს. დამსაქმებლები აგროვებენ მონაცემებს დასაქმებულების შესახებ, სხვადასხვა მიზეზით: კანონის დაცვა, სამუშაო პირობების ხელშეწყობის, ტრენინგის და დაწინაურების მიზნით, პირადი უსაფრთხოების, ხარისხის კონტროლის გაუმჯობესების, საკუთრების დაცვის მიზნით და ა. შ. „პირადი მონაცემების“ დამუშავებისათვის უნდა არსებობდეს „იურიდიული საფუძველი“.[104]

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის თანახმად, პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.

“პერსონალურ მონაცემთა დაცვის შესახებ” კანონი ასევე ითვალისწინებს პერსონალურ მონაცემთა სახეებს:

განსაკუთრებული კატეგორიის მონაცემი - მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, რელიგიური ან ფილოსოფიურ მრწამსთან, სქესობრივ ცხოვრებასთან, პროფესიულ კავშირში გაწევრიანებასთან, ნასამართლობასთან, ჯანმრთელობასთან და სხვა. ასევე განსაკუთრებული კატეგორიის მონაცემი შეიძლება დაიყოს: ა. ბიომეტრიულ მონაცემად - ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური

[103] ზ. შველიძე, შრომით დავებზე საქართველოს სასამართლო პრაქტიკა, (გადაწყვეტილებათა კრებული), თბილისი, 2020, გვ. 11-12.

[104] ადამიანის უფლებათა ევროპული სასამართლოს 2000 წლის 16 თებერვალი გადაწყვეტილება საქმეზე Aman v. Switzerland, პარ. 76.

და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი); ბ. და გენეტიკურ მონაცემად - მონაცემთა სუბიექტის უნიკალური და მუდმივი მონაცემი გენეტიკური მემკვიდრეობის ან/და დნმ-ის კოდის შესახებ, რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება;

რაც შეეხება ჩვეულებრივ კატეგორიის მონაცემს, ეს არის ნებისმიერი მონაცემი, რომელიც არ არის განსაკუთრებული კატეგორიის მონაცემი.

შრომით ურთიერთობებში ხშირად გამოიყენება როგორც ჩვეულებრივი, ასევე განსაკუთრებული კატეგორიის მონაცემების დამუშავება. „ორგანიზაციები ხშირად ახდენენ ბიომეტრიული მონაცემების დამუშავებას დასაქმებულთა შენობაში შესვლის/გადაადგილების, ელექტრონულ სისტემებსა და ტექნოლოგიებზე წვდომის პროცესში. „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის-ის თანახმად, ბიომეტრიული მონაცემების დამუშავება შესაძლებელია მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის მიზნით, აგრეთვე საიდუმლო ინფორმაციის გამჟღავნების თავიდან ასაცილებლად. კერძო დაწესებულებათა მიერ ბიომეტრიული მონაცემების გამოყენება დასაშვებია საქმიანობის განხორციელების მიზნითაც, თუ ამ მიზნების მიღწევა სხვა საშუალებებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. „ბიომეტრიული მონაცემების დამუშავება უნდა ხდებოდეს შრომითი ხელშეკრულების ან სპეციალური რეგულაციის საფუძველზე, სადაც დეტალურად იქნება გაწერილი ამ სახის მონაცემების დამუშავების 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".[105]

მაგალითის სახით, შესაძლოა განვიხილოთ ერთ-ერთი წარმატებული ბიზნეს კომპანიის შინაგანაწესი, რომლის მე-2 მუხლში მოწესრიგებულია წინასახელშეკრულებო ურთიერთობები. დამსაქმებელმა კანდიდატისგან შესაძლოა მოითხოვოს: ა) პირადობის მოწმობა; ბ) განათლების დამადასტურებელი დოკუმენტი; გ) CV; დ) სერთიფიკატები; ე) 2 ფოტო სურათი; ვ) სარეკომენდაციო წერილი წინა დამსაქმებლისგან; ზ) ცნობა ჯანმრთელობის მდგომარეობის შესახებ კვების ბლოკში მომუშავე პერსონალისთვის, კერძოდ, ცხვირ-ხახიდან ნაცხის ბაქტერიოლოგიური კვლევა, ხელის მტევნიდან ჩამონაბანის ბაქტერიოლოგიური ანალიზი, თერაპევტის ზოგადი დასკვნა.

მოცემულ შემთხვევაში, ე) სახის ფოტოსურათი - წარმოადგენს ბიომეტრიულ მონაცემს, კერძოდ, სახის მახასიათებელს და ზ) ქვეპუნქტებით განსაზღვრული ინფორმაცია პირის ჯანმრთელობის მდგომარეობასთან არის დაკავშირებული, რაც, ასევე, წარმოადგენს განსაკუთრებული კატეგორიის ინფორმაციას, რომელთა დამუშავება მხოლოდ კანონით მკაცრად განსაზღვრულ შემთხვევებშია დასაშვები. ვფიქრობ, აღნიშნულ მონაცემთა საფუძველი მოცემულია "პერსონალურ მონაცემთა

[105] პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, რეკომენდაციები შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ, გვ. 9.

დაცვის შესახებ" კანონის-ის მე-6 მუხლის მე-2 ნაწილის გ) ქვეპუნქტში, რომლის მიხედვითაც, განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია, როცა მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის. შესაბამისად, კვების ბლოკში მომუშავე ადამიანის შესახებ ჯანმრთელობის მდგომარეობასთან დაკავშირებული ინფორმაციების დამუშავება არ ეწინააღმდეგება საქართველოს კანონმდებლობას, რადგან მესამე პირთა სიცოცხლე აღმატებულ საჯარო ინტერეს წარმოადგენს.

ზემოაღნიშნულს ასევე ითვალისწინებს შრომის საერთაშორისო ორგანიზაციის (ILO) პრაქტიკის ამსახველი კოდექსი, რომელიც ეხება დასაქმებულთა პერსონალურ მონაცემთა დაცვის წესრიგს. აღნიშნული რეკომენდაციის 6.7 მუხლის თანახმად, „პირის ჯანმრთელობის მდგომარეობასთან დაკავშირებული პერსონალური მონაცემები არ შეიძლება დამუშავდეს გარდა კანონით განსაზღვრული შემთხვევებისა, დაცული უნდა იყოს ჯანმრთელობისა და უსაფრთხოების ძირითადი პრინციპები, მათ შორის ინფორმაციის კონფიდენციალობა. სამედიცინო ინფორმაცია, ასევე, უნდა დამუშავდეს იმის განსასაზღვრად, პირი შეესაბამება თუ არა თანამდებობას, აკმაყოფილებს თუ არა სამუშაოს შესასრულებლად ჯანმრთელობის დადგენილ სტანდარტებს და სხვ".[106]

3. მონაცემთა დამუშავების პრინციპები შრომით ურთიერთობებში

3.1. კანონიერების და სამართლიანობის პრინციპი

ხშირად არის შემთხვევები, როდესაც დამსაქმებლები არ იცავენ "პერსონალურ მონაცემთა დაცვის შესახებ" კანონის-ით და სშკ-ით დადგენილ მოთხოვნებს დასაქმებულთა პერსონალურ მონაცემთა დამუშავებისას, რამაც შესაძლოა მნიშვნელოვნად დააზიანოს ადამიანის კონსტიტუციითა და ადამიანის უფლებათა ევროპული კონვენციით განსაზღვრული ძირითადი უფლებები და თავისუფლებები, მაგ., ღირსების უფლება, პირადი და ოჯახური თავისუფლება სხვ. შესაბამისად, მონაცემთა დამუშავებისას როგორც საქართველოს კანონმდებლობა, ასევე საერთაშორისო ნორმები ითვალისწინებენ მონაცემთა დამუშავების სამართლიანობისა და კანონიერების პრინციპებს.

მონაცემთა დამუშავება უნდა განხორციელდეს სამართლიანად და კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად, რაც გულისხმობს, რომ მონაცემთა დამუშავებისას დაცული უნდა იქნეს საქართველოს კონსტიტუციით განსაზღვრული ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრებისა და პიროვნების თავისუფალი განვითარების უფლებები. მონაცემთა დამუშავება უნდა განხორციელდეს კანონით დადგენილი წესით, ე. ი. დამუშავებისას უნდა არსებობდეს "პერსონალურ მონაცემთა დაცვის შესახებ" კანონის-ის მე-5 და მე-6 მუხლებით დადგენილი საფუძვლები და ასევე, უნდა შეესაბამებოდეს როგორც ამ კანონს, ასევე სხვა საკანონმდებლო აქტებს, საერთაშორისო ხელშეკრულებებსა თუ შეთანხმებებს.

[106] The International Labour Organization (ILO), An ILO code of practice: Protection of workers' personal data, 6.7.

შრომის სამართალში გამოყოფენ მონაცემთა დამუშავების სამართლიანობის ოთხ ძირითად ელემენტს: „1. მონაცემთა დამუშავების გამჭვირვალობის უზრუნველყოფა მონაცემთა სუბიექტების წინაშე; 2. მონაცემთა დამუშავების დაწყებამდე სუბიექტებისათვის დამუშავების მიზნის, დამმუშავებლების ვინაობისა და მისამართის შესახებ შეტყობინება; 3. მონაცემთა ფარული და საიდუმლო დამუშავებისგან თავის შეკავება (თუ კანონით სხვა რამ არ არის დადგენილი); 4. ნებისმიერ დროს მონაცემთა სუბიექტებისათვის დამუშავებული მონაცემების შესახებ ინფორმაციის მიწოდების უზრუნველყოფა.[107]

მონაცემთა დამუშავების კანონიერების მოთხოვნიდან გამომდინარე, მოცემულია შემდეგი დებულებები: „1. დამუშავების საფუძველია მონაცემთა სუბიექტის თანხმობა (გამონაკლისია კანონით გათვალისწინებული საფუძველი დამუშავებისა); 2. დამუშავება გათვალისწინებულია მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად; 3. სხვათა ლეგიტიმური ინტერესები არის დამუშავების საფუძველი, თუმცა მხოლოდ იმ შემთხვევაში, თუ ისინი აღმატებულია მონაცემთა სუბიექტის ფუნდამენტური უფლებების დაცვის ინტერესებზე; 4. განსაკუთრებული კატეგორიის ინფორმაციის კანონიერი დამუშავება ექვემდებარება სპეციალურ, მკაცრ რეჟიმს.[108]

პერსონალური მონაცემების დაცვის ზოგადი სახელმძღვანელოს მიხედვით, შრომით ურთიერთობებში ინფორმაციის დამუშავებისას უნდა არსებობდეს კანონით განსაზღვრული საფუძველი („კანონიერი საფუძველი“), რომელიც გულისხმობს შიდა კანონმდებლობაში რაიმე საფუძვლის ქონას, რომელიც უნდა ასახავდეს კანონის ხარისხს, ხელმისაწვდომი და განჭვრეტადი უნდა იყოს დაინტერესებული პირთათვის.[109]

დამსაქმებლის ვალდებულებაა მონაცემთა დამუშავებისას იმოქმედოს კეთილსინდისიერების პრინციპიდან გამომდინარე, დამსაქმებელი და დასაქმებული, რომლებიც შრომითი ხელშეკრულებით არიან დაკავშირებულნი ერთმანეთთან, ერთის მხრივ, დამსაქმებელს წარმოეშობა ნდობა დასაქმებულის მიმართ, რომ იგი თავის სამუშაოს შეასრულებს კეთილსინდისიერად, ხოლო, მეორეს მხრივ, დასაქმებულს უჩნდება მოლოდინი, რომ დამსაქმებელი კეთილსინდისიერად მოეკიდება მის შრომას.[110] სწორედ კეთილსინდისიერების პრინციპია დაკავშირებული კანონიერად დამუშავების პრინციპთან, რადგან დამმუშავებელმა კეთილსინდისიერად უნდა მოიპოვოს მონაცემები და შემდეგ დაამუშავოს დასაქმებულის თანხმობის საფუძველზე.[111]

მონაცემები შეიძლება დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან

---

[107] Council of Europe, European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2013, 76/გოშაძე კ., გვ. 34.

[108] Council of Europe, European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2013, 76/გოშაძე კ.,გვ. 26.

[109] Guide to the General Data Protection Regulation (GDPR), ICO, 2019, გვ. 21.

[110] საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2015 წლის 22 მაისის გადაწყვეტილება საქმე №ას-243-230-2015.

[111] ე. შერმადინი, პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში, თბილისი, 2020, გვ. 27.

შეუთავსებელი მიზნით - მიზანი უნდა შეესაბამებოდეს საქართველოს კანონმდებლობას და სამართლიანობის პრინციპებს, უნდა იყოს მკაფიოდ და გასაგებად ჩამოყალიბებული, არ უნდა იყოს ორაზროვანი და გაუგებარი.

დამსაქმებლების მიერ ხშირად ხორციელდება დასაქმებულთა კონტროლი და მონიტორინგი, აღნიშნული ასევე გამომდინარეობს შრომითი ურთიერთობების სპეციფიკიდან, კერძოდ, სუბორდინაციის (დაქვემდებარების) პრინციპიდან. აღნიშნული დამსაქმებლის მხრიდან შესაძლოა განხორციელდეს სხვადასხვა მიზნით, მაგ., დასაქმებულის თანამდებობასთან მისი კვალიფიციური უნარ-ჩვევების შესაბამისობის დასადგენად, მომსახურების გასაუმჯობესებლად, დარღვევების აღკვეთისა და გამოვლენისთვის და სხვ. ამ დროს „დამსაქმებელმა უნდა განასხვავოს ნებადართული და აკრძალული მონიტორინგის მიზნები, რომელიც შეიძლება იყოს: ა) სისტემის სტაბილურად ფუქნციონირების უზრუნველყოფა; ბ) უზრუნველყოს მონაცემთა კანონიერი დამუშავება; დ) თანამშრომლების ეფექტური მუშაობის უზრუნველსაყოფად.“[112] კონტროლი ბევრნაირად შეიძლება განხორციელდეს, მაგ., ელექტრონული ფოსტის კონტროლი, სამუშაო ოთახში ვიდეო კამერების დაყენება და სხვ.

აღნიშნულთან დაკავშირებით საინტერესოა საქართველოს უზენაესი სასამართლოს გადაწყვეტილება ერთ-ერთ საქმეზე, სადაც პირი გათავისუფლებულ იქნა სამსახურიდან ელექტრონული კომუნიკაციის „სკაიპის“ საშუალების მეუღლესთან მიმოწერის გამო, რომელზედაც წვდომა ჰქონდა დამსაქმებელს. მეუღლეები დასაქმებულები იყვნენ მოპასუხე კომპანიაში, რომლებიც სარგებლობდნენ ზემოაღნიშნული ელ. კომუნიკაციის საშუალებით და ერთ-ერთ მიმოწერაში (რომელიც გათავისუფლების საფუძველი გახდა) დასაქმებულმა პარტნიორი კომპანიის წარმომადგენელი მოიხსენია შეურაცხმყოფლად, ამასთანავე, აღნიშნა, რომ მისთვის სულ ერთი იყო წაიკითხავდა თუ არა მიმოწერას ადრესატი. ქვემდგომი ინსტანციის სასამართლოების მიერ განხორციელებული ქმედება მიიჩნიეს შრომითი ვალდებულების უხეშ დარღვევად, თუმცა საქართველოს უზენაესმა სასამართლომ განმარტა, რომ მიმოწერის დროს შესაფასებელია პირის სტატუსი. „...სამსახურებრივი „სკაიპის“ გამოყენების მიუხედავად მოსარჩელე ესაუბრებოდა მეუღლეს, შესაბამისად, მეუღლესთან პირად მიმოწერაში, რომელიც შეიძლება პარტნიორ კომპანიაშიც კი იყოს დასაქმებული, მოსარჩელე არ შეიძლება განვიხილოთ კომპანიის წარმომადგენლად, რომელიც პირადი საუბრისას გამოხატავს ამა თუ იმ პირის მიმართ დამსაქმებლის დამოკიდებულებას და აჟღერებს მის პოზიციას, ამასთანავე, უდავოა, რომ მას, როგორც ფიზიკურ პირს გააჩნია აზრის და მისი გამოხატვის თავისუფლება...“ საკასაციო სასამართლომ აღნიშნულ გადაწყვეტილებაში დაადგინა, რომ მეუღლესთან პირადი საუბარი არის მოსარჩელის გამოხატვის უფლება, რომელშიც ჩარევისათვის აუცილებელია ლეგიტიმური მიზნის არსებობა, რაც მოცემულ შემთხვევაში არ დგინდება და დასაქმებულის მხრიდან შრომის პირობების განზრახ დარღვევა და დამსაქმებლისათვის მიყენებული ზიანი არ იქნა გაზიარებული.[113]

[112] Paul p. K and Reiner. S “Manual on Data Protection in Employment Context”, Ludwig Boltzmann Institute of Human Rights, Vienna Mandated Body, November 2006, გვ. 35.

[113] საქართველოს უზენაესი სასამართლო, საქმე № ას-1696-2018, 2020 წლის 31 ივლისი.

ადამიანის უფლებათა ევროპული სასამართლოს პრეცედენტული სამართლის თანახმად, დამსაქმებლის მხრიდან პირადი მიმოწერის კონტროლს გააჩნია გარკვეული ჩარჩოები და ის უპირობოდ დასაშვებ ქცევად არ შეიძლება ყოველთვის შეფასდეს. საქმე „ბარბულეშკუ რუმინეთის წინააღმდეგ“ სწორედ მსგავს საკითხს ეხება, კერძოდ, ერთ-ერთმა კერძო კომპანიამ რუმინეთის მოქალაქე ბარბულეშკუ სამუშაო დროს სამსახურებრივი მიზნებისთვის შექმნილი „Yahoo Messenger-ის“ პირადი მიმოწერისთვის გამოყენების გამო სამსახურიდან გაათავისუფლა. კომპანიის შიდა რეგულაცია კრძალავდა სამუშაო დროს ორგანიზაციის საკომუნიკაციო საშუალებების პირადი მიზნებისთვის გამოყენებას. რუმინეთის სასამართლომ ბარბულეშკუსა და კომპანიის დავის განხილვისას მითითება არ გააკეთა არც პირადი კომუნიკაციის შინაარსზე და არც იმ პირთა იდენტიფიცირება მოახდინა, ვისთანაც ბარბულეშკუს ჰქონდა კომუნიკაცია. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ კომუნიკაციის შინაარსი ადგილობრივი სასამართლოს გადაწყვეტილების განმსაზღვრელი ფაქტორი არ ყოფილა. დასაქმებულმა ვერ დაასაბუთა, რატომ გამოიყენა „Yahoo Messenger-ი“ პირადი მიზნებისთვის, შესაბამისად, ევროპის სასამართლომ დაადგინა, რომ რუმინეთის სახელმწიფომ დაიცვა სამართლიანი ბალანსი პირის პირადი ცხოვრების ხელშეუხებლობასა და დამსაქმებლის ინტერესებს შორის, რადგან დამსაქმებელმა შეამოწმა კომუნიკაცია მხოლოდ „Yahoo Messenger-ზე“ და არა დასაქმებულის კომპიუტერში არსებული სხვა დოკუმენტები, შესაბამისად, დამსაქმებელი მოქმედებდა უფლებამოსილების ფარგლებში და თანამშრომლის მონიტორინგი ლიმიტირებული და პროპორციული იყო.

„პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით არ არის აკრძალული საჯარო და კერძო დაწესებულებებში სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის გამოყენებით დასაქმებულთა მონიტორინგი. ამისათვის უნდა არსებობდეს შემდეგი წინაპირობები: მე-12 მუხლის მე-3 პუნქტის თანახმად, სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის დაყენება შეიძლება მხოლოდ გამონაკლის შემთხვევებში, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, საიდუმლო ინფორმაციის დაცვის და გამოცდის/ტესტირების მიზნებისათვის და თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია, ასევე ამის შესახებ დასაქმებული ყველა პირი წერილობითი ფორმით უნდა იყოს ინფორმირებული.

მონიტორინგთან დაკავშირებით საინტერესოა ერთ-ერთ საქმეზე ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება, სადაც სასამართლომ განმარტა: „პირადი ცხოვრების უფლება თავის თავში მოიცავს პირის უფლებას, განავითაროს ურთიერთობები სხვა ადამიანებთან მაშინაც კი თუ ეს ურთიერთობა სამუშაო პროცესის დროს ხდება.

სასამართლომ გაითვალისწინა წარსულში მიღებული არაერთი გადაწყვეტილებაც, სადაც აღნიშნულია, რომ პირადი ცხოვრების ცნება მოიცავს პროფესიული ხასიათის საქმიანობასაც, ვინაიდან ადამიანების უმეტესობას გარე სამყაროსთან კომუნიკაციის საშუალება სწორედ სამსახურებრივი ურთიერთობის ფარგლებში ეძლევა. უნივერსიტეტის აუდიტორია პროფესორების სამუშაო სივრცეა. ეს ადგილია, სადაც ისინი არა მხოლოდ ასწავლიან სტუდენტებს, არამედ ურთიერთობა აქვთ მათთან, რითაც ავითარებენ ორმხრივ ურთიერთობებს და აყალიბებენ საკუთარ სოციალურ იდენტობას. შესაბამისად, სასამართლომ სამუშაო სივრცეში დასაქმებულის მიმართ განხორციელებული ფარული თუ აშკარა ვიდეოთვალთვალი მის პირად ცხოვრებაში

მნიშვნელოვან ჩარევად ჩათვალა, ევროპული კონვენციის მე-8 მუხლის დარღვევა დაადგინა და მონტენეგროს პროფესორების სასარგებლოდ 1000 ევროს ანაზღაურება დააკისრა.[114]

მონაცემთა სამართლიანად დამუშავება დასაქმებულის ვალდებულებაცაა. ერთ-ერთ საქმეზე, საქართველოს უზენაესმა სასამართლომ გაიზიარა სააპელაციო სასამართლოს მსჯელობა, რომ დასაქმებულმა დაარღვია შრომითი ხელშეკრულების პირობები, რაც გამოიხატა აბონენტთა სატელეფონო ცნობარის შედგენაში, და შემდეგ გავრცელებაში, რამაც დაარღვია დამსაქმებლის კომერციული საიდუმლოება, კონფიდენციალური მონაცემები, და მომხმარებელთა პირადი ინფორმაცია.[115] მოცემულ შემთხვევაში, მონაცემთა დამმუშავებელს დასაქმებული წარმოადგენდა, რომლის ვალდებულება იყო კანონიერად და სამართლიანად განეხორციელებინა მონაცემთა დამუშავება.

3.2. მიზნის შესაბამისობის პრინციპი

მონაცემები შეიძლება დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან შეუთავსებელი მიზნით.

პერსონალურ მონაცემთა დამუშავებული და შენახული უნდა იქნეს ზუსტად განსაზღვრული კანონიერი მიზნებისთვის და არ უნდა იქნეს გამოყენებული მათთან შეუთავსებელი გზით. „პერსონალური მონაცემები უნდა დამუშავდეს კანონიერი და მკაფიოდ განსაზღვრული მიზნით, მონაცემთა დამუშავება თავად არ წარმოადგენს მიზანს, ისევე როგორც მიზანი არ შეიძლება იყოს აბსტრაქტული და ზოგადი ხასიათის, მიზანი უნდა იყოს კონკრეტული, მკაფიო და მარტივად გასაგები“.[116]

პერსონალურ მონაცემთა დაცვის სამართალში, ასევე, მოქმედებს „მინიმიზაციის“ პრინციპი, რომელიც გულისხმობს, რომ უნდა დამუშავდეს მხოლოდ ის მონაცემები, რომელიც არის რელევანტური და დამუშავების მიზნების მიღწევისთვის საჭირო.[117] „ამ პრინციპის თანახმად, პერსონალური მონაცემები უნდა იყოს ადეკვატური, შესაბამისი და შემოიფარგლოს მხოლოდ დაზუსტებული, მკაფიო და ლეგიტიმური მიზნებისათვის“.[118]

[114] დამატებით იხ. „მათემატიკის პროფესორები მონტენეგროს წინააღმდეგ - რა გადაწყვიტა ევროსასამართლომ აუდიტორიებში ვიდეოთვალთვალის საქმეზე“, ხელმისაწვდომია: https://bit.ly/3jo5N2m წვდომის თარიღი: 25.08.2021.

[115] საქართველოს უზენაესი სასამართლოს სამოქალაქო საქმეთა პალატის 2016 წლის 18 მარტის განჩინება საქმე N:ას-50-49-2016, პარ. 13.

[116] საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი, „რეკომენდაციები

შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის შესახებ“, თბილისი, 2014, გვ. 6.

[117] ე. შერმადინი, „პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში“, თბილისი, 2020წ, გვ. 17,

[118] დამატებით ი. “Six data protection principles“, ხელმისაწვდომია: https://bit.ly/3mt8rpl წვდომის თარიღი: 05.07.2021.

სშკ-ის მე-11 მუხლში წინასწარ ჩამოყალიბებულია დამსაქმებლის პერსონალურ მონაცემთა დამუშავების მიზანი, კერძოდ, დადგენა იმისა, თუ რამდენად შეესაბამება კანდიდატი კონკრეტულ სამუშაოს და შესაბამისი გადაწყვეტილების მიღება. შრომითი ურთიერთობების დაწყების დროს შრომით სფეროში პერსონალური მონაცემები შესაძლოა მიმართული იყოს პირის სამუშაო გამოცდილებასთან და ჯანმრთელობის მდგომარეობასთან დაკავშირებით (კანონით განსაზღვრულ შემთხვევებში). „მონაცემები უნდა შეგროვდეს დაზუსტებული, მკაფიო, რელევანტური, აშკარა და ლეგიტიმური მიზნით, და არ უნდა დამუშავდეს შემდგომ თავდაპირველ მიზანთან შეუთავსებლად. (მაგ: სახელფასო მიზნით შეგროვებული მუშაკთა პირადი მონაცემები არ შეიძლება შემდგომ გამოყენებული იყოს პირდაპირი მარკეტინგის მიზნით. სიმართლის დადგენის მიზნით, თანამშრომლებზე ასევე არ უნდა იქნეს გამოყენებული პოლიგრაფია (სიმართლის გადამოწმების მოწყობილობა), ან სხვა მსგავსი ტესტირების პროცედურები".[119]

3.3. პროპორციულობის პრინციპი

მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი.[120] მონაცემები, რომელიც მუშავდება უნდა იყოს ადეკვატური, რელევანტური, და არა გადაჭარბებული იმ მიზნისთვის რისთვისაც ისინი ინახება.[121]

თუკი დასაქმებული დამსაქმებელს მიაწვდის იმ ინფორმაციას, რომელიც არ არის საჭირო შრომითი ურთიერთობის მიზნებისთვის, დოკუმენტები უნდა დაუბრუნდეს მონაცემთა სუბიექტს ან განადგურდეს დადგენილი წესის შესაბამისად.

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.[122]

საქმე Copland v. the United Kingdom შეეხებოდა კოლეჯის თანამშრომლის მიერ ელფოსტისა და ინტერნეტის მოხმარების ფარულ მონიტორინგს. დამსაქმებელს სურდა, დაედგინა, გადაჭარბებულად ხომ არ იყენებდა დასაქმებული კოლეჯის კუთვნილ მოწყობილობებს პირადი მიზნებისთვის. ECtHR-მა დაადგინა, რომ საწარმოს ტერიტორიიდან განხორციელებულ სატელეფონო ზარებზე ვრცელდება პირადი ცხოვრებისა და კორესპონდენციის პატივისცემის უფლების გარანტიები. შესაბამისად, ევროპული კონვენციის მე-8 მუხლი იცავს სამსახურიდან განხორციელებულ ზარებს და ელფოსტით გაგზავნილ წერილებს, ასევე, ინტერნეტის მოხმარებაზე

[119] Protection of worker's personal data, International Labour Office Geneva; ILO; 4.

[120] „პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს კანონის მუხლი 4, „გ" ქვეპუნქტი.

[121] Convention to the Protection Individual with regard to Automatic Processing of Personal Data, Strasburg.28.I.1981, Article 5/ c.

[122] მ. წერეთელი, პერსონალური მონაცემების დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში, თბილისი, 2019, გვ. 39.

მონიტორინგით მოპოვებულ ინფორმაციას. განმცხადებლის შემთხვევაში, არ არსებობდა დებულებები, რომლებიც დაარეგულირებდა, რა პირობებში შეუძლია დამსაქმებელს, მონიტორინგი გაუწიოს დასაქმებულის მიერ ტელეფონის, ელფოსტისა და ინტერნეტის გამოყენებას. შესაბამისად, ჩარევა არ იყო კანონიერი. სასამართლომ საქმეში დაადგინა კონვენციის მე-8 მუხლის დარღვევა.

3.4. შენახვის ვადის შეზღუდვის პრინციპი

მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს ან განადგურდეს ან შენახული უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით, თუ კანონით სხვა რამ არ არის დადგენილი.

სშკ-ის ახალი რედაქციით დამსაქმებელს წარმოეშვა ვალდებულება სამუშაო დღეს წერილობით ან/და ელექტრონულად აღრიცხოს დასაქმებულთა მიერ ნამუშევარი დრო და სამუშაო დროის (ნამუშევარი საათების) აღრიცხვის ყოველთვიური დოკუმენტი გააცნოს დასაქმებულს, გარდა იმ შემთხვევისა, როდესაც, სამუშაოს ორგანიზების სპეციფიკიდან გამომდინარე, ეს შეუძლებელია. დამსაქმებელი ვალდებულია სამუშაო დროის (ნამუშევარი საათების) აღრიცხვის დოკუმენტი შეინახოს 1 წლის განმავლობაში.

აღნიშნული გამომდინარეობს კონკრეტული, მიზანთან შესაბამისი ვადით პერსონალურ მონაცემთა შენახვის პრინციპიდან. კერძოდ, დამსაქმებელი ვალდებულია 1 წლის განმავლობაში შეინახოს დასაქმებულის მიერ ნამუშევარი საათები, შემდგომ კი წაშალოს, გაანადგუროს, დაბლოკოს და სხვ. აღნიშნული ასევე გამომდინარეობს სშკ-ს 74-ე მუხლიდან, რომლის თანახმად, პირს უფლება აქვს 48-ე მუხლის გათვალისწინებული მოთხოვნის გარდა, შრომითი ურთიერთობებიდან გამომდინარე სხვა მოთხოვნები გაასაჩივროს 1 წლის ვადაში. შესაბამისად, როდესაც სარჩელით მოთხოვნა ზეგანაკვეთურად ნამუშევარი საათების ან სახელფასო დანაკლისების ანაზღაურებაა, დამსაქმებელი ვალდებულია დაამტკიცოს, რომ პირს არ აქვს ზეგანაკვეთურად ან საერთოდ ნამუშევარი. ზემოაღნიშნული ინფორმაცია მტკიცების ტვირთის შემამსუბუქებელი საშუალებაა.

3.5. უსაფრთხოების პრინციპი

“პერსონალურ მონაცემთა დაცვის შესახებ” კანონის-ის მე-17 მუხლის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან. მონაცემთა უსაფრთხოებისათვის მიღებული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

პერსონალური მონაცემების უსაფრთხოებასა და კონფიდენციალობას უდიდესი მნიშვნელობა ენიჭება მონაცემთა სუბიექტებზე უარყოფითი გავლენისაგან თავიდან ასაცილებლად.[123] მონაცემთა უსაფრთხოების პრინციპი მოითხოვს სათანადო ტექნიკური ან ორგანიზაციული ღონისძიებების გატარებას პერსონალური მონაცემების დამუშავების პროცესში.[124] მონაცემთა უსაფრთხოების ასეთი ზომები შეიძლება მოიცავდეს დაშიფვრის, აუთენტიფიკაციის და ავტორიზაციის მექანიზმების გამოყენებას.[125]

მონაცემთა უსაფრთხოების უზრუნველყოფა და გარანტირება როგორც დამსაქმებლის, ასევე დასაქმებულის ვალდებულებაა. უსაფრთხოების პრინციპი დამმუშავებელს აარიდებს ზარალს მონაცემთა არასანქცირებული წვდომის შეცვლისა და გავრცელებისათვის.[126]

3.6. გამჭირვალობის პრინციპი

ევრორეგულაციის მიხედვით, აუცილებელია განისაზღვროს პასუხისმგებელი პირი, მონაცემთა უკანონო დამუშავების თავიდან ასაცილებლად. სწორედ ამიტომ რეგულაციას შემოაქვს ეს პრინციპი, რათა დარღვევის შემთხვევაში განსაზღვრული იყოს თუ ვის დაეკისრება შესაბამისი პასუხისმგებლობა. პასუხისმგებლობის განსაზღვრა ძალიან მნიშვნელოვანია, რადგან დამმუშავებელი მეტი ყურადღებით მოეკიდება მონაცემთა დამუშავებას.[127]

4. პერსონალურ მონაცემთა დაცვა წინასახელშეკრულებო ურთიერთობებში

შრომის სამართალი მოიცავს როგორც გასაუბრების ეტაპს, ასევე მუშაობისა და ხელშეკრულების შეწყვეტის შემდგომ ეტაპებსაც, შესაბამისად, დამსაქმებლის ვალდებულებაა სამივე ეტაპზე მაქსიმალურად დაცული იქნეს დასაქმებულის კონსტიტუციით გარანტირებული უფლებები და ინტერესები. წინასახელშეკრულებო ურთიერთობების პროცესი მოიცავს განცხადებას ვაკანსიაზე, ტესტირებას, გასაუბრებასა და კანდიდატის შესარჩევად გამოყენებულ ნებისმიერ სხვა ფორმას.[128]

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. პერსო-

[123] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო ევროკავშირის საგამომცემლო სახლი, ლუქსემბურგი, 2018, გვ. 148.

[124] იხ. იქვე გვ. 149.

[125] იხ. Six data protection principles, ხელმისაწვდომია: https://bit.ly/3mt8rpl წვდომის თარიღი: 04.07.2021.

[126] იხ. Convention to the Protection Individual with regard to Automatic Processing of Personal Data., Strasburg.28.I.1981, Article 7.

[127] ე. შერმადინი, პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში, თბილისი, 2020წ, გვ. 19.

[128] საქართველოს საკონსტიტუციო სასამართლოს 2010 წლის 27 დეკემბრის N1/1/493 გადაწყვეტილება, II.პ.6; დისკრიმინაციის აკრძალვა (საქართველოს კანონმდებლობისა და პრაქტიკის ანალიზი), გვ. 17.

ნალურ 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.[129] შრომითი ურთიერთობის უშუალო დაწყებამდე, დამსაქმებელი დასაქმების კანდიდატისგან მოიპოვებს სხვადასხვა სახის ინფორმაციას, რომელიც საჭიროა დასაქმებისათვის. სშკ-ის მე-11 მუხლის თანახმად, დამსაქმებელს უფლება აქვს, მოიპოვოს კანდიდატის შესახებ ინფორმაცია, გარდა იმ ინფორმაციისა, რომელიც არ არის დაკავშირებული სამუშაოს შესრულებასთან და არ არის საჭირო კანდიდატის მიერ კონკრეტული სამუშაოს შესრულების შესაძლებლობის შესაფასებლად და შესაბამისი გადაწყვეტილების მისაღებად, ხოლო კანდიდატი ვალდებულია დამსაქმებელს აცნობოს ნებისმიერი გარემოების შესახებ, რომელმაც შეიძლება ხელი შეუშალოს მას სამუშაოს შესრულებაში ან საფრთხე შეუქმნას დამსაქმებლის ინტერესებს. შესაბამისად, როდესაც დამსაქმებლის მიერ ხდება დასაქმებულის პერსონალურ მონაცემთა დამუშავება, მისი ვალდებულებაა გაითვალისწინოს პერსონალურ მონაცემთა დამუშავების პრინციპი - პროპორციულობა, რომელიც გამოიხატება მხოლოდ იმ ინფორმაციის მოპოვებაში, რაც აუცილებელია დასაქმებულის პროფესიონალიზმისა და კვალიფიციური უნარ-ჩვევების სამუშაო პოზიციასთან შესაბამისობის დასადგენად.

პერსონალური ინფორმაციის მოპოვება უნდა განხორციელდეს უშუალოდ დასაქმებულისგან. თუკი საჭიროება მოითხოვს, რომ დასაქმებულის შესახებ პერსონალური ინფორმაცია მოპოვებული იქნეს მესამე მხარისგან, ამისათვის დასაქმებული უნდა იყოს წინასწარ ინფორმირებული და წინასწარ, მკაფიოდ უნდა ჰქონდეს თანხმობა გაცხადებული.[130]

პერსონალურ მონაცემთა მოპოვებისას, დამსაქმებელს არ აქვს უფლება კანდიდატს დაუსვას შეკითხვები, რომელთა პასუხიც მოიცავს კანდიდატის პირადი ცხოვრების სფეროს.[131] მაგ., შეკითხვა ორსულობის, მშობიარობის, ოჯახური და ფინანსური მდგომარეობის, რწმენისა და აღმსარებლობის, პარტიული კუთვნილებისა და ნასამართლობის შესახებ დაუშვებელია.

ნასამართლეობის შესახებ ინფორმაცია შესაძლოა მოპოვებულ იქნეს მხოლოდ კანონით განსაზღვრულ შემთხვევებში, მაგალითად, სშკ-ის მე-10 მუხლის თანახმად, აკრძალულია ბაღებში, სკოლებში, თავშესაფარში და სხვა აღსაზრდელ/საგანმანათლებლო დაწესებულებებში იმ პირის

---

[129] მ. წერეთელი, პერსონალური მონაცემების დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში, თბილისი, 2019 წ., გვ. 37.

[130] The International Labour Organization (ILO), An ILO code of practice, Protection of workers' personal data, International Labour Office, Geneva, 6.1-6.2, p. 3.

[131] თ. კერესელიძე, შრომის ხელშეკრულების დადებამდე დამსაქმებლის მიერ კანდიდატისათვის დასმული დისკრიმინაციული შეკითხვის სამართლებრივი შედეგები, შრომის სამართალი (სტატიათა კრებული) I, ზაალიშვილი ვ. (რედ.), 2011 წელი, გვ. 201.

დასაქმება, რომელიც ნასამართლევია „სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართულ დანაშაულთან ბრძოლის შესახებ“ საქართველოს კანონით გათვალისწინებული სქესობრივი თავისუფლებისა და ხელშეუხებლობის წინააღმდეგ მიმართული დანაშაულის ჩადენისთვის, მიუხედავად ნასამართლობის მოხსნისა ან გაქარწყლებისა. ნასამართლობის შესახებ ინფორმაცია ასევე შესაძლებელია მოთხოვნილ იქნეს საჯარო სამსახურშიც, მაგ., პროკურატურაში მუშაობის დასაწყებად პირს აუცილებლად უნდა ჰქონდეს ნასამართლობის შესახებ ცნობა და ნარკოლოგიური ტესტირება ჩატარებული.

5. დასკვნა

საქართველოს კონსტიტუციით დაცულია ადამიანის ღირსების, თავისუფლების, პირადი და ოჯახური ცხოვრების უფლებები. აღნიშნულ უფლებათა რეალიზაციისათვის ერთ-ერთი მნიშვნელოვანი ასპექტი სწორედ პირთა პერსონალური მონაცემების სამართლიანად და კანონიერად დამუშავებაა. პირს უნდა ჰქონდეს მოლოდინი, რომ ის ინფორმაცია, რომელიც მას იდენტიფიცირებადს ხდის, კანონით დადგენილი წესით დაცული და გარანტირებული იქნება დამმუშავებლის ან უფლებამოსილი პირის მიერ. წინააღმდეგ შემთხვევებში, მას უნდა გააჩნდეს სამართლებრივი ბერკეტები, რომლითაც მოახდენს დარღვეულ უფლებათა რესტიტუციას. აღნიშნულის უზრუნველსაყოფად არსებობს სასამართლო და სახელმწიფო ინსპექტორის სამსახური, რომელსაც გააჩნია მთელი რიგი უფლებამოსილებები: განახორციელოს სადამსჯელო ღონისძიებები დამრღვევის მიმართ, გაუწიოს რეკომენდაციები, მისი ქვემდებარე დანაშაულის ნიშნების არსებობის შემთხვევაში დაიწყოს გამოძიება და სხვ.

დღევანდელი საქართველოს შრომის კოდექსით თუ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონით ზუსტად არ არის დადგენილი, თუ რა პერსონალური მონაცემები შეიძლება იქნეს მოპოვებული და დამუშავებული დამსაქმებლის მიერ დასაქმებულისგან როგორც წინასახელშეკრულებო პერიოდში, ასევე, დასაქმებისა და შეწყვეტის შემდეგ. შესაბამისად, გონივრული გადაწყვეტილება იქნება მიღებული, თუკი კანონი ამომწურავად განსაზღვრავს იმ პერსონალურ მონაცემთა ჩამონათვალს, რომლის მოპოვებისა და დამუშავების უფლებამოსილება ექნება დამსაქმებელს. როგორც უკვე ზემოთ ვახსენებთ, შრომის უფლება ერთ-ერთი უმნიშვნელოვანესი უფლებაა, რომელიც მნიშვნელოვან გავლენას ახდენს როგორც მოსახლეობის ცხოვრებისეულ დონეზე, ასევე, სახელმწიფო ეკონომიკაზე, შესაბამისად, აღნიშნული უფლების უზრუნველყოფა უნდა განხორციელდეს ყოველი მხრიდან, მათ შორის, დასაქმებულთა პერსონალური მონაცემის დამუშავების მხრიდანაც.

მონაცემთა უსაფრთხოების თანამედროვე გამოწვევები

ავტორი: თამარ მეხრიშვილი
თავისუფალი უნივერსიტეტი

1. შესავალი

თანამედროვე სამყაროში, ტექნოლოგიური პროგრესის პარალელურად, ფინანსურმა მომსახურებამ დიდ წილად ციფრულ სფეროში გადაინაცვლა. გაიზარდა, როგორც ფინანსური სტრუქტურების რაოდენობა, ასევე მათზე წვდომაც. იმის გათვალისწინებით, რომ დღევანდელი ტექნოლოგიები საშუალებას გვაძლევს დღის ნებისმიერ მონაკვეთში, ნებისმიერ ადგილას შევამოწმოთ ჩვენი საბანკო ანგარიში და თავისუფლად მივიღოთ ან გადავრიცხოთ თანხა ნებისმიერ მომენტში, რა თქმა უნდა, კომფორტულია, თუმცა ყოველდღიურ ცხოვრებაში ბევრი ჩვენგანი უგულებელყოფს რისკებს, რომლებიც ამ ყველაფერს თან ახლავს. ფინანსურ მომსახურებებზე ხელმისაწვდომობის ზრდამ, ციფრული ტექნოლოგიების განვითარებასთან ერთად, ფინანსური თაღლითობის ახალი რისკებიც წარმოშვა, მაგალითად ის, რომ თქვენს ინფორმაციას ვიღაც მიითვისებს და თავის სასარგებლოდ გამოიყენებს, უკვე უამრავ პლატფორმას ეხება. შესაბამისად, მომხმარებელს საკუთარი თითოეული პლატფორმის უსაფრთხოებაზე ცალკეულად უწევს ზრუნვა, რაც საკმაოდ შრომატევად საქმედ ითვლება. ამ მიზეზით, საზოგადოებაში ხშირად უგულებელყოფილია პირადი მონაცემების გაზიარებასთან დაკავშირებული საფრთხეები და შესაბამისად, იზრდება ამ ტიპის დანაშაულები.

ფაქტია, რომ ციფრული სფერო საკუთარი განვითარების ზენიტშია, გაზრდილია მასზე მოთხოვნა და ეტაპობრივად იზრდება მისი მომხმარებელთა რიცხვი. უნდა აღინიშნოს, რომ ამ ყველაფერს აქვს როგორც დადებითი, აგრეთვე უარყოფითი მხარე. ინტერნეტის საშუალებით, ყოველდღიურად უამრავი ადამიანის მიერ ხორციელდება სხვადასხვა კომუნიკაციები, პროდუქციისა და მომსახურების ონლაინ შესყიდვები, კომუნალური გადასახადების გადახდა. მრავალმა სახელმწიფო და საბანკო პლატფორმამაც ონლაინ რეჟიმში გადაინაცვლა. აქედან გამომდინარე, უნდა გავითვალისწინოთ, რომ ამ ყველაფრის განვითარება, ინტერნეტში ჩვენი პერსონალური მონაცემების დიდი მოცულობით დაგროვებას განაპირობებს. ამ თემასთან დაკავშირებულ საკითხებს საქართველოს კანონმდებლობაში „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი არეგულირებს. იგი მოქალაქეებს საკუთარ ზოგად უფლებებს აცნობს, რომ ყოველთვის აქვთ შესაძლებლობა გაიგონ თუ მათი პირადი ინფორმაციის რა ნაწილი მუშავდება სხვადასხვა უწყების მიერ, ხდება თუ არა მონაცემთა მესამე პირებისთვის გადაცემა და ასე შემდეგ. თუმცა, მხოლოდ ეს არ არის საკმარისი. პრობლემაა, რომ საზოგადოება არ არის ინფორმირებული პირადი მონაცემების უსაფრთხოების უზრუნველყოფის გზების შესახებ და მისმა უმეტესობამ არ იცის ამ მხრივ პოტენციურ დანაშაულთა მრავალფეროვნება. ჩვენს პირად მონაცემებზე წვდომას თავად გავცემთ, თუნდაც როდესაც ნებისმიერი ვებ-გვერდის ქუქი (cookie) ფაილების მიღებას

ვთანხმდებით, რაც ინტერნეტ ბრაუზერის საშუალებით მოწყობილობის ოპერაციულ სისტემაში ინახება. რასაკვირველია, მომხმარებლებს ძირითადად აქვთ საშუალება გაეცნონ საკუთარ უფლებებს და მხოლოდ მას შემდეგ დათანხმდნენ წამოყენებულ პირობებს, თუმცა ამას მხოლოდ მცირედი ნაწილი აკეთებს და დაუფიქრებლად გასცემს ინფორმაციაზე წვდომის უფლებას.

2. თანამედროვე გამოწვევები

დღევანდელი ციფრულის სფეროს ერთ-ერთ მნიშვნელოვან გამოწვევად საკუთარი მომხმარებლების უსაფრთხოების უზრუნველყოფა გვევლინება. კიბერდანაშაულის შემთხვევები მსოფლიოში დღითიდღე მატულობს და ეს გამოწვევა საქართველოსაც შეეხო, 2018-2019 წლის შუალედში კიბერდანაშაულის რიცხვი 53.28%-ით გაიზარდა. კიბერდანაშაულის შემთხვევების შემცირების მიზნით, საქართველოს შინაგან საქმეთა სამინისტრომ სპეციალურად შექმნა „კიბერდანაშაულთან ბრძოლის სამმართველო“, რომელიც შეძლებისდაგვარად უზრუნველყოფს მოსახლეობის ინფორმირებულობას, თუმცა პრობლემის აღმოსაფხვრელად თითოეული მხარის, მათ შორის რიგითი მოქალაქეების, ჩართულობა აუცილებელია. სახელმწიფოს მხრიდან აღსანიშნავია კიბერუსაფრთხოების საკითხების „ეროვნული უსაფრთხოების საბჭოსთვის“ გადაბარება. საბჭოს საქმიანობის ძირითადი მიმართულებაა ინფორმაციული უსაფრთხოების პოლიტიკის ანალიზი, საფრთხეების იდენტიფიცირება და შეფასება, თუმცა მისი საქმიანობის მიუხედავად, საქართველოში მონაცემთა უსაფრთხოების მხრივ, არასახარბიელო სიტუაციაა. ძირითადი პრობლემაა, კიბერდანაშაულის ტიპების მრავალფეროვნება, რომელსაც ერთი ან ორი სახელმწიფო სტრუქტურა ერთობლივად ვერ უმკლავდება. ამ მხრივ, სახელმწიფოს მხრიდან, საჭიროა სიტუაციის სექტორული მენეჯმენტი და მოვალეობების გადანაწილება, რა მხრივაც, ეტაპობრივად ხორციელდება ცვლილებები. შეიქმნა ცალკეულად კერძო და საჯარო სექტორზე ზედამხედველობის დეპარტამენტები, რაც სექტორული მენეჯმენტის გზაზე, მნიშვნელოვანი მიღწევაა, თუმცა პერსონალური მონაცემების უსაფრთხოების კუთხით, კვლავ უარყოფითი სიტუაციაა. აღსანიშნავია ისიც, რომ დღეს საქართველოს არ გააჩნია მოქმედი კიბერუსაფრთხოებასთან ბრძოლის ეროვნული სტრატეგია და მხოლოდ არსებობს ამ დოკუმენტის სამუშაო, დაუმოწმებელი ვერსია. დღეს, ქვეყანაში გატარებული ღონისძიებები და მიმდინარე კიბერპოლიტიკა არ არის საკმარისი კიბერუსაფრთხოების უზრუნველსაყოფად და თანამედროვე გამოწვევების საპასუხოდ.

იმის გათვალისწინებით, რომ კიბერუსაფრთხოების უზრუნველყოფა და შესაბამისად პერსონალური მონაცემების დაცვა, როგორც სახელმწიფოს, ასევე მოქალაქის საერთო პასუხისმგებლობაა, ამ მიმართულებით ორივე მხარემ ურთიერთშეთანხმებულად უნდა იმუშაოს. ამასთანავე, საჭიროა სამოქალაქო სექტორის ინფორმირება პოტენციური კიბერდანაშაულის შესახებ და სახელმწიფოს მხრიდან, მათი მაქსიმალური ჩართულობის უზრუნველყოფა სიტუაციის მართვისა და უსაფრთხოების პროცესში. სახელმწიფოს ანგარიშვალდებულება და გამჭვირვალობა დემოკრატიულობის მნიშვნელოვანი პრინციპებია და მოცემული საკითხი აქ განსაკუთრებით მნიშვნელოვანი ხდება, ვინაიდან კიბერდანაშაული ჩვეულებრივი დანაშაულის ტიპია, რომელიც საფრთხეს უქმნის ეროვნულ უსაფრთხოებას, განსაკუთრებით კი მაშინ, როდესაც საქმე პირადი

მონაცემების უსაფრთხოებას ეხება. აქედან გამომდინარე, ამ სფეროს სტრუქტურირებასთან ერთად, მიზანშეწონილი იქნებოდა „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის გაფართოვება და მასში თუნდაც ისეთი დეტალების შეტანა, როგორიც თითოეული სტრუქტურის მოვალეობების მკაფიოდ განსაზღვრაა. საბოლოოდ, აუცილებელია, რომ კიბერუსაფრთხოების პოლიტიკის აღმასრულებელმა უწყებებმა ითანამშრომლონ მოქალაქეებთან და საზედამხედველო ორგანიზაციებთან, რათა პერსონალურ მონაცემებთან დაკავშირებული რისკები და საფრთხეები თავიდან იქნეს აცილებული. ამ გზით, კიბერუსაფრთხოება უნდა გახდეს სახელმწიფოს ერთ-ერთი პრიორიტეტი, რომლის განვითარებასაც მეტი ფინანსური და ინტელექტუალური რესურსი უნდა მოხმარდეს.

იმის გათვალისწინებით, რომ თანამედროვე მსოფლიოში კიბერდანაშაულის უმრავლესობა ფინანსების მითვისებაზეა ორიენტირებული, აქ მნიშვნელოვანი ხდება ფინანსური სექტორის როლი საკუთარი მომხმარებლების ფინანსური დაცულობის უზრუნველყოფაში. ამ მხრივ, განსაკუთრებული აქტიურობით გამოირჩევა საქართველოს ეროვნული ბანკი, რომელმაც სპეციალურად ფინანსური უსაფრთხოების უზრუნველსაყოფად გახსნა ფინანსური განათლების პორტალი - „ფინედუ“. კონკრეტული პროექტი გამოირჩევა იმით, რომ იგი უშუალოდ ხელს უწყობს მონაცემთა უსაფრთხოების უზრუნველყოფის პროცესში მოქალაქეების ჩართვას. ნებისმიერ პრობლემასთან ბრძოლის გზა, ხალხის ინფორმირებით უნდა დაიწყოს და სწორედ საზოგადოებისათვის ინფორმაციის მიწოდებას ემსახურება „ფინედუ“, სადაც მარტივად და გასაგებად არის აღწერილი ბანკთან დაკავშირებული ნებისმიერი კომუნიკაცია, პირადი მონაცემების დაცვის გზები და ყველაფერი ფინანსური უსაფრთხოების შესახებ. კონკრეტული პლატფორმა, ერთ-ერთი კარგი მაგალითია თუ როგორ უნდა მიეწოდოს ხალხს ინფორმაცია და ეს პროცესი იყოს ეფექტური. ეროვნული ბანკის აქტივობებიდან, ასევე განსაკუთრებულია კონკურსები, რომელიც პირადი მონაცემების უსაფრთხოებასთან დაკავშირებით, ყოველწლიურად ტარდება და ამ საკითხზე ცნობიერების ამაღლებას უწყობს ხელს. ამ გზით, მოქალაქეები მარტივად და გასაგებად იღებენ შესაბამის ინფორმაციას და მაქსიმალურად ერთვებიან პირადი მონაცემების უსაფრთხოების უზრუნველყოფის პროცესში. ამ მხრივ, ვფიქრობ, საინტერესო იქნებოდა აქტივობები კონკრეტულად სახელმწიფოს მხრიდანაც.

დღესდღეობით, ფინანსური სექტორი, ძირითადად ბანკები, წარმოადგენენ ერთ-ერთ უმაღლეს ინსტანციას, რომელსაც მომხმარებელმა საკუთარი პირადი მონაცემები, ბარათის ნომერი, მისი მოქმედების ვადა, პინკოდი, უნდა გაუზიაროს. შესაბამისად, წარმოიქმნება მომხმარებლის პირადი, სენსიტიური ინფორმაციის უსაფრთხოების უზრუნველყოფის ვალდებულება. თუმცა, უნდა აღინიშნოს რომ აქ მთავრი პასუხისმგებლობა კვლავ მომხმარებელს ეკისრება. შესაბამისად, აუცილებელია ვაკონტროლოთ თუ კონკრეტულად ვის ან რა ორგანიზაციას ვუზიარებთ ჩვენს პირად ინფორმაციას. ნებისმიერი სახის პირად უსაფრთხოებას, პირველ რიგში, თავად მომხმარებელი უზრუნველყოფს და მართლაც უმთავრეს ბერკეტს სწორედ ჩვენი პირადი სურვილები წარმოადგენს, სურვილები რომელთა მიხედვითაც ვწყვეტთ თუ ვის, სად და როგორ გავუზიაროთ ჩვენი პირადი ინფორმაცია. ფინანსური სექტორის შემთხვევაში, ეს კონკრეტულად ეხება ბანკებსა და მიკროსაფინანსო ორგანიზაციებს.

ბანკი, დღესდღეობით, ერთ-ერთ ყველაზე სანდო, უმაღლეს ინსტანციად გვევლინება, რომელიც მაქსიმალურ ხელმისაწვდომობასა და პირადი ინფორმაციის დაცულობას გვთავაზობს. პირველი ნაბიჯი, რასაც იგი ჩვენი ფინანსებისა და პირადი ინფორმაციის უსაფრთხოების მიზნით აკეთებს, ესაა თითოეულ ანგარიშზე პინკოდის დაწესება. თუმცა, აქაც უნდა აღინიშნოს, რომ მაქსიმალური უსაფრთხოებისთვის საჭიროა მთავარი ინიციატივა მომხმარებელმა გამოიჩინოს და იფიქროს უფრო მეტზე ვიდრე დაბადების წელზე ან თარიღზე. რთული, არაფერთან დაკავშირებული, თუმცა მომხმარებელზე ინდივიდუალურად მორგებული პინკოდი ან პაროლი თითქმის ყოველთვის აღწევს შედეგს - იცავს ჩვენს პირად ანგარიშს. ამასთან ერთად, მაქსიმალური დაცულობის უზრუნველსაყოფად, მიზანშეწონილია ამ პაროლის პერიოდულად ცვლაც. ფინანსური უსაფრთხოება მეტწილად დამოკიდებულია ჩვენი ტექნოლოგიური მოწყობილობების უსაფრთხოებაზეც, იქნება ეს კომპიუტერი თუ მობილური ტელეფონი. ორიგინალური პაროლის დაყენებასთან ერთად, უსაფრთხოების უზრუნველყოფაში ლიცენზირებული პროგრამებისა და ანტივირუსული სისტემის დაყენებაც აუცილებელია. თუმცა, გასათვალისწინებელი ფაქტორია, რომ ეს ყველაფერი მაინც ვერ უზრუნველყოფს პირადი მონაცემების სრულყოფილ უსაფრთხოებას, ვინაიდან საბოლოოდ ეს პროცესი მომხმარებლის პირად გადაწყვეტილებებზე გადის.

3. მონაცემთა უსაფრთხოების უზრუნველყოფა

ეს ყველაფერი ერთი შეხედვით მარტივია, თუმცა არ უნდა დაგვავიწყდეს, რომ დღევანდელი საზოგადოება თანამედროვე ტექნოლოგიური განვითარების ეპოქაში იმყოფება და შესაბამისად, დამატებით წარმოიქმნება ჩვენი ფინანსებისა და პირადი ინფორმაციის მთავარი საფრთხე - ინტერნეტი. იმის გათვალისწინებით, რომ თანამედროვე საზოგადოების დიდი ნაწილი აქტიურად იყენებს ინტერნეტს, რასაკვირველია, ფინანსურმა საფრთხეებმა უკვე ამ სფეროშიც გადაინაცვლა და ფინანსური თაღლითობის თვალსაზრისით, ახალი რისკები წარმოქმნა. თუმცა, აღსანიშნავია, რომ ჩვენი ფინანსებისა და ინფორმაციის მითვისებისკენ მიმართული ნებისმიერი სახის კიბერდანაშაულის თავიდან არიდება სავსებით შესაძლებელია. პირად ანგარიშებზე რთულად ამოსაცნობი პაროლის დაყენების გარდა, მომხმარებელს საკუთარი უსაფრთხოების უზრუნველყოფა თავადაც შეუძლია შესაბამისი ინფორმაციის, კვლავ ინტერნეტიდან, მიღების საფუძველზე.

სენსიტიური და პერსონალური ინფორმაციის მოპარვის/მითვისების ხერხები მრავალფეროვანია. თაღლითები მომხმარებლებს ელექტრონული ფოსტის, სოციალური ქსელის, სატელეფონო ზარისა და ვირუსების საშუალებით სძალავენ პირად ინფორმაციას და ამ ყველაფერს თავიანთ სასარგებლოდ იყენებენ. როგორც აღვნიშნეთ, ინფორმირებულობა ამ პრობლემის გადაჭრის ერთ-ერთი უმთავრესი გზაა და პირველ რიგში, უსაფრთხოების ომების მიღებამდე, საჭიროა ვიცოდეთ, რისგან ან ვისგან გამომდინარეობს საფრთხე. ინტერნეტ-სივრცის განვითარებასთან ერთად, დღითიდღე ფართოვდება კიბერდანაშაულის სახეობები. შესაბამისად, მომხმარებელი მაქსიმალურად უნდა იყოს ინფორმირებული თითოეული მათგანის შესახებ, იქნება ეს პირადი მონაცემების მითვისება, ფულის გაყალბება, „ფიშინგი“, ე. წ „ფინანსური პირამიდები“ თუ რაიმე სხვა. მხოლოდ საფრთხის იდენტიფიცირებისა და შესწავლის შემდეგ, შესაძლებელია

თავდაცვაზე გადასვლა. აქედან, მომხმარებლის მოტყუების ალბათ ყველაზე ეფექტური საშუალება „ფიშინგია“, თაღლითობის ფორმა, რომლის ფარგლებშიც მომხმარებელი საკუთრი ნებით გადასცემს თაღლითს საკუთრ პირად ინფორმაციას. ეს პროცესი სპეციალურად შექმნილ, ყალბ ვებ-გვერდზე მომხმარებლის შესვლით იწყება. მათ რომელიმე სოციალური საკომუნიკაციო საშუალებით მისდით შეტყობინება, წერილის ავტორად კი ხშირად ფინანსური ორგანიზაცია ან სხვა, მომხმარებლისათვის ნაცნობი ორგანიზაცია მიეთითება. თაღლითები ცდილობენ, მოტყუებით გადაიყვანონ მომხმარებელი შეტყობინებაში მოცემულ ბმულზე, რომელიც ყალბი ვებგვერდის მისამართს წარმოადგენს და ჩამოატვირთინონ მიმაგრებული მავნე ფაილი, რომელიც წარმოდგენილია როგორც ლეგიტიმური დოკუმენტი. ამ და სხვა საშუალებებით, მრავალი მომხმარებელი მართლაც ტყუვდება და საკუთარი ნებით გასცემს პირად ინფორმაციას, რის შედეგადაც თაღლითები მოიპოვებენ თუნდაც მათ საბანკო ანგარიშზე წვდომას, რაც ნიშნავს, რომ მათ შეუძლიათ მსხვერპლის სახელით სესხის აღება, სხვადასხვა ტრანზაქციის წარმოება, სესხის აღებაც კი. კიბერდანაშაულის ამ ტიპის თავიდან აცილება, განსაკუთრებულ დაკვირვებას მოითხოვს შემოსული შეტყობინების ელექტრონული ფოსტის მისამართზე, ტექსტისა და ვებ-გვერდის დეტალებზე, რომლის შესახებაც ცნობადობა მოსახლეობის დიდ ნაწილს არ აქვს. შესაბამისად, დღესდღეობით, საქართველოში „ფიშინგის“ მსხვერპლი ჩვეულებრივად შესაძლოა გახდეთ.

თუკი მომხმარებელი იცნობს კიბერთაღლითობის სხვადასხვა ტიპს და მისი განხორციელების სხვადასხვა გზას, მის მიმართ ფინანსური თაღლითობის რისკი ეტაპობრივად მცირდება. თუმცა, იმის მტკიცება, რომ ბანკები ან თუნდაც სახელმწიფო არასაკმარისად უზრუნველყოფს მოსახლეობის კიბერუსაფრთხოებაზე ინფორმირებას, არ იქნებოდა სამართლიანი, რადგანაც ინფორმირების პრობლემა ძირითადად ასაკოვან ადამიანებში გამოიხატება. ვფიქრობ, პრობლემა იმაში მდგომარეობს, რომ ინტერნეტ-თაღლითობის თავიდან არიდების გზები კვლავ ინტერნეტში მოიძებნება. საპენსიო ასაკისა და მას გადაცილებულ მოსახლეობას იშვიათად თუ მოეპოვებათ ინფორმაცია კიბერდანაშაულის ნებისმიერ სახეობაზე, რადგან არ აქვთ წვდომა შესაბამის ინტერნეტ-რესურსებზე და მარტივად შეიძლება დაიჯერონ თაღლითური სახის მესიჯი თუნდაც იმის შესახებ, რომ მილიონი მოიგეს.

საქართველოს ინტერნეტსივრცეში ფინანსური უსაფრთხოება განსაკუთრებული რისკის ქვეშაა. იმის გათვალისწინებით, რომ მოსახლეობის უმრავლესობა შუა ხნის ან საპენსიო ასაკისაა და დიდი ნაწილის ინტერნეტთან შეხება მხოლოდ სოციალური ქსელებით შემოიფარგლება, გვაქვს ინფორმირებულობის პრობლემა. ნებისმიერი სოციალური პრობლემის სათავე შეგვიძლია ინ-ფორმაციის სიმცირეში ვეძიოთ და აქედან გამომდინარე, მსგავსი პრობლემების გადაჭრისას აუცილებელია თითოეული მომხმარებლის ასაკობრივი ინტერესების გათვალისწინება. მხოლოდ და მხოლოდ ამ შემთხვევაში გადაიჭრება პრობლემა ეფექტურად. ფინანსური უსაფრთხოების შესახებ ქართულ ინტერნეტ-სივრცეში არაერთი სტატია და ანგარიში არსებობს, თუმცა კიბერ-დანაშაულის შემთხვევები ასე მაღალი არასდროს ყოფილა. ფინანსური უსაფრთხოების ზოგადი პრინციპები, შესაძლოა, ნებისმიერმა რიგითმა მოქალაქემ იცოდეს - ის, რომ საჭიროა ანგარიშის პაროლის პერიოდულად შეცვლა, პირადი ნომრის არავისთვის გაზიარება და ასე შემდეგ, თუმცა დღევანდელი კიბერდანაშაულის განმახორციელებლები სწორედ იმ სიტუაციებით სარგებლობენ,

რომელშიც ნაკლებად ინფორმირებული საზოგადოების წევრები არიან წარმოდგენილნი. შესაბამისად, საჭიროა ინფორმაციის გავრცელების საშუალებების გამრავალფეროვნება და მათი მორგება ყველა ასაკობრივ კატეგორიაზე. ასაკოვანი მოსახლეობისთვის ინფორმაციის წყაროების მრავალფეროვნების უზრუნველყოფა უნდა მოხდეს, იმ საინფორმაციო საშუალებებით, რომლებსაც ისინი განსაკუთრებულ ყურადღებას უთმობენ და შესაბამისად, პირადი ინფორმაციის უსაფრთხოებასთან დაკავშირებული კამპანია, უნდა მოერგოს ყელაზე მეტად დაზარალებული საზოგადოებრივი ჯგუფის პლატფორმებს. ამ შემთხვევაში, კონკრეტულ თემასთან დაკავშირებით, მეტი ინფორმაცია უნდა გავრცელდეს ტელევიზიისა და ჟურნალ-გაზეთების საშუალებით, ვინაიდან საქართველოს ასაკოვანი კატეგორიის ინფორმაციის მთავარი წყარო სწორედ ესაა.

მომხმარებლის უსაფრთხოებაზე მთავარი პასუხისმგებელი, პირველ რიგში, თავად მომხმარებელია და ფინანსური სექტორის, ასევე როგორც მთავრობის, ერთგვარი ვალდებულებაა დაეხმაროს მას ამის გააზრებაში. კიბერდანაშაულის ტიპებში გარკვევის შემდეგ, საჭიროა თავდაცვის გეგმის შემუშავება. პირადი მონაცემების უსაფრთხოების უზრუნველყოფის პროცესში, მნიშვნელოვანია ყურადღება ნებისმიერი საეჭვო პირის მიმართ, რომელიც ინფორმაციის მოპოვებას ეცდება. დაკვირვებულობასთან ერთად, საჭიროა, რომ პერსონალური მოწყობილობები და მათში არსებული მონაცემები, მართლაც პერსონალურად დარჩეს. აუცილებელია პირად ანგარიშებზე, განსაკუთრებით კი ინტერნეტ-ბანკის ანგარიშზე, რთული პაროლის დაყენება და მისი დროთა განმავლობაში შეცვლა. ეს რეკომენდაციები ერთად, ერთგვარ ფორმულას წარმოადგენს, რომელიც მომხმარებლის პერსონალური ინფორმაციის უსაფრთხოების დაცვას უზრუნველყოფს, თუმცა, გასათვალისწინებელია, რომ არსებობს ცალკეული შემთხვევებიც, როდესაც იგი არ ამართლებს. ამ შემთხვევებშიც, მთავარი პასუხისმგებლობა მომხმარებელზე გადის, ვინაიდან სწორედ ჩვენზეა დამოკიდებული რა შეტყობინებას გავხსნით, რა ვებ-გვერდზე გადავალთ და გავუზიარებთ თუ არა სხვას ჩვენს პირად ინფორმაციას. საჭიროა მეტი დაკვირვება დეტალებზე, ყურადღება უნდა დავუთმოთ ვინ, სად და როგორ აზიარებს შესაბამის ინფორმაციას, უმისამართოდ არ გავავრცელოთ ჩვენი საბანკო ბარათის ანგარიშის ნომერი და არასდროს შევინახოთ ის რომელიმე ვებ-გვერდზე. ონლაინ მაღაზიები ხშირად გთავაზობენ ბარათის მონაცემების დამახსოვრებას, რათა ყოველ ჯერზე თავიდან არ მოგიწიოთ მისი შეყვანა. მიუხედავად კომფორტისა, ეს რისკის შემცველიცაა, ვინაიდან თუ თაღლითმა საბანკო ანგარიში გატეხა, ის უკვე შეძლებს დამახსოვრებული ბარათის მონაცემებით სარგებლობას. ონლაინ შესყიდვების განხორციელებისას, მეტი უსაფრთხოებისთვის, რეკომენდირებულია ცალკე ბარათის გამოყენება, ასევე ანგარიშის ამონაწერის რეგულარულად შემოწმება. ნებისმიერი საეჭვო ტრანზაქციის დეტალების დროულად გარკვევა აუცილებელია და საჭირო შემთხვევაში, ბარათის დაბლოკვა მაქსიმალურად უზრუნველყოფს მომხმარებლის პირადი ინფორმაციის უსაფრთხოებას. ამავდროულად, ყურადსაღებია თავად ვებ-გვერდის მისამართის დეტალებიც, რომლებიც ხშირად მაქსიმალურად მიმსგავსებულია ორიგინალს და მხოლოდ ერთი ასო აქვს შეცვლილი. ამასთან ერთად, მისამართი უნდა იწყებოდეს https://-ით და არა http://-ით ან მსგავსით, ვინაიდან ეს პირადი თუ ბარათის მონაცემების არა ღია, არამედ დაშიფრული სახით გაგზავნას ნიშნავს. ასევე, მისამართის ველში უნდა ჩანდეს მწვანე ჩაკეტილი ბოქლომის სიმბოლო, რომელიც პირადი ინფორმაციის დაცულობაზე მიანიშნებს. კიბერთაღლითობაში გამოკვეთილი ტენდენციაა, პირადობის მოწმობის, პასპორტის ან საბანკო ბარათის ასლის მოთხოვნა, რაც, რასაკვირველია, არ არის მიზანშეწონილი,

ვინაიდან ეს ადამიანის ალბათ ყველაზე სენსიტიური და მნიშვნელოვანი ინფორმაციაა. პირადი მონაცემების უსაფრთხოების უზრუნველყოფის ერთ-ერთი გამართლებული ხერხია ანგარიშებზე მრავალფაქტორიანი აუთენტიფიკაციის დაყენება, რაც პაროლის გარდა, გულისხმობს თითის ანაბეჭდის ან სახის ამოცნობის სისტემის დაყენებასაც.

4. დასკვნა

პირადი მონაცემების უსაფრთხოების საკითხში თანაბრად პასუხისმგებელია მომხმარებელი და სახელმწიფოც. მოქალაქე, პირველ რიგში თავად განსაზღვრავს ვის და როგორ უნდა გაიზიაროს ინფორმაცია საკუთარი თავის შესახებ, შესაბამისად ნებისმიერი ამ მხრივ განხორციელებული ქმედება, მის სრულ ყურადღებასა და პასუხისმგებლობას მოითხოვს. რაც შეეხება სახელმწიფოს, ამ შემთხვევაში, მისი მოვალეობაა ეფექტურად გააცნოს საზოგადოებას საკუთარი უფლებები და დაეხმაროს მათ ამ ყველაფრის რეალიზებაში. საქართველოს მოსახლეობის პირადი ინფორმაციის საფრთხის ქვეშ ყოფნის მიზეზად, ძირითადად, საზოგადოების ინფორმირების დაბალი დონე გვევლინება. ამ დეტალის გამოსასწორებლად, აუცილებელია საჯარო და სამოქალაქო სექტორის გაერთიანება და პრობლემის გადასაჭრელად ერთობლივი მუშაობა.

შესაბამისად, მართებულია დავასკვნათ, რომ არსებობს სახელმწიფო სექტორსა და მოქალაქეებს შორის თანამშრომლობის პრობლემა და მიუხედავად იმისა, რომ ყველა სახის ინფორმაციის მიწოდება უზრუნველყოფილია, არ ხდება მის სრულყოფილად გააზრებასა და ათვისებაზე ზრუნვა, განსაკუთრებით ქვეყანაში წარმოდგენილ ცალკეულ ასაკობრივ კატეგორიებში. საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სფეროს განვითარებასთან ერთად, საჯარო სექტორის სამუშაოებში საზოგადოების მონაწილეობა კიდევ უფრო რეალური და მარტივი გახდა, ვინაიდან მკვეთრად შემცირდა ამგვარი ურთიერთქმედებისა და დიალოგისთვის საჭირო როგორც ხარჯები, ისე დრო. ტექნოლოგიური პროგრესისა და ამ კუთხით სამოქალაქო გათვითცნობიერების გამოყენება შეიძლება პიროვნული მონაცემების უსაფრთხოების უზრუნველყოფის პროცესში ჩართულობის პრობლემის გადასაჭრელად, შესაბამისად, მოქალაქეებსა და სახელმწიფოს შორის ახალი ფორმის ურთიერთქმედების ჩამოსაყალიბებლად. გარდა ამისა, აუცილებელია ამ თანამშრომლობას მონიტორინგი გაუწიოს შესაბამისმა არასამთავრობო ორგანიზაციებმა, რომლებიც ერთგვარი ხიდის ფუნქციას შეასრულებენ ხალხსა და ხელისუფლებას შორის და გაამარტივებენ კომუნიკაციას. წარმატებული თანამშრომლობის შედეგად, ნამდვილად გამოსწორდება სიტუაცია, მოხდება შესაბამისი კანონის გაფართოვება და დაიგეგმება ინფორმირებასთან დაკავშირებული, მართლაც მოსახლეობის ინტერესებსა და საჭიროებებზე მორგებული პროექტები.

ჩემი აზრით, დღეს სახელმწიფო უნდა ეცადოს მაქსიმალურად გაამარტივოს პირადი მონაცემების საფრთხეებისა და მისი უსაფრთხოების უზრუნველყოფის შესახებ ინფორმაციაზე წვდომა, გაამარტივოს შესაბამისი საინფორმაციო ტექსტები და გახადოს ისინი რიგითი მოქალაქეებისთვის გასაგები და საინტერესო. იმის გათვალისწინებით, რომ პირადი მონაცემების დაცვა, პირველ რიგში, თავად მოქალაქის საზრუნავია, მნიშვნელოვანია რომ სახელმწიფო დაეხმაროს მათ ამის გააზრებაში. ეს კი, რასაკვირველია, შესაბამისი ინფორმაციის საზოგადოებისთვის ეფექტურად მიწოდებით მიიღწევა.

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა (პანდემიის პერიოდში დაწესებული ცალკეული შეზღუდვის განხილვის მაგალითზე)

ავტორი: ირაკლი ლეონიძე[132]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

სტატიაში განხილულია ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვის აქტუალური საკითხები, პანდემიის პერიოდში დაწესებული ცალკეული შეზღუდვის მოქმედების მაგალითზე.

ვიდეოთვალთვალის განხორციელების მიზნით დაწესებულებისა თუ სივრცის შესაბამისი საშუალებით აღჭურვა ქმნის მოლოდინს რომ ამ სივრცეში მყოფი ნებისმიერი პირი ინფორმირებული იქნება ვიდეოთვალთვალის ნებადართულ სივრცულ და ტერიტორიულ არეალში განხორციელების შესახებ.[133] საკითხავია, თუ რამდენად პასუხობს კანონისმიერ მოლოდინს საკანონმდებლო და გარკვეული მიზნით განსაზღვრული რეალობა, რომელიც კონსტიტუციური უფლების შეზღუდვის თვალსაზრისით, ახალი კონცეფციით განავითარა მსოფლიოში მიმდინარე პანდემიამ, უფრო მეტად კი მისგან გამომდინარე: ეკონომიკურმა, ფინანსურმა, სამართლებრივმა, სოციალურმა, მორალურმა და სხვა სახის შეზღუდვის წინაპირობებმა.[134]

ვიდეოთვალთვალის განხორციელებისას სხვადასხვა სამართლებრივი თუ არასამართლებრივი ინტერესის თანაკვეთას შეფასების მეთოდური და რაციონალური სტანდარტი ესაჭიროება, ხოლო სახელმწიფოში კოვიდ-19 პანდემიით გამოწვეული საფრთხეები და მოსალოდნელი რისკები კი დღის წესრიგში აყენებს ვიდეოთვალთვალის შედეგად მოპოვებული ინფორმაციის დამუშავების, მოხმარებისა თუ განადგურების საკითხებს, რომელთა პრობლემურობა არ ახალია, მაგრამ პანდემიის მიმდინარეობისას მკვეთრად გამოხატული ხასიათი აქვს.[135] პანდე-

[132] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ზეინაბ შავაძე.

[133] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“, მუხლი 48.

[134] მ. კაკულია, ნ. კაპანაძე, „ანტიპანდემიური შეზღუდვების და მთავრობის ანტიკრიზისული ღონისძიებების გავლენა დასაქმებაზე, შემოსავლებსა და სიღარიბის დონეზე საქართველოში“, ფრიდრიხ

ებერტის ფონდის გამოცემა, 2020. გვ. 7.

[135] სახელმწიფო ინსპექტორის სამსახური, „სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, 2020. გვ. 47, მითითებულია: „2020 წელს სამსახურმა შეისწავლა ვიდეოთვალთვალის სისტემების მეშვეობით პერსონალურ მონაცემთა დამუშავების 30 შემთხვევა (16 მოქალაქეთა განცხადების/შეტყობინების საფუძველზე, ხოლო 14 - სამსახურის ინიციატივით).“

მიის მიმდინარეობისას დამკვიდრდა ტერმინი კოვიდ ინფიცირებული პირი / პაციენტი.[136] განსაკუთრებით, საწყის ეტაპზე, როდესაც საქართველოში კოვიდ-19 ეპიდემია გავრცელდა - კოვიდ ინფიცირებული პირი ითვლებოდა ერთგვარ ნიშნულად იმ ადამიანისა, რომელიც უნდა შეზღუდულიყო კონსტიტუციური უფლების განხორციელების ჭრილში, გარკვეული დროითა და სივრცით.[137] ამ მიზნით ვიდეოთვალთვალის განხორციელებას კოვიდ ინფიცირებული პირის გარკვევის, მოძიებისა თუ გადაადგილების კონტროლის, კოვიდ კონტაქტების განსაზღვრის საკითხისთვის დამახასიათებელი მნიშვნელობა მაღალ საზოგადოებრივ ინტერესს დაუკავშირდა.

მნიშვნელოვანია შეფასდეს საკანონმდებლო რეალობა და არსებული გამოწვევები. კვლევის მიზანია ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვის კომპლექსური საკითხების განხილვა. კვლევის აქტუალურობას განაპირობებს საკითხი, თუ როგორ და როდის შეიძლება აღმოჩნდეს მოქალაქის კონსტიტუციური უფლების შეზღუდვა და ინტერესი პირის საუარესოდ. კვლევის მიზნების მისაღწევად გამოყენებულია ნორმატიული, დოგმატური, სინთეზისა და ანალიზის მეთოდები.

2. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმები ვიდეოთვალთვალის განხორციელების შესახებ

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ადგენს ვიდეოთვალთვალის განხორციელების სამ კანონისმიერ შემთხვევას:

- ქუჩაში და საზოგადოებრივ ტრანსპორტში ვიდეოთვალთვალის განხორციელება.[138]
- საჯარო და კერძო დაწესებულებათა შენობების ვიდეო თვალთვალი.[139]
- საცხოვრებელი შენობის ვიდეო თვალთვალი.[140]

ზემოთ ჩამოთვლილ სამ შემთხვევას კანონმდებელი მიზნისა და საკანონმდებლო რეგულირების სხვადასხვაობის გათვალისწინებით განსაზღვრავს. ამ კანონის მე-11 მუხლის თანახმად, ქუჩაში ვიდეოთვალთვალის განხორციელების საკითხისთვის ასევე იგულისხმება პარკში, სკვერში, სათამაშო მოედანთან, საზოგადოებრივი ტრანსპორტის გაჩერებასთან და სხვა თავშეყრის ადგილზე

[136] იხ. ვებგვერდი კორონავიურის საქართველოში გავრცელების პრევენცია, „ვინ ითვლება კოვიდინფიცირებულად?“, მითითებულია: „COVID19 ინფიცირებულად ითვლება ადამიანი, რომელსაც ინფექცია დაუდასტურდა ლაბორატორიაში ჩატარებული კვლევით (პჯრ ტესტი- PCR) ან სწრაფი ანტიგენ ტესტით.“. ვებგვერდი ხელმისაწვდომია აქ: https://stopcov.ge წვდომის თარიღი: 27.06.2021.

[137] დამატებით იხ. ავტორთა კოლექტივი, რედაქტორი ნ. ქურდოვანიძე, „COVID-19-ის გავლენა სამართლებრივ ურთიერთობებზე“, საქართველოს ახალგაზრდა იურისტთა ასოციაციის გამოცემა, 2020. გვ. 36, მითითებულია: „საზოგადოებრივი ჯანმრთელობის სამსახურს უფლება აქვს, ფიზიკურ პირს მოსთხოვოს სამედიცინო შემოწმების გავლა, თუ არსებობს საფუძვლიანი ეჭვი, რომ იგი გადამდები დაავადების მატარებელია და საფრთხეს უქმნის საზოგადოების ჯანმრთელობას“.

[138] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ, მუხლი 11.

[139] იქვე, მუხლი 12.

[140] იქვე, მუხლი 13.

ვიდეოთვალთვალის განხორციელების შესაძლებლობა, რაც საჯარო სივრცის ტერიტორიულ არეალს ფართო მასშტაბიან მნიშვნელობას ანიჭებს, შემდგომში სძენს წინასწარ განუსაზღვრელ, თუმცა განმარტების ფორმით დაკონკრეტებულ ხასიათს.

მე-12 მუხლის მიხედვით, „საჯარო და კერძო დაწესებულებებს შესაბამისი მონიტორინგის განხორციელების მიზნით შეუძლიათ განახორციელონ თავიანთი შენობების ვიდეოთვალთვალი“,[141] აღნიშნული დებულება კონკრეტდება შემდეგი დათქმით: „შესაძლებელია მხოლოდ შენობის გარე პერიმეტრისა და შესასვლელის მონიტორინგის განხორციელება“.[142] რაც შეეხება უშუალოდ შიდა სივრცეს, კანონმდებელი განმარტავს რომ სამუშაო ადგილზე ვიდეოთვალთვალის სისტემის დაყენება შეიძლება მხოლოდ გამონაკლის შემთხვევებში,[143] ხოლო „ვიდეოთვალთვალის განხორციელება დაუშვებელია გამოსაცვლელ ოთახებსა და ჰიგიენისათვის განკუთვნილ ადგილებში“.[144] ამიტომ, ნორმით ჩამოთვლილ სივრცით ტერიტორიულ არეალში ვიდეოთვალთვალის განხორციელების მიზანი, წესი და იქ მყოფ პირთა ინფორმირების სტანდარტი დამოკიდებულია შესაბამისი სივრცის ნებადართული კონტროლის განხორციელების წესსა და მოქმედი კანონმდებლობის სავალდებულო მოთხოვნებზე.

მე-13 მუხლის შესაბამისად, „საცხოვრებელ შენობაში ვიდეოთვალთვალის სისტემის დასაყენებლად აუცილებელია ამ შენობის მესაკუთრეთა ნახევარზე მეტის წერილობითი თანხმობა“.[145] სასურველია, სამართლის ნორმა და სიტყვათწყობა: საცხოვრებელი ბინა ტელეოლოგიური განმარტების მეთოდით განიმარტოს. ასევე, ამავე მუხლში განსაზღვრულია რომ „ვიდეოთვალთვალის სისტემის მეშვეობით ბინის შესასვლელის მონიტორინგის განხორციელება დასაშვებია მხოლოდ ამ ბინის მესაკუთრის გადაწყვეტილებით ან მისი წერილობითი თანხმობის საფუძველზე“.[146] საცხოვრებელი შენობისა და საცხოვრებელი ბინის ვიდეოთვალთვალის დაწესების შესაძლებლობას კანონმდებელი შესაბამისი წესით იქ მცხოვრები და მყოფი პირებისგან თანხმობის მოპოვებას უკავშირებს. ერთი მხრივ, ვიდეოთვალთვალის ინიციატორი მხარის მიერ და მეორე მხრივ, არაინიციატორი მხარეების უფლების დაცვის მიზნიდან გამომდინარე. საინტერესოა შემთხვევა, როდესაც საცხოვრებელი ბინა საცხოვრებელი შენობის ნაწილს წარმოადგენს,[147] მაგალითად, მრავალბინიანი კორპუსის ნებისმიერ სართულზე მცხოვრები პირის ინტერესი დაცულია ამ კანონის

[141] იქვე, მუხლი 12, პუნქტი პირველი.

[142] იქვე, პუნქტი 2.

[143] შენიშვნა: შესაბამისი მიზნის დასაბუთებით. „თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, საიდუმლო ინფორმაციის დაცვის და გამოცდის/ტესტირების მიზნებისათვის და თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია.“. თუ ამ ფორმით მოპოვებულ მონაცემს უფლებამოსილი ორგანო პირის დასაჯარიმებლად გამოიყენებს ეს იქნება კანონისმიერი მიზნის ინტერპრეტაციის პრობლემა და ასევე უფლებამოსილი ორგანოს თვითნებობის გამოვლინება, რომელიც ლეგიტიმური საჯარო მიზნით აღემატება ნორმის წესს.

[144] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ, მუხლი 12, პუნქტი 4.

[145] იქვე, მუხლი 13, პუნქტი პირველი.

[146] იქვე, პუნქტი 4.

[147] სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „სახელმწიფო ინსპექტორის სამსახურმა ვიდეოთვალთვალის წესების დარღვევისთვის ფიზიკურ პირს ადმინისტრაციული პასუხისმგებლობა დააკისრა“, მითითებულია: „დადგინდა, რომ ფიზიკური პირი სხვა პირთა საცხოვრებელი სახლების შესასვლელებისა და საერთო სარგებლობის შიდა ეზოს ვიდეომონიტორინგს მესაკუთრეთა წერილობითი თანხმობების გარეშე ახორციელებდა“. ვებგვერდი ხელმისაწვდომია: https://bit.ly/3BpLkjK წვდომის თარიღი: 27.06.2021.

მე-13 მუხლის მე-4 პუნქტით, თუმცა, დაცვის ღირსი ინტერესი შესაძლოა წინააღმდეგობაში აღმოჩნდეს მე-13 მუხლის მე-3 პუნქტის ფარგლებში მოქმედ დანაწესთან: საცხოვრებელი შენობის საერთო სივრცის მონიტორინგის დათქმით, საზიარო სივრცითი არეალის მონიტორინგის თვალსაზრისით. ამიტომ, ყოველ კონკრეტულ შემთხვევაში, საცხოვრებელ შენობაში ვიდეოთვალთვალის სისტემის დამონტაჟებისას გათვალისწინებული უნდა იყოს მე-13 მუხლის პირველი პუნქტის მოთხოვნა, რომელიც ფართოდ უნდა განიმარტოს ამავე მუხლის მე-3 და მე-4 პუნქტებთან მიმართებით.[148]

თითოეულ შემთხვევაში გარკვეული ტერიტორიული არეალი (ქუჩა, საზოგადოებრივი ტრანსპორტი, საჯარო დაწესებულება, კერძო დაწესებულება, საცხოვრებელი შენობა) ვიდეოთვალთვალის განხორციელების კანონისმიერი შესაძლებლობით განიხილება, როგორც სამართლის ნორმის მოქმედების კონკრეტული სივრცითი განზომილების მქონე ტერიტორიული სივრცე. შესაბამისად, ამ არეალის მიზნობრივი კონტროლი ვიდეოთვალთვალის წესების დაცვისა და დარღვევის შემთხვევაში დამრღვევის მიმართ შესაბამისი პასუხისმგებლობის დადგომის აუცილებლობას აყენებს დღის წესრიგში. განსაკუთრებით მაშინ, როდესაც კოვიდ-19 პანდემიით გამოწვეული ცალკეული შეზღუდვები, მათი მონიტორინგი და დამრღვევთა დაჯარიმების წესი თანაკვეთაშია ვიდეოთვალთვალის განხორციელების წესსა და ტერიტორიულ არეალთან. ამგვარად, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის სამართლის ნორმები ვიდეოთვალთვალის განხორციელების შესახებ შეესაბამება საქართველოს კონსტიტუციას.[149] შესაბამისობის თვალსაზრისით აღსანიშნავია კანონის მიზანი და ის მეთოდური საშუალებები, შემდგომში სტანდარტები, რომლებიც პერსონალური მონაცემების დაცვას უზრუნველყოფს. ასევე, „ამ კანონის მიზანია, პერსონალური მონაცემის დამუშავებისას უზრუნველყოს ადამიანის უფლებათა და თავისუფლებათა, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა“.[150]

3. სახელმწიფო ინსპექტორის სამსახურის ბოლო ორი წლის ანგარიშის მონაცემთა შედარება ვიდეოთვალთვალის სისტემის მეშვეობით პერსონალურ მონაცემთა დამუშავების საკითხისთვის

3.1. 2019 წლის ანგარიში ვიდეოთვალთვალის სისტემის შესახებ

2019 წელს სახელმწიფო ინსპექტორის სამსახურმა „შეისწავლა სახელმწიფო სტრუქტურებში, უნივერსიტეტებში, სავაჭრო ობიექტებში, სამედიცინო დაწესებულებებში, სპორტულგამაჯანსაღებელ კომპლექსებში, რესტორნებში, სასტუმროებსა და საცხოვრებელ შენობებში განთავსებული ვიდეოთვალთვალის სისტემებით პერსონალურ მონაცემთა დამუშავების 48 შემთხვევა: 9 - საჯარო სექტორში (აქედან, 4 - სამართალდამცავ ორგანოებში), ხოლო 39 - კერძო სექტორში“.[151]

---

[148] იქვე, „ამავდროულად, მას დაევალა ზემოაღნიშნული სივრცეების ვიდეოთვალთვალის შეწყვეტა ან ვიდეოთვალთვალის განსახორციელებლად სხვა მესაკუთრეთა წერილობითი თანხმობის მოპოვება“.

[149] საქართველოს კონსტიტუცია, მუხლი 15.

[150] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ, მუხლი პირველი.

[151] სახელმწიფო ინსპექტორის სამსახური, „სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, 2019. გვ. 50.

დებულებიდან გამომდინარე, შესაძლოა ერთმანეთს შევადაროთ სამიზნე ტერიტორიული არეალები და უფლებამოსილი ორგანოს საქმისწარმოების წესი. მაგალითად, ტერიტორიული არეალი (ქუჩა, საზოგადოებრივი ტრანსპორტი, საჯარო დაწესებულება, კერძო დაწესებულება, საცხოვრებელი შენობა), ანგარიშის საფუძველზე განიმარტა და დაკონკრეტდა, როგორც: სახელმწიფო სტრუქტურები, უნივერსიტეტები,[152] სავაჭრო ობიექტები, სამედიცინო დაწესებულებები, სპორტულგამაჯანსაღებელი კომპლექსები, რესტორნები, სასტუმროები და საცხოვრებელი შენობები. ჩამოთვლილ დაწესებულებათა მიმართ სახელმწიფო ინსპექტორის სამსახურის დაინტერესების კანონისმიერ საფუძვლებთან ერთად საგულისხმოა მოქალაქეთა გადაადგილების მაღალი მაჩვენებელი და გარკვეული რისკების არსებობის წინასწარგანწყობა. საკითხის შესწავლის შედეგად „გამოვლინდა ადმინისტრაციული სამართალდარღვევის 17 ფაქტი. ადმინისტრაციული პასუხისმგებლობა 12 შემთხვევაში დაეკისრა კერძო ორგანიზაციას, ხოლო 5 შემთხვევაში - საჯარო დაწესებულებას“.[153] ე. ი. უფლებამოსილი ორგანოს მიერ შესწავლილი 48 შემთხვევიდან რისკუნარიანობის მაჩვენებელი, შემდგომში ადმინისტრაციული სამართალდარღვევის ფაქტის საფუძველი შეადგენს 35%-ს. მათ შორის სამართალდამრღვევთა პროცენტული თანაფარდობა შეადგენს კერძო ორგანიზაციის 71%-ს, ხოლო საჯარო დაწესებულების 29%-ს.

ანგარიშის მიხედვით მთავარ გამოწვევას წარმოადგენს ფიზიკური პირების მიერ საცხოვრებელ შენობებში ვიდეოთვალთვალის სისტემის განხორციელების შედეგად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის სამართლის ნორმების / მოთხოვნების გაუთვალისწინებლობა. ასევე, სარეკომენდაციო თვალსაზრისით აღნიშნულია კერძო დაწესებულებებში დასაქმებულთა აუდიო-ვიდეო თვალთვალის ხარვეზების გამოსწორების აუცილებლობა და „სამართალდამცავი ორგანოების მიერ შესაბამისი ორგანიზაციული-ტექნიკური ზომების მიღება ვიდეოთვალთვალისას“.[154]

3.2. 2020 წლის ანგარიში ვიდეოთვალთვალის სისტემის შესახებ

2020 წელს სახელმწიფო ინსპექტორის სამსახურმა „შეისწავლა ვიდეოთვალთვალის სისტემების მეშვეობით პერსონალურ მონაცემთა დამუშავების 30 შემთხვევა (16 მოქალაქეთა განცხადების/შეტყობინების საფუძველზე, ხოლო 14 - სამსახურის ინიციატივით)“.[155] უფლებამოსილი ორგანოს მიერ შერჩეული 30 შემთხვევის განზოგადების მაგალითზე შესაძლოა ჩამოყალიბდეს ის კონკრეტული პრობლემები, რომლებიც სისტემურად დამახასიათებელია სხვადასხვა დაწესებულებისთვის.

---

[152] იხ. სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „პროფესორები VS მონტენეგრო-რა დაადგინა ევროსასამართლომ აუდიტორიებში ვიდეოთვალთვალის საქმეზე“, მითითებულია: „უნივერსიტეტის აუდიტორია პროფესორების სამუშაო სივრცეა. ეს ადგილია, სადაც ისინი არა მხოლოდ ასწავლიან სტუდენტებს, არამედ ურთიერთობა აქვთ მათთან, რითაც ავითარებენ ორმხრივ ურთიერთობებს და აყალიბებენ საკუთარ სოციალურ იდენტობას.“. ვებგვერდი ხელმისაწვდომია: https://bit.ly/3DudvQw წვდომის თარიღი: 27.06.2021. საკითხი განსაკუთრებულ აქტუალურობას იძენს ონლაინ სწავლების პერიოდში სალექციო მიმდინარეობის მონიტორინგისა და ჩაწერის შესაძლებლობის ნაწილში.

[153] სახელმწიფო ინსპექტორის სამსახური, „სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, 2019, გვ. 50.

[154] იქვე, გვ. 55.

[155] სახელმწიფო ინსპექტორის სამსახური, „სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, 2020, გვ. 47.

საკვლევი არეალი კონკრეტული მიზნით შეირჩა.[156] ესენია: სამართალდამცავი ორგანოები, ადგილობრივი თვითმმართველობის ორგანოები, სამედიცინო დაწესებულებები, საცხოვრებელი შენობები, კერძო ორგანიზაციები. „სამსახურის მიერ შესწავლილი საქმეების შედეგად, ადმინისტრაციული პასუხისმგებლობა დაეკისრა 12 პირს 19 სამართალდარღვევისთვის. სანქციის სახით 10 პირის მიმართ გამოყენებულია გაფრთხილება, ხოლო 2 პირის მიმართ - ჯარიმა. საჯარო და კერძო დაწესებულებებში მონაცემთა დამუშავების პროცესების „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონთან შესაბამისობისთვის, ადმინისტრაციული სახდელების პარალელურად, სამსახურმა გასცა შესასრულებლად სავალდებულო 65 დავალება და 12 რეკომენდაცია“.[157] შესწავლილი 30 შემთხვევიდან რისკუნარიანობა შეადგენს 40%-ს. წინა წლის ანგარიშთან შედარებით უფლებამოსილი ორგანოს მიერ შესწავლილი შემთხვევები შემცირებულია 37.5%-ით. ანგარიშში განიმარტა რომ ნებისმიერ დაწესებულებას შესაძლოა გააჩნდეს ვიდეოთვალთვალის განხორციელების ლეგიტიმური საჯარო მიზანი, თუმცა ის აუცილებლად უნდა შეესაბამებოდეს საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს. წინააღმდეგ შემთხვევაში განხორციელებული მოქმედებები გამოიწვევს დამრღვევი პირის ადმინისტრაციულ პასუხისმგებლობას/დაჯარიმებას. სახელმწიფო ინსპექტორის სამსახურის მიერ გაცემული რეკომენდაციები დაგვაფიქრებს რომ „ამ მიმართულებით კვლავ ბევრი გამოწვევაა“,[158] ხოლო მეორე მხრივ ვიდეოთვალთვალის განმახორციელებელი პირის თვითნებობა - განმარტოს სამართლის ნორმის მიზნები მხოლოდ ცალმხრივად ან არაჯეროვნად, განხორციელებული მოქმედების ფარულობა და „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნების აშკარა გაუთვალისწინებლობა შესაძლოა ლატენტური ხასიათის ადმინისტრაციულ სამართალდარღვევად ჩამოყალიბდეს. რაც კიდევ ერთხელ დაგვაფიქრებს ეფექტური კონტროლისა და ცნობიერების ამაღლების აუცილებლობებზე.[159]

4. პანდემიით გამოწვეული შეზღუდვები

4.1. პანდემიით გამოწვეული შეზღუდვების ისტორია

2021 წელს, საქართველოში პანდემიით გამოწვეულ შეზღუდვებს უკვე გარკვეული ისტორია გააჩნია. უპირველესად, მათი დაწესების დროებითი ხასიათიდან გამომდინარე,[160] ხოლო შემდგომში მათი გაუქმებისას შეზღუდვებით გამოწვეული უარყოფითი შედეგების დაძლევის თვალსაზრისით. მათ შორის ეპიდემიოლოგიური მდგომარეობის გართულების შედეგად ან პრევენციის მიზნით

[156] იქვე, გვ. 48, მითითებულია: „შესამოწმებელი დაწესებულებები შეირჩა ვიზიტორთა და დასაქმებულთა სიმრავლისა და ვიდეოთვალთვალის მიზნების მნიშვნელობის გათვალისწინებით“.

[157] იქვე.

[158] სახელმწიფო ინსპექტორის სამსახური, „სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში“, გვ. 56.

[159] ზოგადი ცნობიერების გაზრდის საკითხისთვის დამატებით იხ. სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „პერსონალური მონაცემების ვიდეოგზამკვლევი - ვიდეოთვალთვალი“. ვებგვერდი ხელმისაწვდომია: https://bit.ly/3BiHBo6 წვდომის თარიღი: 27.06.2021.

[160] შენიშვნა: 2020 წლის დასაწყისიდან დღემდე არაერთ ნაშრომში, კვლევასა და ანგარიშში შეფასდა ეპიდემიის შემდგომში პანდემიის მრავალფუნქციური მნიშვნელობები. ფაქტი, რომ პანდემია მრავალი კვლევის საგანია ეს დოქტრინაში ახალი მიმართულების აღმოჩენას მიანიშნებს.

წარმოშობილი მმართველობითი ღონისძიებების გათვალისწინებით. საინტერესოა, რომ ცალკე აღებული კონკრეტული შეზღუდვა, რომელსაც ახასიათებდა ოფიციალური დასაბუთება და შეზღუდვის მიზანი, შესაძლოა განსხვავებული ფორმით განმარტებულიყო არსებული მდგომარეობის რადიკალური ცვლილების - ეპიდემიის გავრცელების კრიტიკული საწყისების გაძლიერების ან შემსუბუქების შემთხვევაში.[161] საკითხავია, თუ რამდენად მეთოდური და კონსტიტუციასთან შესაბამისი იყო ცალკეული შეზღუდვის დადგენა,[162] მოქმედება და მის საფუძველზე მოქალაქეთა დაჯარიმება ან, თუნდაც იყო თუ არა მზად საზოგადოება (წინასწარი, დროული და ეფექტური ინფორმირების თვალსაზრისით) მსგავსი შეზღუდვების მისაღებად, თუმცა დანამდვილებით შეიძლება გამოითქვას მოსაზრებები იმ ხარვეზების შესახებ, რომელიც კოვიდ-19 პანდემიის მიმდინარეობის პერიოდში პერსონალური მონაცემების დაცვის საკითხს უკავშირდება, და არა მხოლოდ სამედიცინო დახმარების გაწევის კუთხით. პერსონალური მონაცემების დარღვევის მრავალ პრობლემას შორის ერთ-ერთია ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვის განუხორციელებლობა ან ამ უკანასკნელის შეუძლებლობა პანდემიის პერიოდში დაწესებული ცალკეული შეზღუდვის მოქმედების პირობებში. ეს შემთხვევა მეტადრე თავისებური ხასიათით ვლინდება, რადგან შესაძლოა მისი ლატენტური ბუნებიდან გამომდინარე არ კვალიფიცირდეს ვიდეოთვალთვალის განხორციელების წესის დარღვევის კონკრეტულ სამართალდარღვევად და სხვა ქმედების / კონსტიტუციური უფლების დროებითი შეზღუდვის მიზნის შემადგენელ ნაწილად ჩამოყალიბდეს. ერთი მხრივ, იმიტომ რომ მაღალი საზოგადოებრივი ინტერესი განაპირობებდა ვირუსის გავრცელების კონტროლის აუცილებლობას, ხოლო მეორე მხრივ, საზოგადოებრივი ინტერესი ცნობიერების დონეზე არ მოიცავდა ინფორმაციას ვირუსის გავრცელების კონტროლის მეთოდური საშუალებების ეტაპობრივი ცვლილების შესახებ, განსაკუთრებით ვირუსის გავრცელების საწყის ეტაპზე უფლებათა შეზღუდვის სიმწვავის გათვალისწინებით.

საკითხის გაშუქების მედია სტანდარტი ამ შემთხვევაში წარმოადგენს განსხვავებულ მიმართულებას, რომელიც შესაბამისი სამართლებრივი აქტებითა და ეთიკის კოდექსის საფუძველზე უნდა დარეგულირდეს.[163] მედია საშუალების მიერ პერსონალური მონაცემების შესაძლო დარღვევის ფაქტის გაშუქება არ უნდა არღვევდეს ადამიანის უფლებებს. ასევე, მედია საშუალების მიერ მიწოდებული ინფორმაცია უნდა იყოს გადამოწმებადი. როგორც ერთ-ერთ სამეცნიერო ესეშია აღნიშნული: „კარგმა გაშუქებამ და მეცნიერებამ უნდა განასხვავოს ინფორმაციის ლეგიტიმური

[161] შეად. ვ. ფაცაცია, „პანდემია, თავისუფლება და კანონი“, თავისუფალი უნივერსიტეტის სტუდენტური ბლოგი, 2021 წლის 17 აპრილი, ხელმისაწვდომია: https://bit.ly/3ysO3ac წვდომის თარიღი: 27.06.2021, მითითებულია: „ზოგადად კი შეილება ითქვას, რომ თავისუფლებისა და კანონის ურთიერთ კავშირი შეიძლება იყოს, როგორც დადებითი ასევე უარყოფითი შედეგის გამომწვევი“.

[162] შეად. კ. კორკელია, „ადამიანის უფლებათა შეზღუდვები საქართველოში პანდემიის დროს“ წიგნში: სტატიათა კრებული - „ადამიანის უფლებათა დაცვა და კოვიდ-19-ის პანდემია“, 2021, გვ. 37.

[163] იხ. ქ. სართანია, „COVID-19-ის გავრცელების ფონზე საქართველოში საინფორმაციო და ონლაინ სივრცეში სიძულვილის ენის, ქსენოფობიის, რასიზმის, ძალადობრივი და რადიკალური მოწოდების შემცველი ნარატივების ტენდენციების მონიტორინგი“, საქართველოს სტრატეგიის და განვითარების ცენტრის პროექტის გამოცემა, 2020. გვ. 7, მითითებულია: „ქართულ ინტერნეტ სივრცეში გავრცელდა ქსენოფობიური შინაარსის შემცველი მასალები ონლაინ საინფორმაციო სააგენტოების ხელშეწყობით თუ ცალკეული მომხმარებლების მხრიდან. ვირუსის შესახებ ინფორმაციის გავრცელება გასცდა სამედიცინო თუ პოლიტიკურ სფეროს.“.

წყაროები ჭორების, ნახევრად სიმართლეების, „გველის სამკურნალო ზეთის“, ფინანსურად მოტივირებული რეკლამებისა და პოლიტიკურად მოტივირებული პროპაგანდისგან“.[164] დღესდღეობით, არასწორი ტერმინების გამოყენება კვლავ გამოწვევაა.[165] კვლევის მიზნებიდან გამომდინარე ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა შესაძლოა გულისხმობდეს ცალკეული შეზღუდვის მოქმედების დროით პერიოდში „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11, მე-12 და მე-13 მუხლებით დადგენილი უფლებამოსილების სხვა მიზნით გამოყენებას. რა დროსაც სხვა მიზნის გავრცელება ასევე კანონიდან უნდა გამომდინარეობდეს და უნდა იყოს ნორმატიული თვალსაზრისით დასაბუთებული.

განვიხილოთ ის კანონისმიერი მიზნები, რაც ახასიათებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის დასახელებულ ნორმებს:

- მე-11 მუხლის პირველი პუნქტის თანახმად, „ვიდეოთვალთვალის განხორციელება დასაშვებია მხოლოდ დანაშაულის თავიდან აცილების, აგრეთვე პირის უსაფრთხოებისა და საკუთრების, საზოგადოებრივი წესრიგისა და არასრულწლოვნის მავნე ზეგავლენისაგან დაცვის მიზნებისათვის“.
- მე-12 მუხლის პირველი პუნქტის თანახმად, მონიტორინგის განხორციელების მიზანი დასაბუთებულია „თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, არასრულწლოვნის მავნე ზეგავლენისგან დაცვის, საიდუმლო ინფორმაციის დაცვის და გამოცდის/ტესტირების მიზნებისათვის“.[166]
- მე-12 მუხლის მე-3 პუნქტის თანახმად, სამუშაო ადგილზე ვიდეოთვალთვალის განხორციელება დასაშვებია „თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების დაცვის, საიდუმლო ინფორმაციის დაცვის და გამოცდის/ტესტირების მიზნებისათვის და თუ ამ მიზნების სხვა საშუალებით მიღწევა შეუძლებელია“.[167]
- მე-13 მუხლის მე-2 პუნქტის თანახმად, „საცხოვრებელ შენობაში ვიდეოთვალთვალის სისტემის დაყენება დასაშვებია მხოლოდ პირისა და ქონების უსაფრთხოების მიზნებისათვის“.[168]

ზემოთ ჩამოთვლილი მიზნები შევადაროთ კოვიდ-19 პანდემიასთან ბრძოლის სტრატეგიულ მიზნებს.[169] საქართველოს მთავრობის მიერ გატარებული ღონისძიებების ანგარიშში ვკითხულობთ:

[164] ბ. ჰენჯი, მ. ლიპსიჩი, „როგორ გავაშუქოთ Covid-19-ის გავრცელება პასუხისმგებლობით“, მითითებულია წიგნში: „ეთიკა, უსაფრთხოება და ფსიქიკური ჯანმრთელობა კორონავირუსული პანდემიის (COVID-19) გაშუქებისას - სახელმძღვანელო წესები მედიისათვის“, საქართველოს ჟურნალისტური ეთიკის ქარტია, 2020 წლის 19 აპრილი, ხელმისაწვდომია: https://www.qartia.ge/ka/covid/ წვდომის თარიღი: 27.06.2021.

[165] იქვე, გვ. 7. ასევე, მედია სტანდარტების გავლენა ორმაგ ეფექტს ახდენს საკითხის რეგულირებაზე, როდესაც ხდება მსგავსი ფაქტის ან ინფორმაციის გაშუქება. 34 პირველი, მუხლი 11, პუნქტი პირველი.

[166] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ, მუხლი 12, პუნქტი პირველი.

[167] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ, მუხლი 12, პუნქტი 3.

[168] იქვე, მუხლი 13, პუნქტი 2.

[169] შენიშვნა: დროებითი ხასიათის მიუხედავად, შეზღუდვის ხასიათი გაუტოლდა სამართლის ნორმის მოქმედების ნორმატიულ ბუნებას, რამაც წარმოშვა კითხვები მათი თანაბრობის შესახებ.

„საქართველოს პრეზიდენტის მიერ 2020 წლის 21 მარტს გამოცემული დეკრეტის საფუძველზე გამოცხადდა საგანგებო მდგომარეობა და შეიზღუდა საქართველოს კონსტიტუციის მე-2 თავით („ადამიანის ძირითადი უფლებები“) გათვალისწინებული გარკვეული უფლებები და თავისუფლებები. ამასთან, დეკრეტმა მოიცვა მხოლოდ ის უფლებები და თავისუფლებები, რომელთა შეზღუდვა კრიტიკულად მნიშვნელოვანი იყო ეპიდემიოლოგიური მდგომარეობის მართვისთვის“.[170] საქართველოს პრეზიდენტის დეკრეტით საქართველოს მთელს ტერიტორიაზე საგანგებო მდგომარეობის მოქმედების ვადით შეიზღუდა საქართველოს კონსტიტუციით განსაზღვრული შემდეგი კონსტიტუციური უფლებები:

- ადამიანის თავისუფლება;[171]
- მიმოსვლის თავისუფლება;[172]
- პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებები;[173]
- სამართლიანი ადმინისტრაციული წარმოების, საჯარო ინფორმაციის ხელმისაწვდომობის, ინფორმაციული თვითგამორკვევისა და საჯარო ხელისუფლების მიერ მიყენებული ზიანის ანაზღაურების უფლებები.[174]
- საკუთრების უფლება;[175]
- შეკრების თავისუფლება;[176]
- შრომის თავისუფლება, პროფესიული კავშირების თავისუფლება, გაფიცვის უფლება და მეწარმეობის თავისუფლება.[177]

უფლების შეზღუდვის ნაწილში განსხვავდებოდა შეზღუდვის ფორმა და ხასიათი. კონკრეტულად, დასაბუთდა იმ უფლებების შეზღუდვა, „რომელთა შეზღუდვა პირდაპირ კორელაციაში იყო ეპიდემიოლოგიური მდგომარეობის მართვასთან“.[178] აღნიშნული უკვე წარმოადგენს აქტისმიერ მიზანს, რომელიც შემდგომში განიმარტება კონსტიტუციური მსაზღვრელით, მაგალითად პროპორციულობის პრინციპით.

[170] საქართველოს მთავრობის მიერ გატარებული ღონისძიებების ანგარიში, „ადამიანის უფლებების დაცვა COVID-19-ით გამოწვეული კრიზისისას, 2020, გვ. 14.

[171] საქართველოს კონსტიტუცია, მუხლი 13.

[172] იქვე, მუხლი 14.

[173] იქვე, მუხლი 15.

[174] იქვე, მუხლი 18.

[175] იქვე, მუხლი 19.

[176] იქვე, მუხლი 21.

[177] იქვე, მუხლი 26.

[178] საქართველოს მთავრობის მიერ გატარებული ღონისძიებების ანგარიში, „ადამიანის უფლებების დაცვა COVID-19-ით გამოწვეული კრიზისისას, 2020, გვ. 16.

ადამიანის თავისუფლების, მიმოსვლის თავისუფლებისა და შეკრების თავისუფლების შეზღუდვის ნაწილში განსაკუთრებით საინტერესო ხასიათი შეიძინა შეზღუდვის საყოველთაო გავრცელებისა და ასახვის ფუნქციამ მოქალაქეთა და დაწესებულებათა საქმიანობის მიმართ. ამ შემთხვევაში, ვიდეოთვალთვალის შედეგად მოპოვებული ნებისმიერი ინფორმაცია, მოპოვების მიზნის არაჯეროვანი განმარტების პირობებში შესაძლოა ამ სამი კონსტიტუციური უფლების დამატებითი შეზღუდვის ფორმად ჩამოყალიბებულიყო. მაგალითად, ადამიანის თავისუფლების უფლების შეზღუდვის შედეგად „შესაბამის ორგანოებს მიეცათ უფლება, მთავრობის მიერ დადგენილი იზოლაციის ან კარანტინის წესების დარღვევისათვის პირი იძულებით გადაეყვანათ შესაბამის დაწესებულებაში“.[179] არსებობდა რისკი რომ დადგენილი უფლებამოსილება გადაფარავდა კანონისმიერ მოთხოვნებს და დროებითი ხასიათის რეგულირება შთანთქავდა სამართლის ნორმის მოქმედების ინსტიტუციურ ფარგლებს. მიმოსვლის თავისუფლების შეზღუდვის შედეგად „მთავრობას მიეცა უფლება, დაედგინა იზოლაციისა და კარანტინის წესები; შეჩერდა საერთაშორისო სამგზავრო საჰაერო, სახმელეთო და საზღვაო მიმოსვლა, გარდა მთავრობის დადგენილებით გათვალისწინებული გამონაკლისი შემთხვევებისა; მთავრობას მიეცა უფლება, მოქმედი კანონმდებლობისაგან განსხვავებული წესით, დაერეგულირებინა საქართველოს ტერიტორიაზე მგზავრთა გადაყვანა და ტვირთის გადაზიდვა“.[180] შეკრების თავისუფლების შეზღუდვის შედეგად „შეიზღუდა ნებისმიერი სახის შეკრება, მანიფესტაცია და ადამიანების თავშეყრა, გარდა მთავრობის დადგენილებით განსაზღვრული გამონაკლისი შემთხვევებისა“.[181] ვიდეოთვალთვალი პერსონალურ მონაცემთა დამუშავების მეტად გავრცელებული და ნებადართული საშუალებაა. მიუხედავად, მისი გამოყენების დასაშვებობისა ვიდეოთვალთვალის განხორციელებისას აუცილებლად უნდა იქნეს გათვალისწინებული საქართველოს კანონმდებლობით დადგენილი რეგულაცია და სტანდარტები. ასევე, ვიდეოთვალთვალის განმახორციელებელი პირი ან ორგანიზაცია უნდა აცნობიერებდეს ამ უფლებამოსილების მიმართ მომეტებულ პასუხისმგებლობას, რომ ლეგიტიმური საჯარო მიზნის არსებობის მიუხედავად, არ უგულებელყოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მიზნები და მოთხოვნები.

4.2. შეზღუდვით გამოწვეული უარყოფითი შედეგების შეფასება

შეზღუდვით გამოწვეული უარყოფითი შედეგების შეფასება მრავალ საკითხს უკავშირდება, რომელთა შორის აღსანიშნავია ის კვლევები და ანგარიშები, რომლებიც უშუალოდ მიეძღვნა კონსტიტუციური უფლებების შეზღუდვის შედეგად დამდგარ უარყოფით შედეგებს. მათ შორის აღსანიშნავია: შრომითი ხელშეკრულებით დასაქმებულ პირთა და მომხმარებლის უფლებების დაცვა, სასესხო ვალდებულებების გადავადების შეთავაზება და საპროცენტო განაკვეთის ცვლილება, ჯარიმის გასაჩივრებისა და ადმინისტრაციული წესით დაჯარიმებულ პირთა უფლებების დაცვა.[182] საინტერესოა, რამდენად მოიცავს უარყოფითი შედეგების კვლევა ისეთ სპეციფიკურ

[179] იქვე, გვ. 14.

[180] იქვე.

[181] იქვე, გვ. 15.

[182] საგულისხმოა ინიციატივა, რომელიც 245 000 მოქალაქეს და 344 იურიდიულ პირს ეხება და ის ათავისუფლებს ადმინისტრაციული, ასევე სისხლის სამართლებრივი პასუხისმგებლობისგან.

საკითხებს, რომელიც ვიდეოთვალთვალის განხორციელების წესსა და რეგულაციას უკავშირდება. მედია სტანდარტის თვალსაზრისით ყალბი ინფორმაციის ამოცნობა, შეფასება და შესაბამისი ეთიკური საფუძვლით უკუგება ვერ აღმოფხვრის სპეციფიკურ პრობლემას, რადგან ამ პრობლემის ბუნება სხვა ქმედების მოაზრებასა და ფარულობაში მდგომარეობს. მაგალითად, ვიდეოთვალთვალის განმახორციელებელი პირი შესაძლოა მოქმედებდეს მხოლოდ კერძო ინტერესის გათვალისწინებით და ეფექტური კონტროლის არ არსებობის პირობებში ის აგრძელებდეს ამ ქმედებას წლების განმავლობაში. შესაბამისად, კონსტიტუციური უფლებების შეზღუდვებმა, მიუხედავად მათი კონსტიტუციურობის დასაბუთებისა მაინც გამოიწვია ცალკეული უარყოფითი შედეგები,[183] მოსაზრებები და დამოკიდებულებები.

ვიდეოთვალთვალის განხორციელების შემთხვევაში კონსტიტუციური უფლებების შეზღუდვით გამოწვეული უარყოფითი შედეგები აისახება კანონისმიერი მიზნების არაჯეროვანი განმარტებისა და პროცესის განხორციელების შედეგად მოპოვებული პერსონალური მონაცემების დამუშავების საკითხზე. კაცობრიობისთვის პანდემია საყოველთაო გამოწვევაა, თუმცა სხვადასხვა სახელმწიფოს საკანონმდებლო რეალობა რადიკალურად განსხვავებულია იმ ნაწილში, თუ როგორ უნდა შეფასდეს ერთი მხრივ, კონსტიტუციური უფლებების შეზღუდვის წესის დარღვევა ხოლო მეორე მხრივ, ვიდეოთვალთვალის შედეგად აღბეჭდილი ფაქტის - შეზღუდვის მოქმედების წესის დარღვევის შეფასება. მაგალითად, სამუშაო ადგილას სოციალური დისტანციის დაცვის წესის დარღვევის გამო დიდი ბრიტანეთის გაერთიანებული სამეფოს ჯანდაცვის მინისტრს თანამდებობის დატოვება მოუწია.[184] საკონსტიტუციო სასამართლოს სამართალწარმოებისას „ევროპის ქვეყნებში პანდემიის პირობებში დადგენილი შეზღუდვები ადამიანის უფლებათა ძალიან ფართო სპექტრს შეეხო, წარმოშვა განსხვავებული მიდგომები და ბევრგან დავის საგანიც გახდა“.[185]

4.3. მოქმედი შეზღუდვები

2021 წლის 28 ივნისის მდგომარეობით მოქმედებს შემდეგი სახის შეზღუდვები:

- „უწყებათაშორისი საბჭოს გადაწყვეტილებით, 1-ლი ივნისიდან, სახმელეთო საზღვრები გაიხსნება. სახმელეთო საზღვრის კვეთა შესაძლებელი იქნება სრული ვაქცინაციის დამადასტურებელი დოკუმენტით და PCR-ტესტის უარყოფითი პასუხით, ან მხოლოდ ბოლო

[183] იხ. მ. ნაკაშიძე, „ადამიანის თავისუფლების შეზღუდვა კოვიდ-19-ის პანდემიის პირობებში: ევროპული სტანდარტები და საქართველოს კანონმდებლობა“, წიგნში: სტატიათა კრებული - „ადამიანის უფლებათა დაცვა და კოვიდ-19-ის პანდემია“, 2021, გვ. 182, მითითებულია: „ბევრ ქვეყანაში პანდემიის გამო დადგენილმა წესებმა სხვადასხვა ხარისხით შეზღუდა ადამიანთა პირადი ცხოვრების უფლება, სინდისის თავისუფლება, გამოხატვის თავისუფლება, გაერთიანების თავისუფლება, ინფორმაციის თავისუფლება, მედიის თავისუფლება, ოფიციალური ინფორმაციის ხელმისაწვდომობა და საფრთხე შეუქმნა პერსონალური მონაცემების დაცვას. ვირუსის გავრცელებასთან ბრძოლის მიზნით გატარებულმა ღონისძიებებმა ბევრი ადამიანი დისკრიმინაციის საფრთხის წინაშე დააყენა, ხოლო საკარანტინე, იზოლაციის ნორმებმა და გადაადგილების შეზღუდვამ ოჯახში ძალადობის შემთხვევები გაზარდა.“.

[184] ვებგვერდი ხელმისაწვდომია: https://bbc.in/38oh7Fp წვდომის თარიღი: 27.06.2021.

[185] იხ. მ. ნაკაშიძე, „ადამიანის თავისუფლების შეზღუდვა კოვიდ-19-ის პანდემიის პირობებში: ევროპული სტანდარტები და საქართველოს კანონმდებლობა“, წიგნში: სტატიათა კრებული - „ადამიანის უფლებათა დაცვა და კოვიდ-19-ის პანდემია“, 2021, გვ. 186.

72 საათში ჩატარებული PCR-ტესტის უარყოფითი პასუხით და ამ შემთხვევაში, ისინი ვალდებული იქნებიან, მესამე დღეს განმეორებით ჩაიტარონ PCR-ტესტირება“.[186]

- „PCR რეჟიმით შემოსვლის შემთხვევაში სავალდებულოა ელექტრონული აპლიკაციის შევსება, რომელიც განთავსებულია stopcov.ge-ზე https://registration.gov.ge/pub/form/8_protocol_for_arrivals_in_georgia/tk6157/ “.[187]
- „იმ ქვეყნების ჩამონათვალს, რომელთა მოქალაქეებს და რეზიდენტებს საქართველოს საზღვრის კვეთა ბოლო 72 საათში ჩატარებული PCR-ტესტის უარყოფითი პასუხით შეუძლიათ, ემატება კანადა, იაპონია, ქუვეითი, ჩინეთი, სამხრეთ კორეა, მოლდოვა, ომანი“.[188]
- „იმ შემთხვევაში, თუ ეპიდემიოლოგიური ვითარების სტაბილიზაციის ტენდენცია შენარჩუნდება, 1-ლი ივნისიდან, კვების ობიექტებისთვის შაბათ-კვირას მოქმედი შეზღუდვა სრულად მოიხსნება, რაც ნიშნავს იმას, რომ მათ საშუალება ექნებათ, სტუმრები შაბათ-კვირას დახურულ სივრცეშიც მიიღონ“.[189]
- „კვლავ ძალაშია შეზღუდვა ისეთი სოციალური ღონისძიებების გამართვასთან დაკავშირებით, როგორიცაა, ქორწილი, ქელეხი, ბანკეტი და სხვადასხვა სახის იუბილე“. [190]
- „კვლავ ძალაში რჩება გადაადგილებაზე შეზღუდვა 23:00-დან 04:00 საათამდე პერიოდში“.[191]
- „სავალდებულო რეგულარული ტესტირება დადგენილებით განსაზღვრულ ჯგუფებზე ივნისის განმავლობაშიც სახელმწიფო დაფინანსებით გაგრძელდება“.[192]
- „უწყებათაშორისი საკოორდინაციო საბჭო კიდევ ერთხელ მიმართავს მოქალაქეებს, დაიცვან მოქმედი რეგულაციები, ატარონ პირბადე და დაიცვან სოციალური დისტანცია, რაც, ვაქცინაციასთან ერთად, ვირუსის გავრცელების პრევენციისთვის კვლავ უმნიშვნელოვანეს ღონისძიებებად რჩება“.[193]

საუკუნის წინ საქართველოს დემოკრატიული რესპუბლიკის მთავრობა ცდილობდა სახელმწიფოებრივი დამოუკიდებლობის შენარჩუნებას, ადამიანის უფლებების დაცვასა და ისეთი სოციალური პროექტების განხორციელებას, რომელთა შორის დიდ ეპიდემიებთან: ქოლერასთან, ტიფთან და მალარიასთან ბრძოლა, ასევე შიმშილისა და შიმშილით გამოწვეული დაავადებების აღმოფხვრა იყო.[194] რესპუბლიკის მთავრობის ამოცანას კონსტიტუციური მექანიზმების შემუშავება წარმოადგენდა, შემდგომში დიდ ეპიდემიასთან ბრძოლის ეფექტური სტრატეგიის დასაგეგმად

[186] ვებგვერდი კორონავირუსის საქართველოში გავრცელების პრევენცია, „მოქმედი შეზღუდვები“, ვებგვერდი ხელმისაწვდომია აქ: https://stopcov.ge/ka/shezgudvebi წვდომის თარიღი: 27.06.2021.

[187] იქვე.

[188] იქვე.

[189] იქვე.

[190] იქვე.

[191] იქვე.

[192] იქვე.

[193] იქვე.

[194] ხ. ქართველიშვილი, ს. გელაძე (მთარგმნელები), „საქართველოს რესპუბლიკის დამფუძნებელი კრების 1921 წლის გამოცემა, საქართველო ბოლშევიკური არმიის ბატონობის ქვეშ“, ნოე ჟორდანიას ინსტიტუტის გამოცემა, პარიზი-თბილისი, 2018, გვ.3.

და სოციალური ღონისძიებების განსახორციელებლად. მართალია, იმ დროისთვის, ვიდეოთვალთვალის განხორციელების წესი განხილვის საგანს არ წარმოადგენდა, თუმცა დღეს როცა ეს საკითხი რეალური, აქტუალური და პრობლემურია მისი გადაფარვა ისევ და ისევ კონსტიტუციური უფლებების შეზღუდვის დღის წესრიგით დაუშვებელია. სამართლებრივი ინსტიტუტებისა და მექანიზმების მიმართ დროებითი შეზღუდვის წესით სრულებით ახალი დღის წესრიგის დავალდებულება ან მსგავსი საფრთხეების არსებობა, ერთ-ერთ რთულ პრობლემას წარმოაჩენს, რასაც შემდგომში ვიდეოთვალთვალის განხორციელების ანომია[195] შეიძლება ეწოდოს.[196]

5. საფრთხეებისა და რისკების ანალიზი ცალკეულ შემთხვევათა განხილვის მაგალითზე

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვის საფრთხეები და რისკები პანდემიის წინარე პრობლემების გარკვევით უნდა დავახასიათოთ, რადგან პანდემიის მოქმედებით ეს პრობლემები არ აღმოფხვრილა. ცალკეულ შემთხვევათა შესაფასებლად გავეცანი სახელმწიფო ინსპექტორის სამსახურის ვებგვერდზე გამოქვეყნებულ ოფიციალურ ინფორმაციას. ერთ-ერთ საქმესთან დაკავშირებით აღნიშნულია, რომ ვიდეოთვალთვალის განხორციელების „შესახებ ინფორმაციას ფლობდნენ დასაქმებული პირები, თუმცა აუდიომონიტორინგის თაობაზე გამაფრთხილებელი ნიშნების არარსებობის გამო, კლინიკის ვიზიტორები არ იყვნენ ინფორმირებულნი“.[197] ამ საკითხთან დაკავშირებით სტომატოლოგიური კლინიკის განმარტება სახელმწიფო ინსპექტორის სამსახურმა არ გაიზიარა.

კიდევ ერთ საქმესთან დაკავშირებით აღინიშნა, რომ „პირის უფლება, გარეშე პირთა დაკვირვების გარეშე, ისარგებლოს საკუთარი საცხოვრებელი სივრცით ისე, რომ არ მოხდეს საკუთარ საცხოვრებელ შენობაში ან/და ეზოში მისი გადაადგილების/ქცევის მონიტორინგი, პირადი ცხოვრების ხელშეუხებლობის ერთ-ერთი მნიშვნელოვანი გარანტია“.[198] ორივე შემთხვევაში ვიდეოთვალთვალის განმახორციელებელ პირს ჩამოყალიბებული ჰქონდა კონკრეტული პოზიცია, რომლის არგუმენტაცია არ შეესაბამებოდა სამართლის ნორმის მოთხოვნებს. ე. ი. საფრთხეს წარმოადგენს სამართლის ნორმის გაუთვალისწინებლობა ან არამიზნობრივი ინტერპრეტაცია.[199]

[195] ანომიის განმარტებასთან დაკავშირებით იხ. სოციალურ მეცნიერებათა ცენტრის ვებგვერდი, ლექსიკონი-ცნობარი სოციალურ მეცნიერებებში, „ანომია“, ვებგვერდი ხელმისაწვდომია: https://bit.ly/3DxeLCg წვდომის თარიღი: 27.06.2021.

[196] იხ. სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ“. ვებგვერდი ხელმისაწვდომია: https://personaldata.ge/ka წვდომის თარიღი: 27.06.2021.

[197] იხ. სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „სახელმწიფო ინსპექტორის სამსახურმა სტომატოლოგიურ კლინიკას ადმინისტრაციული პასუხისმგებლობა დააკისრა“, ვებგვერდი ხელმისაწვდომია: https://bit.ly/3jtgyQW წვდომის თარიღი: 27.06.2021.

[198] იხ. სახელმწიფო ინსპექტორის სამსახურის ვებგვერდი, „სახელმწიფო ინსპექტორის სამსახურმა ვიდეოთვალთვალის წესების დარღვევისთვის ფიზიკურ პირს ადმინისტრაციული პასუხისმგებლობა დააკისრა“, ვებგვერდი ხელმისაწვდომია აქ: https://bit.ly/3zsUXOh წვდომის თარიღი: 27.06.2021.

[199] იხ. ე. შერმადინი, „პერსონალურ მონაცემთა დამუშავების პრინციპების რეალიზება მიმდინარე შრომით ურთიერთობებში“, სამაგისტრო ნაშრომი, სულხან-საბა ორბელიანის სასწავლო უნივერსიტეტი, 2020, გვ. 32, მითითებულია: „გაუმჯობესების მიზანი არ შეიძლება იყოს გასახდელი და ჰიგიენისთვის განკუთვნილი ოთახების ვიდეოკონტროლი. უსაფრთხოების და საკუთრების დაცვის მიზნით დაუშვებელია საპირფარეშოების და თანამშრომელთა გამოსაცვლელი ოთახების ვიდეოკონტროლი“.

მეორე მხრივ, რისკები, შესაძლოა იქამდე შენარჩუნდეს, სანამ უფლებამოსილი ორგანო არ განახორციელებს შესაბამის კონტროლს. კონტროლის მნიშვნელობა განსაკუთრებულ ხასიათს სწორედ ცნობიერების შესწავლის პროცესში იძენს. ასევე, სახელმწიფო ინსპექტორის სამსახურის მიერ გაცემული რეკომენდაციები საინტერესოა მათი შესრულების შესაძლებლობისა და რისკების პრევენციის თვალსაზრისით.[200] შემთხვევათა ანალიზი მიგვანიშნებს, რომ ეფექტური კონტროლის მექანიზმი აუცილებელია. ვიდეოთვალთვალის განხორციელების წესთან ერთად საგულისხმოა ვიზუალური ჩანაწერის აღბეჭდვის სხვა შესაძლებლობების შედარება. ერთ-ერთ საქმეში კომპანიის „Facebook“ გვერდზე ვიდეოჩანაწერი ყველასთვის ხელმისაწვდომი იყო გარკვეული დროის განმავლობაში. კომპანიის მტკიცებით, „ზოგადად მისი მომხმარებლების, მათ შორის განმცხადებლის მონაცემების კომპანიის „Facebook“-ის გვერდზე ყველასათვის ხელმისაწვდომი ფორმით გასაჯაროების საფუძველია მხოლოდ მომხმარებლების თანხმობა და მონაცემთა დამუშავების სხვა სამართლებრივი საფუძველი კომპანიას არ აქვს“.[201] მტკიცება ნაწილობრივ გაიზიარა საქმის განმხილველმა ორგანომ.

6. დასკვნა

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა ერთ-ერთი მნიშვნელოვანი საკითხია, რომლის მიმართ სახელმწიფოს მიერ საკანონმდებლო რეგულირებისა და ეფექტური კონტროლის მექანიზმის შემუშავება ინსტიტუციებისა და მოქალაქეთა საქმიანობის ჰარმონიზაციის, მათ შორის სამართალგანვითარების საკითხისთვის გადადგმული სასიკეთო ნაბიჯია.

კვლევის პროცესში, პანდემიის პერიოდში დაწესებული ცალკეული შეზღუდვის განხილვის მაგალითზე შეფასდა ვიდეოთვალთვალის განხორციელებისას გამოვლენილი სხვადასხვა ხარვეზი. ერთი მხრივ, ხარვეზი, რომელსაც პანდემიამდელი/წინარე ისტორია გააჩნია, ხოლო მეორე მხრივ, დარღვევა, რომელიც პანდემიის მიმდინარეობისას შეზღუდვებისა და სწრაფი რეაგირების მაგალითზე ჩამოყალიბდა. პანდემიის რამდენიმე „ტალღის“ შემდეგ, როდესაც საზოგადოებრივ ცხოვრებასა და რეალობაში კონკრეტულმა შეზღუდვებმა ქცევის ზოგადი წესის სახე შეიძინა, შეიქმნა განწყობა/რისკები იმის შესახებ რომ ვიდეოთვალთვალის ფუნქცია უნდა გამოყენებულიყო არა მხოლოდ კონტროლის, არამედ „დამრღვევთა“ დაჯარიმების შესაძლებლობის კუთხითაც.

საკითხის კვლევის პრეისტორია და ახლად გამოვლენილი ხარვეზები უფლებამოსილი ორგანოს რეაგირების მიუხედავად, საჭიროებს დამატებით კვლევას გამოწვევის საწყისის გამოსავლენად,

[200] შეად. კ. ჯიაკუმოპულოს, ჯ. ბუტარელი, მ. ო'ფლერთი, „მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018 წლის გამოცემა“, ლუქსემბურგი: ევროკავშირის საგამომცემლო სახლი, 2018, გვ. 107.

[201] იხ. საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2018 წლის 20 ივლისის გადაწყვეტილება, გ. ა.-ს განცხადების განხილვის დასრულების შესახებ, საქმე №:გ-1/420/2018, გვ. 6-7, ხელმისაწვდომია: https://personaldata.ge/ka წვდომის თარიღი: 27:06.2021.

რადგან შესაძლოა პანდემია წლების შემდეგ დავიწყებულ ისტორიად გადაიქცეს, ხოლო მასთან ბრძოლის კონკრეტული მეთოდები ცალკეულ პირთა და ორგანიზაციათა საქმისწარმოების წესად ჩამოყალიბდეს.

საკითხის გადაწყვეტის რეკომენდაციები:

- ვფიქრობ რომ სახელმწიფო ინსპექტორის სამსახურის მიერ გაცემულ სარეკომენდაციო ხასიათის წინადადებებს შესასრულებლად სავალდებულო სამართლებრივი ძალა უნდა მიენიჭოს. დაწესდეს გარდამავალი და საბოლოო ნიშნულები სარეკომენდაციო ხასიათის წინადადებათა შესასრულებლად.

- დაიგეგმოს აქტივობები შემდეგი მიმართულებით: ცნობიერების შესწავლა და ამაღლება. კანონმდებლობის მოთხოვნების სიზუსტის შემეცნება სხვადასხვა სამიზნე აუდიტორიისთვის უშუალოდ პანდემიის მიმდინარეობისას. ერთი მხრივ, ვიდეოთვალთვალის განმახორციელებელი პირების ცნობიერების გაზრდა, ხოლო მეორე მხრივ მოქალაქეთა დაკვალიანება უფლების დაცვის საშუალებების გამოყენების საკითხისთვის.

ეფექტური კონტროლის მექანიზმის შემუშავება და არსებული პროცესების გაჯანსაღება ფართო მასშტაბიანი კონტროლის განხორციელების მიზნით. ასევე, მიზანშეწონილია, დაიგეგმოს კვლევა პანდემიით გამოწვეული ცვლილებების შესახებ ვიდეოთვალთვალის განხორციელების პროცესებზე.

ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვა

ავტორი: მაკა პაპაშვილი [202]
საქართველოს ეროვნული უნივერსიტეტი

1. შესავალი

„ვიდეოთვალთვალის სისტემების გამოყენება საშუალებას იძლევა, მრავალი კანონმორჩილი ადამიანის ყოველდღიური ცხოვრება დაექვემდებაროს კონტროლს. ის, რომ ვიდეოთვალთვალის განხორციელება ნებადართული და იაფია, ავტომატურად არ ნიშნავს, მისი გამოყენების მიზანშეწონილობას“ ეს სიტყვები ეკუთვნის რიჩარდ ტომასს.[203] საკონფერენციო ნაშრომში გამოკვლეული იქნება ერთ-ერთი პრობლემატური საკითხი, რომელიც ეხება ვიდეოთვალთვალის მონიტორინგის განხორციელებისას პერსონალური მონაცემების დაცვას. XXI საუკუნეში, როდესაც ყველა საზოგადოებრივი თავშეყრის ადგილას ხორციელდება ვიდეოთვალთვალი დღითიდღე იზრდება კონფიდენციალობის პრინციპის დარღვევის რისკი, რა თქმა უნდა, არსებობს საფუძვლები, რომელთა არსებობის შემთხვევაში ვიდეოკონტროლის განხორციელება გამართლებულია, მაგალითად: დანაშაულის თავიდან აცილების, აგრეთვე პირის უსაფრთხოებისა და საკუთრების, საზოგადოებრივი წესრიგისა და არასრულწლოვნის მავნე ზეგავლენისაგან დაცვის მიზნებისათვის,[204] მიუხედავად ლეგიტიმური წინაპირობებისა, დიდია ალბათობა, რომ ამ ჩარევით შესაძლოა პერსონალური მონაცემების უკანონო დამუშავება განხორციელდეს. ზემოთ ხსენებული, თეზიდან გამომდინარე, პერსონალური მონაცემების დაცვის უზრუნველსაყოფად შესაბამისი კანონმდებლობის შექმნა და რელევანტური ქმედითი მექანიზმების უზრუნველყოფა მნიშვნელოვან გამომწვევად იქცა. აღსანიშნავია, რომ საკითხის პრობლემატიკას ამწვავებს ის გარემოებაც, რომ სწორედ ვიდეოთვალთვალის დროს ხორციელდება ჩარევა საქართველოს კონსტიტუციით გარანტირებულ საყოველთაოდ აღიარებულ ადამიანის უფლებებსა და თავისუფლებებში, რაც თავის მხრივ ქმნის არამართლზომიერი შეზღუდვის საფრთხეს, თუ კერძო ან საჯარო სუბიექტი წესების დარღვევით განახორციელებს ვიდეო მონიტორინგისას მოპოვებული პერსონალური ინფორმაციის დამუშავებას. წინამდებარე ნაშრომის მიზანია წარმოდგენილ იქნას უკანონო ვიდეო კონტროლის მძიმე შედეგი პერსონალური მონაცემების არამართლზომიერად დამუშავების თვალსაზრისით და ჩამოყალიბდეს რეკომენდაციათა ერთიანი სისტემა, რომელთა პრაქტიკაში განხორციელებაც უზრუნველყოფს ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვას.

[202] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - გვანცა სოფრომაძე.

[203] Richard Thomas CBE LLD was the Information Commissioner from November from 2002 to 2009, ხელმისაწვდომია: https://bit.ly/2XPW6Bj წვდომის თარიღი: 25.08.2021.

[204] იხ. მე-11 მუხლის 1-ლი პუნქტი საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ამოქმედდა 2012 წლის 1 მაისიდან, ხელმისაწვდომია: https://bit.ly/2WiB2To წვდომის თარიღი: 25.08.2021.

2. ვიდეოთვალთვალის განხორციელებასთან დაკავშირებით არსებული კანონმდებლობით მიმოხილვა

ვიდეოთვალთვალი ეს არის ვიდეო გამოსახულების დაფიქსირება და შემდგომში მიღებული პერსონალური მონაცემების დამუშავება (შენახვა/დაარქივება და სხვა). როგორც წესი, მიღებული მონაცემები შეზღუდულ (დახურულ) მონიტორზე გადაეცემა ვიდეო კონტროლის განმახორციელებელ სუბიექტს, აღსანიშნავია, რომ ვიდეო მონიტორინგის განხორციელება მიმდინარეობს საზოგადოებრივი წესრიგის დაცვისა და უსაფრთხოების უზრუნველყოფის მიზნით. ვიდეოთვალთვალის განხორციელება საერთაშორისო და ქართული კანონმდებლობით დასაშვებია, შესაბამისად ნებადართულია პერსონალური მონაცემების შეგროვება და მისი დამუშავება, თუმცა სავალდებულოა დაცულ იქნას, როგორც საერთაშორისო, აგრეთვე შიდასახელმწიფოებირივი (ქართული) კანონმდებლობით გათვალისწინებული დებულებები. „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ 1981 წლის კონვენციის მე-4 მუხლი[205] განამტკიცებს იმ პრინციპებს, რომელთა გათვალისწინებაც მონაცემთა დამუშავებისას სავალდებულო ხასიათის მატარებელია. პერსონალური მონაცემები უნდა დამუშავდეს სამართლიანად, კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად და იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. რაც შეეხება შიდასახელმწიფოებრივ კანონმდებლობას საქართველოს კონსტიტუციის მე-15 მუხლი[206] იზიარებს „ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის ევროპული კონვენციის“ სულისკვეთებას ადამიანის პირად ცხოვრებაში ჩარევის დასაშვებობის თვალსაზრისით. ეს უკანასკნელი კი განმარტავს, რომ, როდესაც არსებობს კანონით გათვალისწინებული შემთხვევები და აუცილებელია დემოკრატიულ საზოგადოებაში საზოგადოებრივი უსაფრთხოების ინტერესების, საზოგადოებრივი წესრიგის, ჯანმრთელობისა ან მორალის, ანდა სხვათა უფლებების და თავისუფლებების დაცვა, შესაძლებელია კონსტიტუციურ რანგში აყვანილ სიკეთეში ჩარევა. იქიდან გამომდინარე, რომ შიდასახელმწიფოებრივი კანონმდებლობის იერარქიის სათავეში მყოფი ნორმატიული აქტი (საქართველოს კონსტიტუცია) იძლევა ლავირების შესაძლებლობას, ამის შესაბამისად „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11 და მე-12 მუხლების პირველი პუნქტები ადგენენ იმ ლეგიტიმურ საჯარო მიზანთა ჩამონათვალს, რომელთა მისაღწევად ვიდეოთვალთვალის განხორციელება დასაშვებია. მე-11 მუხლის თანახმად, საზოგადოებრივი თავშეყრის ადგილებში ვიდეოთვალთვალი შეიძლება განხორციელდეს, მხოლოდ დანაშაულის თავიდან აცილების, აგრეთვე პირის უსაფრთხოებისა და საკუთრების, საზოგადოებრივი წესრიგისა და არასრულწლოვნის მავნე ზეგავლენისაგან დაცვის მიზნებისათვის, ხოლო მე-12 მუხლის შესაბამისად საჯარო და კერძო დაწესებულებებს შეუძლიათ განახორციელონ შენობების ვიდეოთვალთვალი, თუ ეს აუცილებელია პირის უსაფრთხოებისა და საკუთრების, არასრულწლოვნის მავნე ზეგავლენისგან დაცვის, საიდუმლო ინფორმაციის შენახვის და გამოცდის/ტესტირების მიზნების უზრუნველსაყოფად. მიუხედავად იმისა, რომ კანონმდებელი განამტკიცებს ვიდეო კონტროლის განხორციელების შესაძლებლობას,

[205] იხ. მე-4 მუხლი „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ 1981 წლის კონვენცია, ხელმისაწვდომია: https://bit.ly/3gx1dNo წვდომის თარიღი: 25.08.2021.

[206] „საქართველოს კონსტიტუცია“, მე-15 მუხლი.

ამავდროულად ეს უკანასკნელი ადგენს იმ პირობებს რომელთა შესრულებაც აუცილებელია იმისათვის, რომ პერსონალურ მონაცემთა დამუშავება კანონიერად იქნეს მიჩნეული. მაგალითად, ვიდეოკონტროლის განხორციელებისას სავალდებულოა თვალსაჩინო ადგილას იყოს განთავსებული შესაბამისი გამაფრთხილებელი ნიშანი (ვიდეო მონიტორინგის მიმდინარეობის შესახებ), დაუშვებელია ვიდეო კონტროლის განხორციელება ისე, რომ საზოგადოებას არ ჰქონდეს ინფორმაცია ამის შესახებ. ამდენად, ზემოთ გაჟღერებული დებულებებიდან გამომდინარე შეგვიძლია აღვნიშნოთ, რომ საქართველოს კანონმდებლობამ ამომწურავად განსაზღვრა ის ლეგიტიმური საჯარო მიზნები, რომელთა უზრუნველყოფისათვის გამართლებულია ვიდეოთვალთვალის განხორციელება. ამის მიუხედავად, მაინც ბუნდოვანია თუ რა მექანიზმებით უნდა განხორციელდეს ვიდეო კონტროლის კანონიერების შემოწმება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის, მხოლოდ სამი მუხლი ეხება ვიდეოთვალთვალის კანონიერად განხორციელების მოწესრიგებას, ამასთან აღნიშნული კანონი ბუნდოვან განმარტებებს გვთავაზობს, მაგალითად მე-11 მუხლის მესამე პუნქტის მიხედვით, ვიდეო ჩანაწერები დაცული უნდა იყოს არამართლზომიერი ხელყოფისა და გამოყენებისაგან,[207] მიუხედავად ამისა, აღნიშნული ჩანაწერი არის ზოგადი ხასიათის მატარებელი, ხოლო როგორ უნდა განხორციელდეს ქმედითი მექანიზმების შექმნა და აღნიშნული ზოგადი დანაწესის პრაქტიკაში რეალიზება, ამასთან დაკავშირებით ეს უკანასკნელი სამართლებრივი აქტი არ გვაწვდის ინფორმაციას.

2.1. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის პრაქტიკა უკანონო ვიდეოთვალთვალის განხორციელებასთან დაკავშირებით

პერსონალურ მონაცემთა დაცვას პრაქტიკული თვალსაზრისით უზრუნველყოფს 2018 წელს შექმნილი სახელმწიფო ინსპექტორის სამსახური, რომლის ყოველწლიურ ანგარიშებშიც ნათლად არის გამოკვეთილი ვიდეოთვალთვალის განხორციელებისას პერსონალური მონაცემების დაცვის პრობლემატიკა. სახელმწიფო ინსპექტორის 2020 წლის საქმიანობის ანგარიშის[208] შესაბამისად, ვიდეო მონიტორინგის 30 შესწავლილი საქმიდან გამოვლინდა 19 სამართალდარღვევა და გაიცა 77 დავალება და რეკომენდაცია. პერსონალურ მონაცემთა დამუშავებისას სამართალდარღვევები იკვეთება, როდესაც საქმე ეხება:

- ვიდეოთვალთვალის შედეგად მოპოვებული მონაცემების შენახვის ვადებს;
- ვიდეოთვალთვალის სისტემების ადმინისტრირების წესებსა და დაარქივების სისტემას;
- მოპოვებულ ინფორმაციაზე წვდომის უფლებამოსილების მქონე პირთა წრეს და მათ უფლებებს;

[207] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მე-11, მე-12, მე-13 მუხლების 1-ლი პუნქტები, ამოქმედდა 2012 წლის 1 მაისიდან, ხელმისაწვდომია: https://bit.ly/3jdQmcP წვდომის თარიღი: 25.08.2021.

[208] იხ. სახელმწიფო ინსპექტორის სამსახურის 2020 წლის საქმიანობის ანგარიში, გვ. 49-53, ხელმისაწვდომია: https://bit.ly/3jfukqf წვდომის თარიღი: 25.08.2021.

ამავდროულად, 2020 წლის ანგარიშის შესაბამისად, აღსანიშნავია, რომ პრაქტიკული თვალსაზრისით, ვიდეოთვალთვალის განხორციელებისას პერსონალურ მონაცემთა დაცვის საკითხი, კიდევ უფრო სენსიტიური ხდება, როდესაც საქმე ეხება სპეციალურ პენიტენციურ სამსახურში ვიდეო კონტროლის განხორციელებას. ამდენად, არსებული პრობლემატიკა ეხება ბრალდებულთა/მსჯავრდებულთა ელექტრონული საშუალებით მეთვალყურეობის დაწესებაზე მიღებული გადაწყვეტილებების დასაბუთებულობის საკითხს და აღნიშნულის შესახებ ბრალდებულთა/მსჯავრდებულთა ჯეროვან ინფორმირებას. ზემოთ ხსენებულ, გამოწვევებს ნათლად ასახავს 2020 წელს გასაჯაროებული ვიდეო მასალა. 2020 წლის 21 იანვარს ადამიანის უფლებათა დაცვის და სამოქალაქო ინტეგრაციის კომიტეტის სხდომაზე გასაჯაროვდა პენიტენციურ დაწესებულებაში გადაღებული 4 ვიდეო ჩანაწერი,[209] რომელიც შეიცავდა პერსონალურ ინფორმაციას. ზემოთ ხსენებულ კადრებში ასახული იყო საქართველოს სახალხო დამცველის აპარატის თანამშრომელისა და N9 პენიტენციურ დაწესებულებაში მყოფი მსჯავრდებულის შეხვედრა და მათ შორის მიმდინარე კომუნიკაცია. პარლამენტის კომიტეტის სხდომის ვიდეოჩანაწერი, რომელიც აგრეთვე შეიცავდა სპეციალურ პენიტენციურ დაწესებულებაში გადაღებულ კადრებს გაზიარებულ იქნა საქართველოს პარლამენტის და სპეციალური პენიტენციური სამსახურის ოფიციალურ ვებგვერდზე, ყოველივე ზემოთ ხსენებულთან ერთად აღსანიშნავია ის ფაქტი, რომ საქართველოს კანონმდებლობის შესაბამისად, კერძოდ „საქართველოს სახალხო დამცველის შესახებ“ საქართველოს ორგანული კანონის მე-19 მუხლის[210] თანახმად, „სახალხო დამცველის/სპეციალური პრევენციული ჯგუფის წევრის შეხვედრა პატიმრობაში მყოფ პირებთან კონფიდენციალურია. რაიმე სახის მიყურადება ან თვალთვალი დაუშვებელია.“ აგრეთვე საქართველოს სისხლის სამართლის კოდექსის 352-ე მუხლის[211] შესაბამისად, სახალხო დამცველის აპარატის თანამშრომლის საქმიანობის ხელის შეშლის მიზნით ნებისმიერი ფორმით ზემოქმედება წარმოადგენს დანაშაულს. ამდენად, სპეციალურ პენიტენციურ დაწესებულებაში განხორციელებული ვიდეო მონიტორინგი ეწინააღმდეგებოდა საქართველოს კანონმდებლობით გათვალისწინებულ მოწესრიგებას, ამ უკანასკნელზე დაყრდნობით კი შეიძლება ითქვას, რომ უკანონოდ ხდებოდა პერსონალურ მონაცემთა დამუშავება და შემდგომში ვიდეო მასალების გასაჯაროვება.

2020 წლის სახელმწიფო ინსპექტორის ანგარიშიდან კიდევ ერთ გახმაურებულ საქმეს წარმოადგენს სამედიცინო ფსიქიატრიული განყოფილების მიმღებში ვიდეო მონიტორინგის განხორციელების შემთხვევა.[212] ყურადსაღებია ის ფაქტიც, რომ ამასთან ერთად მიმდინარეობდა აუდიოჩაწერაც, თუმცა შესწავლილი ფაქტობრივი გარემოებებიდან არ იკვეთებოდა ამ უკანასკნელის განხორციელების აუცილებლობა (ლეგიტიმური საჯარო მიზანი). სამედიცინო ფსიქიატრიული დაწესებულების მიმღებში მიმდინარე ვიდეო და აუდიო მონიტორინგის ქვეშ ექცეოდა, როგორც პაციენტების ასევე დაწესებულების თანამშრომლების სამსახურებრივი და პირადი საუბრები თუ აქტივობები, რაც თავის მხრივ წარმოადგენს პერსონალურ მონაცემთა დაცვის შესახებ არსებული

[209] სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილება №-1/100/200, 2020 წლის 23 ოქტომბერი, გვ. 1-5.

[210] საქართველოს ორგანული კანონი “საქართველოს სახალხო დამცველის შესახებ“ , მე-19 მუხლი.

[211] საქართველოს კანონი „სისხლის სამართლის კოდექსი“, 352-ე მუხლი.

[212] იხ. სახელმწიფო ინსპექტორის სამსახურის საქმიანობის 2020 წლის ანგარიში, გვ.53, ხელმისაწვდომია: https://bit.ly/3jfukqf წვდომის თარიღი: 25.08.2021.

შიდასახელმწიფოებრივი კანონმდებლობის უარყოფას და უხეშ დარღვევას. ყურადსაღებია, რომ ამ ფსიქიატრიულ დაწესებულებაში მკურნალობის კურსს გადიოდნენ არასრულწლოვანი პაციენტებიც, რომლებიც აგრეთვე ექცეოდნენ უკანონო ვიდეო მონიტორინგისა და აუდიო ჩაწერის ქვეშ. უკანონო ვიდეოთვალთვალის განხორციელებისას პერსონალურ მონაცემთა მოპოვება/დამუშავება არღვევს საქართველოს კონსტიტუციის მეორე თავის მე-15 მუხლით[213] გათვალისწინებულ სამართლებრივ სიკეთეს (ადამიანის პირადი ცხოვრების ხელშეუხებლობას). სახელმწიფო ხელისუფლებას და მის მიერ შექმნილ კონსტიტუციურ ინსტიტუციებს აქვთ პირდაპირი ვალდებულება, არათუ ჩაერიონ უკანონოდ ადამიანის პერსონალურ მონაცემებში, არამედ აღმოფხვრან სხვა, ყველა მესამე პირის მიერ მსგავსი ქმედების განხორციელების შესაძლებლობა და მოახდინონ უკანონოდ პერსონალურ მონაცემთა დამუშავების პრევენცია. ამდენად, სპეციალურ პენიტენციურ დაწესებულებებში მყოფი ბრალდებულის/მსჯავრდებულის, აგრეთვე ფსიქიკური აშლილობის მქონე პირების (მათ შორის არასრულწლოვანთა) მიმართ ვიდეო და აუდიო მონიტორინგის განხორციელება სენსიტიური საკითხია და განსაკუთრებულ სიფრთხილეს მოითხოვს, რათა არ მოხდეს მათი კონსტიტუციურ რანგში აყვანილი უფლებების დარღვევა. ყოველივე ზემოთ აღნიშნულიდან გამომდინარე საგულისხმოა ის ფაქტი, რომ ვიდეო მონიტორინგის განხორციელებისას პერსონალური მონაცემების დამუშავების პრობლემატიკა საკმაოდ აქტუალური საკითხია, მათ შორის საჯარო დაწესებულებებში და განსაკუთრებულ ყურადღებას საჭიროებს განსხვავებული პრაქტიკის ჩამოსაყალიბებლად.

2.2. საერთაშორისო პრაქტიკა

ანგლო-ამერიკული სამართლის ქვეყნები განსხვავებულად აწესრიგებენ ვიდეო მონიტორინგის გარკვეულ საკითხებს,[214] აღნიშნული თეზა ნათლად არის ასახული ამერიკის შეერთებული შტატების კანონმდებლობაში, სადაც არ არსებობს ერთიანი ფედერალური კანონი, რომელიც უზრუნველყოფს ვიდეოთვალთვალის განხორციელების მოწესრიგებას. ყოველივე ზემოთ ხსენებულიდან გამომდინარე, თითოეული შტატი განსხვავებულად არეგულირებს ამ უკანასკნელთან დაკავშირებულ ასპექტებს, მაგალითად ნიუ-იორკში, როდ-აილენდში და კალიფორნიაში, ვიდეოკამერები დაიშვება ყველგან, გარდა იმ ადგილებისა, სადაც არსებობს გონივრული მოლოდინი ადამიანის პირად სივრცეში უხეში ჩარევისა. ამდენად, ვიდეო კონტროლი აკრძალულია გამოსაცვლელ ოთახებში, სასტუმროს ნომრებში, სველ წერტილებსა და საძინებლებში. ამერიკის შეერთებული შტატებისაგან განსხვავებული მოწესრიგება არსებობს კანადაში,[215] სადაც მოქმედებს კონფიდენციალობის შესახებ კანონი, რომლის შესაბამისადაც ვიდეოთვალთვალის განხორციელება კერძო და საჯარო სივრცეებში დასაშვებია IPC სახელმძღვანელოს მითითებების გათვალისწინებით. ზემოთ ხსენებული სახელმძღვანელო აწესებს შეზღუდვებს, შესაბამისად მის ფარგლებს მიღმა ვიდეო მონიტორინგი დაუშვებელია. ვიდეოთვალთვალის განხორციელებისას

[213] „საქართველოს კონსტიტუცია“, მე-15 მუხლი.

[214] “Video Surveillance Laws by State“ 30.06.2020, ხელმისაწვდომია: https://bit.ly/3znyaDy წვდომის თარიღი: 25.08.2021.

[215] “Rights to Privacy- What are The Legalities of Security Cameras in Ontario“, ხელმისაწვდომია: https://bit.ly/3zg4ata წვდომის თარიღი: 25.08.2021.

პერსონალური მონაცემების უკანონოდ დამუშავება არ წარმოადგენს, მხოლოდ საქართველოს გამოწვევას, აღნიშნული საკითხის პრობლემურობა ნათლად არის ასახული დიდი ბრიტანეთის პრაქტიკულ მაგალითებშიც.[216] სამართალდამცავი ორგანოები და უსაფრთხოების მართვის სპეციალისტები დიდ ბრიტანეთში მნიშვნელოვან ბერკეტად მიიჩნევენ ვიდეოთვალთვალს, როგორც დანაშაულის წინააღმდეგ ბრძოლის და ტერორიზმის პრევენციის საშუალებას, ამდენად გაერთიანებულ სამეფოში ჯერ კიდევ 2014 წლის მონაცემებით მთელი ქვეყნის მასშტაბით 5.2 მილიონი კამერა ფუნქციონირებდა. მიუხედავად, ვიდეოთვალთვალის დადებითი ეფექტისა საზოგადოებრივი უსაფრთხოების დაცვის კუთხით, პრაქტიკაში ხშირია უკანონო ვიდეო კონტროლის შემთხვევები, რის საფუძველზეც ხორციელდება არამართლზომიერად პერსონალური მონაცემების დამუშავება. გაერთანებული სამეფოს პრაქტიკიდან ერთ-ერთი ასეთი გახმაურებული საქმეა Woolley & Woolley v Akbar or Akram (ვული & ვული v ნაჰიდ აკრამის წინააღმდეგ).[217] ანტონ და დებორა ვულებსა და ნაჰიდ აკრამს შორის არსებობდა მრავალი წლის განმავლობაში ბიზნეს პარტნიორული ურთიერთობა, რომელიც შეწყდა მათ შორის 2013 წელს სასამართლოში ქონებრივი დავის დაწყების საფუძვლით. ამავე წლიდან ანტონ და დებორა ვულებმა და ნაჰიდ აკრამმა განათავსეს ვიდეოთვალთვალის სისტემა, რომლითაც აკონტროლებდნენ მათი უძრავი ქონების გარე პერიმეტრს, თუმცა ვულებმა ამავე წელს სათვალთვალო (მათ შორის აუდიო ჩაწერის) სისტემა დააყენეს შიდა ტერიტორიის მონიტორინგისათვის, აღსანიშნავია ის ფაქტი, რომ კონტროლის სივრცეში ექცეოდა მეზობლის ბაღი და მისი მიმდებარე ტერიტორიაც. უკანონო ვიდეოთვალთვალი ხორციელდებოდა ყოველ დღიურად 24 საათის განმავლობაში, ამავდროულად, ხდებოდა უკანონოდ მოპოვებული პერსონალური მონაცემების ავტომატური დამუშავება. საყურადღებოა, რომ ვიდეო მონიტორინგის სისტემა დამონტაჟდა მეორე მხარისათვის გაფრთხილების, კონსულტაციისა და ინფორმირების გარეშე. აგრეთვე უცნობი იყო ვიდეოკონტროლის მიზანი და მასშტაბები. საბოლოოდ, სასამართლომ უკანონო ვიდეო თვალთვალის განმახორციელებელ პირებს დააკისრა 18 000 (ათასი) ფუნტი სტერლინგის გადახდა მოწინააღმდეგე მხარის სასარგებლოდ. ამავდროულად სასამართლომ განმარტა, რომ ვიდეო კონტროლის განხორციელება დასაშვებია, მხოლოდ მეორე მხარის თანხმობით, როდესაც ამ უკანასკნელს აქვს შესაძლებლობა მიიღოს ვიდეო/აუდიო ჩანაწერის ასლი და გაეცნოს მონიტორინგის მიზნებსა და საშუალებას. არამართლზომიერად განხორციელებული ვიდეო მონიტორინგისას მოპოვებული ინფორმაცია წარმოადგენს უკანონოდ დამუშავებულ პერსონალურ მონაცემებს, შესაბამისად ჩარევა ხორციელდება ადამიანის ძირითად უფლებებსა და თავისუფლებებში. ამავე საქმეში სასამართლომ განმარტა, რომ 2017 წლის მონაცემების შესაბამისად, დიდ ბრიტანეთში არამართლზომიერი ვიდეო მონიტორინგის 3 ძირითადი მიზანი არსებობდა, ესენია:

- დანაშაულებრივი ქმედების განხორციელება, როდესაც უკანონო ვიდეოთვალთვალი ეს არის დამხმარე საშუალება ძირითადი მართლსაწინააღმდეგო ქმედების ჩასადენად;

[216] "video surveillance as a primary tool to monitor population movements and to prevent crime and terrorism, both in the private and public sectors" IFSECBLOBAL.COM, 01.01.2020, ხელმისაწვდომია:

https://bit.ly/3kmv8ZF წვდომის თარიღი: 25.08.2021.

[217] Case ref: Woolley & Woolley v Akbar or Akram [2017] SC EDIN 7, ხელმისაწვდომია: https://bit.ly/3msA9mh წვდომის თარიღი: 25.08.2021.

- ინსტიტუციური ძალადობა, როდესაც სახელმწიფოს მიერ ხორციელდება უკანონო ვიდეოთვალთვალი, რომელიც თავის მხრივ პირთა მაქსიმალური კონტროლის მიზნით არის დაწესებული;

- პირადი მიზნებისთვის გამოყენება, ამ კონკრეტულ შემთხვევაში უკანონო ვიდეოთვალთვალის მიზანია პირადი უსაფრთხოება, თუმცა აღნიშნული ცდება კანონმდებლობით მოწესრიგებულ სფეროს.

საბოლოოდ კი, ვიდეოთვალთვალი ხელს უწყობს საზოგადოებრივი წესრიგისა და უსაფრთხოების დაცვას, თუმცა ხშირად ეს უკანასკნელი ხდება არამართლზომიერი მოქმედების განხორციელების ძირითადი საშუალება. ამდენად, სახელმწიფო ინსტიტუციებმა უნდა უზრუნველყონ გარანტიების შექმნა, რომელიც მინიმუმამდე დაიყვანს უკანონოდ პერსონალური მონაცემების მოპოვების შესაძლებლობის რისკებს.

3. რეკომენდაციები

ვიდეოთვალთვალის პოლიტიკის შემუშავებისას უნდა გავითვალისწინოთ კონფიდენციალობის საკითხები, რომლის მთავარ მიზანსაც წარმოადგენს პერსონალური მონაცემების დაცვა და მათი უკანონო დამუშავების პრევენცია. ერთის მხრივ, ვიდეოკონტროლის განხორციელება მიზნად ისახავს ისეთი ლეგიტიმური მიზნების უზრუნველყოფას, როგორებიცაა: დანაშაულის თავიდან აცილება, კერძო საკუთრების უსაფრთხოება, საზოგადოებრივი წესრიგისა და არასრულწლოვნის მავნე ზეგავლენისაგან დაცვა, ხოლო მეორეს მხრივ, თავად ვიდეო მონიტორინგი არ უნდა გახდეს ადამიანის კონსტიტუციურ რანგში აყვანილ სიკეთეებში უხეშად ჩარევის საშუალება. პერსონალურ მონაცემთა დაცვისათვის აუცილებელია მაქსიმალურად აღირიცხოს ყველა ტექნოლოგიური საშუალება, რომელიც ახორციელებს ვიდეოთვალთვალს ქუჩაში, მრავალბინიანი საცხოვრებელი სახლების საჯარო სივრცეებში, კერძო და საჯარო დაწესებულებებში. მრავალი ქვეყნის, მათ შორის ამერიკის შეერთებული შტატების პრაქტიკამ აჩვენა, რომ საზოგადოებრივ თავშეყრის ადგილებში ვიდეო მონიტორინგის განხორციელება 35%-ით ამცირებს დანაშაულის სტატისტიკურ მაჩვენებელს,[218] ამდენად ვიდეო მონიტორინგის მნიშვნელობა არ წარმოადგენს დავის საგანს, თუმცა აუცილებელია მისი განხორციელებისას გარკვეული საკითხების გათვალისწინება. უკანონო ვიდეოთვალთვალი XXI საუკუნის ერთ-ერთი მნიშვნელოვანი გამოწვევაა, რაც ბუნებრივია იქიდან გამომდინარეობს, რომ ყველა ადამიანს მიუწვდება ხელი სათვალთვალო სისტემის დაყენების შესაძლებლობაზე, შესაბამისად სახელმწიფომ უნდა უზრუნველყოს ისეთი კანონმდებლობისა და ქმედითი მექანიზმების შექმნა, რომლებიც მინიმუმამდე დაიყვანენ აღნიშნული თემის პრობლემატიკას. ამისათვის კი მნიშვნელოვანია შეიქმნას განჭვრეტადი (განსაზღვრადი) კანონმდებლობა, რომელიც ზუსტად ჩამოაყალიბებს რა შემთხვევაში იქნება ვიდეოთვალთვალი მართლზომიერი, აგრეთვე, როგორ უნდა მოხდეს ვიდეო კონტროლის განხორციელებისას მოპოვებულ ინფორმაციათა დამუშავება, დაარქივება და სხვ. კანონმდებლობის შექმნასთან ერ-

[218] «video surveillance as a primary tool to monitor population movements and to prevent crime and terrorism, both in the private and public sectors“ IFSECBLOBAL.COM, 01.01.2020, ხელმისაწვდომია: https://bit.ly/2WCj9Pp წვდომის თარიღი: 30.08.2021.

თად კანონმდებელმა ზუსტად უნდა ჩამოაყალიბოს ის ლეგიტიმური საჯარო მიზნები, რომელთა მისაღწევადაც დასაშვებია ვიდეო მონიტორინგი, ამავდროულად უნდა გამოვიყენოთ თანაზომიერების ტესტი, რომლითაც უნდა განისაზღვროს, რამდენად რელევანტურია ვიდეოთვალთვალი ლეგიტიმური მიზნის მისაღწევად და თუ არსებობს უფრო მსუბუქი საშუალება, რომელიც არ განახორციელებს ჩარევას ადამიანის ძირითად უფლებებში. ამდენად, საჭიროა შეფასდეს საზოგადოებრივ სივრცეში ვიდეოთვალთვალის სისტემის გავლენა ადამიანის კონსტიტუციურ რანგში აყვანილ უფლებებსა და ღირებულებებზე. იმისათვის, რომ დაცული იყოს პერსონალური მონაცემები უკანონო დამუშავებისაგან არამართლზომიერი ვიდეოთვალთვალის განხორციელებისას, უნდა შემოწმდეს ვიდეო კონტროლის სისტემის მასშტაბები და აუცილებელია შეიქმნას ტექნოლოგიური, ადმინისტრაციული გარანტიები, რომელთა არსებობაც მნიშვნელოვნად შეამცირებს მოპოვებული პერსონალური მონაცემების ბოროტად გამოყენების შესაძლებლობას.

4. დასკვნა

საკონფერენციო ნაშრომში, თვალნათლივ იქნა წარმოდგენილი უკანონო ვიდეოთვალთვალთან დაკავშირებული გამოწვევები და სახელმწიფო ინსტიტუციათა როლი ამ უკანასკნელის აღმოფხვრის თვალსაზრისით. მიუხედავად განხილული განსხვავებული სამართლის ქვეყნების მაგალითებისა, ცალსახაა, რომ თითოეული პრაქტიკის შემთხვევაში აუცილებელია ერთიანი რეგულირების არსებობა, რომლის ფარგლებშიც სახელმწიფო ინსტიტუცია უზრუნველყოფს პერსონალური მონაცემების დაცვას. ვიდეოთვალთვალთან დაკავშირებული ამბივალენტური დამოკიდებულების მიუხედავად ეჭვგარეშეა, მისი, როგორც საზოგადოებრივი წესრიგის უზრუნველყოფის საშუალების საჭიროება, შესაბამისად საკანონმდებლო ორგანომ უნდა დაადგინოს ის სამართლებრივი ჩარჩო, რომელშიც დასაშვები იქნება ვიდეო კონტროლის განხორციელება შეუზღუდავად. ნიშანდობლივია, რომ ზემოთ ხსენებული საზღვრები იქნება სახელმძღვანელო, ამდენად, მის მიღმა განხორციელებული ვიდეო მონიტორინგი მიჩნეულ იქნება უკანონოდ პერსონალურ მონაცემთა დამუშავებად. საქართველოს კონსტიტუცია განამტკიცებს სამართლებრივი სახელმწიფოს იდეას, ეს უკანასკნელი კი დგას სწორედ სამ ფუნდამენტურ ღირებულებაზე, ესენია: დემოკრატია, ხელისუფლების დანაწილების პრინციპი და ადამიანის ძირითადი უფლებებისა და თავისუფლებების დაცვა. აქედან გამომდინარე აუცილებელია მაქსიმალურად იყოს დაცული კონსტიტუციის მეორე თავით გათვალისწინებული ღირებულებები, რათა შედგეს საქართველო, როგორც სამართლებრივი სახელმწიფო. პერსონალური მონაცემების დაცვა კი ერთ-ერთი პირველი ფუნდამენტური სიკეთეა, რომლის უზრუნველყოფაც საფუძველს უქმნის სამართლებრივი სახელმწიფოს არსებობას და ქმედით მექანიზმებს აყალიბებს კონსტიტუციურ რანგში აყვანილი პრინციპების პრაქტიკაში განხორციელებისათვის.

სახის ამომცნობი სისტემების მიერ პერსონალური მონაცემების დამუშავება

ავტორი: მარიამ გიორგაძე
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

დიდი ხნის განმავლობაში პირთა პერსონალურ მონაცემებს აგროვებდნენ და სხვადასხვა მიზნით იყენებდნენ, ისე რომ ეს ჩვეულ მოვლენად ითვლებოდა. ვფიქრობ, კაცობრიობას საკმაოდ დიდი ხანი დაგვჭირდა იმისათვის, რათა გაგვეაზრებინა თუ რამდენად მნიშვნელოვანია პირისათვის მისი პერსონალური მონაცემები და მათი დაცვის მიზნით სამართლის შესაბამისი დარგი ჩამოგვეყალიბებინა. აღსანიშნავია რომ, თავდაპირველად იგი ადამიანის უფლებათა და თავისუფლებათა ჭრილში განიხილებოდა, კონკრეტულად კი ადამიანის უფლებათა ევროპული კონვენციის მერვე მუხლის კონტექსტში - „ყველას აქვს უფლება დაცული იყოს მისი პირადი და ოჯახური ცხოვრება, საცხოვრისი და მიმოწერა“. პრაქტიკაში ამის დამკვიდრებასა და ჩემი აზრით, პერსონალურ მონაცემთა დაცვის სამართლის ჩამოყალიბებისათვის „საფუძვლის ჩაყრაში“ უდიდესი წვლილი მიუძღვის წინა საუკუნის 70-იან წლებში მიღებულ ევროპული სასამართლოს გადაწყვეტილებას „Klass and others V. Germany”, სადაც სახელმწიფოს განესაზღვრა პოზიტიური ვალდებულება შეექმნა პერსონალურ მონაცემთა დაცვის საკმარისი და ეფექტიანი გარანტიები.

თუმცა, რა თქმა უნდა, აღნიშნული არ იქნებოდა საკმარისი უფლებათა დაცვის მიზნით და მნიშვნელოვანი გახდა უკვე შემდგომში შესაბამისი ნორმატიული საფუძველი ჩაყროდა ზემოთ აღნიშნულ სამართლის დარგს, რაც გამოიხატა ევროპის საბჭოს 108-ე კონვენციის „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ შექმნით. ასევე უმნიშვნელოვანესია დღევანდელი მდგომარეობით არსებული მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR), რომლითაც გაუქმდა 1995 წლის ევროპარლამენტისა და ევროსაბჭოს 95/46/EC დირექტივა.

რაც შეეხება უშუალოდ საქართველოს, 2012 წელს ძალაში შევიდა „პერსონალურ მონაცემთა დაცვის შესახებ კანონი“, რომელიც შექმნილია სწორედ ზემოთ აღნიშნული კანონმდებლობის საფუძველზე და დღესაც იხვეწება ევროკავშირის სტანდარტების შესაბამისად. აღნიშნული კანონმდებლობის ეფექტურობისა და დაცვის მიზნით კი 2018 წლიდან მოქმედებს „სახელმწიფო ინსპექტორის სამსახური“.

როგორც ზემოთ აღვნიშნეთ პერსონალურ მონაცემთა დაცვის, შედარებით ახალგაზრდა სამართლის დარგის, ჩამოყალიბება საზოგადოების განვითარების, პირთა მონაცემების მზარდი დამუშავების შედეგი შეიძლება იყოს - ამაში კი ვფიქრობ უმნიშვნელოვანესი როლი მათ შორის ციფრული ტექნოლოგიების განვითარებამ შეიტანა, რის შედეგადაც გაიზარდა მონაცემთა შეგროვების მოცულობა, ამისი ერთ-ერთი მაგალითი კი რომელიც საკმაოდ აქტუალურია დღევანდელ დღეს, ნაშრომის მთავარი თემა - სახის ამოსაცნობი ტექნოლოგიებია.

კაცობრიობას მისმა ტექნოლოგიურმა განვითარებამ ცალსახად უამრავი დადებითი შედეგი მოუტანა, როგორც მის ყოველდღიურ ცხოვრებაში, ასევე ისეთი მიმართულებებით როგორიცაა მედიცინა, განათლება, თავდაცვა და სხვა. თუმცა ამ შემთხვევაშიც გარდაუვალია მედლის მეორე მხარის არსებობა - ჩემს მიერ ნახსენები უპირატესობების „ფასი“ ხშირად პირთა პერსონალური მონაცემების დამუშავება ხდება, რაც განსაკუთრებით აქტუალურია სახის ამოსაცნობი ტექნოლოგიების შემთხვევებში. იქიდან გამომდინარე რომ ამ დროს მუშავდება პირის სენსიტიური მონაცემები, რაზეც უფრო დეტალურად შემდგომში ვისაუბრებთ, მნიშვნელოვანია როგორ იქნება გამოყენებული იგი. ადამიანის უფლებათა მიმართ მაღალი რისკის არსებობის გამო 2020 წელს ევროკავშირმა გადაწყვიტა მორატორიუმი გამოეცხადებინა საჯარო ადგილებში სახის ამომცნობი სისტემების გამოყენებაზე, სანამ შესაბამის რეკომენდაციებს არ მიიღებდნენ.

2. სახის ამომცნობი ტექნოლოგია, როგორც პირთა პერსონალურ მონაცემებზე მოქმედების უშუალო მექანიზმი

2.1. სახის ამომცნობი ტექნოლოგია - FRT

მანამ, სანამ უშუალოდ სახის ამომცნობი ტექნოლოგიების მიერ, პერსონალურ მონაცემებზე მოქმედების განხილვაზე გადავიდოდეთ მნიშვნელოვანია განვსაზღვროთ რა არის იგი , როგორ მუშაობს, რისთვის გამოიყენება და სად შეიძლება შევხვდეთ მას.

სახის ამოცნობის პირველი მცდელობა 1960-იან წლებში იყო, თუმცა არ გაამართლა ვინაიდან სახის მონაცემების „კოორდინირება“ ადამიანის მიერ უნდა მომხდარიყო. მართალია ამ ტექნოლოგიების განვითარება კვლავაც გრძელდებოდა და იხვეწებოდა, თუმცა ერთ-ერთი უმნიშვნელოვანესი იყო 1991 წელს მეთიუ ტურკის და ალექს პენტლანდის აღმოჩენა, რომლის შედეგადაც შესაძლებელი გახდა ავტომატური სისტემის მეშვეობით სახის ამოცნობა, არა უშუალოდ პორტრეტის მეშვეობით, არამედ გამოსახულების ამოცნობა სხვა ობიექტებიდან.

სახის ამოცნობის ტექნოლოგიები არის ბიომეტრიული სისტემები, რომლითაც ხდება ადამიანის სახის ავტომატური იდენტიფიცირება და “შესაბამისობა“ უკვე არსებულ ციფრულ გამოსახულებასთან.[219] აღნიშნული ტექნოლოგია ქმნის ერთგვარ „ბიომეტრიულ შაბლონს“ - ე. ი. ინდივიდის სახის სხვადასხვა ნაწილის, ნაკვთების ამოცნობით, გაზომვით, შეგროვებით - ხდება შემდგომში პირის იდენტიფიცირება, ვერიფიკაცია.[220]

ე.ი. სახის ამომცნობი ალგორითმები იყენებს ფოტოზე ან ვიდეოზე გამოსახული ინდივიდის „ბიომეტრიულ შაბლონს“ და ამ გზით მოპოვებულ ინფორმაციას ადარებს ბაზაში არსებულ მონაცემებს.

[219] Article 29 Data Protection Working Party (2012), Opinion 3/2012 on developments in biometric technologies, 00720/12/ EN, WP193, Brussels, 27 April 2012.

[220] Introna, L. and Nissenbaum, H. (2010), Facial Recognition Technology: A Survey of Policy and Implementation Issues, Lancaster University Management School Working Paper 2010/030.

შესაბამისად, ძირითად შემთხვევებში, აღნიშნული შეგვიძლია მოკლედ 4 ეტაპად გამოვყოთ:

- ინდივიდის სახის აღმოჩენა გამოსახულებაზე;
- სახის ანალიზი - რომლის დროსაც მისი „საკვანძო წერტილების“ გამოყოფა ხდება (დაახლოებით 80, თითოეულ ინდივიდზე) და შესაბამისი ნაკვთების აზომვა;
- გამოსახულების მონაცემებად ქცევა - თითოეული „საკვანძო წერტილი“ ანალიზის შემდეგ ციფრებად აისახება აპლიკაციის სისტემაში, რაც ერთობლიობაში „სახის ანაბეჭდს“ ქმნის;
- თანხვედრა (ე. წ. “matching”) - ბოლო ეტაპია, რა დროსაც ინდივიდის „სახის ანაბეჭდის“ ბაზაში უკვე არსებულთან შედარება და „თანხვედრა“ ხდება. მაგ., FBA ის დაახლოებით 21 ბაზაზე აქვს წვდომა, სადაც ჯამში 641 მილიონი ფოტოსურათის მოძიებაა შესაძლებელი.[221]

2.2. სახის ამომცნობი სისტემები ჩვენს გარშემო

ჩვენი პერსონალური მონაცემების დამუშავება ყოველდღიურად ხდება, ისე რომ ხშირად ამას ვერც ვამჩნევთ, ამ შემთხვევაში არც სახის ამომცნობი ტექნოლოგიებია გამონაკლისი.

პირველი ყველაზე მარტივი მაგალითი ამასთან მიმართებით არის თანამედროვე მობილური ტელეფონები, ე.წ. Smartphone-ები, რა დროსაც სახის ამოცნობა ძირითადად ხდება მოწყობილობის უსაფრთხოების მიზნით. ამ მხრივ საკმაოდ არის განვითარებული “Face ID” – „Apple“ -ის მიერ შემუშავებული სისტემა, რომელსაც პიროვნების ამოცნობა შეუძლია პირბადის ან სათვალის ტარების შემთხვევაშიც. ამ დროს პირის მონაცემთა შეგროვება, რა თქმა უნდა, მისი ნებართვის საფუძველზე ხდება. ანდროიდის შემთხვევაში მომხმარებელს სისტემის გამოყენებამდე აფრთხილებენ მისი ბიომეტრიული მონაცემების გამოყენების შესახებ, რაც უშუალოდ მის მოწყობილობაზე ინახება.

გარდა სმარტფონებისა, FRT-ის გამოყენება ხდება ჩვენთვის ყველასთვის ნაცნობი სოციალური ქსელებისა თუ ტექნოლოგიური კორპორაციების მიერ. 2014 წელს, ფეისბუქმა დააანონსა „Deepface“ პროგრამა, რითიც შესაძლებელი გახდებოდა 97,25% -იანი სიზუსტით დადგენა, წარმოადგენდა თუ არა ორ ფოტოზე გამოსახული პიროვნება ერთსა და იმავე ადამიანს. ამისი რეკორდი კი შემდეგ წელს „Google“-მა „Facenet“-ით მოხსნა 99.63%იანი სიზუსტით. ეს უკანასკნელი კი შემდგომში დაინერგა ჩვენთვის ყველასთვის ნაცნობ „Google Photos“-ში, რომელიც ფოტოებში ამოცნობილი ადამიანების მეშვეობით არჩევს მათ.

როგორც პროცესის დაჩქარების, ასევე უსაფრთხოების უზრუნველყოფის მიზნით, სახის ამომცნობი სისტემები გამოიყენება აეროპორტებში, მსოფლიოს სხვადასხვა ქვეყანაში, რაშიც დიდ როლს თამაშობს ბიომეტრიული პასპორტები. ამის დანერგვა დაწყებულია ისეთ ქვეყნებში რო-

[221] „How Facial Recognition Works: Technology Explained in Detail“, RecFaces, ხელმისაწვდომია: https://bit.ly/3mxTDpu წვდომის თარიღი: 25.08.2021.

გორიცაა ჩინეთი, საფრანგეთი და სხვა. ასევე ბოლო დროინდელი ინფორმაციით, შინაგან საქმეთა სამინისტროს საზოგადოებრივი უსაფრთხოების მართვის ცენტრ „112“-ს, ევროკავშირის ფინანსური მხარდაჭერით, სახის ამომცნობი კამერების სისტემა გადაეცა. აღნიშნული ტექნიკა საერთაშორისო აეროპორტების ტერიტორიაზე დამონტაჟდება და მათი საშუალებით მოხდება როგორც შემომსვლელ, ასევე, გამსვლელ მგზავრთა ნაკადის მონიტორინგი, რაც უსაფრთხოების მაღალ სტანდარტს უზრუნველყოფს.[222] შესაბამისად აღნიშნული ტექნოლოგიების დანერგვა უკვე საქართველოშიც აქტიურად მიმდინარეობს.

აღსანიშნავია რომ FRT-ის მნიშვნელოვანი როლი შეიძლება ჰქონდეს საზოგადოებისა და სახელმწიფოს უსაფრთხოების დაცვის მხრივაც. ამ ტექნოლოგიით აღჭურვილი სათვალთვალო კამერები (CCTV) შესაძლებელს ხდის უგზო-უკვლოდ დაკარგულ პირთა აღმოჩენას, ასევე ტრეფიკინგის, ბავშვების ექსპლოატაციის აღმოჩენასა და აღკვეთას, ძებნილ კრიმინალთა მიგნებას და გამოძიებისათვის სხვაგვარად ხელის შეწყობას.

გარდა ზემოთ აღნიშნულისა, ზოგიერთ სახელმწიფოში, FRT-ი გამოიყენება ჯანდაცვის სისტემაში, საბანკო სექტორში. მაგ., 2016 წელს “Mastercard”-მა “Check Mobile” -სისტემა წარადგინა, რომელიც მომხმარებელს საშუალებას მისცემს გადახდა მარტივად, საკუთარი ფოტოსურათის გაგზავნით განახორციელოს. თუმცა ამ შემთხვევაში საინტერესოა რამდენად უსაფრთხოა მსგავსი სიმარტივე, მაშინ როდესაც ჯერ კიდევ 2020 წლისთვის კიბერდანაშაულების შემთხვევები 600%-მდე იყო გაზრდილი.

ასეთივე ტექნოლოგიების გამოყენება დაიწყეს სასტუმროების ნაწილმა ე.წ. „Check-in“-ის გასამარტივებლად, ასევე ნომერში შესასვლელად. ამის ერთ-ერთი მაგალითი კი “Marriot”ის სასტუმროების ქსელია.[223] მართალია მეცნიერების მსგავსი განვითარება სასიხარულოა და სავარაუდოდ მსგავსი ტექნოლოგიები, რომლებიც ადრე მართლაც მხოლოდ ფილმებში წარმოგვედგინა მომხიბვლელად გამოიყურება, თუმცა როგორც ჩვენთვის ყველასთვის ნაცნობი ფრაზა აღწერს „მედალს ორი მხარე აქვს“ - ამ შემთხვევაშიც ჩემს მიერ აღნიშნული შთამბეჭდავი მოწყობილობების უკან თითოეული ჩვენგანის ფუნდამენტური უფლებები დგას, რომლებზეც ზემოთ აღნიშნულ FRT-ის დიდი ზეგავლენის მოხდენა შეუძლია. უფრო ნათელი რომ იყოს, წარმოვიდგინოთ რომ ჩვენთვის უცნობი პირი მის ხელთ არსებული ციფრული მოწყობილობებით „გვმეთვალყურეობს“, შეუძლია ნებისმიერ დროს სახის ამომცნობი კამერების გამოყენებით დაგვაკვირდეს - ჩვენი გამოსახულება გამოიყენოს იმგვარად, რომ ჩვენ ამაზე ინფორმირებულები არ ვიყოთ. შესაძლებელია აღნიშნული სისტემის შედეგად მოხდეს ჩვენი კატეგორიზაცია სქესის, კანის ფერის, ასაკის და სხვა ნიშნის მიხედვით. ცალკეულ შემთხვევაში მსგავსი ქმედებებით ზიანი შეიძლება მიადგეს ისეთ უზენაეს ღირებულებებს როგორიცაა ადამიანის ღირსება, პირადი ხელშეუხებლობა და ნაშრომის მთავრი თემა - პირის პერსონალური მონაცემები.

[222] „112-ს ევროკავშირის ფინანსური მხარდაჭერით სახის ამომცნობი კამერების სისტემა გადაეცა“- შსს, ხელმისაწვდომია: https://bit.ly/3zjAwD9 წვდომის თარიღი: 25.08.2021.

[223] Jenna Wang,“ You Can Now Check In With A Facial Scan At Marriott In China“, Forbes.

2.3. სახის ამომცნობი სისტემები ადამიანის უფლებათა ჭრილში

ადამიანის ფუნდამენტური უფლებები წესრიგდება ევროპის 1950 წლის კონვენციით და მათ შორის სხვადასხვა ნორმატიული აქტით ხდება მათი უსაფრთხოების გარანტირება და უზრუნველყოფა.

როგორც ნაშრომის დასაწყისშივე აღვნიშნე, საზოგადოება მუდმივად წინ მიდის, რაც მოიცავს მის ზოგად სოციალურ, ასევე ტექნოლოგიურ განვითარებას - ეს უკანასკნელი კი უფრო "დაუცველს" ხდის ინდივიდთა ძირითად უფლებებსა და თავისუფლებებს, ვინაიდან მსგავსი ევოლუციისას გარდაუვალია მათზე უშუალო ზემოქმედება. მაგალითად, ჩვენს შემთხვევაში სახის ამომცნობი სისტემები თავისი არსით ადამიანის უფლებებში ჩარევას მოიცავს, რომლის გარეშეც უბრალოდ ამ ტექნოლოგიების გამოყენება შეუძლებელი იქნებოდა.

კანონმდებლობა, რომელიც დასაშვებს ხდის ინდივიდების მასშტაბურ მეთვალყურეობას პირდაპირ წინააღმდეგობაში მოდის მათ პირადი ცხოვრების ხელშეუხებლობასთან.

ამასთან ერთად, იქიდან გამომდინარე რომ მსგავსი სისტემებისა და მათ შორის FRT ტექნოლოგიების გამოყენებისას ხშირ შემთხვევაში არ არსებობს იმ ინდივიდთა თანხმობა (ისინი ზოგადად არც იაზრებენ მასზე მსგავს ზედამხედველობას), რომელთა ბიომეტრიული მონაცემებიც მუშავდება, მით უმეტეს იმის გათვალისწინებით რომ მოსახლეობის უმეტესი ნაწილის ციფრული ფოტოსურათების მოპოვება ინტერნეტ სივრცეში უფრო ამარტივებს სახის ამოცნობის პროცესს - სერიოზული საფრთხე ექმნება პირის როგორც პრივატულობას, პერსონალურ მონაცემებს, ასევე სხვა ფუნდამენტურ უფლებებს.

ზოგადად ხელოვნური ინტელექტი მუდმივ განვითარებაშია და ჯერ კიდევ არ მიუღწევია თავისი იდეალური ფორმისათვის, შესაბამისად, მაგ., განსხვავებით სხვა ბიომეტრიული მონაცემებით ამომცნობი სისტემებისა სახის ამომცნობი სისტემები, მიუხედავად მათი პროვაიდერების დაპირებებისა, ხშირ შემთხვევებში არაზუსტი შეიძლება იყოს. ეს სისუსტე კი განსაკუთრებით ვლინდება საზოგადოების ისეთი „მოწყვლადი" ჯგუფის შემთხვევაში როგორებიცაა ეთნიკური, რასობრივი უმცირესობები, ბავშვები, მოხუცები, ასევე ხშირ შემთხვევებში ქალები.[224]

არასრულწლოვნების შემთხვევაში აუცილებლად უნდა აღვნიშნოთ, რომ მათ საუკეთესო ინტერესები ყოველი სახელმწიფოსთვის ერთ-ერთ უმაღლეს ღირებულებას უნდა წარმოადგენდეს, შესაბამისად მათი პერსონალური მონაცემების დაცვაც საკმაოდ დიდი რისკის ქვეშ დგება ციფრული ტექნოლოგიის დღევანდელი განვითარების ეტაპზე, ამასთან დაკავშირებით კი მისასალმებელია და მოსაწონია საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ" კანონის ახალ პროექტში ასახული ცვლილებები, რომელიც ახლა უკვე არასრულწლოვანთა უფლებების დაცვაზეცაა ორიენტირებული და აღნიშნულია რომ „არასრულწლოვანი პირის მონაცემთა დამუშავება მისი თანხმობის საფუძველზე დასაშვებია თუ მან მიაღწია 14 წლის ასაკს, ხოლო 14 წლამდე ასაკის არასრულწლოვანი პირის - მისი მშობლის ან სხვა კანონიერი წარმომადგენლის

[224] Drew Harwell, „Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use", The Washington Post.

თანხმობის საფუძველზე.“[225] ზემოთ აღნიშნულიდან გამომდინარე, ყველაზე მეტად საშიშია სწორედ სახის ამომცნობი სისტემით პირთა დამახასიათებელი ნიშნების კატეგორიზაცია, რაც საფრთხის ქვეშ აყენებს საზოგადოების მარგინალიზებულ ჯგუფებს (სქესის მიხედვით ამომცნობი სისტემების შემთხვევაში კი უშუალოდ ე.წ. „არატრადიციული ორიენტაციის“ პირთა მიმართებით) და საფუძველს ქმნის შემდგომი დისკრიმინაციისთვის. ამ მხრივ, განსაკუთრებით შემაშფოთებელი შეიძლება იყოს ჩინეთის მაგალითი, სადაც სახის ამომცნობი სისტემებით აღჭურვილი CCTV-ი, ეთნიკურად თურქი უიღური ჩინელების ამოცნობაზე იყო ორიენტირებული და მათი იდენტიფიკაციის შემთხვევაში შესაბამის უწყებებს ე.წ. „გამაფრთხილებელ სიგნალებს“ უგზავნიდა, რაც თითქოსდა ტერორიზმთან ბრძოლისათვის გამოიყენებოდა.[226] საინტერესოა ფართოდ გავრცელებული ჩინური აპლიკაციის “TIKTOK”-ის შემთხვევაც რომელიც, როგორც აღმოჩნდა მარკეტინგული მიზნებისთვის მომხმარებლების ვიდეოების მიმართ სახის ამომცნობ სისტემას იყენებდა, ალგორითმი კი მათ სქესს, ასაკსა და ეთნიკურ კუთვნილებას ადგენდა.[227] აღნიშნული ქსელი მსოფლიოს სხვადასხვა ქვეყანაში, განსხვავებული ასაკის ჯგუფების მიერ გამოიყენება - შესაბამისად რთული წარმოსადგენი არ უნდა იყოს მონაცემთა უკანონო დამუშავების რა ფართო მასშტაბთან შეიძლება გვქონდეს შემთხვევა მის მიერ სახის ამომცნობი სისტემების დაურეგულირებელი გამოყენებისას.

ამასთან ერთად, ბოლო დროინდელი პრაქტიკით FRT-ი გამოიყენება შეკრებებსა და მანიფესტაციებზე პირთა ამოცნობისათვის, მათ შორის “Black lives matter”-კამპანიასთან დაკავშირებულ აქციებზე.[228] საჯარო სივრცეში ვიდეო კამერების მიერ გადაღებული სახის გამოსახულებების დასამუშავებლად FRT-ის გამოყენება შეიძლება ჩაითვალოს პირის აზრისა და გამოხატვის თავისუფლებაში შეჭრად, იმის გათვალისწინებით, რომ აღნიშნული უფლება მათ შორის მოიაზრებს ჯგუფურ ანონიმურობას.[229] ამასთან დაკავშირებით საინტერესოა გერმანიის სასამართლოს გადაწყვეტილება, რომელმაც დემონსტრაციებზე გადაღებული სურათების სოციალური მედიით გავრცელება არალეგალურად გამოაცხადა, ზემოთ აღნიშნულ უფლებაზე მისი ნეგატიური გავლენის გამო.[230] იმის გააზრება, რომ საჯარო სივრცეში გვაკვირდებიან და ჩვენი ამოცნობა ნებისმიერ დროს შესაძლებელი გახდება, ჩემს მიერ უკვე მრავალჯერ ნახსენები მოწყობილობების დახმარებით, თითოეულ ჩვენგანს გვაიძულებს ჩვეულებრივი ქცევის შეცვლას და უფრო ფრთხილები ვხდებით. შესაბამისად მას ე. წ. „მსუსხავი ეფექტი“ აქვს ადამიანის აზრისა და გამოხატვის უფლებაზე - ამან კი შეიძლება „გამოიწვიოს საზოგადოების გაუმართლებელი ჩაკეტვა, მისი მოქმედების თავისუფლების თვითშეზღუდვა, აიძულოს ადამიანები, მოახდინონ თვითცენზურა გამოხატვის

[225] საერთაშორისო გამჭირვალობა - საქართველო, პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში დაგეგმილი ცვლილებების შეფასება - 04 ოქტომბერი, 2019.

[226] Paul Mozur, “ One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority”, The New York Times.

[227] TikTok agrees legal payout over facial recognition“, BBC NEWS, ხელმისაწვდომია: https://bit.ly/3DiNZO3 წვდომის თარიღი: 26.08.2021.

[228] Matt Mahmoudi “Ban dangerous facial recognition technology that amplifies racist policing”, Amnesty International.

[229] International Justice and Public Safety Network (2011), Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 June 2011, p. 18.

[230] Verwaltungsgericht Gelsenkirchen (2018), 14 K 3543/18 (ECLI:DE :VGGE:2018:1023.14K3543.18.00).

თავისუფლებით დაცული სფეროს იმ ნაწილში, რომლის შეზღუდვის აუცილებლობაც არ არსებობს, რაც, თავისთავად, ამ უფლების არათანაზომიერად შეზღუდვის ტოლფასია.“[231]

სახის ამომცნობი სისტემები გარდა ზემოთ აღნიშნულისა უარყოფით ზეგავლენას ახდენს პირადი ცხოვრების ხელშეუხებლობის (იგივე „right to privacy”, (რომელიც მოიცავს ინტიმურ, კერძო, საჯარო სფეროებს, ასევე ისეთ ასპექტებს პიროვნების თვითგამორკვევას, სახელის, ოჯახური ცხოვრების ხელშეუხებლობას და მათი დაცვაც შესაბამისად განსხვავებული სტანდარტებით ხდება)) და პირის პერსონალურ მონაცემთა დაცვის უფლებაზე, რასთან დაკავშირებითაც უკვე შემდგომ ნაწილში ვისაუბრებთ .

2.3.1 სახის ამომცნობი სისტემების მიერ პირის პერსონალურ მონაცემთა დამუშავება

როგორც დასაწყისშივე აღვნიშნე, სახის ამომცნობი სისტემების გამოყენება თავისი არსიდან გამომდინარე უშუალოდ ზემოქმედებს და ერევა პირის პერსონალურ უფლებებში, რომელიც კანონმდებლობით გარანტირებულ და დაცულ სფეროს წარმოადგენს.

პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.

პირი იდენტიფიცირებადი იქნება, თუ მისი იდენტიფიცირება შესაძლებელია პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან მისი მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით.[232] ამასთან აღნიშნულის განხორციელება უნდა მოითხოვდეს გონივრულ დროს, ხარჯებსა და რესურსებს, რაც ყოველ შემთხვევაში ინდივიდუალურად განისაზღვრება.

მნიშვნელოვანია, ერთმანეთისგან განვასხვაოთ ორი კატეგორიის პერსონალური მონაცემი, ჩვეულებრივი რომელზეც ზემოთ უკვე ვისაუბრეთ და განსაკუთრებული კატეგორიის ე. წ. „სენსიტიური“ მონაცემები, რომლებიც მათი ბუნებიდან გამომდინარე, განსაკუთრებულად მგრძნობიარეა ფუნდამენტურ უფლებებთან და თავისუფლებებთან მიმართებაში, საჭიროებს განსაკუთრებულ დაცვას, რადგან მათი დამუშავების კონტექსტი შეიძლება მნიშვნელოვანი რისკის ქვეშ აყენებდეს ფუნდამენტურ უფლებებსა და თავისუფლებებს.“[233] საქართველოს კანონმდებლობის თანახმად ასეთია მონაცემი, რომელიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული ორგანიზაციის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ან ნასამართლობასთან, ასევე ბიომეტრიული მონაცემები, რომლითაც შესაძლებელია პირის იდენტიფი-

[231] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე 2/2/516,542 „საქართველოს მოქალაქეები - ალექსანდრე ბარამიძე, ლაშა ტუღუში, ვახტანგ ხმალაძე და ვახტანგ მაისაია საქართველოს პარლამენტის წინააღმდეგ“ 14 მაისი, 2013წ.

[232] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ, „მუხლი 2 „ა “ ქვეპუნქტი.

[233] Recital 51.The General Data Protection Regulation (EU) 2016/679.

ცირება ზემოთ აღნიშნული ნიშნებით.[234] მსჯელობისას არაერთხელ ვახსენე, რომ სახის ამომცნობი სისტემების მიერ ხდება პირის ბიომეტრიული მონაცემების დამუშავება, რომელიც საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მიხედვით შემდეგნაირადაა განმარტებული - „ბიომეტრიული მონაცემი – ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, ტერფის ანაბეჭდი, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებელი);“[235] როგორც ზემოთ აღნიშნულიდან ჩანს, ნებისმიერი გამოსახულება, არ შეიძლება ჩაითვალოს სენსიტიურ მონაცემად, თუმცა ამგვარ შემთხვევასთან გვაქვს საქმე თუ ამ ბიომეტრიული მონაცემებით პირის კანონით განსაზღვრული ნიშნებით „უნიკალური იდენტიფიცირებაა“ შესაძლებელი და სოციუმის შესაბამის ჯგუფთან ასოცირება. აქედან გამომდინარე FRT-ის მიერ დამუშავებული ინფორმაცია, რომელიც სოციალური ქსელის მეშვეობით კიდევ უფრო მარტივად მოიპოვებს პირის ფოტოსურათს შესაბამისი პირადი ბაზის არსებობის გარეშეც, თავისთავად წარმოადგენს განსაკუთრებული ხასიათის პერსონალურ მონაცემებს.

მიუხედავად იმისა, რომ მნიშვნელოვანია თითოეული ინდივიდის ფუნდამენტურ უფლებათა დაცულობა, მათი უმეტესობა არაა აბსოლუტური და შესაბამისი წინაპირობების არსებობისას აღნიშნული „დახურული კარი“ იხსნება. თუმცა ამისათვის საჭიროა არსებობდეს ამ ჩარევაზე უფლებამოსილი პირი, შესაბამისი ლეგიტიმური ინტერესი და ჩარევის პროპორციულობა.

ზემოთ აღნიშნულიდან გამომდინარე, არც პირის პერსონალური მონაცემების დაცვაა აბსოლუტური ღირებულება, თუმცა აქაც აღსანიშნავია, რომ ზემოთ ნახსენებ მონაცემთა სენსიტიურობიდან გამომდინარე შედარებით „დიდი ზღურბლია“ დაწესებული.[236] სახის ამომცნობი სისტემები იმდენად მალე და მრავალმხრივად განვითარდა და მისი გამოყენება როგორც კერძო, ისე საჯარო სექტორში ინტენსიურად დაიწყო, რომ პირთა ზემოთ აღნიშნული უფლებების შეზღუდვის პრეცენდენტები შექმნა (მაგ. დასაქმების ადგილას დასაქმებულთა ოფისში შესვლას შესაბამისი FRT-ით უზრუნველყოფდნენ.) [237]

ამას დაემატა Covid-19-იც რომელთან ბრძოლისათვის, ასევე მის თანმდევ შედეგებთან გამკლავებისათვისაც სწორედ ციფრული ტექნოლოგია და, ზოგიერთ შემთხვევებში, სახის ამომცნობი სისტემები გამოიყენებოდა - მაგ., რუსეთი, სადაც ვიდეო კამერების მეშვეობით ხდებოდა სავალდებულო კარანტინში მყოფ პირთა ამოცნობა,[238] თუმცა როგორც შემდგომში გაირკვა უმეტესი შემთხვევა „ცრუ-დადებითი“ იყო.

იქიდან გამომდინარე რომ სახის ამომცნობი ტექნოლოგიები ნელ-ნელა ჩვეულებრივ მოვლენად იქცა, ევროკავშირის შემთხვევაში, დღის წესრიგში დადგა აღნიშნული სფეროს მოწესრიგება და

[234] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ, „მუხლი 2 „ბ “ ქვეპუნქტი.

[235] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ, მუხლი 2, „გ“ ქვეპუნქტი.

[236] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ, მუხლი 6.

[237] Henry Kronk, “Facial Recognition Technology in the Workplace: Employers Use It, Workers Hate It, Regulation Is Coming for It”, ხელმისაწვდომია: https://bit.ly/2XTGQn3 წვდომის თარიღი: 26.08.2021.

[238] Dixon,“ In Russia, facial surveillance and threat of prison being used to make coronavirus quarantines stick“, The Washington Post.

რამდენიმეხნიანი მუშაობის შედეგად ჩამოყალიბდა „სახის ამოცნობის სახელმძღვანელო“[239] - მონაცემთა დაცვის 108-ე კონვენციის ფარგლებში - რომელიც ახლა უკვე მოდერნიზებული სახით მოქმედებს, რისი ერთ-ერთი განმაპირობებელიც სწორედ ციფრული ტექნოლოგიების განვითარებასთან მისადაგება და შესაბამისი ქმედითი მექანიზმების შექმნა იყო.

აქვე უნდა აღვნიშნოთ რომ ეს რეკომენდაციები განკუთვნილია როგორც სახის ამომცნობი სისტემის შემქმნელთათვის, ასევე მის საფუძველზე მონაცემთა დამმუშავებლისთვის და კონვენციის ხელშემკვრელ მხარეთათვის.

2.3.1.1. სახის ამომცნობი სისტემების პეჰსონაღუჰი მონაცემების დაცვის გათვაღისწინებით შემუშავება

დასაწყისში არაერთხელ ვახსენე რომ FRT-ის მიერ სენსიტიური მონაცემების დამუშავება ხდება, მართალია კანონმდებლობით მოწესრიგებულია მათ დამუშავების ზოგადი საფუძვლები, მაგრამ ციფრული ტექნოლოგიების მიერ მონაცემთა შეგროვება-გამოყენების შემთხვევაში ადამიანის უფლებათა ზემოქმედებაზე რისკი უფრო გაზრდილია და მნიშვნელოვანია მათი ცალკეული მოწესრიგება მოხდეს - მით უმეტეს კი როდესაც აღნიშნული ზემოქმედება ინდივიდებზე „მეთვალყურეობასაც“ შეიძლება მოიცავდეს.

უშუალოდ როდესაც ზემოთ აღნიშნული სისტემების შემქმნელებზე გვაქვს საუბარი, აუცილებელია მათ მიერ წინასწარვე, მოწყობილობების „ბაზარზე ჩაშვებამდე“, მიმართონ კომპეტენტურ ორგანოებს პირთა ფუნდამენტურ უფლებებზე მათი ზემოქმედების შეფასების მიზნით. ასევე როგორც ზემოთ მოყვანილი სტატისტიკები გვაჩვენებს, ყოველგვარი დისკრიმინაციის თავიდან აცილების მიზნით, ამ ტექნოლოგიის შექმნისას კვლევებში მონაწილეობას უნდა იღებდნენ სხვადასხვა სქესის, კანის ფერის, რასის, ასაკის პიროვნებები, რაც უზრუნველყოფს ტექნოლოგიის მოქნილობას. გარანტირებული უნდა იყოს მონაცემთა სიზუსტე, ასევე მათი უსაფრთხოება - განსაკუთრებით კი ისეთი ბიომეტრიული მონაცემებისა, რომელიც პირის შეზღუდულ შესაძლებლობასთან ან რაიმე სახის დაავადებასთანაა კავშირში. ასევე ინტეგრირებული უნდა იყოს ხელსაწყოები, ისე რომ უზრუნველყონ „ნედლი მონაცემების“ ავტომატური წაშლა ბიომეტრიული შაბლონის შექმნის შემდეგ. იმისათვის რომ ამ წინაპირობების არსებობა იყოს გარანტირებული, საჭიროა სახის ამომცნობი ტექნოლოგიების ხელმისაწვდომობამდე მისი სერტიფიცირებისა თუ ლიცენზირების გაცემა და მხოლოდ ამის საფუძველზე მათი გამოყენება.

[239] Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data convention 108 - guidelines on facial recognition, t-pd (2020)03rev4, 28/01/2021.

2.3.1.2. სახის ამომცნობი სისტემების მიერ პერსონალურ მონაცემთა დამუშავების რეგულირება

108-ე კონვენციის მოდერნიზებული რედაქციის მე-6 მუხლის თანახმად, სპეციალური კატეგორიის მონაცემების დამუშავება დასაშვები უნდა იყოს თუ მსგავსი დამუშავება შესაბამის საკანონმდებლო ბაზისს ეყრდნობა და ამასთან ერთად ადგილობრივი კანონით განმტკიცებულია დამატებით, ადეკვატური უსაფრთხოების ზომები, რომლებიც ადაპტირებული უნდა იყოს მსგავსი დამუშავებისას არსებულ რისკებთან იმგვარად, რომ პირის უფლებები და თავისუფლებები, ინტერესები დაცული იყოს.[240] სახის ამომცნობი სისტემების გამოყენების შეზღუდვა, აკრძალვა დამოკიდებული უნდა იყოს მის სახეზე და უფლებაში ჩარევის სავარაუდო ხარისხზე. ამასთან ერთად გათვალისწინებული უნდა იყოს, თუ რომელ სექტორში ხდება მისი გამოყენება.

მაგალითად, FRT-ის გამოყენება აკრძალული უნდა იყოს პიროვნების კანის ფერის, რასობრივი, ეთიკური კუთვნილების, მისი ასაკის, ჯანმრთელობის მდგომარეობის გამოსარკვევად, გარდა იმ შემთხვევისა, როდესაც შესაბამისი კანონმდებლობით მკაცრად განსაზღვრული საფუძველი არსებობს, და ამასთან ერთად გარანტირებულია და ყოველმხრივ აღმოფხვრილია პირის ნებისმიერი ნიშნით დისკრიმინაცია - რისი მიღწევაც ამ ეტაპზე ვფიქრობ, მით უმეტეს სტატისტიკას თუ დავეყრდნობით, შეუძლებელია.

ვფიქრობ FRT-ის ისეთი გამოყენება, რომელიც თავის მხრივ ორიენტირებულია ადამიანის ემოციის ამოცნობაზე აკრძალული უნდა იყოს. განსაკუთრებით კი ისეთ სფეროებში, როგორიც არის განათლება, პირთა დასაქმება და სხვა.

ზოგადად, სენსიტიური მონაცემების დამუშავების საფუძველი შეიძლება იყოს სუბიექტის თანხმობა, სახელმწიფო ან საზოგადოებრივი ინტერესი, რაც ჩვენს შემთხვევაში საქართველოს „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-6 მუხლში დეტალურად გვაქვს გაწერილი. სხვა ყველა დანარჩენ შემთხვევაში კი განსაკუთრებული კატეგორიის მონაცემთა დამუშავება აკრძალულია.

როდესაც სუბიექტის თანხმობაზე გვაქვს საუბარი, იგი აუცილებლად არ უნდა იყოს ბუნდოვანი და წერილობით ფორმით ან ელექტრონული ფორმით უნდა იყოს გამოხატული. ამასთან გასათვალისწინებელია რეკომენდაცია რომ სუბიექტის თანხმობა, მაშინ როდესაც მონაცემთა დამუშავებას ახდენს სახელმწიფო ორგანო, ან კერძო სექტორში მსგავს სიტუაციაში მყოფი პირი - ძალაუფლების დისბალანსიდან გამომდინარე, როგორც წესი, არ უნდა წარმოადგენდეს შესაბამის კანონიერ საფუძველს. საინტერესოა რა ხდება სოციალურ ქსელში განთავსებულ ფოტოსურათების შემთხვევაში. ისეთი ციფრული სურათები, რომლებიც ინტერნეტში, სოციალურ მედიაში ან რაიმე სხვა მსგავს ვებსაიტზეა განთავსებული, არ შეიძლება ჩაითვალოს კანონიერად იმ არგუმენტით თითქოსდა პიროვნებამ მისი ინფორმაცია საჯარო გახადა თავისივე სურვილით. გასათვალისწინებელია ის რომ ამ შემთხვევაში მის მიერ ფოტოსურათის გასაჯაროვების მიზანს, მისი შემდგომი FRT-ის სისტემით დამუშავება არ წარმოადგენდა და არც ვარაუდობს ამას. წინააღმდეგ

[240] Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data convention 108 - guidelines on facial recognition, t-pd(2020)03rev4, 28/01/2021, გვ. 4.

შემთხვევაში აქაც გვექნებოდა ისეთი სიტუაცია როდესაც პირი თავს იკავებს თავისი უფლების გამოყენებისგან - მასზე სავარაუდო „მეთვალყურეობის“ გამო, რაც ვფიქრობ ამ უფლების შეზღუდვას უტოლდება.

თუ სახის ამომცნობი სისტემების გამოყენება საჯარო სექტორის მიერ ხდება, მკაცრად უნდა განისაზღვროს მასზე უფლებამოსილი ორგანო, რომელიც აუცილებლად სახელმწიფოსა და საზოგადოების უსაფრთხოებაზე პასუხისმგებელი უნდა იყოს. აღნიშნულის განხორციელება კი ყოველ კონკრეტულ შემთხვევაში უნდა მოხდეს აუცილებლობისა და პროპორციულობის ტესტის გათვალისწინებით.

რაც შეეხება სხვა საჯარო დაწესებულებებს, იქნება ეს საავადმყოფოები, სკოლები თუ სხვა საჯარო სივრცეები, სადაც მიზნის მიღწევა უფლებათა ნაკლებად შემზღუდავი საშუალებებით არის შესაძლებელი, აკრძალული უნდა იყოს სახის ამომცნობი ტექნოლოგიის გამოყენება. აქ გავიხსენებდი შვედეთის შემთხვევას სადაც, ერთ-ერთ სკოლაში მოსწავლეთა დასწრების ჩასანიშნად FRT გამოიყენებოდა და მათ შორის მოსწავლეთა გადაადგილებასაც ასახავდა, რითიც მასწავლებლებს უადვილებდა საქმეს. აღნიშნული სკოლის მიმართ საქმე 2018 წელს აღიძრა და საბოლოოდ შვედეთში GDRP-ის ამოქმედებიდან პირველი პრეცენდენტი შეიქმნა სუბიექტის მონაცემთა უკანონო, არამართლზომიერი დამუშავებისა, რის გამოც შესაბამისი დაწესებულება ადგილობრივი უფლებამოსილი ორგანოს მიერ დაჯარიმდა.[241]

რაც შეეხება კერძო დაწესებულებებს, აქ განსხვავებით საჯარო სექტორისგან სენსიტიური მონაცემების დამუშავების საფუძველი შეიძლება იყოს მხოლოდ მონაცემთა სუბიექტის უშუალო თანხმობა, რომელიც მისი შესაბამისი ინფორმირებულობის და ნების თავისუფალი გამოხატვის შედეგადაა მიღებული. ამ შემთხვევაში განსაკუთრებული ყურადღება უნდა მიექცეს თანხმობის ხარისხს - რასაც ზემოთ უკვე ნაწილობრივ შევეხეთ. რაც შეეხება სხვა საჯარო სივრცეებს, როგორიცაა მაგალითად სავაჭრო ცენტრები,[242] მარკეტები და სახის ამომცნობი ტექნოლოგიების გამოყენება, იქნება ეს მარკეტინგის თუ უსაფრთხოების მიზნებისათვის არამართლზომიერია.

ნებისმიერ შემთხვევაში მიუხედავად იმისა სახის ამომცნობი სისტემების გამოყენება საჯარო თუ კერძო სექტორში მოხდება, მნიშვნელოვანია თანაბრად იყოს დაცული მონაცემთა დამუშავების პრინციპები. წინააღმდეგ შემთხვევაში თუნდაც აღნიშნული სისტემების გამოყენება კანონიერ საფუძველზე ხდებოდეს იგი არალეგალურად ჩაითვლება.

მონაცემთა დამუშავება უნდა იყოს კანონიერი, სამართლიანი, გამჭირვალე (რაც მის მიმართ ნდობასაც განაპირობებს, მნიშვნელოვანია სუბიექტმა იცოდეს მისი ინფორმაციის დამუშავების შესახებ, ასევე ვის მიუწვდება ხელი ინფორმაციაზე და რისთვის გამოიყენება იგი), ამასთან ერთად მისი ლეგიტიმური მიზანი უნდა იყოს მკაფიო და კონკრეტული, დამმუშავებელი კი შეზღუდული უნდა იყოს კონკრეტულ მონაცემთა დამუშავების თავდაპირველი მიზნით და სხვა შემთხვევაში მისი გამოყენება არ უნდა შეეძლოს, ასევე მნიშვნელოვანია მინიმიზაციის პრინციპის დაცვა, რაც

[241] Facial recognition: School ID checks lead to GDPR fine, BBC NEWS, ხელმისაწვდომია: https://bbc.in/3mBoUIe წვდომის თარიღი: 26.08.2021.

[242] Esther Fung , “Shopping Centers Exploring Facial Recognition in Brave New World of Retail “, The Wallstreet Journal.

უზრუნველყოფს სუბიექტის მონაცემების მხოლოდ იმ მინიმალური მოცულობით დამუშავებას, რაც მიზნის მიღწევისთვისაა საჭირო. ამასთან ერთად უზრუნველყოფილი უნდა იყოს დამმუშავებლის მიერ მონაცემთა სიზუსტე და სანდოობა და სუბიექტს უნდა მიეცეს შესაძლებლობა მოითხოვოს მის შესახებ არსებული არაზუსტი მონაცემების შესწორება ან წაშლა. გარდა ამისა, ასევე კრიტიკულად მნიშვნელოვანია მონაცემთა დამუშავების ვადა (იგი უნდა შემოიფარგლებოდეს მიზნის მიღწევისათვის აუცილებელი პერიოდით), რაზეც ზემოთაც გვქონდა საუბარი. ასევე დაუშვებელია მონაცემების რაიმე ფორმით მესამე პირთათვის უნებართვოდ გამჟღავნება.

მონაცემთა დამუშავებისას არანაკლებ მნიშვნელოვანია სუბიექტის ინფორმირებულობა, პროცესის გამჭირვალობა. წინააღმდეგ შემთხვევაში სახეზე გვექნება არამხოლოდ პერსონალურ მონაცემთა დაცვის უფლების, არამედ მათ შორის ინფორმაციული თვითგამორკვევის, ცალკეულ შემთხვევებში სამართლიანი ადმინისტრაციული წარმოების, სამართლებრივი დაცვის ქმედითი საშუალების უფლების შეზღუდვა - ვინაიდან პირის პირადი მონაცემების დამუშავება მოხდება მისი ინფორმირების გარეშე, რაზეც მას ზემოქმედების საშუალება არ ექნება და ვერ შეძლებს მისთვის არასასურველი ქმედებების აღკვეთას, არ ექნება მასზე არსებული ინფორმაციის ხელმისაწვდომობა, ვერ შეძლებს უკანონო ქმედებებზე შესაბამისად რეაგირებას, რაც ფაქტობრივად ზემოთ აღნიშნული უფლებების შეზღუდვას უტოლდება.

3. დასკვნა

დღევანდელი საზოგადოება მართლაც ციფრული ტექნოლოგიების ეპოქაში ცხოვრობს და რაც უფრო დრო გადის ეს უკანასკნელი უფრო დიდი ტემპით მიდის წინ. მსგავსი ევოლუციის პირობებში კი გარდაუვალია თითოეული ჩვენგანის უფლებებზე გავლენის ქონა, შესაბამისად, მათი ხელშეუხებლობის რისკიც იზრდება - რაც თავისთავად მოიაზრებს სახის ამომცნობ სისტემებსაც, რომლებსაც როგორც ნაშრომში გავეცანით ბევრი დადებითი შედეგი მოაქვს საზოგადოების, სახელმწიფოს უსაფრთხოების, დანაშაულის თავიდან აღკვეთისა და ცალკეული პროცესების გამარტივებაში, თუმცა სასწორის მეორე პინაზე დგას ადამიანის უფლებათა დიდი ნაწილი, მათ შორის აღნიშნული ნაშრომის თემა - პერსონალური მონაცემები, რომლებსაც უზარმაზარი ზიანი შეიძლება მიადგეს FRT-ის გამოყენებისას. როგორც უკვე აღვნიშნე, ადამიანის უფლებათა დიდი ნაწილი არაა აბსოლუტური, მათ შორის არც პერსონალური მონაცემების დაცვა. აღნიშნული „დახურული კარის“ გადალახვა კი შესაძლებელია - უფლებამოსილი ორგანოს მიერ, კანონიერი საფუძვლით, ლეგიტიმური მიზნის მისაღწევად, ჩარევის პროპორციულობისა და აუცილებლობის შემთხვევაში - ისე როგორც დემოკრატიულ საზოგადოებაშია მისაღები. ამასთან ერთად, ყოველგვარი გამონაკლისის გარეშე სახის ამომცნობი სისტემების საშუალებით მონაცემთა დამუშავებისას აუცილებლად დაცული უნდა იყოს კანონმდებლობით განმტკიცებული პრინციპები.

რაც შეეხება საქართველოს, მართალია, ჩვენთან ჯერ კიდევ არ არის ფართოდ შემოსული სახის ამომცნობი სისტემები, თუმცა ვფიქრობ იმისათვის, რომ მომავალში პირის პერსონალური მონაცემების ამ გზით დარღვევის პრეცენდენტები ავიცილოთ თავიდან, კარგი იქნებოდა ევროკომისიის ნაშრომში წარდგენილი რეკომენდაციების გათვალისწინება და ამასთან ერთად როგორც საჯარო, ისე კერძო სექტორის ინფორმირებულობის გაზრდა აღნიშნულ საკითხთან დაკავშირებით.

პერსონალური მონაცემების დამუშავება მედია საშუალებების მიერ

ავტორი: მარიამ კახიძე [243]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

მედია საშუალებები ინფორმაციის მიღების ყველაზე სწრაფ და გავრცელებულ საშუალებას წარმოადგენს. თუმცა ხშირად მაღალი რეიტინგისა თუ ექსკლუზიური კადრების გავრცელების მიზნით, მედია საშუალებები სცდებიან პერსონალურ მონაცემთა დამუშავების კანონიერ ფარგლებს და მათ ინტერესებს მოქალაქეთა პერსონალური მონაცემების უსაფრთხოება ეწირება. ეს თემა საზღვარგარეთის ქვეყნებში დიდი ხნის წინ მოექცა ყურადღების ქვეშ, ხოლო საქართველოში განსაკუთრებით ბოლო წლებში გახდა აქტუალური.

ხშირდება მედიის მხრიდან მოქალაქეთა პირადი ცხოვრების შესახებ ინფორმაციის გავრცელების ფაქტები, რაც ზოგჯერ სცდება კანონის ფარგლებს. ბოლო პერიოდში ვხედავთ ტელევიზიების მხრიდან არასრულწლოვანთა თუ ზრდასრულთა პერსონალური მონაცემების გამჟღავნების შემთხვევებს, რაც შემაშფოთებელია.

ამ მხრივ მხოლოდ ტელევიზიებზე არ უნდა გაკეთდეს აქცენტი, აღსანიშნავია ასევე სხვა სახის მედია საშუალებები. სოციალური მედია საშუალებები ხშირად ამუშავებენ მომხმარებელთა პერსონალურ მონაცემებს, ეს კი ზოგჯერ იწვევეს არა მარტო ამ მოქალაქეთა უფლებების დარღვევას, ასევე შესაძლოა გამოიწვიოს სხვა მძიმე შედეგები. მაგალითისთვის, სოციალური ქსელების მიერ შეგროვებული ინფორმაცია 2016 წელს რუსეთმა გამოიყენა აშშ-ს საპრეზიდენტო არჩევნებში ჩარევისთვის. ეს საკითხი 2020 წელსაც კვლავ აქტუალური გახდა, მათ შორის, COVID- 19-თან ბროლის მიმართულებით.

მედია საშუალებები ხშირად ნაკლები ყურადღებით ეპყრობიან პერსონალური მონაცემების გავრცელებისას მის სისწორეს მომხმარებელთა მოსაზიდად. მიუხედავად იმისა, რომ გარკვეულ შემთხვევებში განსაკუთრებული საჯარო ინტერესი არსებობს ზოგიერთი სახის პერსონალური ინფორმაციის მიმართ, მნიშვნელოვანია რომ ბალანსი იქნას დაცული.

ავტორის მიზანია განიხილოს ყველა ზემოთ აღნიშნული საკითხი, მედიის მხრიდან პერსონალურ მონაცემთა დამუშავების სახეები, დასაშვებობა, ფარგლები და რისკები, მიმოიხილოს საქართველოს რეალობა საზღვარგარეთის ქვეყნების პრაქტიკასთან შედარებით-სამართლებრივ კონტექსტში, ყურადღება გაამახვილოს მთავარ გამოწვევებზე და შეიმუშაოს პრობლემათა გადაჭრის სავარაუდო გზები.

[243] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნინო ჯავახიშვილი.

2. პერსონალური მონაცემები და მათი მნიშვნელობა

პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომლითაც ფიზიკური ან იურიდიული პირის იდენტიფიცირება არის შესაძლებელი. პერსონალური მონაცემებია მაგალითად: სახელი და გვარი, პირადი ნომერი, ფოტო, ვიდეოგამოსახულება, თითის ანაბეჭდი, მისამართი, ადგილმდებარეობა, ტელეფონის ნომერი, IP მისამართი. აღნიშნული ჩამონათვალი ამომწურავი არ არის და ის შესაძლოა, გაფართოვდეს.

პერსონალური ინფორმაციის ამომწურავი დეფინიციას ვერ გვთავაზობს საერთაშორისო და ეროვნული კანონმდებლობა. მონაცემი „პერსონალური“ ხდება მაშინ, როდესაც კავშირშია კონკრეტულ პიროვნებასთან, ინდივიდთან და გადმოსცემს რაიმეს მის შესახებ.[244] ამ მხრივ მნიშვნელოვანია იდენტიფიცირების საკითხი. ინდივიდის ვინაობის დადგენა შეიძლება მაშინ, როდესაც ინფორმაცია შეიცავს პირის იდენტიფიცირების დამდგენ ელემენტებს.[245]

პერსონალურ მონაცემთა ცნება საერთაშორისო სამართლებრივი რეგულირებით პირველად შემოთავაზებული იქნა „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ ევროპის საბჭოს კონვენციით,[246] რომლის მიხედვითაც პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომელიც შეეხება განსაზღვრულ ან განმსაზღვრელ პირს.[247] მოგვიანებით, პერსონალურ მონაცემთა უფრო ფართო დეფინიცია დამკვიდრდა, რომელიც მოცემული იყო ევროპის კავშირის 95/46/EC დირექტივაში.[248] თუმცა, ეს დირექტივა 2018 წლის 26 მაისს ძალადაკარგულად გამოცხადდა და ძალაში შევიდა ევროპული კავშირის ფარგლებში მონაცემთა დაცვის ზოგადი რეგულაცია.[249] რეგულაციის მიხედვით პერსონალურ მონაცემთა შემდეგნაირი დეფინიცია ჩამოყალიბდა: პერსონალური მონაცემი ნიშნავს ნებისმიერ ინფორმაციას, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, თუ მისი ვინაობის დადგენა შეიძლება პირდაპირ ან არაპირდაპირ, კერძოდ ისეთი იდენტიფიკატორებით, როგორიც არის სახელი, საიდენტიფიკაციო ინფორმაცია, ადგილმდებარეობის მონაცემი, ონლაინ იდენტიფიკატორი ან ერთი ან მეტი ფაქტორით, რომელიც უკავშირდება ფიზიკურ, ფიზიოლოგიურ, გენეტიკურ, ფსიქოლოგიურ, ეკონომიკურ, კულტურულ ან ფიზიკური პირის სოციალურ კუთვნილებას.[250]

[244] კ. გოგშაძე, პერსონალურ მონაცემთა დაცვის ძირითადი უფლება, გამომცემლობა „იურისტების სამყარო“, 2020, გვ. 43.

[245] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018 წლის გამოცემა, ლუქსემბურგი, ევროკავშირის საგამომცემლო სახლი, 2018, ISBN 978-9941-9658-9-0, გვ. 24.

[246] პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, ევროპის საბჭო, CETS No. 108, 28 იანვარი, 1981.

[247] მუხლი 2, პარაგრაფი „ა“, პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ, ევროპის საბჭო, CETS No. 108, 28 იანვარი, 1981.

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

[249] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation).

[250] იქვე, Art. 4.

მონაცემების ღირებულება როგორც კერძო, ისე საჯარო ორგანიზაციებისთვის, შეუფასებელია. პერსონალურ მონაცემებს 21-ე საუკუნის ნავთობსაც კი უწოდებენ, რადგან მიიჩნევა, რომ თანამედროვე ტექნოლოგიები პერსონალურ მონაცემებს ადამიანებისთვის სწრაფი, ეფექტიანი და ეკონომიური მომსახურების შესათავაზებლად საწვავივით იყენებენ. განსაკუთრებულად დიდი რაოდენობის მონაცემებს სახელმწიფო აგროვებს და იყენებს. ეს გამოწვეულია სხვადასხვა კანონიერი მიზნით, დანაშაულის გახსნის თუ აღკვეთის მიზნით სახელმწიფოს მოქმედების ფარგლები კიდევ უფრო იზრდება. თუმცა, აღსანიშნავია, რომ რაც უფრო მეტი მონაცემია სახელმწიფოს ან კერძო კომპანიის ხელში, მით უფრო მაღალია ამ მონაცემების ბოროტად გამოყენების რისკი. შესაბამისად, საჭიროა პერსონალური მონაცემების დამუშავებისას განსაკუთრებული ყურადღება იქნას გამახვილები უსაფრთხოების ზომებზე. პერსონალური მონაცემების უკანონოდ გამჟღავნებამ შესაძლოა გამოიწვიოს როგორც ფინანსური, ასევე მორალური ზიანი.

3. მედიის მხრიდან პერსონალური მონაცემების დამუშავება

პერსონალურ მონაცემთა დაცვის საკითხი ბოლო წლებში მედიის თავისუფლებასთან სულ უფრო მჭიდროდ არის დაკავშირებული. მნიშვნელოვანია, ზუსტად დადგინდეს თუ რას გულისხმობს უშუალოდ მედიის მიერ პირის პერსონალური მონაცემების დამუშავება.

პერსონალური მონაცემების დამუშავების შემდეგი ძირითადი სახეები არსებობს: ავტომატური, არაავტომატური და ნახევრად ავტომატური.

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.

მედია საშუალებები იყენებენ მონაცემთა დამუშავების ყველა ზემოთ ჩამოთვლილ ხერხებს. „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი მონაცემთა ავტომატური დამუშავებას განმარტავს მონაცემთა ინფორმაციული ტექნოლოგიების მეშვეობით დამუშავებად.[251] კანონი არ აიდენტიფიცირებს მონაცემთა ინფორმაციული 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.[252] მედია საშუალებები ხშირად სწორედ რომ ჟურნალისტური გამოძიების და დანაშაულის თავიდან აცილების მიზნით ელექტრონული საშუალებებით ინფორმაციის დამუშავების ხერხს იყენებენ, გან-

[251] მუხლი 3, პუნქტი 1-ლი, საქართველოს კანონი ,პერსონალურ მონაცემთა დაცვის შესახებ“, 28 დეკემბერი, 2011

[252] იქვე, მუხლი 3, პუნქტი 1-ლი.

საკუთრებით მაშინ როცა საკითხის მიმართ არსებობს მაღალი საზოგადოებრივი ინტერესი. მიუხედავად იმისა, რომ მონაცემთა აარავტომატური საშუალებით დამუშავება ნაკლებად აქტუალურ და გამოყენებად ხერხს წარმოადგენს, ის კანონმდებლის მიერ მაინც რეგულირებულია პრობლემების თავიდან არიდების მიზნით, რადგან ზოგჯერ მსგავსი საშუალებებიც გამოიყენება. არაავტომატური საშუალებით მონაცემების დამუშავება გულისხმობს ხელით წერია მეშვეობით ხელნაწერი „ფაილების“ შექმნას.[253] საქართველოში არაავტომატური საშუალებებით მონაცემთა დამუშავების განხორციელების შეტყობინება მაკონტროლებელი ორგანოსადმი, პრაქტიკაში დამკვიდრებული არ არის, ამ მხრივ კარგი იქნება თუკი ქართული კანონმდებლობა გაითვალიწინებს დირექტივა 95/46/EC[254]-ის შესაბამის წესს, რომლის მიხედვითაც ყველა მონაცემის, მათ შორის პირადი მონაცემების დამუშავების შესახებ უნდა ეცნობოს საზედამხედველო ორგანოს გამარტივებული წესით, ვინაიდან თუკი ავტომატური წესით მონაცემთა დამუშავებისას, თანამედროვე ტექნოლოგიების დახმარებით მარტივია იმის გარკვევა, თუ ვინ გამოიყენა, გადასცა ან თუნდაც ნახა ინფორმაცია, ხელით დამუშავების შემთხვევაში, აღნიშნულის გარკვევა თითქმის შეუძლებელია და დიდ სირთულეებთანაა დაკავშირებული.[255] მედიის მიერ ამ ხერხის გამოყენებისას პროცესები ინფორმაციის კანონიერ ფარგლებში დამუშავების საკითხი კიდევ უფრო რთულდება. ვინაიდან ხშირად მედიის მხრიდან ხდება სხვადასხვა სახის ინფორმაციის მათ შორის არაავტომატური საშუალებით დამუშავება, ჟურნალისტები ზოგჯერ არაოფიციალური წყაროდან იღებენ ინფორმაციას, ეს წყარო ხშირად კონფიდენციალურია, ხშირია ასეთ დროს გადაუმოწმებელი, არასწორი ინფორმაციის გავრცელების რისკებიც და არაავტომატური საშუალებებით ინფორმაციის დამუშავებისას ეს რისკები განსაკუთრებით მაღალია, ვინაიდან ფაქტობრივად წარმოუდგენელია ასეთ შემთხვევაში იმ პირის მოძიება, ვინც გაავრცელა, გამოიყენა და გადასცა ინფორმაცია. ეს კი გარკვეულწილად არამართლზომიერი მიზნების მქონე პირებისთვის წარმოადგენს შენიღბვის და კანონსაწინააღმდეგო ქმედებისთვის პასუხისმგებლობისგან თავის არიდების საფუძველს. ასეთი საშუალებებით მოპოვებული არასწორი ინფორმაცია შესაძლოა მძიმე სოციალური, ეკონომიკური თუ პოლიტიკური შედეგების გამომწვევი აღმოჩნდეს საზოგადოებისთვის.

ნახევრად-ავტომატური საშუალებებით ინფორმაციის დამუშავება გულისხმობს ერთდროულად ინფორმაციული ტექნოლოგიებისა და არაავტომატური საშუალებებით მონაცემთა დამუშავებას. ასეთ დროს მედიის მხრიდან შეცდომის დაშვების საფრთხე მაღალია. ვინაიდან, როდესაც ერთდროულად ავტომატურად და არაავტომატურად მუშავდება სხვადასხვა ტიპის ინფორმაცია, აქ უკვე წარმოიშობა დამუშავებულ მონაცემებზე კონტროლის პრობლემა. შესაძლებელია მონაცემთა არაავტომატური საშუალებით ისეთი ინფორმაცია დამუშავდეს, რისი დამუშავებაც მსგავსი სახით

[253] თ. არჩუაძე, პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 0178, 2016, გვ. 27, ხელმისაწვდომია: https://bit.ly/38ebJ7w წვდომის თარიღი: 05.07.2021. Büllesbach A., Concise European IT Law, USA, Kluwer Law International, 2010, გვ. 94.

[254] ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის № 95/46/EC დირექტივა პერსონალურ მონაცემთა დამუშავებასა და აღნიშნულ მონაცემთა თავისუფლად მოძრაობასთან დაკავშირებით ფიზიკური პირების უფლებების დაცვის შესახებ, 11 მარტი, 2015.

[255] თ. არჩუაძე, პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 2016, გვ. 28, ხელმისაწვდომია: https://bit.ly/38ebJ7w წვდომის თარიღი: 05.07.2021.

დაუშვებელია და მიზნად ისახავს კანონის გვერდის ავლას. ასეთი ქმედების მიზანი ხშირად მედია წარმომადგენლებისთვის მონაცემების სწრაფად მოპოვება, ექსკლუზიური ინფორმაციის გავრცელება და მომხმარებელთა რაოდენობის გაზრდა მაღალი კონკურენციის პირობებში.[256]

რაც შეეხება მედიის მხრიდან მონაცემთა დამუშავების წინაპირობებს, იგი განსხვავებულია სხვადასხვა სახის პერსონალური მონაცემისთვის. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება მონაცემთა სუბიექტის თანხმობის გარეშე აკრძალულია, ასეთი ტიპის მონაცემთა დამუშავების ლეგიტიმურ საფუძველს წარმოადგენს 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.[257] აღსანიშნავია, რომ ამ ინფორმაციათა გამოყენების საჭიროება აუცილებელი უნდა იყოს კონკრეტული მიზნის მისაღწევად, სხვა შემთხვევაში მონაცემთა დამმუშავებელს დამუშავების შესაძლებლობა არ უნდა გააჩნდეს. ასევე, გათვალისწინებულია სპეციალური წესები ბიომეტრიული მონაცემების დამუშავების, გარდაცვლილი პირის მონაცემთა დამუშავების, მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის დამუშავების, ვიდეოთვალთვალის მეშვეობით პერსონალურ მონაცემთა დამუშავების მიზნით. ვიდეოთვალთვალის განხორციელების ზოგადი მიზნებია: დანაშაულის თავიდან აცილება, პირის უსაფრთხოებისა და საკუთრების დაცვა, საზოგადოებრივი წესრიგისა და არასრულწლოვანის მავნე ზეგავლენისგან დაცვა, საიდუმლო ინფორმაციის გამჟღავნებისგან დაცვა. მედიასაშუალებები ზოგჯერ ამ ხერხს მიმართავენ კანონიერი მიზნების დასაცავად. მაგალითისთვის, 2002 წლის სექტემბერში, მილიონობით ადამიანმა საინფორმაციო პროგრამების მეშვეობით ნახა „კოლის“ ავტოსადგომის ვიდეოჩანაწერი, თუ როგორ სცემდა მადელინ თაგუდი, 25 წლის დედა, საკუთარ ქალიშვილს ავტომობილის უკანა სავარძელზე.[258] თუმცა ვიდეოთვალთვალის მეშვეობით მონაცემთა დამუშავება, როგორც წესი, მედიის კომპეტენციაში არ შედის, რადგან ეს სამართალდამცველების კომპეტენციას მიეკუთვნება. მაგრამ, ჟურნალისტური გამოძიებისას გარკვეულ შემთხვევებში სამართალდამცავ ორგანოთა თანხმობის საფუძველზე შესაძლებელია მედიას მიეცეს ვიდეოთვალთვალის უფლება. თუმცა ამ დროს რთულია ბალანსის დაცვა, რომ მედიამ არაკანონიერი მიზნებისთვის არ გამოიყენოს ეს უფლება. ფარული კამერების გამოყენებისას მედიამ უნდა დაიცვას შემდეგი პრინციპები: 1) საკითხი ხელს უწყობს საზოგადოებრივ დებატებს, 2) გაშუქება არ არის მიმართული პიროვნებაზე, არამედ მის ერთ-ერთ პროფესიულ ასპექტზე, 3)პირის სახე და ხმა არის დაფარული/შეცვლილი და დ) ინტერვიუ არ ტარდება ჩვეულ საქმიან გარემოში.[259]

ჟურნალისტებმა თავი უნდა შეიკავონ სათვალთვალო კამერის მეშვეობით გადაღებული კადრების გამოქვეყნებისაგან, სადაც ასახული არიან კერძო პირები, გამოსახულების დაფარვის გარეშე, თუ ინფორმაცია არ უწყობს ხელს საზოგადოებრივი ინტერესის საგნის გარშემო მსჯელობას. საქმე

[256] საქართველოს კანონი ,პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 3, პუნქტი 1-ლი.

[257] იქვე, მუხლი 6.

[258] თ. არჩუაძე, პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 0178, 2016, გვ. 38, ხელმისაწვდომია: https://bit.ly/38ebJ7w წვდომის თარიღი: 05.07.2021.

[259] L. K. Perenic, Media and the Protection of Personal Data, information Commissioner of the Republic of Slovenia, გვ. 11-34, ხელმისაწვდომია: https://bit.ly/3mBJKXY წვდომის თარიღი: 05.07.2021.

Peck V. United Kingdom ეხებოდა კერძო პირის (რომელიც იტანჯებოდა დეპრესიით, თუმცა სისხლის სამართლის დანაშაულის ჩადენისთვის მას ჯერ არ ჰქონდა წაყენებული ბრალი) კადრების ჩაწერას, როდესაც იგი ქუჩაში მიდიოდა სამზარეულოს დანით ხელში და შემდგომ სცადა ვენების გადაჭრა. ეს შემთხვევა ჩაითვალა პერსონალური მონაცემების დარღვევად.

საყურადღებოა გარდაცვლილი პირის პერსონალური ინფორმაციის დამუშავების წესები.[260] ამ მხრივ მედიის საქმიანობა განსაკუთრებულ ყურადღებას იმსახურებს, ვინაიდან გარკვეულ შემთხვევებში, მედიის არასწორმა ქმედებამ და კანონიერი ფარგლების გადაცდომამ შესაძლოა გამოიწვიოს პატივის და ღირსების უფლების შელახვა. მაგალითისთვის, ამ მხრივ საყურადღებო გახლდათ თამარ ბაჩალიაშვილის საქმე, რომლის პირადი ცხოვრების დეტალებსაც მედია გადმოსცემდა. როგორც სამართალდამცავი უწყებები, ასევე არასამათავრობო ორგანიზაციები მოუწოდებდნენ მედიას განსაკუთრებული სიფრთხილე გამოეჩინათ და განუხრელად დაეცვათ პირადი ცხოვრების დაცვის სტანდარტი. ერთ-ერთი მედია საშუალების წამყვანის მიერ დასმული კითხვები, ისევე როგორც ზოგიერთი სხვა მედიასაშუალების მიერ მომზადებული მასალა, შეეხებოდა გარდაცვლილი თამარ ბაჩალიაშვილის პირადი ინტიმური ურთიერთობების დეტალებს, რაც, ერთი მხრივ, თავად გარდაცვლილის, ხოლო მეორე მხრივ, მისი მეგობრების პირადი ცხოვრების უფლებაში უხეშ ჩარევას წარმოადგენდა. მიუხედავად იმისა, რომ არსებობდა საქმის მიმართ მაღალი საზოგადოებრივი ინტერესი და აღსანიშნავი იყო მედიის განსაკუთრებული როლი, გაეკონტროლებინა საჯარო ხელისუფლება, პირის პერსონალური მონაცემების დარღვევა ამ მიზნებით ვერ იქნებოდა გამართლებული. ამ საკითხთან დაკავშირებით საინტერესოა როგორც ეროვნული, ისე საერთაშორისო სტანდარტების მიმოხილვა. საქართველოს საკონსტიტუციო სასამართლო აღიარებს გარდაცვლილი პირის მშობლების კონსტიტუციურ უფლებას, იდავონ გარდაცვლილი შვილის შესახებ გავრცელებული ინფორმაციის თაობაზე, როდესაც აღნიშნული ინფორმაცია, ამავდროულად არღვევს მათ პირად უფლებებს.[261]

4. მედიის მიერ პერსონალურ მონაცემთა დამუშავების საკითხის შედარებით-სამართლებრივი მიმოხილვა

ევროპის ადამიანის უფლებათა სასამართლოს პრაქტიკის თანახმად, კონვენციის მე-8 მუხლით დაცული პირადი ცხოვრების უფლების გარანტიები ვრცელდება ასევე გარდაცვლილ პირებსა[262] და მათი ოჯახის წევრებზე.[263] მაგალითისთვის, ევროპის ადამიანის უფლებათა სასამართლომ საქმეზე Plon v. France (№58148/00) მიიჩნია, რომ საფრანგეთის ყოფილი პრეზიდენტის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გამოქვეყნების გამო ჟურნალისტისთვის პასუხისმგებლობის დაკისრება ემსახურებოდა გარდაცვლილის პატივის, რეპუტაციისა და პირადი ცხოვრების

[260] Journalism and the use of information from social media, Information for the public, IPSO, გვ. 5, ხელმისაწვდომია: https://bit.ly/3kruIRR წვდომის თარიღი: 04.07.2021.

[261] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე №1/6/561,568 „საქართველოს მოქალაქე იური ვაზაგაშვილი საქართველოს პარლამენტის წინააღმდეგ“, 2016 წლის 30 სექტემბერი, პარ. 33.

[262] S. Makhija, Privacy & Media Law, ხელმისაწვდომია: https://bit.ly/38iY9jv წვდომის თარიღი: 05.07.2021.

[263] Putistin v Ukraine No. 16882/03, 21.11.13, §33-40.

დაცვის ლეგიტიმურ მიზანს. ასევე, საქმეზე Almeida Leitão Bento Fernandes v. Portugal (№ 25790/11, 12 მარტი, 2015 წ.), ევროპის ადამიანის უფლებათა სასამართლომ დაადგინა, რომ გარდაცვლილი არასაჯარო პირების პირადი ცხოვრების დეტალების გამოქვეყნება სცდებოდა ავტორის გამოხატვის თავისუფლებით დადგენილ ფარგლებს.

მნიშვნელოვანია საზღვარგარეთის ქვეყნების საკანონმდებლო რეგულირების შესწავლა.[264] კანადის ფედერალური კანონის, „პერსონალურ მონაცემთა დაცვისა და ელექტრონული დოკუმენტბრუნვის შესახებ აქტის“ მიხედვით ინდივიდის მონაცემები უნდა იქნეს დამუშავებისგან დაცული მისი გარდაცვალებიდან 20 წლის განმავლობაში, ან ამ დოკუმენტის შექმნიდან 100 წლის განმავლობაში. ესტონეთის „პერსონალურ მონაცემთა დავის აქტის“ შესაბამისად „მგრძნობიარე პერსონალური მონაცემების შემცველი ინფორმაციის გაცემაზე შეზღუდვა მოქმედებს დოკუმენტების მიღებიდან 75 წლის განმავლობაში ან პირის გარდაცვალებიდან 30 წლის განმავლობაში, გერმანიაში მეფისტოსა და მარლენ დიტრიხის საქმეებზე, სასამართლოებმა გარდაცვლილ პირს მიანიჭეს პირადი (ღირსება, პირადი ცხოვრება) და კომერციული (სახელის გამოყენების უფლება, ხმა, ფინანსური მოგების მიზნით იმიჯის გამოყენების უფლება) ინტერესების დაცვის უფლება. თუმცა არსებობენ სახელმწიფოები, რომლებიც არ აღიარებენ გარდაცვლილი პიროვნების უფლებას პერსონალურ მონაცემთა დაცვაზე და ამ უფლების განხორციელებას უკავშირებენ მხოლოდ ადამიანის სიცოცხლეს. მაგალითად საფრანგეთის საკასაციო სასამართლომ საქმეზე SA Editions Plon v. Mitterand მიიჩნია, რომ პირადი ცხოვრების უფლების პატივისცემა უჩინარი ხდება, როდესაც პიროვნება, რომლის შესახებაც საუბარია, უფლების ერთადერთი მფლობელი, კვდება“.[265]

5. მედიის მხრიდან პერსონალური მონაცემების დამუშავება საქართველოში: კანონმდებლობა და პრაქტიკა

მედიის მხრიდან პერსონალური მონაცემების დამუშავების საკითხი ქართულ კანონმდებლობაში მეტნაკლებად მოწესრიგებულია. მაუწყებელთა ქცევის კოდექსის მე-10 თავი ადგენს წესებს, რომლებიც მაუწყებლებმა პირად მონაცემებთან დაკავშირებით უნდა დაიცვან. კერძოდ, 35-ე მუხლის თანახმად, გარდა იმ შემთხვევისა, როდესაც არსებობს საზოგადოებრივი ინტერესი, მაუწყებელმა არ უნდა გაამჟღავნოს ინფორმაცია პირის საცხოვრებელი ადგილის, ტელეფონის ნომრის, ფოსტის, სხვა პირადი საკონტაქტო მონაცემების შესახებ.

ჟურნალისტის მიერ, პირის ნებართვის გარეშე, მისი პირადი ცხოვრების ხელშეუხებლობის უფლებაში ჩარევის შედეგად მოპოვებული ინფორმაცია ჩაითვლება პერსონალურ მონაცემად, გარდა გამონაკლისი შემთხვევებისა, როდესაც საჯარო ინტერესი გადასწონის პირადი ინფორმაციის დაცვის ვალდებულებას. კოდექსის მე-10 თავი ადგენს დეტალურ წესებს, რომლებიც ჟურნალისტებმა ინფორმაციის გაშუქებისას უნდა დაიცვან. ეს წესები შეეხება: საჯარო თავშეყრის ად-

[264] Journalism, The Arts and Data Protection:the Potential Reach of the Privacy Act, გვ. 1-3, ხელმისაწვდომია: https://bit.ly/3sR0tYd წვდომის თარიღი: 05.07.2021.

[265] თ. არჩუაძე, პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 0178, 2016, გვ. 33, ხელმისაწვდომია: https://bit.ly/38ebJ7w წვდომის თარიღი: 05.07.2021.

გილებში გადაღებული ისეთი კადრების გამოყენებას, რომელიც პერსონალური მონაცემების მატარებელია; სკოლებში, საჯარო და კერძო დაწესებულების ტერიტორიაზე გადაღებული კადრების გამოყენებას; სატელეფონო საუბრის ჩანაწერის გამოყენებას; გარდაცვლილი პირის, დაზარალებულის ან ძალადობის მსხვერპლის იდენტიფიცირებას; არასრულწლოვანის იდენტიფიცირებას; ეჭვმიტანილის იდენტიფიცირებას; სექსუალური ძალადობის მსხვერპლის იდენტიფიცირება.

ყველა ზემოთჩამოთვლილ შემთხვევაში გამონაკლისი პერსონალური მონაცემების უნებართვოდ გამოყენებაზე მაშინ არის დასაშვები, როდესაც არსებობს მაღალი საზოგადოებრივი ინტერესი და საზოგადოების ლეგიტიმური ინტერესი უპირატესი სიკეთეა.

განსაკუთრებით ხაზგასასმელია „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მე-3 მუხლის მე-4 პუნქტი, რომლის მიხედვითაც ამ კანონის (გარდა მე-17 მუხლისა) მოქმედება არ ვრცელდება მონაცემთა მედიასაშუალებების მიერ საზოგადოების ინფორმირების მიზნით დამუშავებაზე, აგრეთვე მონაცემთა სახელოვნებო და ლიტერატურული მიზნებისათვის დამუშავებაზე. მიუხედავად იმისა, რომ მე-17 მუხლი აწესრიგებს მონაცემთა დამუშავების წესებსა და პირობებს, აღნიშნული პუნქტი (მე-3 მუხლის მე-4 პუნქტი) შესაძლოა გახდეს პასუხისმგებლობისგან თავის აცილების საშუალება. იმ რისკებს შორის ბალანსი, რომელიც მე-17 მუხლშია ნახსენები, შესაძლოა ვერ იქნას დაცული დამმუშავებლის მიერ ყოველ კონკრეტულ შემთხვევაში და საზოგადოების ინფორმირების მიზნით მედიის მიერ განხორციელებული ქმედებები იყოს გაუმართლებელი პერსონალური მონაცემების დაცვის კუთხით. აღნიშნული მუხლი ღიად ტოვებს საკითხს, თუ რა ხდება მაშინ, როდესაც მედიასაშუალებები საზოგადოების ინფორმირების მიზნით პერსონალური მონაცემების დამუშავებისას არღვევენ პირის პერსონალურ მონაცემებს.

6. მაღალი საზოგადოებრივი ინტერესისა და პერსონალური მონაცემების დაცვის დილემა

მედიის მიერ პირის პერსონალური მონაცემების დამუშავება და გამჟღავნება ყოველთვის ვერ იქნება გამართლებული საზოგადოებრივი ინტერესით. მაგალითისთვის, კემპბელის საქმეში მოსარჩელე ასაჩივრებდა მის პირად სივრცეში ჩარევას. პრესის მიერ გამოქვეყნებული სტატიებითა და ფოტოებით, რომელიც ეხებოდა საჯარო პირის ჯანმრთელობის საკითხებს, ირკვეოდა, რომ თითქოს ის იყო ნარკოტიკების მომხმარებელი. ეს ფაქტი ექსპერტიზის მიერ არ იქნა დადასტურებული. კემპბელმა მოიგო შიდასასამართლო ინსტანციები, რადგან დადგინდა რომ მოსარჩელის შესახებ პერსონალური მონაცემები არამართლზომიერად იქნა გამჟღავნებული.[266]

პირადი ცხოვრების ხელშეუხებლობის შესახებ იყო დავა 2010 წელს ვახტანგ კომახიძესა და ტელეკომპანია „რეალ TV“-ის შორის, როგორც მოსარჩელე აცხადებდა, ტელევიზიამ მის

[266] გაერთიანებული სამეფოს ლორდთა პალატის გადაწყვეტილება „კემპბელი გაერთიანებული სამეფოს წინააღმდეგ“, 6 მაისი, 2006.

პერსონალური ინფორმაცია გადაუმოწმებლად, არასწორი სახით გაავრცელა.[267] პირის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაციის გავრცელებისას უაღრესად მნიშვნელოვანია არა მხოლოდ პაციენტის პერსონალური მონაცემების ხელშეუხებლობის განცდის პატივისცემა, არამედ აგრეთვე ზოგადად პაციენტის თვალში სამედიცინო და ჯანდაცვის მომსახურების სფეროს მიმართ ნდობის შენარჩუნება. სხვაგვარად რომ ვთქვათ, ზეგავლენა შეიძლება იყოს იმდენად უარყოფითი, რომ სამედიცინო დახმარების საჭიროების მქონე პირებმა თავი შეიკავონ ინფორმაციის გამჟღავნებისაგან და ვერ გაიარონ სათანადო მკურნალობა.[268]

მნიშვნელოვანია ასევე პირის უფლება თავისი გამოსახულების გავრცელებაზე. ის შეადგენს ადამიანის უნიკალურ მახასიათებლებს და გამოარჩევს ადამიანს სხვებისაგან. ყველა ადამიანს აქვს უფლება, გააკონტროლოს საკუთარი გამოსახულების გავრცელება. ჟურნალისტებმა წინასწარ უნდა მოიპოვონ თანხმობა სურათის გადაღებისას და გავრცელებისას. წინააღმდეგ შემთხვევაში, პირის უფლება დაიცვას მისი პერსონალური ინფორმაცია - გამოსახულება - გახდება მესამე მხარეებზე და დაინტერესებული პირი ვეღარ აკონტროლებს მას. საქმეში Muller v. Germany,[269] განმცხადებლებმა შეიტყეს ვაჟის სავარაუდო სუიციდის შესახებ საგაზეთო სტატიიდან, სადაც ვაჟის ფოტო იყო განთავსებული. სასამართლომ ფოტოს თანხმობის გარეშე გამოქვეყნება ჩათვალა პერსონალური ინფორმაციის გამჟღავნებად და პირადი ცხოვრების უფლების დარღვევად.

მედია განსაკუთრებულ როლს ასრულებს დემოკრატიული პროცესების უზრუნველყოფის მიზნით. მათ აქვთ ვალდებულება, გაავრცელონ ინფორმაცია და საზოგადოებას გააცნონ ყველა საინტერესო საკითხი, რომლის მიღების უფლებაც საზოგადოებას გააჩნია. თუმცა, მათი გამოხატვის თავისუფლება არ არის აბსოლუტური. ჟურნალისტმა უნდა იმოქმედოს კეთილსინდისიერად და მიაწოდოს ზუსტი და სანდო ინფორმაცია, ჟურნალისტური ეთიკის შესაბამისად. ჟურნალისტი ვალდებულია, გამოქვეყნებამდე გადაამოწმოს ფაქტები. თუმცა, იგივე მოთხოვნა არ ვრცელდება ჟურნალისტების მიერ მოსაზრების გაშუქებისას ან თვალსაზრისის შესახებ ინფორმაციის გავრცელებისას. ამის მიუხედავად, მოსაზრებებიც უნდა ემყარებოდეს რაიმე ფაქტობრივ საფუძველს. საქმეზე Bodrožić v. Serbia,[270] სასამართლომ დაადგინა, რომ მისაღები იყო ჟურნალისტის მიერ ისტორიკოსის კრიტიკა, მისთვის „იდიოტის“ და „ფაშისტის“ წოდება, ვინაიდან მისი მოსაზრება გამოქვეყნდა ისტორიკოსის სატელევიზიო გამოსვლის საპასუხოდ.[271]

ბუნებრივია, საჯარო და კერძო პირების მიმართ სხვადასხვა სტანდარტი არსებობს, ვინაიდან საჯარო პირს თმენის მეტი ვალდებულება აქვს და მისი პერსონალური ინფორმაციის შესახებ საზოგადოებას შესაძლოა გააჩნდეს მაღალი ლეგიტიმური ინტერესი. მედიის მხრიდან ხში-

[267] Civil.ge, კომახიძე “რეალ TV”-ის სასამართლოში უჩივის, 2010, 20 მაისი, 14:22, ხელმისაწვდომია: https://bit.ly/38j4JXf წვდომის თარიღი: 05.07.2021.

[268] მედია სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, ევროკავშირი საქართველოსთვის, ევროპის საბჭო, გვ. 25.

[269] Müller v. Germany (Dec.), No. 43829/07, 14 September 2010.

[270] Bodrožić v. Serbia, No. 32550/05, 23 June 2009.

[271] მედია სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, ევროკავშირი საქართველოსთვის, ევროპის საბჭო, გვ. 8.

რად ხდება თანამდებობის პირების საკუთრების, ჯანმრთელობის მდგომარეობის, მათი დასვენების ადგილმდებარეობის და სხვა მონაცემების დამუშავება და გავრცელება, რაც უნდა განხორციელდეს პროპორციულად, ისე რომ გაუმართლებელი ზიანი არ მიადგეს პირის უფლებებს.[272]

პირადი ცხოვრების ხელშეუხებლობის უფლება მოიცავს არა მხოლოდ ფაქტობრივი ფიზიკური სივრცის უფლებას, არამედ ამ სივრცით დაუბრკოლებლად სარგებლობის უფლებასაც. საჯარო პირების შესახებ ინფორმაციის გავრცელებისას, უნდა დადგინდეს რამდენად არსებობს საკითხის მიმართ საზოგადოების მაღალი ინტერესი, თანაზომიერი და პროპორციული საშუალებებით ხდება თუ არა პირის პირად ცხოვრებაში ჩარევა. საქმე შეიძლება ეხებოდეს საჯარო პირის ოჯახის წევრების, საცხოვრებლის თუ სხვა სახის ინფორმაციის გავრცელებას. საცხოვრებელის მისამართი წარმოადგენს პერსონალურ ინფორმაციას. ამდენად, იგი დაცულია და პრინციპში არ უნდა გახდეს ხელმისაწვდომი საზოგადოებისათვის ჟურნალისტების მხრიდან. საქმეში Alkaya v. Turkey,[273] ჟურნალისტმა, რომელმაც რეპორტაჟი მოამზადა ცნობილი მსახიობის სახლის გაქურდვის შემთხვევაზე, დაარღვია მისი პირადი ცხოვრების ხელშეუხებლობა, ვინაიდან გაამჟღავნა მისი სახლის მისამართი. სასამართლომ დაადგინა, რომ მიუხედავად იმისა, რომ გაქურდვის შესახებ ინფორმაციით საზოგადოების სავარაუდო დაინტერესების მიუხედავად, ასეთი ინტერესი არ ვრცელდებოდა მომღერლის საცხოვრებელი სახლის მისამართის მიმართ.[274]

საინტერსოა ასევე ცნობილი ადამიანებისთვის ცერემონიებზე და საჯარო დღესასწაულებზე გადაღებული ფოტოების გავრცელების საკითხი. როგორც წესი, მათი საჯარო ასპექტიდან გამომდინარე, გარკვეულ შემთხვევებში, დასაშვებია თანხმობის გარეშე გაშუქებაც.[275]

მედიის მიერ პერსონალური მონაცემების დამუშავება ხშირად უკავშირდება დანაშაულის გამოძიებასა და აღკვეთას. დანაშაულების გაშუქებისას ჟურნალისტებმა განსაკუთრებული ყურადღება უნდა მიაქციონ იმას, შესაბამისი პირი ცნობილია თუ არა საზოგადოებისათვის და არ დაარღვიონ მისი უფლებები. საზოგადოებას აქვს დანაშაულის, გამოძიებისა და სასამართლო პროცესების შესახებ ინფორმაციის მიღების სამართლიანი ინტერესი. მართალია, დანაშაულის შესახებ მოვლენების გაშუქების მიზანია საზოგადოების ინფორმირება, ჟურნალისტმა მაინც კეთილსინდისიერად უნდა გააშუქოს და თავი შეიკავოს უსაფუძვლო და გადაუმოწმებელი ბრალდებების გამოქვეყნებისაგან. კერძოდ, ჟურნალისტებმა არ უნდა წარმოაჩინონ პიროვნება როგორც დამნაშავე, ვიდრე სასამართლო არ გამოაცხადებს მსჯავრდებას. მკაფიოდ უნდა გაიმიჯნოს ეჭვი და მსჯავრდება.

ჟურნალისტმა შეიძლება გამოაქვეყნოს ჩვეულებრივი პირადი ინფორმაცია, როდესაც იგი ემსახურება უფრო მაღალ ღირებულებას და საჭიროა საზოგადოებრივი ინტერესის საკითხის განხილვისათვის. გამოქვეყნებული პირადი ინფორმაცია უნდა ემსახურებოდეს მნიშვნელოვან მიზანს, რომელიც უპირატესი იქნება პერსონალური ინფორმაციის უსაფრთხოებასთან შედარებით. რაც

[272] M. Guzman, Privacy and reporting on personal lives, ხელმისაწვდომია: https://bit.ly/3mwMAgZ წვდომის თარიღი: 04.07.2021.

[273] Alkaya v. Turkey, No. 42811/06, 9 October 2012.

[274] მედია სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, ევროკავშირი საქართველოსთვის, ევრიპის საბჭო, გვ. 24.

[275] Sihler-Jauch and Jauch v. Germany, Lillo-Stenberg and Saether v. Norway.

უფრო მაღალია საზოგადოებისათვის ინფორმაციის ღირებულება, მით უფრო ნაკლები მნიშვნელობა უნდა მიენიჭოს პირის ინტერესს გამოქვეყნებისაგან დაცვის თვალსაზრისით, და პირიქით.[276]

6.1. უდანაშაულობის პრეზუმფცია

საზოგადოებას აქვს დანაშაულის, გამოძიებისა და სასამართლო პროცესების შესახებ ინფორმაციის მიღების სამართლიანი ინტერესი. მართალია, დანაშაულის შესახებ მოვლენების გაშუქების მიზანია საზოგადოების ინფორმირება, ჟურნალისტს აქვს ვალდებულება თავი შეიკავოს უსაფუძვლო და გადაუმოწმებელი ბრალდებებისგან. სასამართლოს მიერ გადაწყვეტილების გამოცხადებამდე, გაუმართლებელია პირის დამნაშავედ გამოცხადება. უნდა გაიმიჯნოს ეჭვი და მსჯავრდება.[277]

ხშირად მედიის მიერ პერსონალური ინფორმაციის დამუშავებისას, რაც დანაშაულის გამოძიების მიზნით ხდება, ირღვევა არა მხოლოდ პირის პერსონალური მონაცემების უსაფრთხოება, არამედ უდანაშაულობის პრეზუმფცია. მაგალითისთვის, 2015 წლის დეკემბერში მედიაში მთავარ თემას წარმოადგენდა ინფორმაცია არასრულწლოვანი შვილისა და ქმრის სავარაუდო მკვლელობისათვის დაკავებული პირის შესახებ. მედია დაწვრილებით ყვებოდა მკვლელობის დეტალებს, მიუთითებდა საქმეში არსებული მტკიცებულების თაობაზე, წერდა დანაშაულის ჩადენის მოტივზეც და რაც ყველაზე მეტად შემაშფოთებელია, ბრალდებულს მკვლელადაც კი მოიხსენიებდა. ეს კი წარმოადგენდა მედიის მხრიდან პირის პერსონალური მონაცემების დარღვევას. მედიას შეუძლია საზოგადოების დარწმუნება, რომ ბრალდებულმა დანაშაული ჩაიდინა. ამან კი, შესაძლოა, ბრალდებულის სამართლიანი სასამართლოს უფლებით სარგებლობაზე უარყოფითი გავლენა იქონიოს.

ეს უარყოფითი გავლენა უცხო არ არის ადამიანის უფლებათა ევროპული სასამართლოსთვისაც. კუზმინი რუსეთის წინააღმდეგ საქმეში[278] მიღებული გადაწყვეტილების 62-ე პუნქტში ადამიანის უფლებათა ევროპულმა სასამართლომ განაცხადა: ბრალდებულის მიმართ წარმოებულმა უარყოფითმა მედიაკამპანიამ ზოგიერთ საქმეში შესაძლოა ზიანი მიაყენოს ბრალდებულის უფლებას სამართლიან პროცესზე, ვინაიდან მედია ქმნის უარყოფით საზოგადოებრივ აზრს ბრალდებულთან დაკავშირებით, რაც, თავის მხრივ, აიძულებს სასამართლოს მიიღოს ბრალდებულის გამამტყუნებელი განაჩენი.[279]

2012 წელს მედიის განვითარების ფონდმა გამოქვეყნა კვლევა იმის შესახებ, თუ როგორ აშუქებდნენ ქართული ტელეარხები სამართლის საკითხებს. კვლევამ აჩვენა, რომ ტელეკომპანიები, ძი-

[276] Guidelines on safeguarding privacy in the media, Council of Europe, გვ. 10-27, ხელმისაწვდომია: https://bit.ly/3gA1M9e წვდომის თარიღი: 04..07.2021.

[277] მედია სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, ევროკავშირი საქართველოსთვის, ევროპის საბჭო, გვ. 31.

[278] Khuzhin and Others v. Russia, No. 13470/02, 23 October 2008.

[279] Guidelines on safeguarding privacy in the media, Council of Europe, გვ. 28, ხელმისაწვდომია: https://bit.ly/3B9x0f2 წვდომის თარიღი: 05.07.2021.

რითადად, არღვევდნენ ადამიანთა უდანაშაულობის პრეზუმფციასა და ერეოდნენ სიუჟეტების გმირების პირად ცხოვრებაში, ავრცელებდნენ მათ პერსონალურ მონაცემებს.[280] მედიის მხრიდან პირის პერსონალური მონაცემების არასწორი დამუშავების, გავრცელების დროს პერსონალურ ზიანთან ერთად საფრთხე ემუქრება მრავალ საზოგადოებრივ სიკეთეს, ამიტომ ეს პროცესი კანონის ფარგლებში უნდა წარიმართოს.

6.2. ჟურნალისტის გამოხატვის თავისუფლება და საზოგადოების უფლება ინფორმაციის მიღებაზე

მკაცრად პირადული საკითხების გაშუქებით ირღვევა პირადი ცხოვრების ხელშეუხებლობის პატივისცემის უფლება, თუ არ მოხდა შესაბამისი პირის თანხმობის მოპოვება, ან თუ გაშუქება საზოგადოებრივი ინტერესის სფეროში არ ექცევა.

მაღალი საჯარო ინტერესის მქონე სისხლის სამართლის საქმეების გაშუქებისას ხშირად ერთმანეთს უპირისპირდება, ერთის მხრივ, ჟურნალისტების გამოხატვის თავისუფლება და საზოგადოების უფლება ინფორმაციის მიღებაზე, მეორეს მხრივ კი, საქმეში მონაწილე პირთა პირადი ცხოვრების ხელშეუხებლობის უფლება.[281] ევროპის ადამიანის უფლებათა სასამართლო ამგვარი კონფლიქტის გადაწყვეტისას მხედველობაში იღებს ინფორმაციის მნიშვნელობას საჯარო ინტერესის მქონე დებატებში ინფორმაციის სუბიექტის ცნობადობას, გავრცელებული ინფორმაციის შინაარსს, ფორმასა და შედეგებს.[282]

საქმე Krone Verlag GmbH & Co KG[283] და Krone Multimedia GmbH & Co KG v. Austria[284] ეხებოდა გაზეთის მიერ სქესობრივი შეურაცხყოფის შედეგად დაზარალებული არასრულწლოვანი პირის ვინაობის გამჟღავნებას, ვებსაიტზე მისი ფოტოს გამოქვეყნებით. საკითხის საზოგადოებრივი ინტერესის ხასიათის მიუხედავად, იმის გათვალისწინებით, რომ არც დამნაშავეები, არც დაზარალებული არ იყვნენ საჯარო პირები ან მანამდე არ მოქცეულან საჯარო სივრცეში, მათი ვინაობის ცოდნა არ იყო აუცილებელი საქმის დეტალების გასაგებად. ბავშვი არ იყო საჯარო პირი და სასამართლომ არ მიიჩნია, რომ იგი შევიდა საჯარო სივრცეში იმის გამო, რომ გახდა სისხლის სამართლის დანაშაულის შედეგად დაზარალებული, რომელმაც მიიპყრო მნიშვნელოვანი საზოგადოებრივი ყურადღება.[285]

---

[280] Netgazeti.ge, ტელეეთერში დარღვეული უდანაშაულობის პრეზუმფცია, 2012, 2 ივლისი, ხელმისაწვდომია: https://bit.ly/3koIFjD წვდომის თარიღი: 05.07.2021

[281] L. K. Perenic, Media and the Protection of Personal Data, information Commissioner of the Republic of Slovenia, გვ. 11-34, ხელმისაწვდომია: https://bit.ly/3BhxXCq წვდომის თარიღი: 05.07.2021.

[282] Axel Springer v. Germany, no. 39954/08, 07.02.2012, §§ 89-95 and Von Hannover v. Germany (No 2), nos. 40660/08 and 60641/08, 07.02.2012, §§ 108-113.

[283] Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 February 2002.

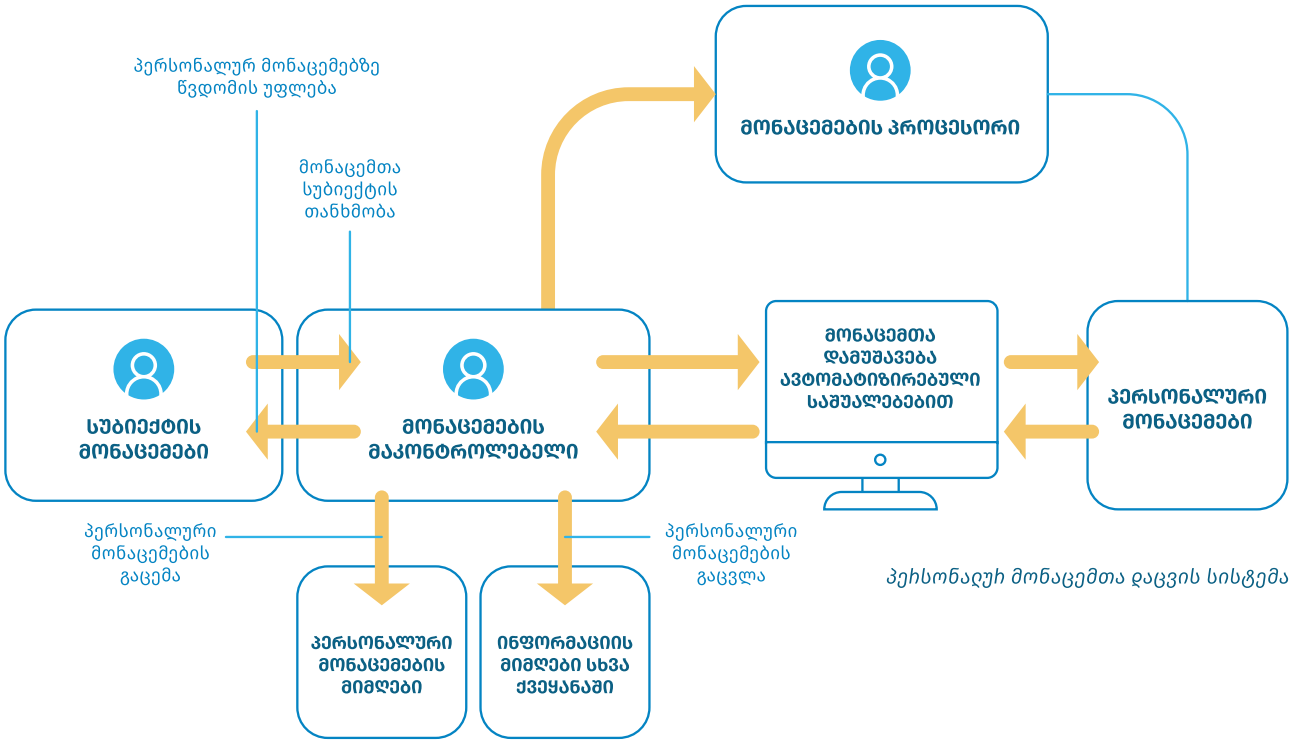
[284] Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria, No. 33497/07, 17 January 2012.

[285] მედია სივრცეში პირადი ცხოვრების ხელშეუხებლობის დაცვის სახელმძღვანელო პრინციპები, ევროკავშირი საქართველოსთვის, ევროპის საბჭო, გვ. 31.

მედიის მხრიდან პერსონალური მონაცემების გაუმართლებელი დამუშავების ფაქტები კიდევ უფრო გახშირდა კოვიდ-19-ის პირობებში. პანდემიის შედეგად განათლებასთან, ჯანდაცვასთან და სხვა სფეროებთან დაკავშირებული სერვისების ნაწილი ონლაინ ფორმატში გადავიდა, რის შედეგადაც პერსონალურ მონაცემთა დიდი რაოდენობა ციფრულ სივრცეში აღმოჩნდა და მოქალაქეთა პერსონალური ინფორმაციის უსაფრთხოება განსაკუთრებული რისკის ქვეშ აღმოჩნდა.

ამავე დროს, განსაკუთრებული ყურადღება უნდა მიექცეს სოციალური მედიის მხრიდან პირის პერსონალური მონაცემების დარღვევის ფაქტებს. განსაკუთრებით ხშირია ინტერნეტსივრცეში ყალბი ანგარიშების შექმნა სხვისი ფოტოსურათით, სახლითა და გვარით. გარდა ამისა, ცოტა ხნის წინ გავრცელდა ინფორმაცია რომ სხვადასხვა აპლიკაციებიდან სოციალური მედიასაშუალებები უკანონოდ ინახავდნენ და იყენებდნენ პერსონალურ მონაცემებს.[286] სოციალური მედიის მიერ დამუშავებული მონაცემები ხშირად გამოიყენება უკანონო მიზნებისთვის სხვადასხვა ჯგუფების მიერ. ზოგჯერ მონაცემები მომხმარებელთა ნებართვის გარეშე მუშავდება და ინახება. სოციალური მედიის მიერ პერსონალური ინფორმაციის დამუშავება შემდეგნაირად მიმდინარეობს:

გრაფიკ. 1. პერსონალური მონაცემების დამუშავება



პერსონალური მონაცემთა დაცვის სისტემა

[286] R. P. Romansky, Social Media and Personal Data Protection, 2014, ხელმისაწვდომია: https://bit.ly/3zkjoNP წვდომის თარიღი: 05.07.2021.

ჟურნალისტებს გააჩნიათ კეთილსინდისიერი საქმიანობის ვალდებულება. მათ უნდა გაავრცელონ ზუსტი და გადამოწმებული ინფორმაცია ჟურნალისტური ეთიკის შესაბამისად. მაგალითად, გარდაცვალების გამო დაზარალებულის ოჯახის წევრების მწუხარების გათვალისწინებით, ჟურნალისტის მხრიდან აუცილებელია წინდახედულობა და სიფრთხილე, რათა უხეშად არ ჩაერიონ პირად და ოჯახურ ცხოვრებაში.

ხშირად ჟურნალისტები მომხმარებლის მოსაზიდად ავრცელებენ გადაუმოწმებელ ინფორმაციას, სურთ ექსკლუზიური კადრების მოპოვება და ასეთ დროს ნაკლებ ყურადღებას აქცევენ პირის პერსონალური ინფორმაციის უსაფრთხოებას. რეიტინგის ამაღლების მიზნით, ხშირია კონტექსტიდან ამოვარდნილი, არასრული და შემოკლებული სტატიები და სათაურები, რომელსაც შეცდომაში შეჰყავს მკითხველი. ნაკლებ სავარაუდოა, რომ მსგავსი სახის ინფორმაცია ხელს შეუწყობს საზოგადოებრივი ინტერესის საკითხის გარშემო მსჯელობას. გავრცელებული ინფორმაციის სიზუსტე პირადი ცხოვრების ხელშეუხებლობის დაცვის ერთ-ერთ ფუნდამენტურ პრინციპს წარმოადგენს.

საზოგადოება იღებს იმ მასალას, რომელსაც აწვდის მედია, შესაბამისად მედიას აკისრია პასუხისმგებლობა ინფორმაციის გამჟღავნების პროცესში იმოქმედოს კეთილსინდისიერად და პატივი სცეს მოქალაქეთა უფლებებს. მედიის თავისუფლებასა და პირის პერსონალური ინფორმაციის უსაფრთხოებას შორის კოლიზიისას უნდა მოხდეს კონკრეტული საქმის გარემოებების შეფასება და ანალიზი, დაცული უნდა იქნეს ბალანსი ინდივიდის და საზოგადოების უფლებებს შორის. გადაწყვეტილება რომელიმე უფლების შეზღუდვის შესახებ უნდა დაეფუძნოს კონკრეტული საქმის ინდივიდუალურ გარემოებებს.

7. მედიის მიერ პერსონალური ინფორმაციის დამუშავება და ბავშვთა უფლებები

ამას გარდა, ჟურნალისტებმა განსაკუთრებული სიფრთხილე უნდა გამოიჩინონ მოწყვლადი ჯგუფების ან სპეციფიკური საჭიროებების მქონე ჯგუფების შესახებ ინფორმაციის გაშუქებისას.

პერსონალურ მონაცემთა დამუშავების პროცესში განსაკუთრებული ყურადღება უნდა მიექცეს ბავშვის ინტერესებს და მათი უფლებები არ უნდა იქნას უგულებელყოფილი. ინფორმაციის გავრცელებისას უნდა იქნას გათვალისწინებული ბავშვის ასაკი. ბავშვს შესაძლოა არ ჰქონდეს გააზრებული საკუთარი სიტყვების მნიშვნელობა და მედიას გააჩნია ეთიკური პასუხისმგებლობა, რათა არ მოხდეს ბავშვის ასოცირება უარყოფით ან უხერხულ კომენტარებთან.

მიუხედავად იმისა, რომ გარკვეულ შემთხვევებში მაღალი საზოგადოებრივი ინტერესი არსებობს, ჟურნალისტებმა განსაკუთრებული ყურადღება უნდა მიაქციონ ბავშვის საუკეთესო ინტერესებს. 2021 წლის 17 აპრილის გავრცელდა ინფორმაციო ნინოწმინდის პანსიონატში ბავშვთა უფლებების უხეში დარღვევის ფაქტების შესახებ, რამაც საზოგადობის დიდი ინტერესი და შეშფოთება გამოიწვია. აუცილებელია, მსგავსი შემთხვევების შესახებ ადამინებმა მიიღონ უტყუარი ინფორმაცია, ამასთანავე დაცული უნდა იყოს ბავშვების უფლებები, მათი პერსონალური მონაცემები უნდა იყო დაფარული, არ უნდა მოხდეს მათი იდენტიფიცირება, რათა ამან დამატებითი წნეხი არ

გამოიწვიოს ბავშვებში. ისეთ შემთხვევებში, როდესაც ბავშვის სახელი არ არის მითითებული და არ ხდება სახის ჩვენება, ჟურნალისტებმა ასევე თავი უნდა შეიკავონ ისეთი ინფორმაციის გამოქვეყნებისაგან, რომლის მიხედვითაც არაპირდაპირ მოხდება ბავშვის ვინაობის გარკვევა (საცხოვრებელი სახლის, ოჯახის ფოტოები, და სხვა.)

8. რეკომენდაციები

მედიამ ინფორმაციის გავრცელებისას უნდა გამოიჩინოს სიფრთხილე და განზრახ თუ უნებლიეთ არ დაარღვიოს პირის პერსონალური მონაცემების უსაფრთხოება. მედიის თავისუფლებასა და პერსონალური მონაცემების უსაფრთხოებას შორის კოლიზიისას გადაწყვეტილება მიღებულ უნდა იქნას ყოველ კონკრეტულ შემთხვევაში კონკრეტული გარემოებების საფუძველზე. მედიასაშუალებებმა უნდა მიიღონ ყველა აუცილებელი ზომა, რათა უზრუნველყონ მონაცემთა დაცვის ყველა მოთხოვნის შესრულება. მედიის მიერ პერსონალურ მონაცემთა დამუშავება უნდა მოხდეს კანონიერ ფარგლებში სამართლიანობის და ეთიკური პრინციპების გათვალისწინებით.

მედიის მიერ პერსონალურ მონაცემთა დამუშავებისას მონაცემთა დაცვის უზრუნველყოფის მიზნით მიზანშეწონილი გატარდეს შემდეგი ღონისძიებები:

- მედია საშუალებების წარმომადგენლებისთვის ტრენინგებისა ჩატარება პერსონალური მონაცემების დაცვის საკითხებზე, თუ როგორ უნდა მოხდეს კანონიერ ფარგლებში მონაცემთა დამუშავება;
- მონაცემთა დაცვისათვის დამუშავების პროცესების ამსახველი ყოველთვიური მოხსენების დანერგვა;
- კონფიდენციალობის პოლიტიკის შემუშავება;
- მედია საშუალებებში შიდა პროცედურების დანერგვა ჟურნალისტური საქმიანობის განხორციელებისას პერსონალური მონაცემების გამჟღავნების შედეგების შესწავლის და შეფასების მიზნით;[287]
- პერსონალური მონაცემების გამჟღავნებისას გადაწყვეტილების მიღება კომპეტენტურ და კვალიფიციურ კადრებთან/ორგანოებთან თანამშრომლობის გზით და პერსონალური მონაცემების დარღვევის შემთხვევაში ფაქტზე სწრაფი რეაგირება დ პრობლემის აღმოფხვრა მყისიერად.
- შიდა მექანიზმების დანერგვა საინფორმაციო შეტყობინებების მომზადების, ფიზიკური პირების მიერ წარდგენილი პრეტენზიების განხილვის, ორგანიზაციის ხელმძღვანელობის გაფრთხილების მიზნით;

[287] Recommendations on the protection of privacy in media coverage, Promotion of European standards in the Ukrainian Environment, prepared by representatives of journalists, mass media associations, other NGOs, national experts, etc. and Council of Europe experts, Journalist Ethics Committee, Council of Europe, გვ. 4-5.

- რეგულარული შემოწმებები პერსონალური მონაცემების დამუშავებისას კანონიერების და მიზანშეწონილების გადამოწმების და შეფასების მიზნით;
- ცნობიერების ამაღლების ღონისძიებების ჩატარება - ფიზიკური და იურიდიული პირებისთვის პერსონალური ინფორმაციის დაცვის უფლების შესახებ ინფორმაციის მიწოდება;
- ვებსაიტების და სხვა ინტერნეტ საშუალებების გამოყენება პერსონალურ მონაცემთა დაცვის საკითხებზე ინფორმირებულობის გაზრდის მიზნით. ონლაინ მედია ჩეკერების გამოყენება მედიის მხრიდან პერსონალური ინფორმაციის უკანონოდ გავრცელების ფაქტების სწრაფი აღმოჩენის და მონაცემთა უსაფრთხოების დარღვევაზე რეაგირების მიზნით.

9. დასკვნა

მედიის მიერ პერსონალური მონაცემების დაცვის საკითხი სულ უფრო მეტ აქტუალობას იძენს. პერსონალურ მონაცემთა დამუშავებისას პირად ცხოვრებაში უხეშად ჩარევის ფაქტები მედიაში ხშირდება. განსაკუთრებით ხაზგასასმელია ბავშვთა უფლებების დაცვა ასეთ პროცესებში.

ნაშრომში წარმოდგენილი იქნა მედიის მხრიდან პერსონალური მონაცემების დამუშავების საშუალებები, წინაპირობები და შედეგები, მიმოხილული იქნა საკითხი საერთაშორისო სამართლებრივ ჭრილში. შეფასებული იქნა მედიის მხრიდან პერსონალური მონაცემების დამუშავების კანონიერების ფარგლები სხვადასხვა შემთხვევებში: დანაშაულის გამოძიებისას, სათვალთვალო და ფარული კამერების გამოყენებისას, საზოგადოებრივი ინტერესის დაკმაყოფილებისას და ა. შ.

მნიშვნელოვანია სასამართლოს როლი ნორმის სწორად და ადეკვატურად განმარტების კუთხით, ვინაიდან მათი გადაწყვეტილებები სავალდებულოა საქართველოს მთელს ტერიტორიაზე და სამოქმედო მიმართულებას წარმოადგენს მონაცემთა დამმუშავებლისათვის.[288]

მედია წარმოადგენს დემოკრატიული პროცესების ჩამოყალიბების ერთ-ერთ მნიშვნელოვან საშუალებას. მედია წარმომადგენლები განსაკუთრებულ როლს ასრულებენ კორუფციის დანაშაულთან და სხვა მართლსაწინააღმდეგო ქმედებებთან ბრძოლის კუთხით. მათ აქვთ ვალდებულება, გაავრცელონ ინფორმაცია და საზოგადოებას გააცნონ ყველა საინტერესო საკითხი, რომლის მიღების უფლებაც საზოგადოებას გააჩნია. თუმცა მედიის უფლებები არ არის შეუზღუდავი და პერსონალური მონაცემების დამუშავებისას და გავრცელებისას მედიამ უნდა დაიცვას პირის უფლებები. საჭიროა ბალანსის დაცვა მედიის თავისუფლებას და პირის პერსონალური მონაცემების უსაფრთხოებას შორის. საჭიროა, რომ მოქალაქეებს ჰქონდეთ ცოდნა საკუთარი უფლებების შესახებ, თუ როგორ უნდა დაიცვან თავიანთი პერსონალური მონაცემები. განსაკუთრებული მნიშვნელობის მქონეა მედია წარმომადგენლების მიერ პერსონალური მონაცემების დამუშავების წესების ცოდნა.

---

[288] თ. არჩუაძე, პერსონალურ მონაცემთა დაცვის გარანტიები, მონაცემთა სუბიექტის თანხმობის გარეშე ინფორმაციის დამუშავებისას, თბილისი, 0178, 2016, გვ. 58, ხელმისაწვდომია: https://bit.ly/38ebJ7w წვდომის თარიღი: 05.07.2021.

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება TIK-TOK-ის მაგალითზე

ავტორი: მელანო ბერიძე[289]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

თანამედროვე სამყაროში სოციალური ქსელები 21-ე საუკუნის ყოველდღიურობის განუყოფელ ნაწილად იქცა. ციფრული პლატფორმების განვითარებამ პრაქტიკულად სრულიად შეცვალა ადამიანთა შორის ინტერაქციის ფორმები, სახელმწიფოთა შიდა და გლობალური პოლიტიკა, საზოგადოების ქცევა, ერთი სიტყვით, მთლიანად სამყარო. თამამად შეიძლება ითქვას, რომ არ დარჩა სფერო, რომელზეც ზოგადად ტექნოლოგიურ სიახლეებს და უფრო კონკრეტულად, სოციალურ ქსელებს, გავლენა არ მოეხდინა. ციფრული სამყაროს სარგებლისა და უარყოფითი მხარეების შეპირისპირების შემთხვევაში დადებითი ასპექტების წილი უდავოდ გადაწონის მის ნეგატიურ მდგენელებს, თუმცა, ცალკეულ შემთხვევებში, იმდენად მნიშვნელოვანი გამოწვევების წინაშე დგება მსოფლიო, რომ მათზე თვალის დახუჭვამ შესაძლოა უთუოდ მძიმე შედეგებამდე მიგვიყვანოს. ერთ-ერთი მთავარი პრობლემა, რომელიც სოციალურ ქსელებს უკავშირდება არის პირადი სივრცის დაცულობა, მათ შორის, პერსონალური მონაცემების უსაფრთხოება და მასთან დაკავშირებული საკითხები. აღნიშნული ნაშრომი, უსაფრთხოების კონტექსტში, ახლად პოპულარობამოხვეჭილი ჩინური აპლიკაციის - Tik-Tok-ის შეფასებას დაეთმობა.

Tik-Tok ძალიან ცნობილი ჩინური აპლიკაცია და მოკლე ვიდეოების გასაზიარებლად შექმნილი სოციალური ქსელია, რომელიც თავდაპირველად 2016 წელს „მუზიქალ.ლი“-ს სახელწოდებით გამოვიდა, თუმცა მაშინ წარუმატებელი აღმოჩნდა. 2018 წელს ჩინური კომპანია - ByteDance -მა „მუზიქალ.ლი“ შეიძინა, კიდევ უფრო განავითარა, დახვეწა და მომხმარებლებს უკეთესი ვერსია უკვე Tik-Tok სახელით შესთავაზა. ამ აპლიკაციამ მზარდი პოპულარობა განსაკუთრებით კოვიდ-პანდემიის გავრცელების დროს შეიძინა, მაშინ როცა მსოფლიოს მოსახლეობის საკმაოდ დიდი რაოდენობა იზოლაციაში იმყოფებოდა, განიცდიდა ფსიქოლოგიურ დაძაბულობას და გასართობ საშუალებებს ეძებდა. ამდენად, სათვალავარეული დღე კარანტინისა, სახლიდან გაუსვლელად, ახლობლებთან რეალურ სივრცეში ურთიერთობის გარეშე დარჩენილმა ადამიანებმა ჩინურ ვირუსთან საბრძოლველად ონლაინ ვიდეოპლატფორმა კარანტინში აღმოაჩინა. ამ აპლიკაციამ მთელ მსოფლიოს ერთი და იგივე მელოდიები აუკვიატა და იმხელა გავლენა მოახდინა, რომ დღეს ყველა ერთნაირად, ისეთივე სიზუსტით ცეკვავს, თითქოს ერთი ანსამბლის წევრები იყვნენ. ეს ყველაფერი კი Tik-Tok-ის დამსახურებაა.

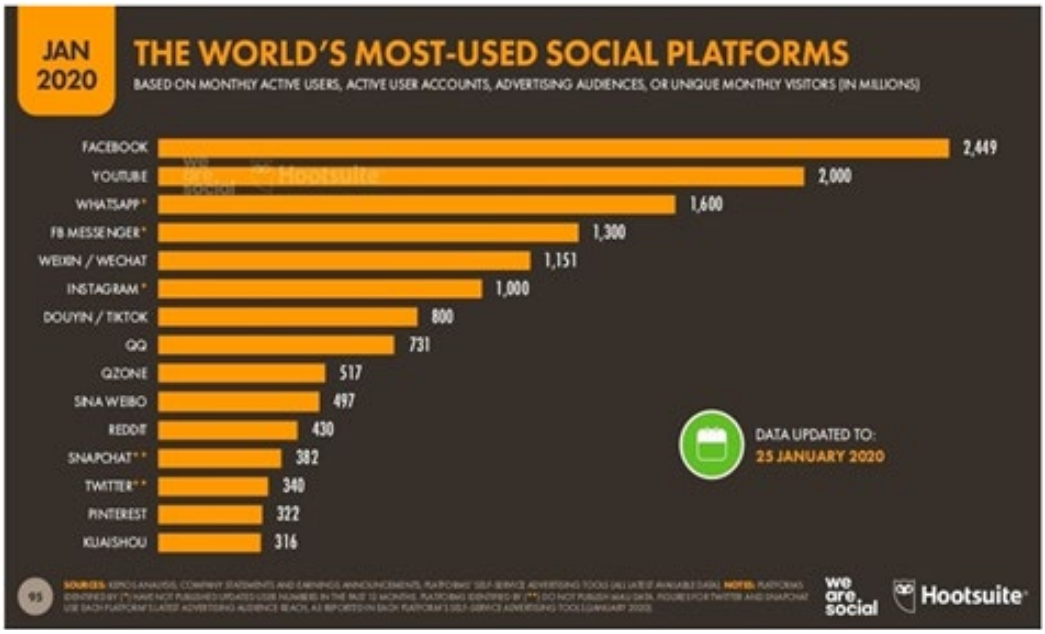
როგორც აღვნიშნე, ეს აპლიკაცია განსაკუთრებით Covid-19-ის გავრცელების შემდეგ გახდა პოპულარული. ამას მოწმობს Statista-ს მონაცემებიც, რომლის მიხედვითაც 2016 წელს მსოფლიოს

[289] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნინო ბოჭოიძე.

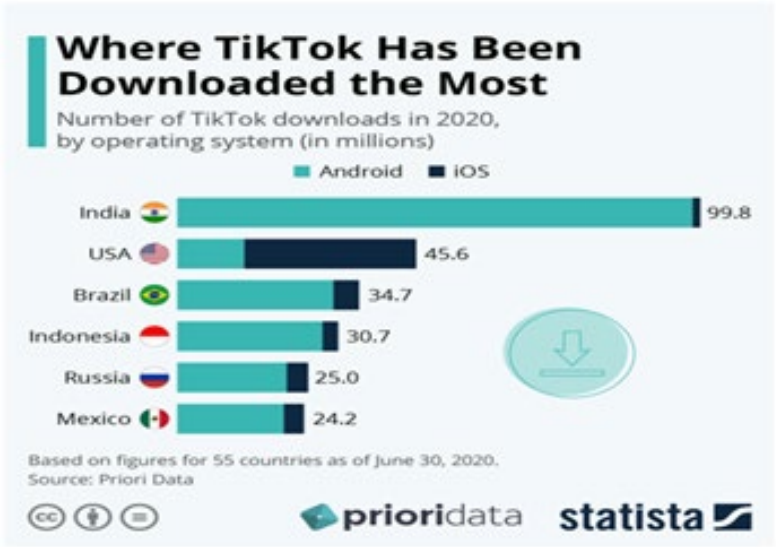
მასშტაბით Tik-Tok დაახლოებით 21 მილიონ მომხმარებელს ჰქონდა გადმოწერილი სხვადასხვა ქვეყნიდან. 2019 წელს ჩინურ აპლიკაციას კიდევ 219 მილიონი მომხმარებელი დაემატა, ხოლო statista-ს 2021 წელს ამ აპლიკაციას მსოფლიოში დაახლოებით 800 მილიონი მომხმარებელი ჰყავს (statista, 2021).

მნიშვნელოვანია მსოფლიოს ყველაზე გამოყენებად სოციალურ პლატფორმებს შორის Tik-Tok-ის პოზიციაც, რომელიც რიცხვებში ასე გამოიყურება:

Business of Apps(2020): მსოფლიოში ყველაზე ხშირად გამოყენებად სოციალური პლატფორმები



აღსანიშნავია ისიც, რომ დღესდღეობით აღნიშნულმა აპლიკაციამ 150-ზე მეტი ქვეყანა მოიცვა და სხვადასხვა ენაზეა ხელმისაწვდომი. Statista-ს 2020 წლის მონაცემების მიხედვით, Tik-Tok-ის მოხმარების მზარდი სტატისტიკა აღინიშნება ისეთ ქვეყნებში, როგორებიც არის: ინდოეთი, აშშ, ბრაზილია, რუსეთი და სხვა. მისი გავლენა კიდევ უფრო იზრდება.



Statista (2020): სად ახის Tik-Tok ყველაზე ხშირად გადმოწეხიღი

კიდევ უფრო საინტერესოა იმის აღნიშვნა, თუ როგორ მოახერხა Tik-Tok-მა ასეთი უზარმაზარი აუდიტორიის შეკრება დროის მოკლე მონაკვეთში. კონტენტი, რომელიც Tik-Tok-ზე იქმნება, ძალიან მალევე გახდა პოპულარული როგორც დასავლეთის, ისე აღმოსავლეთის აუდიტორიისთვის. იმ ფონზე, რომ აპლიკაციამ ძალიან მალევე მზარდი პოპულარობა მოიპოვა, კიდევ უფრო მეტი შეკითხვა გააჩინა მის უსაფრთხოებასთან დაკავშირებით. საკითხი კიდევ უფრო გამწვავდა მას შემდეგ, რაც აშშ-ს ფედერალურმა სავაჭრო კომისიამ 2019 წელს რამდენიმე მილიონი დოლარით დააჯარიმა სოციალური მედია აპლიკაცია - Musical.ly ბავშვთა პირადი ცხოვრების შელახვის საფუძვლით.[290]

შეერთებული შტატების ფედერალური სავაჭრო კომისიის არგუმენტებით, აპლიკაციის უკანონო ქმედება გულისხმობდა არასრულწლოვანთა პირადი მონაცემების, ფოტოებისა და მათი ადგილსამყოფელის შესახებ ინფორმაციის უკანონო შეგროვებას. ეროვნული უსაფრთხოების დონეზე ამ საქმის განხილვის შემდეგ, აშშ-ს პრეზიდენტმა, დონალდ ტრამპმა Tik-Tok-ის გამოყენება აკრძალა კიდეც.[291]

ერთი შეხედვით უწყინარი და გასართობი საშუალება - Tik-Tok საკმაოდ სერიოზულ საფრთხედ აღიქვა მსოფლიოს არაერთმა ქვეყანამ. ისეთმა ციფრულმა ლევიათანმა, როგორიც ჩინეთია, ამით მსოფლიოში რისკების მასშტაბი და სპეციფიკა კიდევ უფრო გაზარდა. ამ თემასთან დაკავშირებით გავრცელებულ არაერთგვაროვან შეფასებებს შორის აღსანიშნავია ისიც, რომ Tik-Tok აღიქმება როგორც უწყინარი სოციალური ქსელი, რომელიც ჩინური რბილი ძალის იმ ფორმას წარმოადგენს, რომლითაც შესაძლებელია მასშტაბურად საზოგადოებრივი აზრის ფორმირებაზე კონტროლი. ამას ემატება ისიც, რომ აპლიკაციას არ აქვს მყარი სამართლებრივი გარანტიები, რითაც დაადასტურებს, რომ ეს სოციალური ქსელი უკანონოდ არ მოიპოვებს მომხმარებელთა პირად მონაცემებს. ამ ყველაფერს ემატება ისიც, რომ აპლიკაცია შეიქმნა იქ, სადაც ჯერ კიდევ კომუნისტური წყობაა, რაც საკითხს, პერსონალური მონაცემების დაცვასთან დაკავშირებით, ეჭვქვეშ აყენებს.

Tik-Tok-ის ტრენდს არ ჩამორჩა ქართველი მომხმარებელიც. ის განსაკუთრებით პოპულარული სავალდებულო კარანტინის დროს გახდა. საქართველოც, როგორც აბრეშუმის გზის შემადგენელი ქვეყანა და Tik-Tok-ის გადმომწერთა მზარდი მაჩვენებლის მქონე ქვეყანას წარმოადგენს ჩინეთის საგარეო პოლიტიკის არამხოლოდ ფიზიკურ, ასევე ციფრული სივრცის ნაწილსაც. საქართველოშიც აქტიურად გავრცელდა მისი გამოყენება. ამდენად, მნიშვნელოვანია სიღრმისეულად შეფასდეს და შესწავლილ იქნას ამ პლატფორმის მუშაობის სპეციფიკა და მისი კონფიდენციალურობის პოლიტიკა სხვადასხვა ქვეყანაში.

საინტერესოა ვიკვლიოთ მომხმარებელთა რა სახის მონაცემებს აგროვებს ეს აპლიკაცია, რამდენად რისკის შემცველია ამ აპლიკაციის გადმოწერა ჩვენი პირადი ინფორმაციის გასაჯაროების კუთხით და ასევე როგორ აფასებენ აღნიშნული აპლიკაციის უსაფრთხოებას მსოფლიოს სხვადასხვა ქვეყანაში. იგულისხმება ის, თუ რამდენად რეგულირდება სამთავრობო დონეზე ამ აპლიკაციის მიერ მომხმარებელთა მონაცემების დამუშავების მეთოდები.

[290] ქ. ტიმბერგ, ტ.რომმი, "The U.S. government fined the app now known as TikTok $5.7 million for illegally collecting children's data" The Washington Post's Blog, 2019 წლის 8 თებერვალი, ხელმისაწვდომია: https://wapo.st/38fCzMP წვდომის თარიღი: 28.06.2021.

[291] BBC,"TikTok: President Trump signs orders to ban it in the US within 45 days", 2020 წლის 7 აგვისტო, ხელმისაწვდომია აქ: https://bbc.in/3DjGLcC წვდომის თარიღი: 29.06.2021.

2. მეთოდოლოგია

კვლევის დროს გამოყენებულ იქნა თვისებრივი სოციოლოგიური კვლევის ერთ-ერთი გავრცელებული მეთოდი - Case Study. ამ შემთხვევაში, მისი გამოყენებით შესწავლილ იქნა სიღრმისეულად Tik-Tok-ის პლატფორმასთან დაკავშირებული ისეთი საკითხები, როგორებიც არის:

- პერსონალური მონაცემების დამუშავების ტექნიკები Tik-Tok-ზე და მისი როლი ამ პლატფორმის მომხმარებელთა მონაცემების დაცვის საკითხში;
- სხვადასხვა ქვეყანაში ამ პლატფორმის კონფიდენციალობის პოლიტიკის განსაზღვრა და კვლევის ველში მოქცეული ქვეყნების შედარება ამ კუთხით;
- აღნიშნულ პლატფორმაზე მომხმარებელთა მონაცემების გამოყენების მიზნების განსაზღვრა;
- მსოფლიოს სხვადასხვა ქვეყანაში აპლიკაციის უსაფრთხოების შეფასება.

ამრიგად, შემთხვევის შესწავლის ანალიზის გამოყენებით კვლევის მიზანს წარმოადგენს კონკრეტული ფენომენის, ამ შემთხვევაში ჩინური აპლიკაციის- Tik-Tok-ის სიღრმისეული შესწავლა. საკითხზე მუშაობისას გამოყენებულ იქნა მეორეული წყაროები.

3. ძირითადი ნაწილი

კვლევის პროცესში ყურადღება გამახვილდა იმაზე, თუ მომხმარებელთა რა ტიპის მონაცემებს აგროვებს და ინახავს ჩინური აპლიკაცია. აღნიშნული საკითხი, როგორც ჩანს, მას შემდეგ დადგა დღის წესრიგში, რაც აშშ-ს ფედერალურმა სავაჭრო კომისიამ ამ აპლიკაციის მფლობელი კომპანია დააჯარიმა არასრულწლოვანთა პირადი მონაცემების, მათი მაიდენტიფიცირებელი ნიშნების გასაჯაროებისთვის. Tik-Tok-ის კონფიდენციალურობის პოლიტიკის გაცნობისა და მისი სიღრმისეულად შესწავლის შემდეგ აღმოჩნდა, რომ ამ კონკრეტულ აპლიკაციაზე მომხმარებელთა რეგისტრაციის შემდეგ, აპლიკაციას წვდომა აქვს მომხმარებელთა მთელ რიგ ინფორმაციაზე. მათ შორის მომხმარებელთა:

- ვიდეოებზე;
- ადგილმდებარეობაზე;
- აპლიკაციით გაგზავნილ პირად შეტყობინებებზე.

აღსანიშნავია ისიც, რომ აპლიკაცია ავტომატურად აგროვებს მომხმარებელთა საიდენტიფიკაციო ისეთ მონაცემებს როგორებიცაა: IP მისამართი, მომხმარებელთა მოწყობილობის ტიპი (სმარტფონი, კომპიუტერი და სხვა), მობილური ოპერატორის ტიპი და სხვა.

Tik-Tok-ის აპლიკაცია Privacy Policy-ს (კონფიდენციალობის პოლიტიკა) ხშირად აახლებს. ბოლოს აპლიკაციამ თავისი კონფიდენციალურობის პოლიტიკის დოკუმენტი 2021 წლის 2 ივნისს განაახლა.[292]

[292] Tik-Tok's Privacy Policy, 2021 წლის 2 ივნისი, ხელმისაწვდომია: https://bit.ly/2XWBVlj წვდომის თარიღი: 27.08.2021.

ამ დოკუმენტის თანახმად, აპლიკაცია მაქსიმალურად ცდილობს მომხმარებელთა უფლებები არ დაარღვიოს და მათი პირადი მონაცემები არ გაამჟღავნოს, თუმცა ინახავს ყველა იმ ვიდეო მასალას, რომელსაც მომხმარებელი აპლიკაციაზე ტვირთავს. ამას კი ჩინური კომპანია იმით ამართლებს, რომ მომხმარებელთა ვიდეო მასალების ატვირთვის სიჩქარე გააუმჯობესოს. კონფიდენციალურობის დოკუმენტში ასევე აღნიშნულია, რომ პლატფორმის მიერ შეგროვებული მომხმარებელთა მონაცემები შესაძლოა Tik-Tok-ის მფლობელ პარტნიორ ორგანიზაციებს ან ჩინეთის სამთავრობო ორგანოებს კანონით გათვალისწინებულ შემთხვევაში გადაეცეს, თუმცა აქ ჩნდება ძალიან მნიშვნელოვანი კითხვა იმასთან დაკავშრებით, თუ რას გულისხმობს ჩინეთში ,,კანონით გათვალისწინებული შემთხვევა“ და როდის ხდება ეს? აღსანიშნავია, რომ ჩინეთის მთავრობამ შეიმუშავა კანონი ,,სახელმწიფო სადაზვერვო საქმიანობის“ შესახებ,[293] რომელიც ავალდებულებს ჩინურ კომპანიებს, რომ მათ გარკვეული სახის მონაცემები სახელმწიფო ორგანოებს გადასცენ. ამ კანონის თითოეული ასპექტის სიღრმისეულად გაშლა შორს წაგვიყვანს, თუმცა უნდა აღვნიშნო, რომ Tik-Tok-ზე დარეგისტრირებულთა მონაცემების გამოთხოვაც სწორედ ჩინეთის მთავრობას შეუძლია მისი მფლობელი ჩინური კომპანიისგან, მიუხედავად იმისა, რომ Tik-Tok-ის მონაცემთა ბაზა ამერიკაში მდებარეობს. ეს კი საკმაოდ საფრთხის შემცველია და აპლიკაციის მიმართ ნდობას გარკვეულწილად ამცირებს.

ზოგიერთმა კრიტიკოსმა TikTok–ის მიდგომა მონაცემთა მოპოვებისადმი აგრესიულად შეაფასა და აღნიშნა, რომ აპლიკაციას აქვს შესაძლებლობა, თვალყური ადევნოს მომხმარებლის ქცევას აპლიკაციის გამოყენების დროს, მას აგრეთვე აქვს მომხმარებლის ფოტოებზე წვდომა, შეუძლია გეოლოკაციის თვალის დევნება (მომხმარებლის ნებართვების საფუძველზე), რაც ნიშნავს, რომ მას შეუძლია შექმნას მისი მომხმარებლების ძალიან დეტალური ქცევითი პროფილები, რომელთა პოტენციურად გაზიარება შესაძლებელია ჩინეთის მთავრობის მიერ.

2020 წლის 7 ივლისს Wall Street Journal-მა გამოაქვეყნა ინფორმაცია, რომ TikTok თავს არიდებს კონფიდენციალურობის დაცვას, Google-ის Android-ისა და MAC-ის ოპერაციულ სისტემებში მომხმარებლების მობილური მოწყობილობიდან აგროვებს უნიკალურ იდენტიფიკატორებს, რომლებიც აპლიკაციას საშუალებას აძლევს თვალყური ადევნოს მომხმარებლებს ინტერნეტით.[294]

თუ შევადარებთ Tik-Tok-ს სხვა სოციალურ პლატფორმებს, რომლებიც ასევე არ უჩივიან მომხმარებელთა რაოდენობას უნდა აღვნიშნოთ, რომ ისეთი სოციალური მედია პლატფორმები, როგორებიც არის Facebook და Twitter, აგროვებენ მომხმარებლებზე ინფორმაციას, თუმცა ეს პლატფორმები ევროკავშირის ტერიტორიაზე ნომინალურად ოპერირებენ და მათ უწევთ ევროკავშირის მონაცემთა დაცვის რეგულაციების გათვალისწინება. რაც შეეხება ჩინურ აპლიკაციას, ძალიან რთულია შევაფასოთ და ზუსტად განვსაზღვროთ, დაემორჩილება თუ არა ის აღნიშნულ რეგულაციებს.

---

[293] Network, C. N. (2019 წლის 26 მარტი). ''National Intelligence Law of the People's Republic'', ხელმისაწვდომია https://bit.ly/3sOG-zNE წვდომის თარიღი: 27.08.2021.

[294] რ.მაქმილანი, ლ. ლინი, შ. ლი, (2020). ''TikTok User Data: What Does the App Collect and Why Are U.S. Authorities Concerned?'' THE WALL STREET JOURNAL, 2.

ერთია ვიკვლიოთ რა სახის ინფორმაციას იტოვებს აპლიკაცია ჩვენს შესახებ და მეორე საკითხია, თუ რამდენად დაცულია თავად აღნიშნულ პლატფორმაზე ეს ინფორმაცია. თავად Tik-Tok-ს ჰქონდა უსაფრთხოების პრობლემა გასულ წელს, რაც გულისხმობდა იმას, რომ ჰაკერებს საშუალება ჰქონდათ წაეშალათ ან აეტვირთათ მომხმარებელთა ვიდეოები, მათ ასევე წვდომა ჰქონდათ მომხმარებელთა პერსონალურ მონაცემებზე, მაგ: ელ-ფოსტის მისამართებზე.

3.1. Tik-Tok- ზე პერსონალური მონაცემების დამუშავება და მისი როლი ამ პლატფორმის მომხმარებელთა მონაცემების დაცვის საკითხში

ზემოხსენებულიდან ჩანს, რომ ჩინური აპლიკაცია მომხმარებელთა ძალიან ბევრ მნიშვნელოვან პირად ინფორმაციას ინახავს. ეს ინფორმაცია შემდეგ გროვდება და მუშავდება, რათა პლატფორმის საბოლოო ანგარიში შეიქმნას. ეს ძირითადად მოიცავს ტექნიკურ და ქცევით ინფორმაციას. რთული ტექნიკური სამუშაოს შესრულების შემდეგ პლატფორმაზე მუშავდება მომხმარებელთა პერსონალური მონაცემები, ასევე მომხმარებელთა კონტენტი (ფოტოები, ვიდეოები, აუდიოები), მომხმარებელთა კომენტარები, სტრიმები, ინახება და პერსონალურ მონაცემთა გარკვეულ ნაწილზე ავტომატური წვდომის უფლებაც ენიჭება.

3.2. Tik-Tik -ის კონფიდენციალობის პოლიტიკა და აპლიკაციის უსაფრთხოების შეფასება სხვადასხვა ქვეყანაში

Tik-Tok-ის კონფიდენციალურობის პოლიტიკა განსხვავდება აპლიკაციის მომხმარებელთა საცხოვრებელი ადგილის მიხედვით. უფრო კონკრეტულად კი, აშშ-ში აპლიკაციის მომხმარებელთათვის მოქმედი კონფიდენციალურობის პოლიტიკა განსხვავებულია ევროკავშირის ზონაში შემავალ ქვეყნებში მოქმედი კონფიდენციალურობის პოლიტიკისგან და თავის მხრივ, ეს უკანასკნელი გასხვავდება ამ ზონის გარეთ არსებული სახელმწიფოებში მოქმედი კონფიდენციალურობის პოლიტიკისგან. კვლევის პროცესში განხილულ იქნა სამივე სახის კონფიდენციალურობის პოლიტიკა, რათა მათ შორის განსხვავება-მსგავსება უკეთ წარმოჩენილიყო.

3.3. აშშ-ს კონფიდენციალურობის პოლიტიკა

Tik-Tok და მასთან დაკავშირებული რისკების მასშტაბი და სპეციფიკა სრულიად განსხვავებულია. ვფიქრობ, რომ დღეს, მტრის ხატად მხოლოდ შეიარაღებული ადამიანი კი არ უნდა წარმოვიდგინოთ, არამედ ჰიბრიდული საფრთხეების ეპოქაში ის ციფრული პლატფორმებიც, რომლებიც ავტონომიურობის დაბალი ხარისხითა და კონკრეტული სახელმწიფოს პოლიტიკის გატარებით გამოირჩევა. ასეთ ციფრულ პლატფორმად დღეს Tik-Tok სახელდება. აშშ სწორედ იმ ქვეყანათა რიცხვს მიეკუთვნება, სადაც ჩინური აპლიკაცია ყველაზე სწრაფად გავრცელდა და ამასთან აშშ ერთ-ერთი პირველი ქვეყანაა, რომელმაც ამ პლატფორმის სანდოობაში ეჭვი შეიტანა. საფრთხე, რომლის საშიშროებასაც ვხედავთ, შესაძლოა სწორად შევაფასოთ და გარკვეული ნაბიჯები გადავდგათ მის აღმოსაფხვრელად, თუმცა ბრძოლის არენაზე, რომელსაც ინფორმაციული ველი ჰქვია, რთულია აქ არსებული ინფორმაციის გაკონტროლება. ეს პრობლემა არ აწუხებს მხოლოდ

ამერიკას, ეს მსოფლიო გლობალური პრობლემაა და იქამდე არსებობდა, სანამ ჩინური კომპანია Tik-Tok-ის აპლიკაციას შექმნიდა. ამით იმის თქმა მსურს, რომ მსოფლიოს ისეთი უძლიერესი სახელმწიფოც კი, როგორიც ამერიკაა, უძლური აღმოჩნდა ტექნოლოგიურად მზარდი ჩინეთის წინააღმდეგ. თამამად შეიძლება ითქვას, რომ საკითხი სახელმწიფოთაშორის ურთიერთობამდეც დადის, რადგან აშშ-მ ჩინეთის სახელმწიფოებრივი ღირებულებების და მასთან არსებული გეოპოლიტიკური დაძაბულობის ფონზე შეაფასა რა აღნიშნული აპლიკაციის საფრთხე, 2019 წელს დაიწყო ეროვნული უსაფრთხოების შემოწმების პროცედურების ფარგლებში აპლიკაციის შესწავლა.[295]

სიღრმისეული კვლევის შედეგად გამოვლინდა, რომ ამერიკაში Tik-Tok კიბერუსაფრთხოებისთვის მნიშვნელოვანი რისკების შემცველია. მეტიც გასულ წელს აშშ-ს თავდაცვის დეპარტამენტმა სამხედრო სამსახურებისთვის აკრძალა Tik-Tok-ის გამოყენება. რეკომენდაცია გაიცა ასევე სახელმწიფო დეპარტამენტის თანამშრომლებზეც აპლიკაციის გადმოწერისგან და მისი გამოყენებისგან თავის შეკავების შესახებ. 2019 წელს კიბერუსაფრთხოების კომპანია ჩეკ პოინტის მიერ გამოქვეყნებული კვლევის თანახმად, Tik-Tok დაუცველია გარე შეღწევებისგან (ერთ-ერთ გზად იდენტიფიცირებულია არაავთენტური მოკლე ტექსტური შეტყობინებები პროგრამაში ავტორიზაციისთვის), შესაბამისად, მნიშვნელოვანი საფრთხის ქვეშ არის მომხმარებელთა მონაცემები. ამდენად, აშშ-სთვის საფრთხის შექმნის კონტექსტში 4 ძირითადი რისკია იდენტიფიცირებული: სახელმწიფო დეპარტამენტის თანამშრომლების მონაცემების შეგროვება, რიგითი მოქალაქეების მონაცემების შეგროვება, დეზინფორმაციის გავრცელება, ჩინეთის მთავრობის მიერ არასასურველი ინფორმაციის ცენზურა. პოლიტიკურად მგრძნობიარე პოსტების დაბლოკვასთან დაკავშირებით ინფორმაცია გაავრცელეს Tik-Tok-ის ამერიკის ოფისის თანამშრომლებმაც. ამ საკითხზე შეშფოთება გამოითქვა შეერთებული შტატების სენატში და გაჟღერდა საკითხის დეტალურად შესწავლის ინიციატივა.[296]

ამდენად, აშშ-ს მთავრობამ 2019 წელს Tik-Tok-ის მზარდი გავრცელების გამო შეშფოთების საპასუხოდ აკრძალა მისი გამოყენება, რადგან თუ აპლიკაცია მომხმარებელთა გარკვეული სახის მონაცემებს აგროვებს, ეს შესაძლებელია ჩინეთის სამთავრობო ხელისუფლების ხელთ აღმოჩნდეს, რაც შესაძლოა შემდეგ მანიპულირების იარაღიც გახდეს.

3.4. ინდოეთის მიერ აპლიკაციის უსაფრთხოების შეფასება

ინდოეთი, თავისი ნახევარ მილიარდი ინტერნეტით მოსარგებლე ადამიანით, გლობალური ტექნოლოგიური კომპანიების განვითარებადი არენაა აშშ-სა და ჩინეთს შორის. ინდოეთმა, როგორც ტიკ-ტოკის გადმომწერთა რეიტინგში მოწინავე პოზიციაზე მყოფმა ქვეყანამ, გასულ წელს აკრძალა შპს ByteDance-ის ვირუსული მოკლე ვიდეოს სერვისი- TikTok და 58 სხვა ჩინური პროგრამა იმის გამო, რომ ის საფრთხეს უქმნიდა მის სუვერენიტეტს და უსაფრთხოებას, რადგან ურთიერთობა მსოფლიოს ორ უდიდეს მოსახლეობას შორის გაუარესდა.

[295] Richter, F. "Where TikTok Has Been Downloaded the Most". statista's blog, 2020 წლის 30 ივნისი, ხელმისაწვდომია: https://bit.ly/2WlHDgl წვდომის თარიღი: 27.08.2021.

[296] Z. Doffman, "TikTok Confirms 'Severe' SMS Security Threat": Critical New Update Released, Forbes'report, 2020.

უპრეცედენტო მორატორიუმის და ჰიმალაიში საზღვართან დაძაბულობის შედეგად 20 ინდოელი ჯარისკაცი დაიღუპა, რომელიც ჩინეთის ტექნოლოგიის ყველაზე ცნობილ სახელებს აყენებდა დარტყმას. აკრძალული სერვისები მოიცავდა ელექტრონული კომერციის გიგანტ Alibaba Group Holding Ltd.- ს UC Web-ს, სოციალური მედიის ლიდერს Tencent Holdings Ltd.-ს WeChat– ს და Baidu Inc.– ს რუკასა და თარგმანულ პლატფორმებს.

ინდოეთის მხრიდან გადადგმული ეს ნაბიჯი აღნიშნავს, იმას, რომ შეამციროს დამოკიდებულება მეზობლის პროდუქტებზე და ხელი შეუშალოს ჩინეთის უდიდესი კორპორაციების მცდელობებს გაფართოვდეს საკუთარი საზღვრების მიღმა - კოლექტიური მცდელობას, რომელიც მოიცავს TikTok–ის ფენომენალურ წარმატებას საზღვარგარეთ და განსაკუთრებით ინდოეთში, ByteDance- ის უდიდეს საერთაშორისო ბაზარზე. ამ ყველაფერმა კი აზიის ორ უდიდეს ეკონომიკას უდიდესი ზიანი მიაყენა. ინდოეთმა ამით ფაქტობრივად ჩინეთის კიბერ ჯაჭვიდან გამოსვლის გადაწყვეტილება მიიღო.

ByteDance-სთვის, რომელიც ინდოეთს თავის უდიდეს ბაზრად თვლის 200 მილიონზე მეტი TikTok მომხმარებლით, ეს ნაბიჯი განსაკუთრებული დარტყმაა, თუმცა ინდოეთის მთავრობამ კომერციული სარგებლის მიღების მიუხედავად, დროებით მაინც აკრძალა Tik-Tok-ის აპლიკაციის გამოყენება თავის ქვეყანაში, რომელიც სხვადასხვა ექსპერტების შეფასებით ეროვნული უსაფრთხოებისთვის უმნიშვნელოვანესი ნაბიჯია. ამდენად, ინდოეთის კონფიდენციალურობის პოლიტიკა Tik-Tok-თან დაკავშირებით ძირითადად მომდინარეობს სახელმწიფოთაშორის ურთიერთობის დაძაბულობით და ინდოეთი კომერციულ სარგებელზეც კი ამბობს უარს, რათა ჩინეთის მძლავრი კიბერ ჯაჭვიდან გამოვიდეს.[297]

3.5. ტიკ-ტოკის კონფიდენციალურობის პოლიტიკა ევროპის ქვეყნებში

ტიკ-ტოკის აპლიკაციის უპრეცენდენტო პოპულარობამ ევროპის ქვეყნებიც შეაშფოთა. ევროპის მომხმარებელთა ასოციაციამ (The European Consumer Organization) საჩივარი შეიტანა TikTok-ის წინააღმდეგ. ასოციაცია ამტკიცებს, რომ პლატფორმა არღვევს ევროკავშირის მომხმარებელთა უფლებებს, განსაკუთრებით ის ვერ იცავს ბავშვებს ბულინგისგან, არასრულწლოვანთათვის შეუსაბამო და მათ შორის სექსუალური ხასიათის კონტენტის გავრცელებისგან. ამის საპასუხოდ ევროპის არაერთმა ქვეყანამ გააძლიერა კონტროლი Tik-Tok-ზე. განსაკუთრებით გასულ წელს, როდესაც ევროპის წამყვან ქვეყნებში კორონავირუსი მძვინვარებდა, აღნიშნული საკითხი დღის წესრიგში დადგა. იტალიაში მონაცემთა დაცვის საზედამხედველო ორგანომ მიმართა ევროპის მონაცემთა დაცვის საბჭოს და მოსთხოვა, რომ აღნიშნული საკითხი სიღრმისეულად შეესწავლათ. ჩემი აზრით, იტალია ამ კუთხით იმიტომ წარმოადგენს საინტერესო მაგალითს, რომ იტალიაში მოქმედი კანონის მიხედვით, 16 წლამდე ასაკის მოზარდთა პირადი მონაცემების დამუშავებისთვის აუცილებელია მშობლების ან მეურვის თანხმობა, რაც იმას გულისხმობს, რომ ამ კანონით Tik-Tok-ის მიერ 13 წლამდე პირთა პერსონალური მონაცემების დამუშავება მშობლების ნებართვის გარეშე აკრძალულია.[298]

---

[297] Rahul Satija, Saritha Rai, "India Bans TikTok and 58 Other Chinese Apps Citing Security Concerns", Bloomberg, 2020, ხელმისაწვდომია: https://bloom.bg/3kwdLpo წვდომის თარიღი: 27.08.2021.

[298] Personali, G. P, "TikTok: the Italian DPA calls for an EU taskforce", 2020 წლის 24 იანვარი, ხელმისაწვდომია: https://bit.ly/3BgtWxN წვდომის თარიღი: 27.08.2021.

Tik-Tok-ის აპლიკაციით დაინტერესდა ასევე დიდი ბრიტანეთიც. აქ მოქმედი საზედამხედველო ორგანო აქცენტს აკეთებს და იკვლევს, არის თუ არა შესაძლებელი, რომ უცხო პირი არასრულწლოვანთან გავიდეს კონტაქტზე და მასთან ჰქონდეს მიმოწერა, რაც თავის მხრივ კიდევ უფრო საფრთხის შემცველი იქნება.

ყველაზე მნიშვნელოვანი, რაზეც ევროპის ქვეყნები აღნიშნულ საკითხთან დაკავშირებით აქცენტს სვამენ არის ის, რომ Tik-Tok არ ემორჩილება და ხშირ შემთხვევაში არ იცავს ევროკავშირის მონაცემთა დაცვის რეგულაციების (GDPR), არ იცავს არასრულწლოვანთა უფლებებს, მეტიც მათ რთავს ისეთ ვირუსულ გამოწვევაში, როგორიც არის "Tide Pod Challenge", რასაც სავალალო შედეგებამდე მივყავართ.

ვინაიდან აღნიშნულ საკითხს უფრო კომპლექსურად უდგებიან ევროპაში, სამომავლოდ იგეგმება TikTok–ის „ევროპული გამჭვირვალობისა და ანგარიშვალდებულების ცენტრი"-ის გახსნა ირლანდიაში. სავარაუდოდ, ცენტრი ევროკავშირის პოლიტიკოსებს და უსაფრთხოების მკვლევარებს მისცემს წვდომას აპის შიდა ტექნიკურ და ბიზნეს საქმიანობაზე, რაც მათ დაეხმარება საზოგადოების დარწმუნებაში, რომ სოციალური მედიის პლატფორმა სერიოზულად ეკიდება ბავშვის უსაფრთხოებას და პირად ცხოვრებას.[299]

3.6. საქართველოს მაგალითი

ვფიქრობ, საინტერესოა ჩვენი ქვეყნის მაგალითის განხილვაც აღნიშნულ საკითხთან დაკავშირებით. საქართველოში Tik-Tok პოპულარული გახდა განსაკუთრებით სავალდებულო კარანტინის დროს. ერთი შეხედვით უწყინარმა გასართობმა ტრენდმა საქართველოშიც უდიდესი პოპულარობა მოიპოვა. აპლიკაციის პოპულარობის ზრდასთან ერთად იმატა მისმა საფრთხეებმა ქართველ Tik-Tok მომხმარებლებზე. განსაკუთრებით კი მისი ზეგავლენა შეიმჩნევა ახალგაზრდებზე, რომლებიც თითქოს უწყინარ პლატფორმას გასართობად და რელაქსაციისთვის იყენებს. ქართველი კიბერუსაფრთხოების ექსპერტების შეფასებით, Tik-Tok ისეთივე მიჯაჭვულობას იწვევს, როგორც ნარკოტიკი. იცვლება ქცევები, მანერები, იკარგება კონცენტრაციის უნარი. მათთვის Tik-Tok-ზე კონტენტის განთავსება იქცა ერთგვარ აზარტად, ჰობად. გარდა ამ საფრთხეებისა, საქმე უფრო სერიოზულადაც არის, რადგან აღნიშნული აპლიკაციის ახალგაზრდა ქართველი მომხმარებლები ხდებიან არამხოლოდ ბულინგის, არამედ სექსტინგის (sexting) მსხვერპლებიც.[300] ეს პრობლემა არ ეხება მხოლოდ ქართველ მომხმარებლებს, ის უფრო გლობალურია, რაც კიდევ უფრო გვაფიქრებს აღნიშნული აპლიკაციის სანდოობაზე.

უფრო გლობალურად თუ შევხედავთ საკითხს, უნდა აღვნიშნოთ, რომ პრეპანდემიურ სამყაროში გააქტიურებული ჩინეთის პოლიტიკური და ეკონომიკური ინტერესები საქართველოს მიმართ პოსტპანდემიურ პერიოდში კიდევ უფრო გაიზარდა ჩვენი ქვეყნის ადგილმდებარეობისა და საერთაშორისო პოზიციონირების გათვალისწინებით. აღნიშვნის ღირსია ის ფაქტიც, რომ გასული

[299] IKEDA, S, "Tiktok Opens Transparency Center in Europe To Address Security and Privacy Concerns". CPO magazine's blog, 2021 წლის 4 მაისი, ხელმისაწვდომია: https://bit.ly/2WmfdTv წვდომის თარიღი: 27.08.2021.

[300] ლ. პატარაია, "Delete TikTok", CAUCASUS ACADEMY OF SECURITY EXPERTS's Blog, 2021 წლის 18 იანვარი, ხელისაწვდომია: https://bit.ly/3DgMFLH წვდომის თარიღი: 01.07.2021.

წლის 12 მაისს სოციალური ქსელების მომხმარებელთა მხრიდან შემჩნეულ იქნა, რომ ტიკ-ტოკ-ს მსოფლიოს ქვეყნებისა და რეგიონების ჩამონათვალში დამატებული აქვს აფხაზეთი და სამხრეთ ოსეთი, როგორც ცალკე სახელმწიფოები.[301] აღნიშნული ფაქტი სერიოზული განხილვის საგანი გახდა საქართველოს საგარეო საქმეთა სამინისტროს მხრიდან. ეს უკანასკნელი ამ ფაქტს გამოეხმაურა. საქართველოს ელჩმა ამის შესახებ ჩინეთში შეხვედრებიც კი გამართა. ამის შემდეგ აპლიკაციამ შეცვალა ეს ინფორმაცია, თუმცა, ჩემი აზრით, განხილვის საგნად მაინც უნდა მივიჩნიოთ, რადგან ჩინურ აპლიკაციას რომ არ შეეცვალა აღნიშნული ინფორმაცია, შესაძლოა ამას გაემწვავებინა ვითარება ჩვენს მეზობელ სახელმწიფოსთან და დაძაბავდა მათთან ურთიერთობას.

მნიშვნელოვანია, რომ ადეკვატურად შეფასდეს საფრთხეები სხვადასხვა ასპექტით. ვფიქრობ, რომ აპლიკაციასთან დაკავშირებული რისკების ფონზე, ქართული ნაციონალური ინტერნეტ პროვაიდერის მხრიდან სოციალური ქსელის პოპულარობის ხელშეწყობა, რაციონალურობის ასპექტში, ბევრ კითხვის ნიშანს აჩენს.

4. დასკვნა

ნაშრომის მთავარ ამოცანას წარმოადგენდა აღნიშნული აპლიკაციის წარმოუდგენლად დიდი პოპულარობის ფონზე, პერსონალური მონაცემების დაცვის პრობლემის ჩვენება. საყურადღებოა ის ფაქტიც, რომ ხშირად ამ აპლიკაციის სამიზნე აუდიტორიას სწორედ არასრულწლოვნები წარმოადგენენ, რომელიც კიდევ უფრო ამძაფრებს და ამავდროულად ართულებს საკითხის სიღრმისეულად შესწავლას და აღნიშნული საფრთხეებისგან თავის დაცვას. Tik-Tok-ის მსოფლიო ბაზარზე გამოჩენიდან დღემდე, გაიზარდა იმ ქვეყნების რაოდენობაც, რომელთა მთავრობებიც დაეჭვდნენ აღნიშნული აპლიკაციის უსაფრთხოებაში. ამ პროცესმა მიიღო უფრო მასშტაბური სახე. განხილვის საგანი გახდა ის, თუ როგორ გროვდება ჩინურ პლატფორმაზე მომხმარებელთა პირადი ინფორმაცია, რა ტიპის ინფორმაციას ინახავს აპლიკაცია და რა საფრთხეებს ქმნის ეს პერსონალურ მონაცემთა დაცვის კუთხით. აღმოჩნდა, რომ კონფიდენციალურობის პოლიტიკა, რომელიც აპლიკაციას აქვს და მუდმივად აახლებს და აწვდის მას მომხმარებლებს, ბოლომდე არ არის საიმედო და არ იძლევა იმის გარანტიებს, რომ არ მოხდება მომხმარებელთა ინფორმაციის გასაჯაროება.

ამდენად, სანამ აპლიკაციასთან დაკავშირებული საფრთხეების შესახებ დამატებითი დეტალები გახდება ცნობილი, მნიშვნელოვანია, თითოეულმა ჩვენგანმა გავაცნობიეროთ, თუ რა პროგრამას ვიწერთ ჩვენს ელექტრონულ მოწყობილობებში, რა მოცულობით ვაძლევთ მას დაშვებას და რა სახის პერსონალურ მონაცემს ვხდით ხელმისაწვდომს. სოციალური ქსელების სპეციფიკა იმითაც არის უნიკალური, რომ პლატფორმაში ინფორმაციის გავრცელებას შეუქცევადობა ახასიათებს. შესაბამისად, მონაცემების უკანონო დამუშავების შემთხვევაში, პრაქტიკულად შეუძლებელია სრულ რეპარაციასა და პირვანდელი მდგომარეობის აღდგენაზე საუბარი. ამდენად, ამ ეტაპზე, ჩემი აზრით, Tik-Tok-ის საფრთხეებისგან თავის დაცვისა და პრევენციის ერთადერთი მექანიზმი საზოგადოების ცნობიერების ამაღლება და პასუხისმგებლობის ტვირთის ინდივიდებზე გადანაწილებაა.

[301] ლ. პერტაია,"საგარეო მუშაობს, რათა TikTok-ზე აფხაზეთი და სამხეთ ოსეთი ცალკე აღარ გამოყონ". ნეტგაზეთი, 2020, ხელისაწვდომია აქ: https://netgazeti.ge/news/451949/ წვდომის თარიღი: 27.08.2021.

სახის ამომცნობი სისტემის მიერ პერსონალურ მონაცემთა დამუშავება

ავტორი: ნათია მეფარიშვილი [302]
თბილისის სახელმწიფო უნივერსიტეტი

1. შესავალი

ადამიანის სხეულის ნაწილები დიდი ხანია გამოიყენება იდენტიფიკაციისათვის, მაგალითად, თითის ანაბეჭდები, გამომდინარე იქედან, რომ ის ყველა ადამიანს ინდივიდუალური აქვს. დღესდღეობით აქტიურად ხდება სახის ამომცნობი სისტემების დანერგვა. ყველა აღნიშნული მონაცემი, რასაც ამომცნობი სისტემა იყენებს, განეკუთვნება ბიომეტრიულ მონაცემებს. მოცემულ ნაშრომში განხილული იქნება სახის ამომცნობი სისტემების მიერ პერსონალური მონაცემების დამუშავება, რისკები, რომლებიც ამ პროცესში შეიძლება წარმოიშვას და მათი გადაჭრის სამართლებრივი გზები. განსაკუთრებული ყურადღება დაეთმობა სახის ამომცნობი სისტემის გამოყენებას კომერციულ ვაჭრობაში, აუთენტიფიკაცია/ვერიფიკაციის დროს სხვადასხვა აპლიკაციაში და სოციალურ ვებგვერდებზე. ამასთან, სხვადასხვა ქვეყანაში განსხვავებული მიდგომაა იმასთან დაკავშირებით, ფოტოთი იდენტიფიკაციისას მოცემული მონაცემი ჩვეულებრივ პერსონალურ მონაცემს განეკუთვნება თუ განსაკუთრებული კატეგორიის პერსონალურ მონაცემს, ასევე ბიომეტრიული მონაცემი თავად არის თუ არა განსაკუთრებული კატეგორიის მონაცემი. შესაბამისად, ნაშრომში განხილული იქნება აღნიშნული საკითხებიც. ასევე, დღესდღეობით პანდემიის პირობებში აქტიურად გამოიყენება პირბადე და საინტერესოა, ახდენს თუ არა სახის ამომცნობი სისტემა ადამიანის იდენტიფიცირებას პირბადით.

2. ბიომეტრიული მონაცემები და მისი მახასიათებლები

ევროკავშირის რეგულაცია EU 2016/679 (GDPR) ბიომეტრიულ მონაცემს განმარტავს, როგორც პერსონალურ მონაცემებს, რომლებიც მიიღება ფიზიკური პირის ფიზიკური, ფიზიოლოგიური ან ქცევითი მონაცემების კონკრეტული დამუშავების შედეგად და რომელიც იძლევა ფიზიკური პირის უნიკალურად იდენტიფიცირების ან იდენტიფიკაციის დადასტურების საშუალებას, მაგალითად, სახის გამოსახულება ან დაქტილოსკოპიური მონაცემები.[303] ბიომეტრიული მონაცემი შესაძლოა იყოს უნივერსალური, უნიკალური და მუდმივი. უნივერსალური - აჩვენებს, რომ ბიომეტრიული მახასიათებლები არსებობს ყველა ადამიანში.[304] შეიძლება ზოგიერთი მნიშვნელოვანი მახასიათებელი

[302] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - გვანცა სოფრომაძე.

[303] GDPR, მუხლი 4(14).

[304] Article 29 Data Protection Working Party, Working document on biometrics, August 1, 2013. 00720/12/EN WP80

რამე უბედური შემთხვევის შედეგად ადამიანმა დაკარგოს, დაზიანდეს, თუმცა, მიუხედავად ამისა, სახეზე ემოციის გამოხატვა მაინც მუდმივი რჩება.[305]

უნიკალური - აღნიშნული სახის მონაცემი გამოიყენება იმისთვის, რომ ორი ერთმანეთისგან განსხვავებული ინდივიდი ერთმანეთისგან გაიმიჯნოს.[306] ყველა ადამიანს აქვს განსხვავებული სახე, რომელიც მხოლოდ მისთვის არის დამახასიათებელი. ადამიანებს შესაძლებლობა აქვთ ერთმანეთი სწორედ ასე გაარჩიონ და ეს უნარი უკვე კომპიუტერებშიც არის ჩანერგილი.

მუდმივი - ბიომეტრიული მონაცემი არის მუდმივი და ის დროის ცვლასთან ერთად ვერ შეიცვლება. მიუხედავად იმისა, რომ დაზიანებების, წონის მომატების ან კლების გამო შეიძლება ადამიანის ვიზუალი შეიცვალოს, მისი სახის მონაცემი მაინც არ იცვლება. აღნიშნულის გამო კომპიუტერულ სისტემას შესაძლოა დამატებითი შემოწმება დასჭირდეს, რაც ასევე უფრო მეტ ფინანსურ რესურსთან იქნება დაკავშირებული.

3. სახის ამომცნობი სისტემა

ევროკავშირის დირექტივა 95/46/EC-ზე მოსაზრება 02/2012 განმარტავს სახის ამოცნობას, როგორც ციფრული სურათების ავტომატურ დამუშავებას, რომელიც შეიცვას ინდივიდების სახეებს იდენტიფიკაციის, აუთენტიფიკაცია/ვერიფიკაციისა და კატეგორიზაციის მიზნით. სახის ამოცნობა შედგება შემდეგი პროცესისგან:[307]

ა) სურათის აღქმა: აქ იგულისხმება პროცესი, როდესაც ადამიანის სახე ფიქსირდება და გადადის ციფრულ ფორმატში.

ბ) სახის გამოსახულების მონიშვნა.

გ) ნორმალიზაცია - გამოსახულების სტანდარტულ ზომაზე გარდაქმნა, ფერის გასწორება და სხვა.

დ) მახასიათებლის მოპოვება: ამ დროს ხდება მახასიათებლის პოვნა, შემდგომ იქმნება ბიომეტრიული შაბლონი და ინახება მონაცემთა ბაზაში. ამ შაბლონიდან მოხდება სხვა ამოცნობების შესრულება.

ე) შედარება-ამოცნობა - ამ დროს ხდება ახალ მახასიათებლებსა და სისტემაში ადრე დარეგისტრირებულს შორის მსგავსების დადგენა. საბოლოო შედეგამდე გასასვლელად, ანუ

[305] Jain Anil და Kumar Ajay, "Biometric Recognition: An Overview in Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context", Springer Netherlands -The

International Library of Ethics, Law and Technology, 2012, გვ. 49- 79.

[306] De Marisico Maria და სხვები, „Face Recognition in Adverse Conditions", IGI Global 2014, გვ. 361. ხელმისაწვდომია: https://bit.ly/2UX4kqs წვდომის თარიღი: 03.07.2021.

[307] Agagu TT და Akinnuwesi B., „ Automated Students' Attendance Taking in Tertiary Institution using Facial Recognition Algorithm" , 19(2) Journal of Computer Science and Its Application, 2012, ხელმისაწვდომია:

https://bit.ly/2WrxwpY წვდომის თარიღი: 03.07.2021; Art. 29 Data Protection Working Party (2012a), Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192.

ამოსაცნობად უკეთესია, რაც მეტი ინფორმაციაა შეგროვებული. სისტემა მიზნად ისახავს ინდივიდუალური მახასიათებლების გაგებასაც, როგორებიც არის სქესი, ასაკი, ეთნიკური ნიშანი, ტანსაცმელი და სხვა. შესაბამისად, სახის ამომცნობი სისტემები გამოიყენება არა მხოლოდ ინდივიდის იდენტიფიკაციისთვის, არამედ მათი ცალკეული მახასიათებლების იდენტიფიცირებისთვისაც.

3.1. ავტომატური სახის ამოცნობა კომერციულ ვაჭრობაში

დღესდღეობით არსებობს ციფრული რეკლამები, რომლებიც იძლევა საშუალებას, გაანალიზოს მომხმარებლის დამოკიდებულება პროდუქციისადმი. დიდ მაღაზიებში დამონტაჟებულია ეკრანები, რომ მიიქციოს მომხმარებელთა ყურადღება და მოხდეს პროდუქციის რეკლამირება.[308] პრაქტიკულად აღნიშნული შემდეგნაირად ხორციელდება: სავაჭრო დაწესებულებებში განთავსებული სარეკლამო ეკრანების წინ დგანან მომხმარებლები, ამ დროს ეკრანზე ჩნდება სხვადასხვა პროდუქციის რეკლამა. ეკრანი ახდენს ბიომეტრიული მონაცემების დამუშავებას, მაგალითად, სქესი, ასაკი, ქცევის კლასიფიკაცია.[309] ამ სისტემის საშუალებით კომპანია ადგენს კონკრეტული პროდუქტის მიმართ მომხმარებელთა ხედვას, ემოციურ რეაქციას და შემდგომში იყენებს ამ ინფორმაციას მომხმარებლისთვის უკეთესი სერვისის შესაქმნელად.[310] ასევე, პროგრამას შეუძლია სქესის მიხედვით განსაზღვროს, რომელი სქესის წარმომადგენელს რომელი პროდუქციის მიმართ რა სახის ემოცია დაუფიქსირდათ. ამის შემდგომ ამ ადამიანებს შეიძლება მეილებიც დაეგზავნოთ პერსონალურად კონკრეტული შეთავაზებით.

აღნიშნული ციფრული მაიდენტიფიცირებლის ტექნოლოგია გადის ამოცნობის იმ საფეხურებს, რომლებზეც წინა თავში ვისაუბრე. ბოლო ეტაპი გულისხმობს შედარება-ამოცნობას. ამ დროს, ასევე ხდება შემდეგ კითხვაზე პასუხის გაცემა: იყო თუ არა ბოლოს ეკრანთან მისული მომხმარებელი იგივე, ვინც უკვე ნამყოფი იყო მასთან?[311]

3.2. სახის ამომცნობი სისტემები აუთენტიფიკაცია/ვერიფიკაციის დროს

აღნიშნული სისტემა ნელ-ნელა უფრო და უფრო ვითარდება, განსაკუთრებით კი საბანკო სფეროში. აღნიშნულის მეშვეობით საბანკო დაწესებულებები ამაღლებენ უსაფრთხოების სტანდარტებს. წამყვანი კომპანიები, რომლებიც რთულ კომპიუტერულ ალგორითმებს ქმნიან, მუშაობენ უსაფრთხოების სტანდარტის გაზრდაზეც, რისთვისაც ნერგავენ სახის ამომცნობ სისტემებს. მაგალითად, ორ უმსხვილეს კომპანიას „Google-სა“ და “Apple-ს“ აღნიშნული უკვე დანერგილი აქვთ. ფინანსური დაწესებულებებისთვის ეს უფრო და უფრო გამოყენებადი ხდება ფინანსური ტრანზაქციების

---

[308] Borut Batagelj და სხვები, „Computer Vision and Digital Signage“ , Tenth International Conference on Multimodal Interfaces, 2009წ, ხელმისაწვდომია: https://bit.ly/3BheLoi წვდომის თარიღი: 03.07.2021.

[309] იქვე.

[310] Exeler J და სხვები, „Digital Signs that react to Audience Emotion, 2nd Workshop on Pervasive Advertising“, გვ. 38-44, 2009, ხელმისაწვდომია: https://bit.ly/3sNTJKU წვდომის თარიღი: 03.07.2021.

[311] Farinella GM და სხვები, „Face Re-Identification for Digital Signage Applications'“ Springer Image Processing Laboratory, Department of Mathematics and Computer Science University of Catania, 2014 წ. ხელმისაწვდომია: https://bit.ly/3yo3LmW წვდომის თარიღი: 03.07.2021.

განხორციელების დროს. როდესაც მომხმარებელს სურს გადაიხადოს ამა თუ იმ ბანკის ანგარიშიდან, სელფის გადაღებით ხდება მათი იდენტობის დადგენა და მხოლოდ ამის შემდეგ ხდება სასურველი პროდუქციის შეძენა.[312] აღნიშნული მეთოდი ანაცვლებს ე. წ. პინ კოდებისა და პაროლების გამოყენებას, ვინაიდან ისინი დღესდღეობით აღარ არის ბოლომდე სანდო.

ჩვენს ეპოქაში ადამიანები სოციალურ ქსელებში განათავსებენ მაღალი რეზოლუციის მქონე ფოტოს, რომელსაც ისეთი კარგი ხარისხი აქვს, რომ მას ხშირად თაღლითები იყენებენ იმისთვის, რომ სახის ამომცნობი სისტემა შეცდომაში შეიყვანონ.[313] აღნიშნულისგან თავდასაცავად სახის ამომცნობ სისტემასთან ერთად მობილურ აპლიკაციებში დამატებით დაშვებაზე თანხმობაც არის გათვალისწინებული ტრანზაქციის განხორციელებისას.

3.3. სახის ამომცნობი სისტემა სოციალურ ქსელებში

დღესდღეობით სოციალურ ქსელში ატვირთული ფოტოების რაოდენობა ძალიან დიდ ოდენობას აღწევს. ადამიანები ასევე ტვირთავენ ვიდეოებს და ლაივ გადაღებებს. ყოველივე აღნიშნული იწვევს იმას, რომ პერსონალური ინფორმაცია ხდება უფრო და უფრო ღია. ამის შედეგად, როცა ეს ინფორმაცია სხვა ადამიანებამდე მიდის, ის ექცევა თანამფლობელობაში და იმისთვის, რომ არ დაირღვეს მონაცემთა დაცვის ნორმები, მათ შორის სწორი კოორდინაციაა საჭირო.[314]

2010 წლის დეკემბერისთვის Facebook-ს დაემატა ახალი ფუნქცია - „მონიშვნის შეთავაზება“ (Photo Tag Suggest). აღნიშნული ფუნქცია იყენებს სახის ამომცნობ სისტემას იმისთვის, რომ მოხდეს ინდივიდთა იდენტიფიცირება და ხდება ახალ ატვირთულ ფოტოზე არსებული პიროვნების შესაბამისობა წარსულში ატვირთულ ფოტოსთან, რომელზეც იგივე პიროვნება იყო მონიშნული.[315] შესაბამისად, როდესაც Facebook-ზე ახალ ფოტოს განვათავსებთ, სისტემა ავტომატურად ატარებს ფოტოზე არსებულ სახეს მეგობრების სიას და ახდენს მის იდენტიფიცირებას.[316]

3.4. შუაღედური დასკვნა

წინა თავებში განსაზღვრულ იქნა ბიომეტრიული მონაცემების რაობა, ის, რომ ის აქტიურად გამოიყენება სახის ამომცნობი სისტემის მიერ. ამასთან დეტალურად იქნა მიმოხილული რა ეტაპებს გადის პროგრამა იქამდე, სანამ უშუალოდ ამოიცნობს პიროვნებას და ბოლოს, რომელი დაწესებულებები იყენებენ მოცემულ სისტემას ძალიან ხშირად და რა მიზანს ემსახურება მისი დანერგვა.

---

[312] Richardson Deidre, „Mastercard’s new “selfie authentication” takes advantage of photo feature Popularity“ Inferse.com, 5 July 2015.

[313] Keyurkumar Patel და სხვები, „Secure Smartphone Unlock: Robust Face Spoof Detection on Mobile“ 15(15) MSU Technical Report MSU-CSE-15-15, 2015წ, გვ. 1-13. ხელმისაწვდომია: https://bit.ly/3DqJNMq წვდომის თარიღი: 03.07.2021.

[314] Wisnieski Pamela და სხვები, „Facebook Apps and Tagging: The Trade-off between Personal Privacy and Engaging with Friends“ 66(9) JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY, 2015, ხელმისაწვდომია: https://bit.ly/3DmUbVj წვდომის თარიღი: 03.07.2021.

[315] Yanna Welinder, „A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS“ 6(1) Harvard Journal of Law & Technology, 2012წ, გვ. 166-192. ხელმისაწვდომია: https://bit.ly/3zmn5CF წვდომის თარიღი: 03.07.2021.

[316] Palmer Maija, „Regulators probe Facebook’s facial recognition“, Financial Times, 2011.

4. იდენტიფიკაციის, უსაფრთხოებისა და პროფილირების რისკები სახის ამომცნობი სისტემის გამოყენებისას მონაცემთა დაცულობისთვის

უპირველეს ყოვლისა, უნდა აღინიშნოს, რომ საქართველოში მოქმედებს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“. აღნიშნული კანონი თითქმის მსგავსია ევროკავშირის (EU)2016/679 დირექტივისა პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ. გამომდინარე იქედან, რომ აღნიშნული დოკუმენტი ვრცელია და საქართველო იზიარებს მის შინაარს, აღნიშნულ რისკებს განვიხილავ ამ დოკუმენტიდან გამომდინარე.

ნებისმიერი სისტემა, რომელიც დაკავშირებულია პერსონალური მონაცემების დამუშავებასთან, არის რისკის შემცველი. შესაბამისად, შემდეგ თავებში განხილული იქნება ის რისკები, რაც შეიძლება არსებობდეს მონაცემთა დამუშავების დროს.

4.1. ჰისკზე დაფუძნებული მიდგომის კონცეფცია მონაცემთა დაცვის ზოგადი ჰეგულაციის მიხედვით

GDPR-ის მე-4 მუხლის თანახმად, პერსონალური მონაცემი ეს არის ნებისმიერი ინფორმაცია, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.[317] რეგულაციის 75-ე მითითების თანახმად, ფიზიკურ პირთა უფლებებისა და თავისუფლებების შელახვის რისკი, შეიძლება გამოწვეული იყოს პერსონალური მონაცემების დამუშავებით, რომელსაც შედეგად შეიძლება მოყვეს ფიზიკური, მატერიალური ან არამატერიალური ზიანი, კერძოდ: როცა დამუშავებას შეიძლება მოყვეს დისკრიმინაცია, პირადობის მოპარვა ან გაყალბება, ფინანსური დანაკარგი, რეპუტაციის შელახვა, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დაკარგვა, ფსევდონიმიზაციით დაცული ინფორმაციის არაუფლებამოსილი გამჟღავნება, ან სხვა სახის ეკონომიკური ან სოციალური პრობლემა; ან როცა მუშავდება იმგვარი პერსონალური მონაცემები, რომლებიც ამჟღავნებს პირის რასობრივ ან ეთნიკური წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიური მრწამსს, პროფესიული კავშირის წევრობას, ასევე გენეტიკურ და ჯანმრთელობასთან დაკავშირებულ მონაცემებს, ან როცა მუშავდება დიდი რაოდენობის პერსონალური მონაცემები, რაც მონაცემთა სუბიექტების უფლებებზე ახდენს სერიოზულ გავლენას და ასე შემდეგ.[318] ამავე დოკუმენტის 89-ე მითითება კი საუბრობს მაღალ რისკზე, ესე იგი, როდესაც მონაცემები მუშავდება ახალი ტექნოლოგიების მეშვეობით, ახალი ტიპის დამუშავების მეთოდებით, რომლის მიმართაც არ არის განხორციელებული რისკების შეფასება.

რისკის ანალიზის მთავარი მიზანი არის, რომ განისაზღვროს რისკი და შემდეგ მოხდეს მისი მართვა.

[317] GDPR, მუხლი 4.

[318] GDPR, მითითება 75.

სოლოვე თავის ნაშრომში მიუთითებს, რომ იდენტობის ქურდობა ერთ-ერთი ყველაზე სწრაფად მზარდი დანაშაულია, რომელის ფინანსური მაქინაციებისთვის გამოიყენება.[319] გარდა ამისა, უსაფრთხოების ხარვეზები, პერსონალური ინფორმაციის უკანონო და ბოროტად გამოყენებაც ამ კატეგორიაში ექცევა.[320] უსაფრთხოების რისკები უფრო მეტად გასათვალისწინებელია და ხშირდა ხდება მისი დარღვევა ონლაინ და მობილური სახის ამომცნობი სისტემების მიერ მონაცემთა გადატანისას. მაგალითად, არსებობს ვებგვერდები, რომლებზე შესასვლელად და შემდგომი მოქმედებების განსახორციელებლად საჭიროა იმწუთიერი ფოტოს გადაღება და ატვირთვა, რათა მექანიზმმა სახე ამოიცნოს.[321] ერთი მხრივ, შეიძლება ითქვას, რომ სახის ამომცნობი სისტემა აუთენტიფიკაცია/ვერიფიკაციის მიზნებისთვის დაცულობის მაღალ მაჩვენებელს ავლენს, თუმცა არსებობს კვლევები, მაგალითად დუკისა და მინის, რომლებიც ამბობენ, რომ მიუხედავად გართულებული სახის ამოცნობის სისტემისა, ადვილად ხდება მისთვის გვერდის ავლა, თუკი სახის ამომცნობ სისტემას იმ ადამიანის ფოტოს წარვუდგენთ, ნაცვლად იმწუთიერი სელფისა.[322] დღესდღეობით საჭიროა პროგრამების კიდევ უფრო დახვეწა უსაფრთხოების მაღალი ზომების მისაღწევად. მაგალითად, დამატებითი დაცვის უზრუნველსაყოფად ზოგიერთი ფინანსური დაწესებულება იყენებს ე. წ. ბლინკინგურ აუთენტიფიკაციას.[323] ეს შეიძლება მოიცავდეს იმას, რომ აუთენტიფიკაციისთვის ერთი ფოტო გადაღებულ უნდა იქნას თვალებგახელილ მდგომარეობაში, ხოლო მეორე თვალებდახუჭულ.

ლიტერატურაში არსებობს სახის ამომცნობ სისტემაზე შეტევის 2 სახე: Hill Climbing attackროდესაც თავდასხმა ხდება გაყალბებული სურათით და მეორე Break-In Set Attack-როდესაც ხდება სურათის რეკონსტრუქცია.[324] თუკი მონაცემების დამმუშავებლები სათანადოდ არ უზრუნველყოფენ მათ დაცულობას, მივიღებთ ცუდ შედეგს, რაც გამოიხატება ბიომეტრიული მონაცემის მოპარვაში, ეს თუ მოხდა, შეგვიძლია, მივიჩნიოთ, რომ ბიომეტრიული მონაცემი სამუდამოდ მოპარულად დარჩება.

GDPR-ის მიხედვით, მონაცემთა პროფილირება არის პერსონალური მონაცემების ავტომატური დამუშავება ფიზიკური პირის გარკვეული პიროვნული მახასიათებლების შესაფასებლად, კერძოდ, ფიზიკური პირის დასაქმების ადგილზე მუშაობის, ეკონომიკური მდგომარეობის, ჯანმრთელობის, პერსონალური მიდრეკილებების, ინტერესების, სანდოობის, ქცევის ასპექტების ანალიზისა და პროგნოზირების, რომელ(ებ)იც წარმოშობს სამართლებრივ შედეგებს სუბიექტისთვის ან მნიშვნელოვან ზეგავლენას ახდენს მასზე.[325]

[319] Solove Daniel, „A TAXONOMY OF PRIVACY“ 154(3) University of Pennsylvania Law Review, 2006.

[320] იქვე.

[321] Article 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192.

[322] Duc Nguyen და Buy Minh, „Your face is not your password“ 1(1) Security Vulnerability Research Team Bach Khoa Internetwork Security (Bkis) Ha Noi University of Technology – VietNam, 2009.

[323] Vincent James, „MasterCard unveils ‘selfie’ security checks, says heartbeat authentication could follow”, The

Verge, 2016, ხელმისაწვდომია: https://bit.ly/3ynDYLV წვდომის თარიღი: 27.08.2021.

[324] Chibba Michelle და Alex Stoianov, „On Uniqueness of Facial Recognition Templates“ 1(1) NTIA US Department of Commerce Privacy Multi-stakeholder Process: Facial Recognition Technology, 2014.

[325] GDPR, მუხლი 4(4).

GDPR-ის 22-ე მუხლის 1-ლი ნაწილის თანახმად, მონაცემთა სუბიექტს აქვს უფლება, არ დაექვემდებაროს/უარი განაცხადოს მხოლოდ ავტომატიზებულად დამუშავებას, მათ შორის პროფილირების გზით მის შესახებ ისეთი გადაწყვეტილების მიღებას, რომელიც მისთვის წარმოშობს სამართლებრივ ან სხვა სახის არსებით შედეგებს.[326] ევროკავშირის დოკუმენტზე მოსაზრება 3/2012 ახსენებს სახის ამომცნობი სისტემის პროფილირების რისკებს. დოკუმენტის მიხედვით, ავტომატური სახის ამომცნობ სისტემას შეიძლება, საშუალება ჰქონდეს, მაგალითად, კომერციულ ვაჭრობაში, საყიდლებზე სიარულისას მიჰყვეს მომხმარებელთა მარშრუტს, ჩვევებს და ასეთი სახის პროფილირებით შემდგომ ისევ მათთვის გამიზნული რეკლამა შექმნას.[327] ამასთან, ამან შეიძლება ის შედეგი გამოიღოს, რომ მაღაზიებმა შექმნან ეგრეთ წოდებული შავი სია ადამიანების, მათი ქცევიდან გამომდინარე.

4.2. ციფრული ფოტო, როგორც პერსონალური მონაცემი

GDPR-ის 32-ე მუხლი საუბრობს მონაცემთა დაცვის უსაფრთხოებაზე. მონაცემთა დამმუშავებლებმა უნდა მიიღონ სავარაუდო რისკების შესაბამისი ტექნიკური და ორგანიზაციული ზომები უსაფრთხოების უზრუნველსაყოფად.[328] ზოგადად დავა არსებობს იმაზე, ციფრული გამოსახულება არის თუ არა პერსონალური მონაცემი. თუკი მას მივიჩნევთ პერსონალურ მონაცემად, მისი დაცულობა გარანტირებული იქნება GDPR-ის მე-5 მუხლით, რომელიც აღწერს როგორ, რა მიზნით, რა მოცულობით უნდა დამუშავდეს და რა ფორმით უნდა იქნეს შენახული პერსონალური მონაცემები.

სახის გამოსახულება რომ განვმარტოთ, ეს შეიძლება, იყოს სურათი, რომელიც პირს გადაუღეს ნებისმიერ ფორმატში, იქნება ეს ნაბეჭდი, თუ ციფრული სახით.[329] როდესაც სახის ამომცნობ სისტემას ვეხებით, ამ დროს ციფრული სურათი არის ორგანზომილებიანი სურათის ციფრული ფორმით გამოსახვა.[330] ასევე, უკვე გამოიყენება სამგანზომილებიანი გამოსახულებები. დღესდღეობით, სახის ამომცნობი სისტემის მომხმარებლებისთვის თითქმის შეუძლებელია ამ სისტემით სარგებლობა ისე, რომ არ დამუშავდეს პერსონალური მონაცემები. კომერციულ ვაჭრობაში სახის ამომცნობი სისტემა აგროვებს მონაცემებს, რომლებიც გადაიტანება ე. წ. ღრუბელზე და არ ხდება მონაცემთა ფაქტობრივი შენახვა. შესაბამისად, როცა ასე შეგროვებული მონაცემები გამოიყენება იდენტიფიკაციისთვის, რა თქმა უნდა, ამ დროს მუშავდება პერსონალური მონაცემები.[331]

---

[326] იქვე, მუხლი 22(1).

[327] Cootes, & Taylor, Statistical models of appearance for computer vision, Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering, 2000, ხელმისაწვდომია: https://bit.ly/3sRd6T8 წვდომის თარიღი: 03.07.2021.

[328] GDPR, მუხლი 32.

[329] Kindt Els, სადოქტორო ნაშრომი 'The processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a Legal framework", Katholieke Univerisiteit Leuven 2012, ხელმისაწვდომია: https://bit.ly/3ztoA20 წვდომის თარიღი: 03.07.2021.

[330] Art. 29 Data Protection Working Party (2012a), Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012, 00727/12/EN WP192.

[331] Mathew Wall, „Is facial recognition tech really a threat to privacy?" BBC Technology, 2015.

არის თუ არა ციფრული ფოტო პერსონალური მონაცემი, ამის დასადგენად ასევე მნიშვნელოვანია, გამოსახულებაზე ინდივიდის სახე არის თუ არა ნათლად გარჩევადი ისე, რომ მისი ამოცნობა ადვილი იყოს. შესაბამისად, სურათის ხარისხსაც ენიჭება მნიშვნელობა. მაგალითად, ადამიანის ფოტო, რომელიც გადაღებულია შორი მანძილიდან და არის ბუნდოვანი, ხშირად არ მიიჩნევა პერსონალურ მონაცემად.

როდესაც კომერციულ ვაჭრობაში სახის ამომცნობ სისტემას იყენებენ, მიზანი არ არის თვითონ ადამიანის ამოცნობა, არამედ მისი ემოცია არის მნიშვნელოვანი. შესაბამისად, მართალია, ამ დროს ხდება მონაცემთა დამუშავება, მაგრამ ადამიანის პერსონალურ მონაცემთა დარღვევის რისკი იკლებს, გამომდინარე იქედან, რომ კომპანიების მიზანი მხოლოდ მათი ემოციების შემოწმებაა.[332]

4.3. ბიომეტრიული მონაცემი, როგორც განსაკუთრებული კატეგორიის ახალი მონაცემი

GDPR-ის მე-9 მუხლი აღწერს განსაკუთრებული კატეგორიის მონაცემების დამუშავების საკითხებს. ამ მუხლის მიხედვით, აკრძალულია ისეთი მონაცემების დამუშავება, რომლებიც ამჟღავნებს პირის რასობრივ ან ეთნიკურ წარმომავლობას, პოლიტიკურ შეხედულებებს, რელიგიურ ან ფილოსოფიურ მრწამსს, პროფესიული კავშირის წევრობას, ასევე დაუშვებელია გენეტიკური და ბიომეტრიული მონაცემების დამუშავება, რომლის მიზანი ფიზიკური პირის უნიკალურად იდენტიფიცირებაა, აგრეთვე ჯანმრთელობასთან, ფიზიკური პირის სქესობრივ ცხოვრებასთან ან სექსუალურ ორიენტაციასთან დაკავშირებული მონაცემების დამუშავება.[333] არსებობს მოსაზრება, რომ სახის გამოსახულება სწორედ განსაკუთრებული კატეგორიის მონაცემებში უნდა მოექცეს, გამომდინარე იქედან, რომ სახის ამომცნობ სისტემას შეუძლია, დაადგინოს პირის რასობრივი ან ეთნიკური წარმომავლობა.[334] ევროკავშირის წევრმა ზოგიერთმა ქვეყანამ, როგორიც არის ესტონეთი და ჩეხეთი, მიიჩნიეს, რომ ფოტოგამოსახულება საჭიროებდა მეტ სამართლებრივ დაცვას და ისინი განსაკუთრებული კატეგორიის მონაცემებში აქცევენ ბიომეტრიულ მონაცემებსაც.

GDPR-ის 51-ე მითითებაში წერია, რომ ფოტოების დამუშავება შეიძლება არ ჩაითვალოს განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავებად, ვინაიდან ფოტოები შეესაბამება ბიომეტრიული მონაცემების განმარტებას მხოლოდ მაშინ, როცა მათ დამუშავება ხდება სპეციალური ტექნიკური საშუალებებით, რომლებიც ფიზიკური პირის ამოცნობის ან დადგენის საშუალებას იძლევა.[335]

[332] Lewinski Peter და სხვები, „Face and Emotion Recognition on Commercial Property under EU Data Protection“, 33(9) Psychology & Marketing, Wiley Periodicals, 2016, გვ. 729-746, ხელმისაწვდომია: https://bit.ly/3kraPdL წვდომის თარიღი: 03.07.2021.

[333] GDPR, მუხლი 9

[334] S. Lu და A. Jain, „Ethnicity identification from face images“ in Proceedings SPIE Defense and Security Symposium, Orlando, 2004, ხელმისაწვდომია: https://bit.ly/38oCbeJ წვდომის თარიღი: 03.07.2021.

[335] GDPR, მითითება 51.

4.4. პერსონალური მონაცემების დამუშავება GDPR-ის მიხედვით

GDPR-ის მე-5 მუხლი ჩამოთვლი პრინციპებს, რომლებიც გათვალისიწინებული უნდა იქნეს პერსონალური მონაცემების დამუშავების დროს. მონაცემები უნდა დამუშავდეს:

- კანონიერად, სამართლიანად, გამჭირვალედ;
- უნდა შეგროვდეს კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნისათვის და არ უნდა დამუშავდეს სხვა, ამ მიზანთან შეუთავსებელი მიზნით ;
- უნდა იყოს ადეკვატური, რელევანტური და დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია დამუშავების მიზნების მისაღწევად;
- უნდა დამუშავდეს იმგვარად, რომ სათანადო ტექნიკური ან ორგანიზაციული ზომების მეშვეობით უზრუნველყოფილი იყოს მათი უსაფრთხოება, მათ შორის, დაცული იყოს უკანონო და არაუფლებამოსილი პირების მიერ დამუშავების, შემთხვევით დაკარგვის, განადგურების ან დაზიანებისაგან.[336]

სამართლებრივი საფუძველი აუცილებელია მონაცემის დასამუშავებლად. განვიხილოთ Facebook-ზე ფოტოზე მონიშვნის შეთავაზება. თუკი მომხმარებელი თანხმობას განაცხადებს მონიშვნაზე, მონაცემის დამუშავება უნდა წარიმართოს პირადი ცხოვრების დაცვის წესით. ფოტოზე მომხმარებლის მონიშვნის შემდეგ ამ სახელთან დაკავშირებული სხვა ფოტოები, ზედმეტსახელები და ყველა სხვა მონაცემი, რაც ამ პირთანაა დაკავშირებული, უნდა წაიშალოს.[337]

თუკი კომერციულ ვაჭრობაში სახის ამომცნობ სისტემას შევეხებით, ამ დროს მონაცემთა მაკონტროლებელი ვალდებულია, განსაზღვროს მიზანი, თუ რისთვის აგროვებს მონაცემებს. ბუნდოვანი ან ზოგადი მიზანი, მაგალითად მომხმარებელთათვის მომსახურების გაუმჯობესება, მარკეტინგული მიზნები, უსაფრთხოების მიზნები ან მომავალ კვლევაზე მითითება არ არის საკმარისი კონკრეტული მონაცემების დასამუშავებლად.[338] მითუმეტეს, თუკი სახის გამოსახულებას მოვაქცევთ განსაკუთრებული კატეგორიის მონაცემთა სფეროში, მისი დამუშავება ზოგადად აკრძალულია, თუ GDPR-ის მე-9 მუხლის მე-2 ნაწილით გათვალისწინებული მოთხოვნები არ იქნება დაკმაყოფილებული, როგორებიცაა მონაცემთა სუბიექტის თანხმობა, თუ დამუშავება აუცილებელია სასიცოცხლო ინტერესების დასაცავად, თუ ეს მონაცემი საჯაროდ გამოაქვეყნა სუბიექტმა და სხვა.[339] აქედან მოკლედ იქნება განხილული თანხმობის ელემენტი. GDPR-ის მე-4 მუხლის მე-11 ნაწილის თანახმად, თანხმობა ნიშნავს მონაცემთა სუბიექტის სურვილს ნებაყოფლობით, კონკრეტულ, ინფორმირებულ, მკაფიო გამოხატულებას, რომელიც გადმოცემულია განცხადებით ან აქტიურად გამოხატული ქმედებით.[340] კომერციულ ვაჭრობაში აღნიშნული

[336] იქვე, მუხლი 5.

[337] Article 29 Data Protection Working Party (2012b), Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193.

[338] იქვე.

[339] GDPR, მუხლი 9(2).

[340] იქვე, მუხლი 4(11).

ქმნის პრობლემას, რადგან მომხმარებელს არც პირდაპირ უარის თქმა შეუძლია და არც მკაფიო თანხმობის გამოხატვა, რომ მისი მონაცემი დამუშავდეს სახის ამომცნობი სისტემის მიერ. ზოგადად ყურადღების მისაქცევი ნიშნები დიდ მაღაზიებში აჩვენებენ, რომ სახის ამოცნობა მიმდინარეობს და ეს შეიძლება გულისხმობდეს მომხმარებლის თანხმობას. თუმცა, ამავდროულად კანონის მოთხოვნაა ნათლად გამოხატული თანხმობა. ასეთ დროს თანხმობის მტკიცების ტვირთი არის მოვაჭრეზე, შესაბამისად ისინი მეტად დაინტერესებული უნდა იყვნენ იმით, რომ თანხმობას უფრო მკაფიო სახე ქონდეს, მაგალითად წერილობითი.[341] უნდა ითქვას, რომ ჩვეულებრივი აღნიშნული თანხმობა მოპოვებულია იმავე კომპანიის მიერ მომხმარებლისთვის შეთავაზებული სხვა მომსახურებიდან გამომდინარე. მაგალითად, როცა მომხმარებელი ერთვება ლოიალობის პროგრამაში.[342] რაც ეხება სახის ამომცნობი სისტემის გამოყენებას აუთენტიფიკაცია/ვერიფიკაციის დროს, აქ თანხმობის გარდა დამატებითი მონაცემიც არის საჭირო, რათა კონფიდენციალურობის მექანიზმი დაცული იყოს. მაგალითად, პაროლის შეტანაც არის აუცილებელი.[343]

4.5. მონაცემთა უსაფრთხოების დაცვა (დაშიფვრა, ფსევდონიმიზაცია, უსაფრთხოების დარღვევის შეტყობინება, მონაცემთა დაცვის ხისკების შეფასება)

GDPR-ის 32-ე მუხლი ჩამოთვლის იმ ზომებს, რომლებიც უფლებამოსილმა პირებმა უნდა მიიღონ მონაცემთა დამუშავებისას უსაფრთხოების უზრუნველსაყოფად. ეს ზომებია: პერსონალურ მონაცემთა ფსევდონომიზაცია და დაშიფვრა, დამუშავების სისტემისა და სერვისების მუდმივი კონფიდენციალურობა, ხელშეუხებლობა, ხელმისაწვდომობა და მოქნილობა, მათი ეფექტიანობის რეგულარული შემოწმება და სხვა.[344]

4.5.1. მონაცემთა დაშიფვრა

მონაცემის დაშიფვრა არის ტექნიკა, რომლითაც კრიპტოგრაფული აღნიშვნები უკავშირდება ბიომეტრიულ მონაცემს. აღნიშნული იწვევს იმას, რომ ნებისმიერი პირისთვის, რომელსაც წვდომა არ აქვს მონაცემზე, გაუგებარია მოცემული პერსონალური ინფორმაცია.[345] ამასთან, შიფრი და მონაცემი ერთმანეთისგან განცალკევებულად უნდა იქნეს შენახული, იმისთვის რომ თავდამსხმელებს არ მიეცეთ შიფრის გახსნის შესაძლებლობა.

[341] Lewinski Peter და სხვები, „Face and Emotion Recognition on Commercial Property under EU Data Protection“, 33(9) Psychology & Marketing, Wiley Periodicals, გვ. 729-746, 2016, ხელმისაწვდომია: https://bit.ly/3ysMv0c წვდომის თარიღი: 04.07.2021.

[342] იქვე.

[343] Yanna Welinder, „A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS“, 6(1) Harvard Journal of Law & Technology, გვ. 166-192, 2012წ, ხელმისაწვდომია: https://bit.ly/3zolUCG წვდომის თარიღი: 04.07.2021.

[344] GDPR, მუხლი 32.

[345] Gerard Spindel დაPhillip Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation“ 7(1) JIPITEC- Journal of Intellectual Property Information technology and E-commerce Law, 2016.

4.5.2. მონაცემთა ფსევდონიმიზაცია

GDPR-ის 28-ე მითითება განმარტავს, რომ პერსონალურ მონაცემთა ფსევდონიმიზაციას შეუძლია შეამციროს მონაცემთა სუბიექტების უფლებების დარღვევის რისკები და ხელი შეუწყოს მონაცემთა დამმუშავებლებს და უფლებამოსილ პირებს მონაცემთა დაცვასთან დაკავშირებული ვალდებულებების შესრულებაში.[346] GDPR-ის მე-4 მუხლის მე-5 ნაწილის თანახმად, 'ფსევდონიმიზაცია' ნიშნავს პერსონალური მონაცემების იმგვარ დამუშავებას, როდესაც დამატებითი ინფორმაციის გამოყენების გარეშე შეუძლებელია პერსონალური მონაცემების დაკავშირება კონკრეტულ მონაცემთა სუბიექტთან, იმ პირობით, რომ ეს დამატებითი ინფორმაცია შენახულია ცალკე და ტექნიკური და ორგანიზაციული ზომების მეშვეობით მონაცემების დაკავშირება არ ხდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირთან.[347]

4.5.3. უსაფრთხოების დარღვევის შეტყობინება

GDPR-ის 33-ე მუხლი ითვალისწინებს პერსონალურ მონაცემთა უსაფრთხოების დარღვევის შემთხვევაში მონაცემთა დამმუშავებლის ვალდებულებას დაუყონებლივ ან არაუგვიანეს 72 საათისა საზედამხედველო ორგანოსთვის შეტყობინების ვალდებულებას.[348] შეტყობინების ვალდებულებას არ წარმოშობს ყველა ტიპის დარღვევა. მონაცემთა დარღვევა 3 კატეგორიად შეიძლება დავყოთ.

პირველი - როცა არავითარი რისკის ქვეშ არ დგას პირის უფლებები და თავისუფლებები. ასეთ დროს შეტყობინების ვალდებულება არ წარმოიშობა.[349] მეორე - თუ უფლებებისა და თავისუფლებების დარღვევის რისკი სავარაუდოა, ასეთ დროს 72 საათში უნდა მოხდეს შესაბამისი უწყებისთვის შეტყობინება.[350]

მესამე - უფლებებისა და თავისუფლებების დარღვევის მაღალი რისკი როდესაც არსებობს. ასეთ დროს სავალდებულოა შეტყობინება ყოველგვარი გადადების გარეშე.[351] აღნიშნული სახის რისკების წარმოქმნა, თუ რამდენად იწვევს სახის ამომცნობი პროგრამა რისკს ან მაღალ რისკს ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ, მსჯელობის საგანია. შეიძლება ითქვას, რომ უმეტეს შემთხვევაში მაღალი რისკისგან დაცულია სახის ამომცნობი სისტემა გამომდინარე იქედან, რომ ის არის ახალი ტექნოლოგია, ამასთან ამოცნობისას უკვე სისტემაში მომხმარებლის მიერ შაბლონის სახით ატვირთულ ფოტოსთან ხდება შედარება და ასევე მისი სისტემური მონიტორინგი მიმდინარეობს.[352]

[346] GDPR, მითითება 28.

[347] GDPR, მუხლი 4(5).

[348] იქვე, მუხლი 33.

[349] იქვე, მუხლი 31.

[350] იქვე, 33(1) მუხლი.

[351] იქვე, 34(1) მუხლი.

[352] Maldoff Gabriel, „The Risk-Based Approach in the GDPR: Interpretation and Implications", 2016, ხელმისაწვდომია: https://bit.ly/3my1nIe წვდომის თარიღი: 04.07.2021.

4.5.4. მონაცემთა დაცვის ჩისკების შეფასება

GDPR-ის 35-ე მუხლის თანახმად, თუკი სავარაუდოა, რომ მონაცემთა კონკრეტული ტიპის დამუშავება თანამედროვე ტექნოლოგიების გამოყენებით შესაძლოა იწვევდეს პირთა უფლებებისა და თავისუფლებების დარღვევის მაღალ რისკებს, მონაცემთა დამმუშავებელმა დამუშავების დაწყებამდე უნდა ჩაატაროს დაგეგმილი ოპერაციების რისკების შეფასება.[353] ამავე მუხლის მე-3 ნაწილის თანახმად რისკების შეფასება განსაკუთრებით მნიშვნელოვანია, თუკი მონაცემთა დამუშავება ავტომატური საშუალებით ხდება, მონაცემთა პროფილირების დროს.[354] ეს კი ის არის, რასაც კომერციულ ვაჭრობაში იყენებენ სახის ამომცნობი სისტემის მეშვეობით. შესაბამისად შეიძლება ითქვას, რომ რისკების წინასწარი შეფასება იმ კომპანიებისთვის, რომლებიც სახის ამომცნობ სისტემას იყენებენ, აუცილებელიც არის.

4.6. შუალედური დასკვნა

მოცემულ თავებში გაანალიზებულ იქნა ის, რომ სახის ფოტო შეიძლება შეფასდეს, როგორც პერსონალური მონაცემი, რამდენადაც ის მიემართება იდენტიფიცირებულ ან იდენტიფიცირებად ადამიანს. ამდენად, მასზე ვრცელდება GDPR რეგულაცია. ასევე, ზოგიერთ ქვეყანაში სახის ფოტო მიჩნეულია ასევე განსაკუთრებული კატეგორიის პერსონალურ მონაცემად. სიტუაცია უფრო რთულად არის, როდესაც ფოტო ბუნდოვანია, შორი მანძილიდან არის გადაღებული. ასეთ დროს ის პერსონალურ მონაცემად არ მიიჩნევა.

ასევე, განხილულ იქნა რისკები, რომლებიც სახის ამომცნობი სისტემის მიერ მონაცემთა დამუშავებამ შეიძლება გამოიწვიოს, უშუალოდ დამუშავების პროცესი და უსაფრთხოების ზომებიც, რომლებიც მონაცემთა დამმუშავებელმა უნდა გაატაროს პერსონალურ მონაცემთა დამუშავების დროს.

5. პრაქტიკული მაგალითები სახის ამომცნობ სისტემასთან მიმართებით

მოცემულ თავში განხილულ იქნება რამდენიმე პრაქტიკული შემთხვევა, როდესაც სახის ამომცნობმა სისტემამ ვერ უზრუნველყო სათანადო დაცულობა.

უპირველეს ყოვლისა, განვიხილავ ორი ტყუპი ძმის საქმეს, რომელთაც სარჩელი შეიტანეს “Apple-ის“ წინააღმდეგ და ითხოვენ კომპენსაციას 357 000 დოლარის ოდენობით. ძმებმა შეიძინეს აიფონ X, რომელიც იყენებს სახის ამომცნობ სისტემას მობილურის განბლოკვისას. ორივე ძმამ შეძლო ერთმანეთის ტელეფონის განბლოკვა თავიანთი სახის დაფიქსირებით. სისტემა ძმებს ვერ აღიქვამს სხვადასხვა პიროვნებად და ნებას რთავს შევიდნენ სისტემაში. ძმების ადვოკატი მიუთითებს, რომ მყიდველები კომპანიის მხრიდან აღნიშნულის თაობაზე არ არიან გაფრთხილებული და ადანაშაულებს კომპანიას პერსონალური მონაცემების დარღვევაში.

---

[353] GDPR, მუხლი 35(1).

[354] იქვე, მუხლი 35(3).

მეორე შემთხვევა კვლავ კომპანია Apple-ის წინააღმდეგ იყო და ამჟამად სახის ამომცნობი სისტემა შეცდომაში შევიდა შემდეგნაირად. 15 წლის ძმამ შეძლო საკუთარი სახით 21 წლის ძმის მობილური ტელეფონის განბლოკვა სახის ამომცნობი სისტემის საშუალებით.

2016 წელს ილინოისის ორმა მაცხოვრებელმა უჩივლა “Snapchat-ს“. ისინი სარჩელში მიუთითებდნენ, რომ აპლიკაციის სახის ამომცნობი სისტემა უკანონოდ ინახავდა მონაცემს, მომხმარებელთა თანხმობის გარეშე, რადგან მითითება იმაზე, თუ რამდენ ხანს შეინახებოდა მათი მონაცემები არსად იყო.

ასევე არსებობს ილინოისის მაცხოვრებლების სტივენ ვანსისა და ტიმ ჯანეკის სარჩელები ამაზონისა და მაიკროსოფტის წინააღმდეგ. როგორც ისინი ამბობენ, მათ 2000 იან წლებში ვებგვერდ Flick-ზე ატვირთეს თავიანთი ფოტოები. შემდგომ მათთვის შეტყობინების გარეშე კომპანია IBM-მა შექმნა მონაცემთა ბაზა 1 მილიონი ფოტოთი, რომელსაც ერქვა მრავალფეროვნება სახეებში და ამ ბაზას იყენებდა დამხმარედ, რომ განევითარებინა სახის ამომცნობი სისტემის ალგორითმი, კერძოდ, უკეთ, რომ განესხვავებინა ხალხი კანის ფერის მიხედვით. ამასთან ხდებოდა მთელი რიგი უკანონო დაკავებები, გამომდინარე იქედან, რომ ამომცნობი სისტემა ფერადკანიანებთან მიმართებით ხშირად ცდებოდა. ამაზონი და მაიკროსოფტი იყენებდნენ აღნიშნულ ბაზას, რათა გაეუმჯობესებინათ თავიანთი პროგრამული უზრუნველყოფა. მოსარჩელეები თავიანთი პერსონალური მონაცემების დარღვევის გარდა უთითებდნენ კომპანიის უსაფუძვლო გამდიდრებაზე, რადგან კომპანიამ მათი სურათების გამოყენებით, რომელზეც თანხმობა არ ჰქონია მოახდინეს თავიანთი სისტემის პროგრამული უზრუნველყოფის გაუმჯობესება. სასამართლომ სარჩელი დასაშვებად ცნო და ამავდროულად მიმდინარეობს მოლაპარაკებები კომპანიებსა და მოსარჩელეებს შორის.[355]

6. სახის ამომცნობი სისტემა და პანდემია

დღესდღეობით მთელი მსოფლიოს მასშტაბით აქტუალური გახდა პირბადეების ტარება. საინტერესოა, ახერხებს თუ არა სახის ამომცნობი სისტემა მონაცემების დამუშავებას მაშინ, როდესაც სახეზე პირბადეა მოთავსებული.

სტანდარტებისა და ტექნოლოგიის ეროვნულმა ინსტიტუტმა გამოსცადა სახის ამომცნობი 89 კომერციული ალგორითმი და აღმოაჩინა 5-50% მდე შეცდომის მაჩვენებელი მაშინ, როდესაც ისინი პირბადეებს ატარებდნენ.

პანდემიის პირობებში კომპანია დისნეიმ პარკის შესასვლელში განათავსა სახის ამომცნობი სისტემა, რომელმაც ჩაანაცვლა ბილეთი. სახის ამომცნობი სისტემა პარკში შემსვლელებს ანიჭებს უნიკალურ ID კოდს. სისტემის გამოსაყენებლად არ არის საჭირო პირბადის მოხსნა. უსაფრთხოებასთან დაკავშირებით კომპანია აცხადებს, რომ მონაცემები ინახება მხოლოდ 30 დღით და ამასთან მომხმარებლისთვის ამ გზით პარკში შესვლა არის ერთ-ერთი ალტერნატივა, შესაბამისად

[355] Katherine Anne Long , „Amazon and Microsoft team up to defend against facial recognition lawsuits“, Seatle times, 2021 April.

ხორციელდება მხოლოდ მათი თანხმობის შემთხვევაში.[356] იაპონიის ბიომეტრიულმა ფირმამ NEC Corporation-მა კი აამოქმედა სახის ამომცნობი სისტემა, სპეციალურად ნიღბის მქონე ადამიანების იდენტიფიკაციისთვის, რომელიც მათი განცხადებით 99,9 %-ით ზუსტია. აღნიშნული სისტემა ძირითადად ფოკუსირებულია ადამიანის თვალების მიმდებარე ტერიტორიაზე. მას შემდეგ რაც სისტემა დაადგენს ნიღბის არსებობას სახეზე, ის ყველა შესაფერისი ალგორითმის გამოყენებით ამოწმებს ადამიანის შესაბამისობას.[357] უნდა აღინიშნოს, რომ ამ სისტემით პოლიციის თანამშრომლებიც სარგებლობენ და მონაცემთა დამუშავების აბსოლუტური კანონიერება კითხვის ნიშნის ქვეშაა. განსაკუთრებით მას შემდეგ, რაც ჯორჯ ფლოიდის საქმის შემდეგ Amazon-მა, Microsoft-მა და IBM-მა შეაჩერეს სახის ამომცნობი ტექნოლოგიის მიყიდვა აშშ-ის სამართალდამცავი ორგანოებისთვის.

7. სახის ამომცნობი სისტემა და საქართველოს საკანონმდებლო რეგულაცია

რამდენიმე სიტყვით მინდა შევეხო საქართველოს კანონმდებლობას. საქართველოში მოქმედებს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“. უნდა აღინიშნოს, რომ მოცემული კანონი არის ძალიან ვიწრო და არ აწესრიგებს ყველა იმ შესაძლო შემთხვევას, რაც შეიძლება წარმოიქმნას მონაცემთა დამუშავების დროს. ამასთან, ვფიქრობ ცალსახად არ არის დადგენილი ფოტოსურათი, რომლითაც ამოცნობა მიმდინარეობს, განეკუთვნება უბრალო პერსონალურ მონაცემს თუ განსაკუთრებული კატეგორიის პერსონალურ მონაცემს. პერსონალური მონაცემების დამუშავების დროს აუცილებელია უსაფრთხოების ზომების დაცვა. ქართული კანონმდებლობა არ აკეთებს აღნიშნულზე არავითარ დათქმას. არ არის მონაცემთა დაშიფვრის, ფსევდონიმიზაციის, წინასწარ რისკის შეფასების მექანიზმები შემუშავებული. საქართველოში არსებული ბანკები ვფიქრობ, მალე დანერგავენ სახის ამომცნობი სისტემის მეშვეობით ტრანზაქციების განხორციელებას. შესაბამისად, საჭიროა ამ კუთხით კანონმდებლობის დახვეწა. ამასთან არავითარი ინფორმაცია არ მოიპოვება ხდება, თუ არა კომერციულ ვაჭრობაში სახის ამომცნობი სისტემების გამოყენება.

მართალია, საქართველოში საპოლიციო ორგანოები იყენებენ სახის ამომცნობ სისტემას, თუმცა უცნობია, რა გზით ხდება მონაცემთა დამუშავება და რა ზომები აქვთ გატარებული შესაბამის ორგანოებს მონაცემთა დასაცავად.

[356] James Clayton, „Facial recognition beats the Covid-mask challenge“, BBC NEWS, 25 March, 2021, სტატია ხელმისაწვდომია: https://bbc.in/3ykryEj წვდომის თარიღი: 04.07.2021.

[357] „Facial recognition identifies people wearing masks“, BBC NEWS, 2021 წლის 7 იანვარი, სტატია ხელმისაწვდომია: https://bbc.in/3ymi8bu წვდომის თარიღი: 27.08.2021.

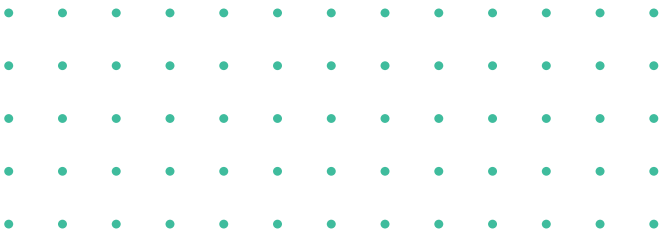
8. დასკვნა

მოცემული ნაშრომის მიზანი იყო ნათლად ყოფილიყო წარმოდგენილი ზოგადად სახის ამომცნობი სისტემის არსი, მისი გამოყენების სახეები, სისტემის მიერ მონაცემთა დამუშავება, რისკები, რომლებიც მონაცემთა დამუშავებამ შეიძლება გამოიწვიოს და უსაფრთხოების ზომები, რომლებიც მონაცემთა დამმუშავებელმა უნდა გაატაროს.

ნაშრომში ძირითადად მიმოხილული იქნა სახის ამომცნობი სისტემის მიერ პერსონალურ მონაცემთა დამუშავება კერძო კომპანიების ასპექტში. კერძოდ, განხილულ იქნა მონაცემთა ავტომატური დამუშავება კომერციული ვაჭრობის სფეროში, მონაცემთა დამუშავება აუთენტიფიკაცია/ვერიფიკაციის დროს და სოციალურ ქსელებში. აღნიშნულ საკითებზე მსჯელობისას გაანალიზებულ იქნა უამრავი უცხოელი ავტორის ნაშრომი.

საბოლოოდ უნდა ითქვას, რომ თითქმის შეუძლებელია სახის ამომცნობი სისტემის ფუნქციონირება პერსონალურ მონაცემთა დამუშავების გარეშე. ვფიქრობ, GDPR მეტნაკლებად საკმარის გარანტიებს ქმნის მონაცემთა დასაცავად, თუმცა საკვანძო რჩება სახის ამომცნობი სისტემის გამოყენებისას სუბიექტის თანხმობის საკითხი. ეს განსაკუთრებით პრობლემურია კომერციულ ვაჭრობაში. შესაბამისად, ვფიქრობ, უფრო ნათლად უნდა იქნეს შესაბამისი დაწესებულებების მხრიდან იმაზე მითითება, რომ ფუნქციონირებს სახის ამომცნობი სისტემა და მუშავდება პერსონალური მონაცემები.

GDPR-ის 22-ე მუხლი საუბრობს მონაცემთა სუბიექტის უფლებაზე, უარი განაცხადოს მონაცემთა ავტომატიზირებულ დამუშავებაზე, თუ ეს მისთვის სამართლებრივ შედეგებს წარმოშობს. აღნიშნული რეგულაცია, ვფიქრობ, ბუნდოვანია. საინტერესოა, ის იმ შემთხვევაზეც ვრცელდება თუ არა, როდესაც მონაცემთა დამუშავება არაავტომატიზირებულად ხდება.



შრომით ურთიერთობებში პერსონალური მონაცემების დაცვა ეროვნული კანონმდებლობისა და საერთაშორისო პრაქტიკის ანალიზზე

ავტორი: ნატა სუხაშვილი [358]
საქართველოს ეროვნული უნივერსიტეტი

1. შესავალი

პერსონალურ მონაცემთა დაცვა წარმოადგენს ერთ-ერთ მთავარ რგოლს, რაზეც დაშენებულია დემოკრატიული და სამართლებრივად განვითარებული სახელმწიფოს მთავარი იდეა. ფაქტობრივად, ყოველდღე იზრდება პირადი ინფორმაციის დამუშავების ინტენსივობა, რაც თავის მხრივ განპირობებულია 21-ე საუკუნის ყოველმხრივი ტექნოლოგიური, ეკონომიკური, საზოგადოებრივი მოთხოვნილებათა განვითარებით და სწრაფი ინტერნეტის კომერციალიზაციით. ნიშანდობლივია, რომ მონაცემთა სუბიექტის[359] პირადი ინფორმაციის დამუშავება შემოიფარგლება სხვადასხვა საქმიანობის არსებობით და ატარებს მუდმივად დინამიურ ხასიათს. საქმიანობის განხორციელების მიზანი და სპეციფიკურობა განსაზღვრავს იმას, თუ რომელი პერსონალური მონაცემი უნდა დამუშავდეს. მაგალითად, ეს შესაძლოა იყოს სესხის აღებისა და დაზღვევის მომენტში, შრომითი ხელშეკრულების დადებისას, პირდაპირი მარკეტინგის განხორციელებისას, მომსახურების გაწევისას და სხვა. ნაშრომში მთავარ განსახილველ თემას წარმოადგენს შრომითი ურთიერთობების დროს დამსაქმებლის მიერ პერსონალურ მონაცემთა დამუშავების პროპორციულობა და განხორციელებული ღონისძიებების შესაბამისობა ადამიანის ძირითად უფლებებსა და თავისუფლებებთან. აღნიშნული საკითხის ფართო ჭრილში განხილვა და მისი ანალიზი შესაძლებლობას მოგვცემს, დავინახოთ რეალური გამოწვევები, შევაფასოთ პრობლემები და შევიმუშაოთ ყველა ის რეკომენდაციები, რომელიც უზრუნველყოფს საზოგადოების ცნობიერების ამაღლებას, დასაქმებულთა ფუნდამენტური უფლებების დაცვას, შრომითი ურთიერთობისას ღირსეული გარემოს შექმნასა და პიროვნების შესაძლებლობების მაქსიმალურ რეალიზებას.

[358] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - გიორგი ლაზარიაშვილი.

[359] საქართველოს კანონი - „პერსონალურ მონაცემთა დაცვის შესახებ“ მე-2 პუნქტის „ვ“ ქვეპუნქტი, ხელმისაწვდომია: https://bit.ly/3mEiMiC წვდომის თარიღი: 27.08.2021.

2. დამსაქმებლის მოქმედების სამართლებრივი ფარგლები და დასაქმებულთა მონაცემების დაცვა

საქართველოს კონსტიტუციის 26-ე მუხლის პირველი პუნქტის თანახმად,[360] ყველას აქვს სამუშაოს თავისუფალი არჩევის უფლება. მოცემული დანაწესი, მიზნად ისახავს შრომის თავისუფლების გარანტირებას, რაც, ერთის მხრივ, კრძალავს იძულებით შრომას, ხოლო, მეორე მხრივ, ავალდებულებს კანონმდებელს, შექმნას ადამიანის თავისუფალი არჩევანის ფარგლებში შრომის თავისუფლების უზრუნველყოფის შესაბამისი მატერიალური კანონმდებლობა. შრომითი უფლებები, როგორც სოციალურ უფლებათა ფუნდამენტი, წარმოადგენს ადამიანის ფიზიკური და სულიერი არსებობის, განვითარებისა და სრულყოფის საფუძველს, რომელიც ადამიანებს შესაძლებლობას აძლევს შრომითი ურთიერთობების პროცესში მოახდინონ საკუთარი უნარჩვევების გამოყენება და ამასთანავე იმ საქმიანობის განხორციელება, რომელიც მათ დაეხმარებათ როგორც საკუთარი, ისე საზოგადოებისა და სახელმწიფოს საუკეთესო ინტერესების წარმართვაში. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ ქვეპუნქტით დადგენილია,[361] რომ პერსონალური მონაცემი ეს არის ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. პირი იდენტიფიცირებადია, როდესაც შესაძლებელია მისი იდენტიფიცირება პირდაპირ ან არაპირდაპირ, კერძოდ, საიდენტიფიკაციო ნომრით ან პირის მახასიათებელი ფიზიკური, ფიზიოლოგიური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური ნიშნებით. შრომითი ურთიერთობების დროს კი, უმეტეს შემთხვევაში ხდება მონაცემების ორ ეტაპად დამუშავება, თუმცა შეიძლება არსებობდეს მესამე ეტაპიც, როდესაც პირი აღარ არის შრომით ურთიერთობაში კომპანიასთან, თუმცა მისი მონაცემები გარკვეული ვადით ინახება დამსაქმებელთან. პირველი ეტაპი, ეს არის გასაუბრების დროს და მეორე - შრომითი ხელშეკრულების მოქმედების პერიოდში. ეს მონაცემები შესაძლოა იყოს კანდიდატის CV, სადაც ასახულია სახელი, გვარი, საკონტაქტო ტელეფონის ნომერი, ელექტრონული მისამართი, სამუშაო გამოცდილება. ამასთანავე, შესაძლოა იყოს შერჩევის პროცესში წარმოებული საგამოცდო შედეგები, გასაუბრების დროს მოპოვებული ინფორმაცია, რომელიც თავისი არსით შესაძლოა იყოს განსაკუთრებული კატეგორიის მონაცემი,[362] ხოლო, სამუშაოს განხორციელებისას შესაძლოა დამუშავდეს დასაქმებულის სამსახურში შესვლისა და გამოსვლის დროები, მათი ვიზუალური გამოსახულება ვიდეოკამერების მეშვეობით და რიგ შემთხვევაში, ბიომეტრიული მონაცემებიც. კომპანიის მხრიდან დამუშავებულ მონაცემთა შორის შესაძლოა იყოს განსაკუთრებულ კატეგორიას მიკუთვნებული მონაცემი, მაგალითად, ნასამართლობა, ჯანმრთელობის მდგომარეობა ან სხვა სახის ინფორმაცია, რომელიც შესაძლოა ინახებოდეს იმ ვადით, რაც არ არის მიზანშეწონილი კონკრეტული მიზნის მისაღწევად. ვიდეოკამერების მეშვეობით დასაქმებული პირის მონაცემთა დამუშავების არაერთი მაგალითი არსებობს, მათ შორის არის 2017 წლის საქმე,[363] რა დროსაც დამსაქმებელმა არ გაატარა შესაბამისი

[360] საქართველოს კონსტიტუციის 26-ე მუხლი - შრომის თავისუფლება, პროფესიული კავშირების თავისუფლება, გაფიცვის უფლება და მეწარმეობის თავისუფლება.

[361] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ, მე-2 მუხლის „ა“ ქვეპუნქტი.

[362] იქვე, მე-2 მუხლის „ბ“ ქვეპუნქტი.

[363] პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილება №გ-1/286/2017 შპს „ა“-ს შემოწმების დასრულების შესახებ ქ. თბილისი 25/05/2017.

ღონისძიებები, რომელიც განაპირობებდა დასაქმებულთა ინფორმირებას ვიდეოკონტროლის თაობაზე. ინსპექტირების ფარგლებში გამოირკვა, რომ დამსაქმებელს პერსონალის მხრიდან არ ჰქონია წერილობით თანხმობა, რომელიც აუცილებელი წინაპირობაა ვიდეკონტროლისთვის. ამდენად, კომპანიის მხრიდან ადგილი ჰქონდა დასაქმებულ პირთა მონაცემების დამუშავების უკანონობას.

იმისათვის, რომ უკეთესად შევძლოთ წარმოვადგინოთ პერსონალურ მონაცემთა დამუშავების ფარგლები, უნდა განვიხილოთ ის საკანონმდებლო ბაზა, სადაც ასახულია მონაცემთა დაცვისა და დამუშავების საფუძვლები. ამ კუთხით, ყურადსაღებია საქართველოს ორგანული კანონი „საქართველოს შრომის კოდექსის“ მე-11 მუხლი,[364] რომელიც მოიცავს სამართლებრივ მდგომარეობას და ხორციელდება შრომით ურთიერთობებში დამსაქმებელსა და დასაქმებულს შორის ინფორმაციის გაცვლის მომენტში. აღნიშნული მუხლის თანახმად, დამსაქმებელს აქვს უფლება, პოტენციური დასაქმებულის შესახებ მოიპოვოს ინფორმაცია, რომელიც პირდაპირ კავშირშია სამუშაოს შესრულებასთან, შესაბამისად ნებისმიერი სხვა სახის ინფორმაციის შეგროვება მის მიერ, დაუშვებელია. შეიძლება ითქვას, რომ შრომის კოდექსშიც არსებობს ხარვეზი ზემოხსენებულ ჩანაწერშიც, ვინაიდან კანონმდებელი არ განსაზღვრას იმ ფარგლებს, რა ფარგლებშიც დამსაქმებელს აქვს ინფორმაციის მოპოვების და გადამოწმების შესაძლებლობა. გარდა ამისა, დამსაქმებელს უფლება აქვს, კანდიდატის მიერ მიწოდებული ინფორმაციის სისწორე გადაამოწმოს, ვინაიდან შემდგომში არ გამოირკვეს ისეთი გარემოება, რომელიც უარყოფითად აისახება კომპანიის საქმიანობის ხარისხზე. რაც შეეხება თავად დასასაქმებელ პირს, მას აქვს ვალდებულება, აცნობოს დამსაქმებელს ყველა იმ ინფორმაციის შესახებ, რომელმაც შესაძლოა ხელი შეუშალოს მას სამუშაოს შესრულებაში ან საფრთხე შეუქმნას დამსაქმებლის ინტერესებს. ამავე მუხლის მე-4 პუნქტი განასაზღვრავს, რომ ნებისმიერი ინფორმაცია, რომელიც მოპოვებულ იქნა დამსაქმებლის მხრიდან, უნდა იყოს დაცული მესამე პირთა ხელყოფისაგან, გარდა იმ შემთხვევაში, თუ თავად მონაცემთა სუბიექტის თანხმობა არსებობს, ან საქართველოს კანონმდებლობით სხვა რამ არ არის გათვალისწინებული. მონაცემთა სუბიექტს უფლება აქვს მათთან დაკავშირებული ნებისმიერი სახის ინფორმაცია გამოითხოვოს, ან მოითხოვოს მისი კორექტირება ან წაშლა. ამ უკანაკნელთან დაკავშირებით სააპელაციო სასამართლო გადაწყვეტილებაში განმარტებულია, რომ მოსარჩელეს უფლება აქვს მოითხოვოს[365] მასზე არსებული პერსონალური მონაცემები, მიუხედავად იმისა დოკუმენტი მოცემულ მომენტში რა სტატუსით იმყოფება,[366] თუმცა სასამართლო აღნიშნავს, რომ ეს უფლება არ არის აბსოლუტური ხასიათის, რაც იმას ნიშნავს, რომ პირის ეს უკანასკნელი შეიძლება შეიზღუდოს, თუ ამ უფლებების რეალიზაციამ შეიძლება საფრთხე შეუქმნას დანაშაულის გამოვლენას, გამოძიებასა და აღკვეთას. საყურადღებოა თავად კომპანიების მიერ მონაცემთა შენახვის ინტერვალობა, სადაც განსაკუთრებული კატეგორიის მონაცემებიც შეიძლება ინახებოდეს, მათ შორის ნასამართლობასთან დაკავშირებით, რომელიც ასახავს სუბიექტის მიერ წარსულში ჩადენილ დანაშაულს. ამასთან დაკავშირებით საინტერესოა ადმიანის უფლებათა ევროპული სასამარ-

[364] საქართველოს ორგანული კანონი „საქართველოს შრომის კოდექსის“ მე-11 მუხლი, „1“, „2“, „3“ „4“ პუნქტები.

[365] საქართველოს კანონი „პერსონალური მონაცემთა დაცვის შესახებ“, მუხლი 15, „დ“ ქვეპუნქტი.

[366] თბილისის სააპელაციო სასამართლოს გადაწყვეტილება 3ბ/1059-15 (2016-04-26).

თლოს გადაწყვეტილება საქმეზე „S. AND MARPER v. THE UNITED KINGDOM“,[367] სადაც სასამართლო ამახვილებს ყურადღებას მონაცემთა სუბიექტის განსაკუთრებული კატეგორიის ინფორმაციის შენახვაზე. მისი განმარტებით, შენახვის ხანგრძლივობა უნდა იყოს გონივრული და მისაღწევი მიზნის შესაბამისი, ვინაიდან ეს გავლენას ახდენს ადამიანის პირად ცხოვრების ინტერესებზე. ამასთან ხაზგასმულია თანამდებობაზე მყოფი პირების სტატუსიც, რომლებიც არ არიან ნასამართლეობის მქონე პირები და ამის დამადასტურებელი დოკუმენტაციაც არსებობს, რომელიც თავის მხრივ, დანაშაულებრივი ქმედების გამომრიცხავი ფაქტია, თუმცა მაინც ინახება. პრაქტიკულად ეს დოკუმენტიც განსაკუთრებულ კატეგორიათა მონაცემად მიიჩნევა და სწორედ ამიტომ, სასამართლო განმარტავს, რომ მისი შენახვისთვის განსაზღვრული არაგონივრული ვადა, ჩარევას ახდენს პირის პირადი ცხოვრების ინტერესებზე. საქართველოში პრაქტიკა შრომით ურთიერთობებში მონაცემთა დაცვასთან დაკავშირებით მცირეა, რაც განპირობებულია დაბალი ცნობიერებითა და საზედამხედველო ორგანოსათვის დაბალი მიმართვიანობით. წარმოდგენილი პრაქტიკა კი, არის მაგალითი იმისა, რომ მსოფლიოს მრავალ ქვეყნაში არსებობს შრომითი ურთიერთობისას მონაცემთა დამუშავების პრობლემა და ამ უკანასკნელის მოწესრიგების მექანიზმებიც.

3. საერთაშორისო ორგანიზაციების მიერ მიღებული სახელმძღვანელო ინსტრუქციები

საერთაშორისო ორგანიზაციების მიერ შემუშავებული გაიდლაინები ხელშემკვრელი სახელმწიფოებისათვის სავალდებულოდ შესასრულებელია, ვინაიდან ისინი ქმნიან ერთიან სისტემას, რის მიხედვითაც სახელმწიფოებს შეეძლებათ იხელმძღვანელონ და გააუმჯობესონ პერსონალური მონაცემების დაცვის ხარისხი.[368] გამონაკლისი არც შრომითი ურთიერთობების დროს დამუშავებული ინფორმაციაა, რომელზეც ცალკე რეკომენდაციები და რეგულაციები ვრცელდება. ევროკავშირის მთავარი საკანონმდებლო აქტი - GDPR (General Data Protection Regulation) განმარტავს,[369] რომ დამსაქმებელსა და დასაქმებულს შორის პრინციპული მნიშვნელობისაა სუბიექტის თანხმობა, რომელიც უნდა იყოს თავისუფლად გაცემული, კონკრეტული, ინფორმირებული და ერთმნიშვნელოვანი. ეს ნიშნავს, რომ მონაცემთა სუბიექტმა უნდა იცოდეს, რომ ისინი თანხმდებიან და მონაცემების დამუშავებაზე გაცემული თანხმობა არ არის იძულებითი. მიუხედავად ზემოაღნიშნული განმარტებისა, GDPR ავალდებულებს დამსაქმებელს, რომ თანხმობის ეტაპამდე მან დასაქმებულს განუმარტოს, თუ რატომ ხდება მათი პირადი მონაცემების შეგროვება, რა დროის ინტერვალში იქნება შენახული მისი ინფორმაცია, რამდენად დაცულია დაშიფვრისა და მისაწვდომობის თვალსაზრისით, ხდება თუ არა მესამე პირებისათვის გადაცემა და თუ ყოფილა პრაქტიკაში ანალოგიური შემთხვევა. ასევე, პირს უნდა განემარტოს მისი უფლება მონაცემთა შეცვლაზე ან გაუქმებაზე. გლობალურმა ცვლილებებმა, რომელიც COVID 19-ის სახელით მოგვევლინა, მასშტაბური ცვლილებები ასახა, როგორც საერთაშორისო ორგანიზაციების რეგულირებაში,

[367] ადმიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე „S. AND MARPER v. THE UNITED KINGDOM“ , პარ. 120-121.

[368] იხ. ევროპის საბჭოს 108-ე კონვენციის მე-5 მუხლი და 95/46/EC დირექტივის მე-6 მუხლი.

[369] იხ. Data protection in the workplace, https://bit.ly/3mDpVQb წვდომის თარიღი: 27.08.2021.

ისე ეროვნულ კანონმდებლობაშიც. ამ კუთხით, კარგი იქნება, განხილულ იქნას საფრანგეთის შიდასამართლებრივი მოწესრიგების ფარგლები შრომის კოდექსისა და CNIL-ის საფუძველზე.

საფრანგეთში მოცემული ვითარებიდან გამომდინარე CNIL (commission natinale de l'informatique et des libertes)-ის პრეზიდენტმა მარი ლოურ დენმა საფრანგეთის ეროვნული ასამბლეის იურიდიულ კომისიასთან ხაზი გაუსვა მონაცემთა დაცვის მნიშვნელობას ჯანმრთელობის არსებული საგანგებო ვითარების ფონზე და ყურადღება გაამახვილა დამსაქმებლის ვალდებულებებზე:

- სამუშაო ადგილზე პერსონალურ მონაცემთა დამუშავების კონტროლი (covid-19-ის ფონზე)
- დამსაქმებელს ვალდებულება არ განახორციელოს ისეთი ქმედებები და ზომები, რომელითაც დაარღვევს მისი თანამშრომლების პირადი ცხოვრების ხელშეუხებლობას, განსაკუთრებით კი, იგულისხმება პირადი ჯანმრთელობის მონაცემების შეგროვება (covid-19 ის დასადგენად).
- დამსაქმებელს არ შეუძლია შეაგროვოს ზოგადი საფუძვლების, უბრალოდ გამოკითხვის, ინდივიდუალური თუ სუბიექტური მოსაზრებებზე დაყრდნობით, რომელიც დაკავშირებულია დასაქმებულ პირსა და მის ნათესავებთან.

გარდა ამისა, საინტერესო იყო თავად საფრანგეთის პრაქტიკა დასაქმებულთა სხეულის ტემპერატურის კონტროლთან მიმართებაში, სადაც CNIL და საფრანგეთის შრომის კოდექსი განსხვავებულ პოზიციას აჩვენებდა. CNIL ამბობს, რომ დამსაქმებელმა არ უნდა განახორციელოს დასაქმებული პირის ყოველდღიური სხეულის ტემპერატურის სისტემატიური კონტროლი, რაც წინააღმდეგობაში მოდიოდა საფრანგეთი შრომის სამინისტროს პოზიციასთან, რადგან მათი განცხადებით, კომპანიებს აქვთ შესაძლებლობა პრევენციული ზომები მიიღონ და განახორციელონ სისტემატიური მონიტორინგი სამუშაო ადგილზე მყოფ პირთა ტემპერატურაზე. მეორე ფაქტორი, რომელსაც ადგილი არ უნდა ჰქონდეს დამსაქმებლის მხრიდან, არის სამედიცინო ცნობარის ან კითხვარების შეგროვება ყველა თანამშრომლისაგან. მიუხედავად ამისა, საფრანგეთის შრომის კოდექსის L 4121-1 მუხლის თანახმად, დამსაქმებელს აქვს პასუხისმგებლობა თავისი დასაქმებული პირების დასაცავად გაატაროს შესაბამისი ღონისძიებები, ჩაატაროს ტრენინგები თუ სხვა პრევენციული ზომები. ამასთანავე, დამსაქმებელს შეუძლია ფლობდეს დასაქმებულის შესახებ ინფორმაციას, რომელიც მოიცავს სუბიექტის სახელს, გვარს, მის მიმართ გატარებულ პრევენციულ ღონისძიებებს, კონტაქტებს და თუ არსებობს ჯანმრთელობის გაუარესების რისკები, დამსაქმებელს წარმოეშობა უფლება დაუკავშირდეს ჯანდაცვის ორგანოებს პირის ჯანმრთელობისა და სამედიცინო მომსახურებისათვის. დამსაქმებელს ასევე შეიძლება მოეთხოვოს ბიზნესის უწყვეტობის გეგმის შედგენა, რომლის მიზანია მისი ბიზნესის არსებითი საქმიანობის შენარჩუნება. აღნიშნული გეგმა ითვალისწინებს თანამშრომელთა უსაფრთხოების დამცავ ყველა აუცილებელ ზომას, რომელიც განისაზღვრება ძირითადი საქმიანობისა და სამსახურის უწყვეტობის შესანარჩუნებლად. იმ შემთხვევაში, თუ რომელიმე თანამშრომელი აღმოჩნდება კარანტინში, კოლეგებს ეცნობებათ იდენტიფიკაციის გარეშე, თუმცა თუ სამედიცინო მოკვლევა აჩვენებს, რომ კონკრეტული პირის მიმართ გაქარწყლდა ჯანმრთელობასთან დაკავშირებული რისკები, ნებისმიერი სახით და გზით მოპოვებული პირის მონაცემები აუცილებლად

იშლება ყოველგვარი სუბიექტური ეჭვის მიუხედავად.[370] რაც შეეხება გერმანიაში შრომითი ურთიერთობისას დამუშავებული მონაცემების სამართლებრივ რეგულირებას, პანდემიის პერიოდში მკაცრად იქნა გაწერილი დამსაქმებლის ვალდებულება მის კომპანიაში დასაქმებული პირების მონაცემების დამუშავებასთან დაკავშირებით, კერძოდ კი, გერმანიაში მონაცემთა დაცვის კანონის შესაბამისად, რომელიც ეხება დამსაქმებელთა და დამსაქმებელთა მიერ პერსონალური მონაცემების დამუშავებას პანდემიის პირობებში.

- მონაცემთა დაცვის კანონის შესაბამისად დამსაქმებლების მიერ პიროვნების მონაცემთა დამუშავება ჩაითვლება კანონიერად, თუ გამოვლინდა ინფიცირება ან კონტაქტი დაინფიცირებულ პირთან და აღნიშნული მოქმედება გაამარტივებს პრევენციული ღონისძიებების გატარებას.[371]

- თუ დასაქმებული იმყოფებდა რობერტ კოხის ინსტიტუტში (RKI), რომელიც რისკის ზონას წარმოადგენდა.

- სტუმრებისა და ვიზიტორების პირადი მონაცემების (ჯანმრთელობის მონაცემების ჩათვლით) შეგროვება და დამუშავება, კერძოდ, დამსაქმებელს შეუძლია დაადგინოს დასაქმებულის კონტაქტი იმ პირთან, რომელიც ცნობილია, რომ დაინფიცირდა[372] ან თუ უკვე გადატანილი აქვს ვირუსი. განხორციელებული ზომები ყოველთვის პროპორციული უნდა იყოს, რაც იმას ნიშნავს, რომ მონაცემები უნდა იქნას დამუშავებული კონფიდენციალურად და გამოყენებული იქნას მხოლოდ კონკრეტული მიზნით. მას შემდეგ, რაც შესაბამისი დამუშავების მიზანი აღარ არსებობს, როგორც წესი, არა უგვიანეს პანდემიის ბოლოს, შეგროვებული მონაცემები დაუყოვნებლივ უნდა წაიშალოს.

4. საერთაშორისო ორგანიზაციების სახელმძღვანელო ინსტრუქციები შრომითი ურთიერთობის მხარეებისათვის

ზოგიერთ კონკრეტულ შემთხვევაში, შეიძლება კომპანიის ინტერესები გაბატონდეს და ჰქონდეს ნება დაამუშაოს კონკრეტული პირთა წრის პირადი მონაცემები. ამ კუთხით, კარგი იქნება, თუ მოვიყვანთ სხვა ქვეყნის პრაქტიკასაც და ამოვიკითხავთ იმ ძირითად თეზისებს, რითაც დადასტურდება ორგანიზაციების მიერ მონაცემთა სუბიექტის დამუშავების რელევანტურობა. ამის გამომხატველია ადამიანის უფლებათა ევროპული სასამართლოს ერთ-ერთი გადაწყვეტილება საქმეზე „LÓPEZ RIBALDA v. SPAIN“.[373] განმცხადებლები წარმოადგენენ ესპანეთის მოქალაქეებს, რომელთა აზრით დამსაქმებლის მხრიდან განხორციელდა პირადი მონაცემების უკანონო დამ-

[370] მორგან ლევისის სტატია - COVID-19 in France: Personal Data Protection in the Workplace, April 29, 2020.

[371] BDSG და მე -9 მუხლის მე -2 პუნქტი.

[372] GDPR. მე-9 მუხლის მე –2 პუნქტის (ბ) ქვეპუნქტი.

[373] ადამიანის უფლებათა ევროპული სასამართლო გადწყვეტილება საქმეზე n°1874/13 and 8567/13, Lopez Ribalda v. Spain, communicated on 17 February 2015, ხელმისაწვდომია: https://bit.ly/3gG9hvh წვდომის თარიღი: 27.08.2021.

უშავება. მოცემულ საქმეში, დამსაქმებელმა დაამონტაჟა თვალსაჩინო სამეთვალყურეო კამერები სუპერმარკეტის მთელს ტერიტორიაზე, მათ შორის სალაროებშიც, იმ მიზნით, რომ მარტივად გამოკვლეულიყო ქურდობის შესაძლო ფაქტები და მომხდარიყო თანამშრომელთა კონტროლი. კომპანიის მიერ განხორციელებული მონიტორინგის შედეგად, სამსახურიდან გათავისუფლებულ იქნა ორი თანამშრომელი ქურდობის საფუძვლით. აქვე ხაზი უნდა გავუსვათ იმას, რომ დამსაქმებლის მიერ გატარებული ღონისძიებების შესახებ, რომელიც ფარული კამერების არსებობას ითვალისწინებდა, არცერთი თანამშრომელი არ ყოფილა ინფორმირებული, მათ შორის საშტატო კომიტეტი და სწორედ ეს გახდა განმცხადებელთა პრეტენზია ECHR-ის მე-6 მუხლის 1-ლი და მე-8 პუნქტების შესაბამისად, რომ დამსაქმებელი ვალდებული იყო წინასწარ ეცნობებინა მათთვის ფარული სათვალთვალო კამერების დამონტაჟების შესახებ. კატალონიის უმაღლესმა სასამართლომ დაადასტურა, რომ სამსახურიდან გათავისუფლება კანონიერი იყო და აღნიშნა, რომ ქურდობის საფუძვლიანი ეჭვი ფარული ვიდეო მეთვალყურეობის განხორციელების ფუნდამენტური საფუძველია. აქედან გამომდინარე, ჩვენ შეგვიძლია დავასკვნათ ის, თუ რამდენად გადაწონა კომპანიის საკუთრების უფლების დაცვის ხარისხმა თანამშრომელთა პირადი სივრცის დაცვის შესაძლებლობა.

ანალოგიურად, საქმეში Köpke v Germany,[374] f Antović and Mirković v. Montenegro,[375] კომპანიის ინტერესები მეტად აღმატებული აღმოჩნდა, ვიდრე დასაქმებულის პირადი ცხოვრება, რომელიც დაცულია ადამიანის უფლებათა ევროპული კონვეციის მე-8 მუხლით.[376] ამასთან მიმართებით, დიდი ბრიტანეთის ინფორმაციის კომისრის ოფიცერმა გამოაქვეყნა მითითებები, სადაც ნათქვამია, რომ ფარული მონიტორინგი იშვიათად არის გამართლებული და ეს უნდა ხდებოდეს მხოლოდ გამონაკლის გარემოებებში, მაგალითად, საეჭვო დანაშაულებრივი საქმიანობის სპეციალურ გამოძიებაში. დამატებით მითითებებში ასევე განმარტებულია, რომ ფარული მონიტორინგი გამართლებული იქნება მხოლოდ იმ შემთხვევაში, თუკი ღიაობა ზიანს აყენებს დანაშაულის პრევენციას ან გამოვლენას, ან დამნაშავეების დაკავებას ან დევნას. სახელმძღვანელოში ნათქვამია, რომ დამსაქმებლებმა ფარული მონიტორინგი უნდა ჩაატარონ მხოლოდ უფროსი მენეჯმენტის ნებართვით, რაც კომპანიის მხრიდან განხორციელდა.

ამ უკანასკნელი მაგალითისაგან განსხვავებით, არსებობს შემთხვევა, როდესაც კომპანიას არ გააჩნია ლეგიტიმური მიზანი იმისა, რომ დასაქმებულის პირადი ინფორმაცია დაამუშავოს. ლეგიტიმური ინტერესის შესაბამისი დეფინიცია არის ის, რომ მონაცემთა დამმუშავებელმა უნდა დაამტკიცოს მყარი ფაქტებისა და ინფორმაციის საფუძველზე, რომ სუბიექტის მონაცემთა დამუშავებით რეალური მიზანი იქნება მიღწეული და ყველა სხვა, ნაკლებად მზღუდავი საშუალება არის უშედეგო. ყოველივე ეს, ადასტურებს პასუხისმგებელ პირზე/ორგანიზაციაზე მომეტებულ პასუხისმგებლობას და ვალდებულებას რომ მართლზომიერი იყოს მონაცემების დამუშავება და ინდივიდუალური ზემოქმედება. ფაქტობრივად, ეს მოითხოვს რისკების შეფასებას ყოველი კონ-

[374] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე Köpke v. Germany ((dec.), no. 420/07, 5 October 2010).

[375] ადამიანის უფლებათა ევროპული სასამართლო გადაწყვეტილება ANTOVIĆ AND MIRKOVIĆ v. MONTENEGRO.

[376] პირადი და ოჯახური ცხოვრების პატივისცემის უფლება (Right to respect for private and family life) ARTICLE 8, ხელმისაწვდომია: https://bit.ly/3Dr8sQE წვდომის თარიღი: 27.08.2021.

კრეტული შემთხვევისას, იმისათვის, რომ მონაცემების დამუშავება იყოს მიზანშეწონილი. შიდა სახელმწიფოებრივი სამართლის მსგავსად საერთაშორისო დონეზეც გამტკიცებულია პირთა უფლებები, კერძოდ GDPR (General Data Protection Regulation)-ის რეგულაციის 15-22 მუხლებით[377] აღიარებულია, რომ პირს შესაძლებლობა აქვს მოითხოვს მონაცემთა, განახლება, წაშლა, გასწორება და ნებისმიერ დროს თანხმობის გაუქმება მონაცემთა დამუშავებაზე. დიდი ბრიტანეთის შიდასახელმწიფოებრივ სამართალში არსებობს სპეციალური მექანიზმი - LIA (Legitimate Interests Assessment),[378] რომელიც უფრო აზუსტებს პერსონალურ მონაცემთა დამუშავების კანონიერებას. LIA, რომელიც თავისი არსით გულისხმობს ლეგიტიმურ ინტერესთა შეფასებას, მოიცავს იმ ტესტების ერთობლიობას, რომელიც საჭიროებს შესაბამისი პასუხების გაცემას, მაგალითად, რატომ არის აუცილებელი მონაცემთა დამუშავება, რა სარგებელი მიიღება, სარგებლობს თუ არა მესამე მხარე, რა მნიშვნელობა აქვს საზოგადოების სარგებლობისათვის, მისი დამუშავების არ გაგრძელება რა გავლენას მოახდენს და ა.შ. ლეგიტიმური ინტერესების შეფასების შაბლონი შექმნილია იმისთვის, რომ გადავწყვიტოთ, მოქმედებს თუ არა ლეგიტიმური ინტერესების საფუძველი მონაცემთა დამუშავებაზე. შესაბამისად, ის უნდა იქნას გამოყენებული ლეგიტიმური ინტერესების სახელმძღვანელოდ. კანონით შეიძლება არსებობდეს ვალდებულება, რომ დამუშავებულ იქნას სუბიექტთა მონაცემები, შესრულდეს ხელშეკრულება ინდივიდუალურ პირთან, ან დამუშავდეს მათი მონაცემები მათი თანხმობის საფუძველზე. ამასთან, ლეგიტიმური ინტერესი ცოტათი განსხვავებულია, ვინაიდან იგი არ არის ორიენტირებული კონკრეტული მიზნის გარშემო და არ ემყარება თანხმობას, ამიტომ LIA არის ის დამატებითი სახელმძღვანელო, რომელიც კიდევ ერთხელ დაადასტურებს, რომ კანონიერი ინტერესი სათანადო საფუძველია. ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე "Bărbulescu v. Romania"[379] შეეხება დამსაქმებლის უსაფუძვლო კონტროლს, რომელიც მის კომპანიაში დასაქმებული პირის მიერ იქნა განხორციელებული. პრაქტიკულად, მის მიერ წარმოებული მონიტორინგი მოიცავდა განმცხადებლის მეილის კონტროლს, რა დროსაც მოწმდებოდა პირად მიმოწერები დასაქმებულის ოჯახის წევრებთან, რაც იმას ნიშნავს რომ შეხება გვაქვს ევროპული კონვეციის მე-8 მუხლთან (მსგავსი მოწესრიგება აქვს Copland v. the United Kingdom-საქმეს),[380] რომელიც მოიაზრებს პირის პირადი ცხოვრების ხელშეუხებლობის დაცვას. სასამართლოს მიერ დგინდება, რომ კომპანიას არ ჰქონდა საფუძვლიანი ეჭვი, რომელიც მას შესაძლებლობას მისცემდა მსგავსი უკიდურესი ზომა გამოეყენებინა. წინა მაგალითებისაგან განსხვავებით, აქ არ იკვეთება კომპანიის საუკეთესო ინტერესი და შესაბამისად, გადაწყვეტილება განმცხადებლის სასარგებლოდ იქნა გამოტანილი.

[377] GDPR (General Data Protection Regulation)-ის რეგულაციები ხელმისაწვდომია: https://bit.ly/3zqehvg წვდომის თარიღი: 27.08.2021.

[378] ლეგიტიმური ინტერესების შეფასების ტესტი - LIA (Legitimate Interests Assessment, ხელმისაწვდომია: https://bit.ly/3BeQIpZ წვდომის თარიღი: 27.08.2021.

[379] ადამიანის უფლებათა ევროპული სასამართლოს გადწყვეტილება საქმეზე BĂRBULESCU v. ROMANIA (Application no. 61496/08).

[380] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე Copland v. the United Kingdom, No. 62617/00.

5. დასკვნა და რეკომენდაციები

შრომითი ურთიერთობები არის პროცესი, რომლის საშუალებითაც ადამიანი ახდენს სოციალიზაციას, საკუთარი თავის, იდეების და შესაძლებლობების ერთგვარ რეალიზაციას. პიროვნების განვითარებისთვის არსებითია თავი იგრძნოს საზოგადოების სრულფასოვან და საჭირო წევრად, რაც მნიშვნელოვნად განსაზღვრავს მის პიროვნულობას და თვითმყოფადობას. შესაბამისად, ეს უფლება პირდაპირ გადაჯაჭვულია პიროვნული განვითარების უფლებასთან.[381]

პიროვნების თავისუფალი განვითარება უპირობოდ გულისხმობს ინდივიდის არჩევანს, თავად გადაწყვიტოს, რომელ ინფორმაციას არ გახდის საჯაროს საკუთარ თავთან მიმართებით. თითოეული ადამიანის არჩევანი საჭიროებს სამართლებრივ დაცვას, რაც გარანტირებულია როგორც პოზიტიური, ისე ნეგატიური თვალსაზრისით. აღნიშნული გულისხმობს ერთი მხრივ, ინდივიდის უფლებას, რომ თავად განსაზღვროს საკუთარი ქმედებები და არჩევანი გააკეთოს იმის სასარგებლოდ, რასაც ყველაზე გონივრულად და შესაფერისად მიიჩნევს, ხოლო, მეორე მხრივ, - სახელმწიფოს ვალდებულებას, არ დაუშვას აღნიშნულ უფლებებში გაუმართლებელი ჩარევა. ინდივიდის თავისუფალი განვითარების პერსპექტივა სუსტდება პერსონალური ავტონომიურობის საეჭვოობის პირობებში, ამიტომ მნიშვნელოვანია ადამიანის პირადი სივრცის არა მხოლოდ რეალური და ფაქტობრივი ხელშეუხებლობა, არამედ ასეთი ხელშეუხებლობის ძლიერი აღქმადობა ადამიანის მხრიდან, ამისთვის კი, აუცილებელია: 1) კომპანიებმა ჩამოაყალიბონ ცალკე პოლიტიკა პერსონალურ მონაცემთა დაცვასთან დაკავშირებით, რომელიც აისახება ორგანიზაციის შინაგანაწესში და ყველა დასაქმებულს მისცემს შესაძლებლობას გაეცნოს, 2) დამუშავდეს მხოლოდ ის მონაცემები და იმ მოცულობით, რომელიც კომპანიის და დასაქმებულის საუკეთესო ინტერესიდან გამომდინარეობს, 3) უკვე დამუშავებული მონაცემები შეინახოს იმ ვადით, რაც წინააღმდეგობაში არ მოვა ადამიანის ძირითად უფლებებთან, 4) დასაქმებული პირისთვის განახლებული ინფორმაციის დროული მიწოდება. კომპანიები ვალდებულნი არიან თითოეული უფლება, რომელიც დასაქმებულებს ეხებათ, გაჯერებულ იქნეს ადამიანის თავისუფალი განვითარების უზრუნველყოფის პერსპექტივით და გათვალისწინებულ იქნას ნაშრომში განხილული რეკომენდაციები, რომლებიც მსჯელობის სახით არის წარმოდგენილი.

[381] საქართველოს კონსტიტუციის მე-12 მუხლი.

მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება

ავტორი: სოფიო დგებუაძე [382]
აკაკი წერეთლის სახელმწიფო უნივერსიტეტი

1. შესავალი

„მეორე მსოფლიო ომის შემდეგ დაწყებულმა ინფორმაციულმა ერამ სულ უფრო გაართულა პირადი ცხოვრების ხელშეუხებლობისა და პერსონალური მონაცემების დაცვა“.[383] საერთაშორისო საზოგადოების ინტერესის ობიექტი ხდება პირადი ცხოვრების ხელშეუხებლობის უფლების ისეთი მნიშვნელოვანი კომპონენტი, როგორიცაა პერსონალური მონაცემების დაცვა და მისი საერთაშორისო სამართლებრივი რეგულირება.

„სწრაფმა ტექნოლოგიურმა განვითარებამ და გლობალიზაციამ წარმოქმნა პერსონალური მონაცემების დაცვის ახალი გამოწვევები. პერსონალურ მონაცემთა შეგროვებისა და გაცვლის მასშტაბი მნიშვნელოვნად გაიზარდა. ტექნოლოგია, როგორც კერძო, ასევე საჯარო უწყებებს თავისი საქმიანობის განხორციელებისას პერსონალური მონაცემების უპრეცენდენტო მასშტაბით გამოყენების შესაძლებლობებს აძლევს“.[384]

მე-20 საუკუნის მეორე ნახევარში პერსონალურ 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.[385] დღესდღეობით, პერსონალურ მონაცემთა დაცვის, როგორც დარგის განვითარების პროცესი, ყველაზე აქტუალური და დინამიკურია და ციფრული ტექნოლოგიების განვითარების კვალდაკვალ ახალ გამოწვევებს წარმოშობს. „პერსონალურ მონაცემთა დაცვა, როგორც დინამიკურად განვითარებადი სამართლის დარგი, ინტენსიურად ვითარდება როგორც ცალკე აღებული ქვეყნების ფარგლებში, ისე რეგიონალურ დონეზეც – განსაკუთრებით კი, ევროპის საბჭოსა და ევროპის თანამეგობრობის სამოქმედო სივრცეში.“[386]

ტექნოლოგიური პროგრესის თანმდევ შედეგს პერსონალური მონაცემებისთვის განსაკუთრებული საფრთხის შექმნა წარმოადგენს. მსოფლიოს მასშტაბით ინტერნეტის ხელმისაწვდომობის ზრდასთან ერთად იზრდება მონაცემთა არაკანონიერად დამუშავებისა და გამოყენების რისკები, რაც

[382] ესეს მომზადებაში ასევე ჩართული იყო სახელმწიფო ინსპექტორის სამსახურის „პერსონალურ მონაცემთა დაცვის ელჩების პროექტის“ მონაწილე ელჩი - ნინო მაჭარაშვილი.

[383] Prof.dr. Lokke Moerel, Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future, 14 Feb, 2014.

[384] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 6.

[385] მერი წერეთელი, „პერსონალური მონაცემების დაცვის სამართლებრივი მნიშვნელობა და სტანდარტები ბიზნეს ურთიერთობებში“ 2019 წელი.

[386] გიორგი ჯოხაძე, „პერსონალურ მონაცემთა დაცვა ადამიანის უფლებათა კონტექსტში: საქართველოს მაგალითი, გამოწვევები და ტენდენციები“ წიგნში - ავტორთა კოლექტივი, რედაქტორი კ. კორკელია „ადამიანის უფლებათა დაცვის საერთაშორისო სტანდარტები და საქართველო (სტატიათა კრებული)“, 2011 წელი.

სათანადო რეაგირების მოთხოვნას წარმოშობს. საერთაშორისო სამართლებრივი რეგულირების მიზანს ინდივიდებისთვის კონფიდენციალურობის დაცვის, უსაფრთხოებისა და პერსონალურ მონაცემებზე კონტროლის მექანიზმის შექმნა წარმოადგენს.

მაშასადამე, როგორც მონაცემთა დაცვის ზოგადი რეგულაცია განმარტავს, „ევროკავშირის ტერიტორიაზე პერსონალური მონაცემების ეფექტური დაცვა საჭიროებს მონაცემთა სუბიექტების უფლებების გაფართოებას და დეტალურ ჩამოყალიბებას, იმ პირთა ვალდებულებების დადგენას, რომლებიც ამუშავებენ პერსონალურ მონაცემებს და განსაზღვრავენ მათი დამუშავების საშუალებებს, ასევე მონიტორინგთან დაკავშირებული სათანადო უფლებამოსილებისა და პერსონალურ მონაცემთა დაცვის წესების დარღვევისთვის შესაბამისი სანქციების დადგენას წევრ სახელმწიფოებში“.[387]

ზემოთქმულზე დაყრდნობით მიმაჩნია, რომ ციფრული ტექნოლოგიების განვითარების კვალდაკვალ იმატებს რისკი პერსონალური მონაცემების უკანონოდ დამუშავების, განსაკუთრებით მობილური აპლიკაციების მეშვეობით. ამ გზით მოპოვებული პერსონალური ინფორმაციის დამუშავების საფრთხეებსა და პრობლემის აღმოფხვრის გზებზე წინამდებარე ნაშრომის შემდეგ თავებში ვისაუბრებთ.

2. პერსონალურ მონაცემთა არსი და მონაცემთა სუბიექტი

ევროპის საბჭოსა და ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია „პერსონალურ მონაცემებს“ განმარტავს როგორც ინფორმაციას, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს (‘მონაცემთა სუბიექტს’)“,[388] ანუ ევროკავშირისა და ევროპის საბჭოს კანონმდებლობით სამართლებრივი დაცვით არა მხოლოდ პირის პირდაპირი, არამედ ირიბი იდენტიფიკაციის შემცველი ინფორმაციაც სარგებლობს.

მონაცემთა დაცვის ზოგადი რეგულაციით იდენტიფიცირებადი ფიზიკური პირი არის ის, ვისი პირდაპირი ან არაპირდაპირი იდენტიფიცირებაც შესაძლებელია ისეთი იდენტიფიკატორების გამოყენებით, როგორიცაა სახელი, პირადი ნომერი, ონლაინ იდენტიფიკატორი, ინფორმაცია ადგილმდებარეობის შესახებ და სხვ.[389]

შესაბამისად, სახელი, გვარი, ტელეფონის ნომერი, პირადი ნომერი, ადგილსამყოფელი ის პირველადი პერსონალური მონაცემებია, რომელთა მეშვეობით პირის პირდაპირი იდენტიფიცირების შესაძლებლობა წარმოიქმნება. ამასთანავე, „პერსონალური წერილობითი ან ვერბალური კომუნიკაცია შესაძლოა შეიცავდეს პერსონალურ ინფორმაციას და გამოსახულებებსაც, ხმას, ან ვიდეოთვალთვალის სისტემის ჩანაწერებს. ელექტრონულად ჩაწერილი ინფორმაცია, ასევე, ინფორმაცია ქაღალდზე, შესაძლოა იყოს პერსონალური მონაცემი.“ [390]

[387] მონაცემთა დაცვის ზოგადი რეგულაცია, პრეამბულა, პუნქტი 11.

[388] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4 (1).

[389] იქვე.

[390] „ვიდეოთვალთვალი და პერსონალური მონაცემების დამუშავება“, ხელმისაწვდომია: https://bit.ly/3jrEPa9 წვდომის თარიღი: 24.06.2021.

იდენტიფიკაციისთვის საჭირო ელემენტების შემცველი ინფორმაციის შეგროვებას, შეცვლას, გაცნობას, გამოყენებას, აღრიცხვა-ჩაწერას მონაცემთა დამუშავება ეწოდება.[391]

საერთაშორისო კონვენციებით/რეგულაციებით გათვალისწინებულ თითოეულ უფლებას თავისი სუბიექტი ჰყავს. გამონაკლისი არც პერსონალურ მონაცემთა დაცვის უფლებაა. როგორც ზემოთ აღვნიშნე, მონაცემთა სუბიექტი არის პირი, რომლის შესახებაც არსებული ინფორმაციით იგი იდენტიფიცირებულია ან იდენტიფიცირებადი. შესაბამისად, მონაცემთა სუბიექტს წარმოადგენს ნებისმიერი პირი, რომლის შესახებაც არსებული ინფორმაცია სხვადასხვა მიზნით მუშავდება.

მიმაჩნია, რომ მონაცემთა სუბიექტის განსაზღვრა არსებითია იმდენად, რამდენადაც მნიშვნელოვანია დადგინდეს ყოველ კონკრეტულ შემთხვევაში ვის გააჩნია დაცვის ღირსი ინტერესი პერსონალური მონაცემების დამუშავებასთან დაკავშირებით, ანუ ვინ არის აღჭურვილი უფლებებით და რამდენად არსებობს სწორედ კონკრეტულ მონაცემთა სუბიექტის „ნებართვა“ როგორც მონაცემთა დამუშავების კანონიერი საფუძველი.[392]

3. ევროპული კავშირის სამართალი და GDPR

1950 წლის ადამიანის უფლებათა ევროპული კონვენცია (ECHR) უზრუნველყოფს პირადი და ოჯახური ცხოვრების, საცხოვრისისა და მიმოწერის დაცვას,[393] ამასთან, ადამიანის უფლებათა ევროპული სასამართლო არაერთ გადაწყვეტილებაში აღნიშნავს, რომ „პირადი ცხოვრება“ არის ფართო ცნება და ამომწურავ განმარტებას არ ექვემდებარება.[394]

მართალია, პერსონალურ მონაცემთა დაცვის უფლება პირადი ცხოვრების ხელშეუხებლობის მნიშვნელოვან კომპონენტად მოიაზრება, თუმცა მხედველობაში უნდა მივიღოთ ის ისტორიული ფონი, რაც საფუძვლად დაედო პირადი ცხოვრების ხელშეუხებლობის უფლების საერთაშორისოდ აღიარებასა და დაცვის სტანდარტების ჩამოყალიბებას. „ECHR მიღებულია კომპიუტერების, ინტერნეტისა და ინფორმაციული საზოგადოების განვითარებაზე გაცილებით ადრე.“[395]

შესაბამისად, მიმაჩნია, რომ პერსონალური მონაცემების დაცვის საჭიროების წარმოქმნასთან ერთად ნათელი გახდა ამ ორი უფლების ურთიერთმიმართება - მათი კავშირი თუ განსხვავება.

ევროპული კავშირის სამართალში ახალი დარგის ჩამოყალიბებამ სათანადო საკანონმდებლო მზაობაც მოითხოვა და დღეს უკვე „წლების განმავლობაში მონაცემთა დაცვის უფლების ცალკე ღირებულებად ჩამოყალიბების შედეგად, იგი არ განიხილება პირადი ცხოვრების პატივისცემის უფლების ქვეშ.[396]

---

[391] მუხლი 4 (2), იქვე.

[392] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 4(11).

[393] ადამიანის ძირითად უფლებათა და თავისუფლებათა დაცვის ევროპული კონვენცია, მუხლი 8 (1).

[394] ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილება საქმეზე № 55480/00 და № 59330/00 „SIDABRAS AND DŽIAUTAS v. LITHUANIA), 2004 წლის 27 ოქტომბერი, § 43.

[395] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018 წელი.

[396] იქვე.

დღესდღეობით, ევროპარლამენტისა და ევროკავშირის საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 ის უმნიშვნელოვანესი საკანონმდებლო საფუძველია, რომელსაც გააჩნია სავალდებულო ძალა და ყველაზე დიდი გავლენა კომპანიების მიერ პერსონალურ მონაცემთა დამუშავების რეგულირებაზე. ვფიქრობ, იგი მნიშვნელოვანია იმდენად, რამდენადაც რეგულაციაში კონკრეტიზებულია ყველა ის სტანდარტი, რომელთა საფუძველზეც კომპანიები ამუშავებენ მონაცემთა სუბიექტის ინფორმაციას.

კერძო კომპანიებს რეგულაციის ძალაში შესვლამდე ორ წლიანი გარდამავალი პერიოდი განესაზღვრათ, რათა უზრუნველეყოთ მათ მიერ მონაცემთა დამუშავების ევროპულ სტანდარტებთან შესაბამისობა, თუმცა როგორც ჩატარებულმა კვლევამ აჩვენა, ევროპული კომპანიების მხოლოდ 50%_ს გააჩნდა საამისო მზაობა.[397]

მომხმარებელთა იდენტიფიცირებისთვის ყველა საჭირო მონაცემზე წვდომა კომპანიების მობილური აპლიკაციების მეშვეობით გააჩნიათ. ისინი იღებენ მომხმარებლის ისეთ პერსონალურ ინფორმაციას, როგორებიცაა სახელი, გვარი, პირადი ნომერი, საბანკო ანგარიში, ელ. ფოსტის მისამართი, მობილური ტელეფონის ნომერი, საცხოვრებელი მისამართი, ხშირ შემთხვევაში, ზუსტი ადგილმდებარეობა, აგრეთვე წვდომა აქვთ მოწყობილობის მიკროფონთან, კამერასთან, შესაძლოა კომუნიკაციებთან და სხვა.

თავის მხრივ, ვფიქრობ, მობილური აპლიკაციების მეშვეობით პერსონალურ მონაცემთა კანონიერი დამუშავება დიდი გამოწვევაა. ერთ-ერთი მიზანი, სხვა მრავალს შორის, რომელსაც GDPR ემსახურება, მობილური აპლიკაციების მიერ პერსონალურ მონაცემთა დამუშავების სამართლებრივი საფუძვლების დადგენაა, რომლებიც დეტალურად წინამდებარე ნაშრომის მომდევნო თავებშია განხილული.

ჩემი აზრით, GDPR-ით დადგენილი სტანდარტები საკმაოდ მაღალია და რეგულაციას პერსონალური მონაცემების დაცვის პროცესში მნიშნელოვანი წვლილის შეტანა შეუძლია. კომპანიების მიერ ამ სტანდარტების შესრულება მნიშვნელოვანი ცვლილებების საწყისია და მონაცემთა სუბიექტის უფლებების დაცვის მყარ სამართლებრივ საფუძველსაც წარმოადგენს.

4. მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავება

მობილურ ტელეფონებში პერსონალური მონაცემების დამმუშავებელი მობილური აპლიკაციების რაოდენობა დღითიდღე იზრდება. ამ პროცესის კვლევისა და მონაცემების დამუშავების GDPR-თან შესაბამისობის უზრუნველსაყოფად ევროკავშირში არაერთი პროფესიონალი გაერთიანდა. ძირითადი, რაზეც ყველა თანხმდება, მონაცემთა დამუშავებისთვის კანონიერი საფუძვლის არსებობაა.

[397] ხელმისაწვდომია: https://gtnr.it/3jtN1q8 წვდომის თარიღი: 25.06.2021.

მობილურ ტელეფონში აპლიკაციის გადმოწერის შემდეგ მისი სრული ფუნქციონირებისთვის საჭიროა რეგისტრაცია, რაც, თავის მხრივ, იმთავითვე გულისხმობს გარკვეულ პერსონალურ მონაცემებზე კომპანიისთვის წვდომის მიცემას. პირველ საფეხურზე, რეგისტრაციის განსახორციელებლად, ასეთები შეიძლება იყოს სახელი, გვარი, ელ. ფოსტა, მობილურის ნომერი. პირველადი ინფორმაციის მოთხოვნის შემდეგ, როგორც წესი, აპლიკაციის სპეციფიკის გათვალისწინებით, მოითხოვენ დაშვებას სხვადასხვა პერსონალურ ინფორმაციაზე, როგორებიცაა ადგილმდებარეობა, წვდომა მოწყობილობის მიკროფონთან, კამერასთან, იშვიათად კომუნიკაციებთან (Read phone call log/Read SMS messages/Access to user's contacts) და სხვ. აქვე, მხედველობაში უნდა მივიღოთ აპლიკაცია რამდენად იყენებს მესამე მხარის მომსახურებას (third-party services – Google Analytics, Crashlytics, Firebase).

შესაბამისად, მობილური აპლიკაციების მიერ ამდენად მოცულობითი პერსონალური ინფორმაციის დამუშავება გარკვეული სტანდარტების დაცვით უნდა განხორციელდეს.

GDPR შესაბამისობაში მყოფი მობილური აპლიკაცია უნდა აკმაყოფილებდეს ისეთ ძირითად მოთხოვნებს, როგორებიცაა:

თანხმობა (Consent)[398] - რეგულაციის თანახმად, აპლიკაციამ მომხმარებლისგან უნდა მოითხოვოს ნებართვა ნებისმიერი სახის ინფორმაციის დასამუშავებლად, რომელიც წარმოდგენილი იქნება მომხმარებლისთვის მარტივი და გასაგები ენით, ამასთანავე წინასწარ მონიშნული ნებართვა არ მიიჩნევა მონაცემთა დამუშავების სამართლებრივ საფუძვლად.

პერსონალურ მონაცემთა დაცვა და უსაფრთხოება (Data protection and privacy) - ნებისმიერი აპლიკაცია უნდა ითხოვდეს მხოლოდ იმ ინფორმაციას, რომელიც აუცილებელია და აპლიკაციის ფუნქციონირებისთვის მნიშვნელოვან ინტერესს ემსახურება.

დავიწყების უფლება (The right to be forgotten)[399] – GDPR-ის ერთ-ერთი მთავარი მოთხოვნაა, მომხმარებელს ნებისმიერ დროს შეეძლოს წაშალოს/ცვლილება შეიტანოს მასზე არსებულ პერსონალურ მონაცემებში, აგრეთვე აკრძალოს ამ მონაცემთა გასაჯაროება ან მესამე პირების მიერ მისი დამუშავება.

უფლება იყო ინფორმირებული (The right to be informed) - არსებითია იმდენად, რამდენადაც აპლიკაციას არ შეუძლია მხოლოდ ერთხელ მიიღოს ნებართვა ყველა სახის ინფორმაციის შესაგროვებლად. ყოველ ჯერზე კომპანია, რომელიც მობილური აპლიკაციის მეშვეობით აგროვებს პერსონალურ ინფორმაციას, უნდა ითხოვდეს სათანადო ნებართვასაც.

უარყოფის უფლება (The right to object) - მომხმარებელს ნებისმიერ დროს უნდა შეეძლოს პერსონალურ მონაცემთა დამუშავებაზე უარის თქმა, რაზეც თავად აპლიკაციაც აუცილებლად უნდა აწვდიდეს მას ინფორმაციას.

---

[398] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 6 (1).

[399] იქვე, მუხლები 16-17.

მონაცემთა სუბიექტის მიერ მონაცემებზე წვდომის უფლება (Right of access by data subject)[400] - აღნიშნული უფლება გულისხმობს მონაცემთა სუბიექტის შესაძლებლობას მონაცემთა დამმუშავებლისგან მოითხოვოს დადასტურება მისი მონაცემების დამუშავების შესახებ და მიიღოს აგრეთვე ინფორმაცია დამუშავების მიზანზე, დამუშავებულ მონაცემთა კატეგორიაზე, მონაცემთა შენახვის ვადაზე და სხვ. ამ ნაწილში მნიშვნელოვანია აპლიკაციებმა განავითარონ უსაფრთხოების პოლიტიკა (Privacy policy), რომ მომხმარებელს მისთვის სასურველ ნებისმიერ დროს ჰქონდეს წვდომა აპლიკაციის მიერ მონაცემთა დამუშავების პოლიტიკაზე.

ვფიქრობ, მობილური აპლიკაციების მიერ სათანადო მოთხოვნების დაცვით შემუშავებული კონფიდენციალურობის პოლიტიკა არსებითია მონაცემთა სუბიექტის უფლებების დაცვისათვის, რადგან ხშირად მომხმარებელი გაუაზრებლად ეთანხმება აპლიკაციის მიერ იმაზე მეტი ინფორმაციის მიღებას, ვიდრე საჭიროა ფუნქციონირებისთვის. ზემოხსენებული მოთხოვნების დაცვას პრობლემის გადაჭრის ეფექტურ ღონისძიებად მივიჩნევ.

5. თანხმობა როგორც პანაცეა?

მონაცემთა დაცვის ზოგადი რეგულაცია მონაცემთა დამმუშავებლის მიერ თანხმობის მიღებას პირველად სამართლებრივ საფუძვლად მიიჩნევს.[401] თანხმობა აღქმულია როგორც ყველაზე პოპულარული სამართლებრივი კრიტერიუმი, რადგან მომხმარებელმა უნდა იცოდეს რა მოცულობის მონაცემებზე მიიღებს აპლიკაცია წვდომას და რა მიზნით დამუშავდება ეს ინფორმაცია.

რეგისტრაცია, რომელიც თავის თავში მოიცავს თანხმობას, ან თანხმობა, რომელიც აპლიკაციის მიერ წინასწარაა მონიშნული არ აღიქმება GDPR-ით გათვალისწინებულ სტანდარტად. აუცილებელია, თანხმობის შესაბამისი გრაფა მომხმარებლის მიერ იყოს მონიშნული, აგრეთვე ჰქონდეს შესაძლებლობა გააუქმონ ნებართვა (Withdraw consent) ამასთანავე მარტივი და გასაგები ენით მომხმარებლისგან თანხმობის მიღების ნებართვას (Consent must be freely given) თან უნდა ახლდეს აღწერა, რა მიზნით ითხოვს აპლიკაცია ამა თუ იმ პერსონალურ ინფორმაციაზე დაშვებას (Consent needs to be specific).

საინტერესოა, მიმოვიხილოთ რამდენად თავსებადია ერთმანეთთან თეორია და პრაქტიკა. სწორედ ამიტომ, აუცილებელია განვიხილოთ ყველაზე ხშირად გადმოწერილი აპლიკაციების მაგალითები.

ერთ-ერთი ყველაზე პოპულარული აპლიკაციის - ინსტაგრამის უსაფრთხოების პოლიტიკის თანახმად, ისინი პერსონალურ მონაცემებს ამუშავებენ მონაცემთა დაცვის ზოგადი რეგულაციის მე-6 მუხლის ყველა მოთხოვნათა დაცვით. ამ შემთხვევაშიც, პირველადი სამართლებრივი საფუძველი მომხმარებლის თანხმობის მოპოვებაა, თუმცა არა ერთადერთი. როგორც ვიცით, Facebook როგორც

[400] იქვე, მუხლი 15.

[401] იქვე, მუხლი 6.

ინსტაგრამის, ასევე ფეისბუქ აპლიკაციის მფლობელია, შესაბამისად მათი უსაფრთხოების პოლიტიკა საკმაოდ მსგავსია, თუმცა არა იდენტური.

Facebook-ის თანახმად, პერსონალური მონაცემების დამუშავებისთვის ყველაზე მნიშვნელოვანი საფუძველი მომხმარებელსა და მათ შორის ხელშეკრულების (Contract)[402] არსებობაა. იგივე შეგვიძლია ვთქვათ აპლიკაციებზე WhatsApp, Spotify. მიუხედავად იმისა, რომ მათ შეიძლება მოითხოვონ თანხმობა ინფორმაციის სპეციფიკური მიზნებით დასამუშავებლად, უპირველესი სამართლებრივი საფუძველი მათთვის შეთანხმებაა, რომ შეასრულონ მომხმარებელთან დადებული შეთანხმება, მიაწოდონ მათ სათანადო მომსახურება და ამ მიზნით დაამუშავონ მათი პერსონალური მონაცემები.

ვფიქრობ, რომ პრაქტიკული მაგალითები საუკეთესოდ ცხადყოფს როგორია მოთხოვნა, კომპანიების მიერ რამდენად სრულდება იგი, თუ პრაქტიკა წარმოშობს თეორიისგან განსხვავებულ რეალობას. შესაბამისად, ობიექტურად შეგვიძლია მივიჩნიოთ, რომ პრაქტიკაში მობილური აპლიკაციის მახასიათებლისა და ფუნქციონირებიდან გამომდინარე თანხმობა არ არის ერთადერთი კანონიერი საფუძველი მონაცემთა დამუშავების დასაწყებად.

6. TIKTOK ყველაზე პოპულარული აპლიკაციის კონფიდენციალურობის პოლიტიკა

გასული 2020 წლის ყველაზე პოპულარულ მობილურ აპლიკაციად თამამად შეგვიძლია დავასახელოთ TikTok, რომელიც საერთაშორისო მასშტაბებით ფუნქციონირებს. აღნიშნულის საფუძველი Covid-19 პანდემიის პირობებში მოსახლეობის აბსოლუტური იზოლაცია და მუშაობისა თუ განათლების მიღების დისტანციურ რეჟიმზე გადასვლაა. ნებისმიერი ასაკის ადამიანი გასული წლიდან დღემდე აქტიურად იყენებს აპლიკაციას ისე, რომ წარმოდგენა არ აქვს, რამდენად დაცულია მისი პერსონალური მონაცემები.

საქართველოს სახელმწიფო ინსპექტორის სამსახურმა შეისწავლა აპლიკაციის კონფიდენციალურობის პოლიტიკა[403] და აღმოჩნდა, რომ:

1. მომხმარებლისგან, რომელიც რეგისტრირდება სხვა პლატფორმის გამოყენებით (Twitter, Facebook), აპლიკაცია მომხმარებლის თანხმობით დამატებით იღებს მის პირად გვერდზე არსებულ ინფორმაციას;

2. აპლიკაციას წვდომა აქვს მომხმარებლის მიკროფონთან, რომლის მეშვეობით ნებისმიერ დროს შეუძლია განახორციელოს ხმის ჩაწერა;

[402] იქვე, მუხლი 6 (2).

[403] საქართველოს სახელმწიფო ინსპექტორის სამსახური „Tik Tok - რამდენად უსაფრთხოა თქვენი საყვარელი აპლიკაცია“, 2020 წელი.

3. სურათებსა და ვიდეოგამოსახულებებთან;

4. კამერასთან, რომლის მეშვეობით ნებისმიერ დროს შეუძლია სურათის/ვიდეოს გადაღება;

5. კონტაქტებთან, ანუ ჩვენ მიერ ჩაწერილი მესამე პირების საკონტაქტო მონაცემებთან.

საინტერესოა ისიც, რომ TikTok აპლიკაციის მომხმარებლებს ზოგიერთ ფუნქციაზე აპლიკაციის წვდომა შეუძლიათ გათიშონ ტელეფონის პარამეტრებიდან, ხოლო ზოგ ფუნქციასთან მიმართებით აპლიკაცია წვდომის გათიშვის შესაძლებლობას საერთოდ არ ითვალისწინებს.[404]

მაშასადამე, ნათელია, რომ ხშირად მობილური აპლიკაციები ამუშავებენ იმაზე მეტ პერსონალურ ინფორმაციას, ვიდრე საჭიროა აპლიკაციის ფუნქციონირებისთვის და ხშირ შემთხვევაში ამისთვის მომხმარებლისგან თანხმობის მოპოვებას არ ცდილობენ ან მომხმარებელს აწოდებენ არასაკმარის ინფორმაციას მონაცემთა დამუშავების დანიშნულებაზე.

7. არასრულწლოვანთა პერსონალური მონაცემების დამუშავება

მობილური აპლიკაციების მიერ არასრულწლოვანთა პერსონალური მონაცემების დამუშავება მნიშვნელოვანი გამოწვევაა.

მონაცემთა ზოგადი რეგულაციით განსაზღვრულია არასრულწლოვნის თანხმობის პირობები ელექტრონული მომსახურების შეთავაზებისას, კერძოდ, „ელექტრონული მომსახურების პირდაპირ არასრულწლოვნისთვის შეთავაზების შემთხვევაში, არასრულწლოვანის პერსონალური მონაცემების დამუშავება კანონიერად ჩაითვლება თუ არასრულწლოვანი სულ მცირე 16 წლისაა. თუ არასრულწლოვანს არ შესრულებია 16 წელი, ასეთი დამუშავება კანონიერი იქნება მხოლოდ იმ შემთხვევაში, თუ თანხმობა გაცემულია ან დამუშავება ნებადართულია მშობლის უფლების მქონე პირის მიერ“.[405] ამასთან, სახელმწიფოებმა ეროვნული კანონმდებლობით შესაძლოა ასაკი შეამცირონ 13 წლამდე.

არასრულწლოვანთა პერსონალური მონაცემების დამუშავება გაცილებით უფრო სენსიტიური საკითხია და მობილურ აპლიკაციებს ამ მხრივ განსაკუთრებული კონფიდენციალურობის პოლიტიკის შემუშავება მართებთ.

ზოგადად, რეგისტრაციისას არასრულწლოვანმა შესაძლოა მიუთითოს მცდარი ინფორმაცია მის ასაკთან დაკავშირებით, რისი იდენტიფიცირებაც მობილური აპლიკაციების მხრიდან რთულია, აგრეთვე რთულია იმის დადგენა, რამდენად არსებობს მშობლის ან მშობლის უფლების მქონე პირის ნებართვა მონაცემთა გაცემასა თუ დამუშავებაზე. სწორედ ამიტომ, ვერიფიკაციის სათანადო სისტემა ყველა მობილურმა აპლიკაციამ უნდა შექმნას არასრულწლოვნებთან მიმართებაში.

[404] იქვე.

[405] მონაცემთა დაცვის ზოგადი რეგულაცია, მუხლი 8 (1).

მაგალითად, TikTok აპლიკაცია არ არის განკუთვნილი 13 წლამდე ასაკის პირთათვის, ამასთანავე TikTok აპლიკაციამ 2017 წლის შემდეგ დანერგა ვერიფიკაციის უფრო მკაცრი ღონისძიებები.[406]

ჩემი აზრით, არასრულწლოვნებთან დაკავშირებულ ყველა საქმეში სახელმძღვანელო პრინციპს არასრულწლოვნის საუკეთესო ინტერესების დაცვა წარმოადგენს, რაც, ცხადია, ყოველ კონკრეტულ შემთხვევაში განსხვავებულია. ამ პრინციპით ხელმძღვანელობა არა მხოლოდ სახელმწიფოს ინტერესებშია, არამედ თავად კერძო კომპანიები უნდა ზრუნავდნენ არასრულწლოვანთან დაკავშირებული ყოველი პრობლემა გადაიჭრას ამ გზით.

ისეთი სენსიტიური საკითხი, როგორიც არასრულწლოვანი პირის პერსონალური ინფორმაციის დამუშავებაა, საკმარის ცოდნასა და სიფრთხილეს საჭიროებს. მონაცემების დამმუშავებელი თავად უნდა ხვდებოდეს რამდენად მნიშნელოვანი კატეგორიის მონაცემებთან აქვს საქმე და იმოქმედოს იმ დაშვებით, რომ მონაცემთა დამუშავება, მისი გასაჯაროების საშიშროება საფრთხეს უქმნის არასრულწლოვნის სათანადო განვითარებასა და ინტერესებს.

8. პერსონალურ მონაცემთა დაცვის სტანდარტები საქართველოში

საქართველოში პერსონალური მონაცემების დაცვის ზოგადი სტანდარტები დადგენილია საქართველოს პარლამენტის მიერ 2011 წლის 28 დეკემბერს მიღებული კანონით „პერსონალურ მონაცემთა დაცვის შესახებ“. კანონის მიზანს პერსონალური მონაცემების დამუშავების პროცესში ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის დაცვა წარმოადგენს.[407]

საქართველოს საკონსტიტუციო სასამართლომ პერსონალური მონაცემების დამუშავებისა და შენახვის საქმეზე მსჯელობისას პირის სახელი, გვარი, პირადი ნომერი, სამსახური/თანამდებობა იმ პირდაპირი იდენტიფიცირების ელემენტების შემცველ პერსონალურ ინფორმაციად მიიჩნია, რომლებიც პირის იდენტიფიცირების შესაძლებლობას იძლევა.[408]

კანონი პერსონალური მონაცემების დამუშავების საფუძვლად მონაცემთა სუბიექტის თანხმობასთან ერთად რამდენიმე გარემოებას მიუთითებს,[409] ამასთანავე აკონკრეტებს, რომ მონაცემთა დამმუშავებელმა ინფორმაციის დამუშავებისას უნდა იხელმძღვანელოს პრინციპით, რომ „მონაცემები დამუშავდეს სამართლიანად, კანონიერად, მონაცემთა სუბიექტის ღირსების შეულახავად“ და „მხოლოდ კონკრეტული მკაფიოდ განსაზღვრული, კანონიერი მიზნებისთვის“ იმ მოცულობით, რომელიც „აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად.“ [410]

[406] საქართველოს სახელმწიფო ინსპექტორის სამსახური „Tik Tok - რამდენად უსაფრთხოა თქვენი საყვარელი აპლიკაცია“ 2020 წელი.

[407] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 1.

[408] საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილება საქმეზე N1/2/622 „საქართველოს მოქალაქე ედიშერ გოდუაძე საქართველოს შინაგან საქმეთა მინისტრის წინააღმდეგ, 2017 წლის 9 თებერვალი, პარაგრაფი II-18.

[409] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 5.

[410] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, მუხლი 4.

საქართველოში პერსონალური მონაცემების კანონიერად დამუშავებაზე ზედამხედველობას საქართველოს სახელმწიფო ინსპექტორის სამსახური ახორციელებს.

საინტერესოა საქართველოში მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავების პრაქტიკა და მიმდინარე გამოწვევები.

Covid-19 პანდემიის განმავლობაში საზოგადოებაში დიდი ინტერესი გამოიწვია მობილურმა აპლიკაციამ „Stop Covid", რომლის მიზანს ინფიცირებულ ადამიანთა რიცხვისა და ვირუსის გავრცელების შემცირება წარმოადგენს. აპლიკაცია აგროვებს ისეთ მონაცემებს, როგორებიც არის ლოკაციის მონაცემები, მობილურის ნომერი, ინფორმაციას Covid-19_ით ინფიცირების შესახებ, მომხმარებლის ID და განხორციელებული კონტაქტების თარიღები, დრო, ხანგრძლივობა.[411] ამასთან, „პროგრამა იყენებს Bluetooth-ს, GPS-სა და Google Nearby ტექნოლოგიას, რათა მაღალი სიზუსტით დაადგინოს, რომელი სმარტფონები იმყოფებოდნენ ერთმანეთთან სარისკო დისტანციაზე (2 მეტრზე ნაკლები მანძილი). ორი სმარტფონის შეხვედრისას, ორივე მომხმარებლის აპლიკაციაში ინახება კონტაქტის ID, ურთიერთობის თარიღი, დრო და ადგილმდებარეობა. თუ მომხმარებელი ტესტ-პოზიტიურია Covid-19-ზე, აპლიკაციაში ადასტურებს ინფიცირებას, შემდეგ კი სისტემა აფრთხილებს ყველა იმ ადამიანს, ვისთანაც ინფიცირებულ ადამიანს ჰქონდა კონტაქტი ბოლო 5 დღის განმავლობაში, რათა დროულად მიიღონ ზომები და მოახდინონ თვითიზოლაცია".[412]

ვფიქრობ, აშკარაა, აპლიკაცია იღებს არაერთ პერსონალურ ინფორმაციას, მათ შორის იმ ინფორმაციასაც, რომელიც საქართველოს კანონმდებლობით განსაკუთრებული კატეგორიის მონაცემებს მიეკუთვნება.[413] მხედველობაში უნდა მივიღოთ ისიც, რომ მონაცემები ზიარდება ავსტრიულ პროვაიდერთან და ამერიკულ კომპანიასთან.

შესაბამისად, ამ კონკრეტული აპლიკაციის კონფიდენციალურობის პოლიტიკა გარკვეულ რისკებს უკავშირდება, როგორებიც არის მათი მესამე პირებისთვის გაზიარება და განსაკუთრებულ კატეგორიას მიკუთვნებული ინფორმაციის გამჟღავნება. ჩემი აზრით, კონტროლის მექანიზმის გამოყენებით აუცილებლად უნდა დადგინდეს აპლიკაციის კონფიდენციალურობის პოლიტიკა რამდენად შეესაბამება საქართველოში პერსონალური მონაცემების დაცვის სტანდარტებს, რამდენად საჭიროა და საშიშროების შემცველია ამ მოცულობის პერსონალური ინფორმაციის დამუშავება, ხომ არ შეიცავს იგი სამომავლო საშიშროებას მონაცემთა უკანონო დამუშავებისა და გადაცემის შესახებ.

9. დასკვნა

თანამედროვე სამყაროში პერსონალური მონაცემების დაცვა ნამდვილ გამოწვევად იქცა. წინამდებარე ნაშრომში განვიხილეთ, რა რისკებს უკავშირდება მობილური აპლიკაციების მიერ მონაცემთა სუბიექტის პერსონალური ინფორმაციის დამუშავება და როგორია საერთაშორისო პრაქტიკა.

---

[411] ხელმისაწვდომია: https://bit.ly/3qJ7n0M წვდომის თარიღი: 30.06.2021.

[412] იქვე.

[413] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", მუხლი 6.

კვლევის ფარგლებში მიმოვიხილეთ ევროპარლამენტისა და ევროკავშირის საბჭოს 2016 წლის 27 აპრილის რეგულაციით (EU) 2016/679 დადგენილი სტანდარტები, რომლითაც კერძო კომპანიებმა უნდა იხელმძღვანელონ, აგრეთვე მიმოვიხილეთ საქართველოში პერსონალურ მონაცემთა დაცვის მექანიზმი და მობილური აპლიკაციის მიერ პერსონალური ინფორმაციის დამუშავების პროცესში წარმოქმნილი გამოწვევები.

ყოველივე ზემოაღნიშნულზე დაყრდნობით, ვფიქრობ, რომ კერძო კომპანიები მობილური აპლიკაციების მიერ პერსონალური მონაცემების დამუშავების პროცესში გარკვეულ სტანდარტთა დაცვით უნდა ხელმძღვანელობდნენ, კერძოდ:

უპირველესად პერსონალური მონაცემების დამუშავების ნებართვის მოპოვებისას მომხმარებლისთვის დამუშავების მიზნის შესახებ ინფორმაციის მიწოდება მიმაჩნია. ამ გზით მომხმარებელი ფლობს სრულ ინფორმაციას, ნებართვის დადასტურების შემთხვევაში რა მიზანს მოემსახურება მის მონაცემებზე წვდომა და ამავე გზით ექნება ნებართვის უარყოფის საშუალებაც, თუ მას შეუსაბამოდ მიიჩნევს.

მნიშნელოვანია ისიც, რომ აპლიკაციებმა მოიპოვონ მხოლოდ ის ინფორმაცია, რაც მათი აპლიკაციის ფუნქციებიდან და მახასიათებლებიდან გამომდინარე აუცილებელია. ამ გზით როგორც მომხმარებელი, ისე კომპანია თავიდან იცილებს მონაცემთა დაცვის სტანდარტების დარღვევას.

მომხმარებლის ინფორმაციული უზრუნველყოფის ნაწილში აუცილებელია ნებისმიერმა დაინტერესებულმა პირმა დროული ინფორმაცია მიიღოს კომპანიისგან, რადგან ინფორმაციის ნაკლებობა ხშირ შემთხვევაში მონაცემთა სუბიექტის მიერ უფლებების სათანადო გამოყენებას აფერხებს.

აუცილებელია, აპლიკაციებმა შეასრულონ GDPR-ის მოთხოვნა და მსხვილმა საწარმოებმა დაიქირავონ მონაცემთა დაცვის ოფიცრები (DPO), რომელთა პასუხისმგებლობაც აპლიკაციების კონფიდენციალურობის პოლიტიკის შემუშავება და მომხმარებლის პერსონალურ მონაცემთა დაცვა იქნება.

პერსონალურ მონაცემთა დამუშავებისა და მონაცემთა სუბიექტის უფლებების დარღვევის ფაქტების შემცირებისთვის, აუცილებლად მიმაჩნია საზოგადოების სრული ინფორმირება მათი უფლებებისა და აპლიკაციების მიერ მომსახურების სათანადოდ მიწოდებაზე. როგორც ზემოთ აღვნიშნე, ინფორმაციულად უზრუნველყოფილი მომხმარებლისთვის ბევრად უფრო მარტივია პრობლემაზე სათანადო რეაგირება და დარღვევის გამოვლენა. მნიშვნელოვანია მოქალაქეთა ჩართულობა ამ პროცესში, რათა საზოგადოებამ იცოდეს პერსონალური მონაცემების შესახებ, თუ როგორ იმოქმედონ მობილური აპლიკაციების მიერ მათი პერსონალური მონაცემების შესაძლო დარღვევის შემთხვევაში. ამ ნაწილში, აუცილებელია თითოეული ქვეყნის პერსონალურ მონაცემთა დაცვაზე ზედამხედველობის ორგანოს ჩართვა, რათა საზოგადოებამ სწორედ მათგან მიიღოს უტყუარი ინფორმაცია და დარღვევის აღმოჩენის შემთხვევაში დროულად მიმართოს სათანადო უწყებას.

ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI)

ტ. შევჩენკოს ქ. 20, თბილისი, 0108;

+995 32 2 92 15 14

Info@idfi.ge

www.idfi.ge

სახელმწიფო ინსპექტორის სამსახური

საქართველო, თბილისი, ნ.ვაჩნაძის N°7, 0105

+995 32 2 42 10 00

office@stateinspector.ge

sis.gov.ge