პერსონალურ მონაცემთა დაცვის ინსპექტორი

ანგარიში
პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში

1 მარტი, 2014 წელი

წინასიტყვაობა

ჩემთვის დიდი პასუხისმგებლობაა საქართველოს მთავრობისა და საზოგადოებისთვის ქვეყანაში პერსონალურ მონაცემთა დაცვის მდგომარეობის შესახებ პირველი ანგარიშის წარდგენა.

წარმოდგენილი დოკუმენტი მოიცავს 2013 წლის აგვისტოდან 2014 წლის მარტამდე მოქალაქეთა განცხადებების განხილვის, ჩატარებული ინსპექტირებისა და გაწეული კონსულტაციების შედეგებს. მართალია, 7 თვე საკმარისი არ არის ემპირიულ მტკიცებულებებზე დამყარებული სრულფასოვანი ანალიზისა და უფლების შელახვის ყველა ფაქტის გამოვლენისთვის, თუმცა ანგარიშში განზოგადებული სახით წარმოდგენილია ისეთ სისტემური ხასიათის პრობლემები, როგორიცაა არაპროპორციულად დიდი მოცულობის მონაცემთა დამუშავება კანონიერი საფუძვლის გარეშე, მათი უკანონოდ გასაჯაროება, ვიდეოთვალთვალის განხორციელებისას კანონის მოთხოვნათა დაუცველობა, პირდაპირი მარკეტინგის დროს მოქალაქეთა უფლებების უგულებელყოფა და სხვა.

სისტემური პრობლემების მოგვარება მხოლოდ მათი იდენტიფიცირების შემდგომ, კომპლექსური მიდგომით არის შესაძლებელი. ამიტომ თანამდებობაზე დანიშვნისთანავე დავიწყე აპარატის ფორმირება, მონაცემთა დამუშავების სპეფიციკის შესწავლა, საზოგადოების ცნობიერების ამაღლების მიზნით გარკვეული ღონისძიებების გატარება, პარლამენტის, მთავრობისა და არასამთავრობო ორგანიზაციების წარმომადგენლებთან თანამშრომლობით მოქმედი კანონმდებლობის და სხვა ქვეყნების გამოცდილების ანალიზი.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პრინციპები და საზედამხედველო ორგანოს ფუნქციები სიახლეს წარმოადგენდა როგორც მოქალაქეებისთვის, ისე მონაცემთა დამმუშავებლებისთვის, ამიტომ სამუშაო დროის დიდი ნაწილი დაეთმო საკონსულტაციო შეხვედრებსა და ტრენინგებს. 6 თვის განმავლობაში 376 კონსულტაცია იქნა გაცემული მონაცემთა დამუშავების კანონიერების საკითხზე, შინაგან საქმეთა სამინისტროს 58 თანამშრომელს ჩაუტარდა პერსონალურ მონაცემთა დაცვის საბაზისო ტრენინგი, ხოლო 163 საჯარო მოხელესა და კერძო კომპანიის წარმომადგენელს მიეცა შესაძლებლობა შრომით ურთიერთობებში მონაცემთა დამუშავების საფუძვლებს გასცნობოდა. მოქალაქეთა 8 განცხადებაზე რეაგირებისა და 2 ინსპექტირების შედეგად, კანონის აღსრულების მიზნით გატარდა ისეთი ღონისძიებები, როგორიცაა დარღვევების მითითებული ფორმითა და ვადებში გამოსწორება, მონაცემთა ბაზებთან წვდომის შეზღუდვა, მათი დამუშავების შეწყვეტა, წაშლა ან განადგურება. საჯარო განცხადებები გავრცელდა პირდაპირი მარკეტინგის, ბიომეტრული მონაცემების დამუშავების, ვიდეოთვალთვალის და განსაკუთრებული კატეგორიის მონაცემთა გასაჯაროების თემაზე.

ეს რთული გზის მხოლოდ დასაწყისია. პერსონალური მონაცემების დაცვის მაღალი სტანდარტების დანერგვა, კონსტიტუციით გარანტირებული უფლებებისა და ადამიანის ღირსების დაცვაზე ორიენტირებული სისტემის შექმნა დიდ ძალისხმევას მოითხოვს ხელისუფლებისა და კერძო სექტორის მხრიდან. თუმცა, ეს ძალისხმევა შედეგის მომტანი ვერ იქნება საზოგადოების დაინტერესებისა და ჩართულობის გარეშე. მნიშვნელოვანია, მოქალაქეებს გაუჩნდეთ იმის მოთხოვნა, რომ მათი პირადი ცხოვრება იყოს ხელშეუხებელი, ხოლო მათ შესახებ ინფორმაცია გროვდებოდეს და ინახებოდეს კანონის სრული დაცვით.

თამარ ქალდანი
პერსონალურ მონაცემთა დაცვის ინსპექტორი

სარჩევი

შესავალი 3

მონაცემთა დამუშავების ძირითადი პრინციპები 4

პერსონალურ მონაცემთა დამუშავების კანონიერი საფუძვლები 6

თანხმობა, როგორც მონაცემთა დამუშავების საფუძველი 6

მონაცემთა დამუშავება ელექტრონული ტექნოლოგიების გამოყენებით 7

ჯანმრთელობის, პოლიტიკური შეხედულებების, ნასამართლობის და სხვა განსაკუთრებული კატეგორიის მონაცემთა შეგროვება, შენახვა, გამჟღავნება და სხვაგვარი დამუშავება 9

ბიომეტრული მონაცემების დამუშავება 11

ფარული მიყურადებისა და მოსმენების კუთხით არსებული გამოწვევები 12

ვიდეოთვალთვალის განხორციელების მიზანი და კანონიერება 15

სხვა სახელმწიფოსთვის ან/და საერთაშორისო ორგანიზაციისათვის პერსონალურ მონაცემთა გადაცემა 18

პირდაპირი მარკეტინგი 19

მოქალაქეთა ინფორმირებულობა და უფლებების დაცვა 20

რეკომენდაციები 22

შესავალი

თანამედროვე დემოკრატიულ ქვეყნებში პერსონალური მონაცემების დაცვა ადამიანის ძირითად უფლებად განიხილება, ამ უფლების რეალიზებისთვის კი მნიშვნელოვანი ინსტიტუციური და საკანონმდებლო რეფორმები ხორციელდება. „ადამიანის ძირითადი უფლებების შესახებ“ ევროპის კავშირის ქარტიაში ცალკე მუხლი ეთმობა პერსონალური მონაცემების დაცვის უფლებას,[1] ხოლო ადამიანის უფლებათა ევროპული სასამართლო პირადი ცხოვრების ხელშეუხებლობას ადამიანის ავტონომიურობის, დამოუკიდებელი განვითარების, მისი ღირსების დაცვის წინაპირობად მიიჩნევს.

საქართველოს კონსტიტუცია ითვალისწინებს ადამიანის პირადი ცხოვრების ხელშეუხებლობის, პიროვნების განვითარების, მისი ღირსების დაცვის, მოქალაქის შესახებ სახელმწიფო დაწესებულებაში არსებული ინფორმაციის გაცნობის უფლებებს, ასევე, სახელმწიფოს ვალდებულებას, დაიცვას ოფიციალურ ჩანაწერებში არსებული ჯანმრთელობასთან, ფინანსებთან ან სხვა კერძო საკითხებთან დაკავშირებული ინფორმაცია. ყოველივე აღნიშნული ქმნის პერსონალურ მონაცემთა დაცვის კანონმდებლობის კონსტიტუციურ გარანტიასა და საფუძველს.

„პირის ინტერესი, არ დაუშვას კერძო საკითხებთან დაკავშირებული ინფორმაციის გამჟღავნება და აკონტროლოს ამ ინფორმაციის გავრცელება, პირადი ცხოვრების ხელშეუხებლობის უფლების ერთ-ერთი უმთავრესი ასპექტია.“[2] კონსტიტუციით გარანტირებული უფლებების რეალიზებისთვის მნიშვნელოვანია, მონაცემთა დამუშავება ხდებოდეს მხოლოდ კანონიერი საფუძვლით. ადამიანმა უნდა იცოდეს, როდის იქნება მის პირად ცხოვრებაში სახელმწიფოს ჩარევა ლეგიტიმური, რა უფლებები აქვს მას და რა გზით დაიცვას საკუთარი ინტერესები.

რამდენადაც ეს არის ქვეყანაში პერსონალურ მონაცემთა დაცვის მდგომარეობის შეფასების პირველი შემთხვევა, ანგარიშში ასახული თემები კონსტიტუციით გარანტირებული უფლებების ჭრილშია გაანალიზებული. ანგარიშის პირველ ნაწილში განხილულია ისეთი ძირეული საკითხები, როგორიცაა მონაცემთა დამუშავების პრინციპები, დამუშავების საფუძვლები და საშუალებები, მონაცემთა დამუშავება ელექტრონული ტექნოლოგიების გამოყენებით, განსაკუთრებული კატეგორიისა და ბიომეტრული მონაცემების დამუშავების სპეციფიკა, ფარული მიყურადება და მოსმენა, ვიდეოთვალთვალი, პირდაპირი მარკეტინგი, მონაცემთა სხვა ქვეყნებში გადაცემა, მოქალაქეთა ინფორმირებულობა და მათი უფლებების დაცვა. დოკუმენტის დასკვნით ნაწილში წარმოდგენილია ინსპექტორის რეკომენდაციები პერსონალურ მონაცემთა დაცვის მიზნით გასატარებელი ღონისძიებების შესახებ.

1 Article 8, Charter of Fundamental Rights of The European Union (2000/C 364/01).

2 საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის #2/3/406.408 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ“.

მონაცემთა დამუშავების ძირითადი პრინციპები

პერსონალური მონაცემების დამუშავების კანონიერება და მაღალ სტანდარტებთან შესაბამისობა არსებითადაა დამოკიდებული მონაცემთა დამუშავების პრინციპების დაცვაზე. კანონში ასახული პრინციპები, მათი მდგრადი ხასიათიდან გამომდინარე, ამკვიდრებენ მონაცემთა დამუშავების ზოგად წესს და განსაზღვრავენ მონაცემთა დამმუშავებლების ქმედების კანონიერებას. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ განამტკიცებს ისეთ პრინციპებს, როგორებიცაა სამართლიანობა და კანონიერება, მონაცემთა სუბიექტის ღირსების დაცვა, მკაფიოდ განსაზღვრული კანონიერი მიზნის არსებობა, პროპორციულობა და ადეკვატურობა, მონაცემების ნამდვილობა და სიზუსტე, მონაცემთა შენახვა მხოლოდ მიზნის მისაღწევად აუცილებელი ვადით.

მონაცემთა დამმუშავებლებთან კონსულტაციებისა და შეხვედრების დროს გამოიკვეთა, რომ პრაქტიკაში ყველაზე პრობლემურია **მკაფიოდ განსაზღვრული კანონიერი მიზნით მონაცემთა დამუშავება.** როგორც საჯარო, ისე კერძო ორგანიზაციების უმრავლესობა ვერ ახდენს მონაცემთა დამუშავების (მაგალითად: შეგროვების, შენახვის, გასაჯაროების და სხვა) კონკრეტული და ლეგიტიმური მიზნის იდენტიფიცირებას. შესაძლოა, ორგანიზაციას ჰქოდეს მონაცემთა შეგროვებისა და გარკვეული ვადით შენახვის მიზანი, რაც იმთავითვე არ გულისხმობს მის მიერ ამ მონაცემების სხვა ორგანიზაციისთვის გადაცემის უფლებამოსილებას. საჯარო სექტორის მიერ მონაცემთა დამუშავების მიზნის განსაზღვრისას ხშირად ხდება მათი საქმიანობის მარეგულირებელი ნორმატიული აქტების ზოგადად მითითება, რასაც მონაცემთა დამუშავების პირდაპირ განსაზღვრული კანონიერი მიზნის არარსებობა განაპირობებს. ეს კი წინააღმდეგობაში მოდის საჯარო სამართლის უმთავრეს პრინციპთან - „რაც კანონით დაშვებული არ არის, აკრძალულია“.

მოქალაქეთა მომართვები ადასტურებს, რომ ისინი ხშირ შემთხვევაში არასათანადოდ ან საერთოდ არ არიან ინფორმირებულნი მონაცემთა დამუშავების მიზნის შესახებ. რამდენიმე მათგანმა ასევე მიუთითა **ღირსების შემლახავ გარემოში მონაცემთა დამუშავების თაობაზე.**

მაგალითად, პირებმა, რომელთაც ნებაყოფლობით გაიარეს ნარკოლოგიური შემოწმება, განაცხადეს, რომ შემოწმება ხორციელდებოდა ვიდეო კონტროლის პირობებში ყოველგვარი ალტერნატიული საშუალების შეთავაზების გარეშე. იმავდროულად, დაკვირვების ოთახში განთავსებულ მონიტორზე გამოსახულების ნახვა არა მხოლოდ პერსონალს, არამედ ნარკოლოგიური შემოწმების სხვა მსურველებსაც შეეძლოთ.

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

გამოვლინდა შემთხვევები, როდესაც ფიზიკური პირისგან მოთხოვნილი ინფორმაციის შინაარსი და მოცულობა აშკარად სცდებოდა კანონიერი მიზნის ფარგლებს. მაგრამ, ამ ინფორმაციის მიუწოდებლობა გამოიწვევდა მოქალაქის განცხადების განხილვაზე უარის თქმას.

ამასთანავე, ადამიანებს პრობლემებს უქმნის ინტერნეტის საშუალებით მონაცემთა არაპროპორციული და მიზნის არაადეკვატური გასაჯაროება. მაგალითად: საკრედიტო ორგანიზაციამ გამოიყენა საჯარო შეტყობინების ფორმა, სადაც მიუთითა არა მხოლოდ ადამიანის სახელი, გვარი და პირადი ნომერი, არამედ ფაქტობრივი და იურიდიული მისამართი, საკონტაქტო ინფორმაცია, დავალიანების ოდენობა, ხელშეკრულების რეკვიზიტები. განმცხადებელსა და მონაცემთა დამმუშავებელს შორის დადებული ხელშეკრულებისა და მხარეთა მიმოწერის ანალიზის შედეგად გამოიკვეთა, რომ ინტერნეტ რესურსის გამოყენებით საჯარო შეტყობინების აუცილებლობა არ არსებობდა. სამწუხაროდ, განხილული მაგალითი არ წარმოადგენს ერთეულ შემთხვევას. არაერთი საფინანსო-საკრედიტო ორგანიზაცია იყენებს საჯარო შეტყობინების ფორმას და, როგორც წესი, დავალიანების გადახდის შემდგომაც არ ან ვერ ხდება ინფორმაციის დახურვა. მონაცემები კვლავ ხელმისაწვდომია ინტერნეტ და საძიებო რესურსებში, რაც ზიანს აყენებს ადამიანის რეპუტაციას, რომ არაფერი ითქვას თავად მონაცემთა გასაჯაროებასთან დაკავშირებულ სხვა საფრთხეებზე.

დამმუშავებლები უმეტესწილად თავადაც აღიარებენ, რომ მონაცემთა შენახვა ხდება **მიზანთან შეუსაბამო ვადით ან სულაც უვადოდ.** წლების განმავლობაში მონაცემთა დამმუშავებლები მოქმედებდნენ პრინციპით **„ვინახავთ ყველაფერს, რისი შეგროვება და შენახვაც შეგვიძლია.“** პრაქტიკაში შენახვის ვადა დამოკიდებულია არა მონაცემთა დამუშავების მიზანზე, არამედ ისეთ ტექნიკურ პირობაზე, როგორიცაა სერვერის მოცულობა ან დაარქივების შესაძლებლობა. მონაცემთა დამმუშავებლები ვერ უზრუნველყოფენ კანონიერი საფუძვლის გარეშე შეგროვებული და დამუშავების მიზანთან შეუსაბამო მონაცემების დაბლოკვას, წაშლას ან განადგურებას, რაც ქმნის სუბიექტის მიმართ არასწორი გადაწყვეტილების მიღების ან მისთვის ზიანის მიყენების საფრთხეს.

პოზიტიურად უნდა შეფასდეს რამდენიმე ორგანიზაციის მიერ მონაცემთა დამუშავებასთან დაკავშირებით შიდა პოლიტიკის შემუშავება და თანამშრომლებისთვის სპეციალური ტრენინგების ორგანიზება. ამ მხრივ, განსაკუთრებით აღსანიშნავია საჯარო სექტორის მონაცემთა ისეთი მსხვილი დამმუშავებლების მიერ გადადგმული ნაბიჯები, როგორიცაა იუსტიციის, შინაგან საქმეთა და ფინანსთა სამინისტროები ან/და მათი მმართველობის სფეროში შემავალი საჯარო სამართლის იურიდიული პირები. სამართლებრივი რეგულირება და კადრების მომზადება მნიშვნელოვანია, მაგრამ - არასაკმარისი პრაქტიკაში დანერგვისა და ქმედითი შიდა კონტროლის მექანიზმის გარეშე.

პერსონალურ მონაცემთა დამუშავების კანონიერი საფუძვლები

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ამომწურავად განსაზღვრავს მონაცემთა დამუშავების საფუძვლებსა და წინაპირობებს. შესაბამისად, ნებისმიერი დამმუშავებელი ვალდებულია უზრუნველყოს კანონით გათვალისწინებული შემდეგი საფუძვლებიდან ერთ-ერთის არსებობა მაინც, კერძოდ:

- მონაცემთა სუბიექტის თანხმობა;
- მონაცემთა სუბიექტის განცხადების განხილვა ან მისთვის მომსახურების გაწევა;
- კანონიერი საფუძველი ან კანონმდებლობით დაკისრებული მოვალეობის შესრულება;
- ინფორმაცია კანონით საჯაროა ან გასაჯაროებულია თავად მონაცემთა სუბიექტის მიერ;
- პირის სასიცოცხლო ინტერესის დაცვა;
- მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესის დაცვა, თუ მათი ინტერესი აღემატება მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის ინტერესს;
- მონაცემთა დამუშავება ხორციელდება მნიშვნელოვანი საჯარო ინტერესის დაცვის მიზნით.

არსებული სიტუაციის ანალიზის საფუძველზე გამოიკვეთა, **რომ მონაცემთა დამუშავება ხშირად ხორციელდება შესაბამისი სამართლებრივი საფუძვლის გარეშე.** როგორც საჯარო, ისე კერძო დაწესებულებები ვერ ახდენენ მონაცემთა დამუშავების კანონით განსაზღვრული საფუძვლის იდენტიფიცირებას, საკმაოდ ფართოდ და არაერთგვაროვნად განმარტავენ ისეთ ცნებებს, როგორიცაა „მნიშვნელოვანი საჯარო ინტერესი“, „კანონმდებლობით დაკისრებული მოვალეობა“ ან „მესამე პირის კანონიერი ინტერესი“.

მიუხედავად იმისა, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონი 2012 წელს შევიდა ძალაში, მისი გავლენით სხვა კანონებსა და კანონქვემდებარე ნორმატიულ აქტებში არ განხორციელებულა ცვლილებები. შესაბამისად, ისეთ მნიშვნელოვანი სფეროების მარეგულირებელ სამართლებრივ აქტებში, როგორიცაა ჯანდაცვა, დაზღვევა, სოციალური უზრუნველყოფა, განათლება, კომუნიკაცია და სხვა ცალსახად და მკაფიოდ არ არის ფორმულირებული მონაცემთა დამუშავების საკითხები, რაც პრაქტიკაში მონაცემთა არაერთ დამმუშავებელს უქმნის პრობლემას. ამ თვალსაზრისით, მნიშვნელოვანია სამართლებრივი ბაზის ჰარმონიზაცია, შესაბამისი გადაწყვეტილებების დასაბუთება და ისეთი სასამართლო პრაქტიკის განვითარება, რომელიც უზრუნველყოფს ბალანსის დაცვას პირად და საჯარო ინტერესს შორის.

თანხმობა, როგორც მონაცემთა დამუშავების საფუძველი

მონაცემთა დამუშავების საფუძვლებს შორის ყველაზე პრობლემური მონაცემთა სუბიექტის თანხმობის საკითხია. კანონის მიხედვით, თანხმობა არის მონაცემთა სუბიექტის მიერ სათანადო ინფორმაციის მიღების შემდეგ, მონაცემთა განსაზღვრული მიზნით დამუშავებაზე ზეპირად, სატელეკომუნიკაციო ან სხვა შესაბამისი საშუალებით გამოხატული ნებაყოფლობითი თანხმობა, რომლითაც შესაძლებელია ნათლად დადგინდეს პირის ნება.

მოქალაქეებისათვის გაწეულმა კონსულტაციებმა ცხადყო, რომ უმეტეს შემთხვევაში, სუბიექტის თანხმობა წარმოადგენს გარკვეული მომსახურების მიღების პირობას და არა ნების თავისუფალ გამოვლენას. მოქალაქეებმა არც კი იციან, თუ რაზე აქვთ თანხმობა გაცემული, ჰქონდათ თუ არა მათი მონაცემების დამუშავებაზე უარის თქმის უფლება და რა იქნებოდა უარის სამართლებრივი შედეგი.

წერილობითი თანხმობის შემთხვევაშიც კი რთულია სუბიექტის ნების ნამდვილობის დადგენა. მაგალითად, მოქალაქეები არ ფლობდნენ ინფორმაციას, რომ მომსახურების ან სხვა ტიპის ხელშეკრულებაზე ხელმოწერით ორგანიზაციებს მიანიჭეს ნებისმიერი ფორმითა და მიზნით მათი მონაცემების დამუშავების უფლება.

სუბიექტის მიერ ხელმოწერილი მომსახურების ან სხვა სახის ხელშეკრულება ხშირად ფორმალური თვალსაზრისით თანხმობის მტკიცებულებას წარმოადგენს, რომლის ერთ-ერთი მუხლი ირიბად ეხება მონაცემთა დამუშავებას. როგორც წესი, მონაცემთა დამმუშავებლები ხელმძღვანელობენ ხელშეკრულების სტანდარტული პირობით ან შაბლონური თანხმობის ტექსტით, შესაბამის განმარტებას არ აძლევენ მოქალაქეებს მონაცემთა დამუშავების მიზნისა და საფუძვლების შესახებ. სამწუხაროდ, ფიზიკური პირებიც არ უთმობენ სათანადო ყურადღებას დოკუმენტის შინაარსს. იმ იშვიათ შემთხვევაშიც კი, როცა მოქალაქეებმა მოითხოვეს განმარტება ან ტექსტის ცვლილება, უარი მიიღეს მომსახურების გაწევაზე.

მონაცემთა დამუშავება ელექტრონული ტექნოლოგიების გამოყენებით

ბოლო წლებში მონაცემთა ავტომატური დამუშავება სულ უფრო ფართომასშტაბიან ხასიათს იძენს, რამაც ხელი შეუწყო გარკვეული პროცესების ოპტიმიზაციას, მომსახურების გამარტივებას, ბიუროკრატული საფეხურების შემცირებას. ელექტრონული მმართველობის პოზიტიური შედეგების მიუხედავად, სრულად ვერ მოხდა პროცესის თანმდევი რისკების შეფასება, ასევე პერსონალური მონაცემების დაცვისა და უსაფრთხოების მინიმალური სტანდარტების დანერგვა. ხშირად ახალ ტექნოლოგიებზე გადასვლა შესაბამისი საკანონმდებლო ბაზის განახლების გარეშე მიმდინარეობდა. მონაცემთა ავტომატური დამუშავების პროცესში **ერთ-ერთ მთავარ პრობლემას წარმოადგენს უწყებებს შორის მონაცემთა გაცვლის ან/და წვდომის მინიჭებისთვის სამართლებრივი საფუძვლის არარსებობა.** ბოლო დროს განსაკუთრებით იზრდება სხვადასხვა საჯარო უწყებებს შორის მონაცემთა გაცვლის, ასევე კერძო სექტორის მიერ დამუშავებულ მონაცემებზე საჯარო უწყებების წვდომის მაჩვენებლები, რაც კიდევ უფრო ამძიმებს მონაცემთა დამუშავების კუთხით არსებულ არცთუ სახარბიელო მდგომარეობას და ქმნის მონაცემთა უკანონო დამუშავებისთვის ხელსაყრელ გარემოს. მონაცემთა დამმუშავებლები ყურადღების მიღმა ტოვებენ იმ მნიშვნელოვან გარემოებას, რომ მონაცემების მოპოვებისა და შენახვის უფლებამოსილება ორგანიზაციას ავტომატურად არ ანიჭებს ამ მონაცემების სხვა უწყებისათვის გადაცემის უფლებას.

ელექტრონული ტექნოლოგიების გამოყენებით პერსონალური მონაცემების მასშტაბური დამუშავების კიდევ ერთი შედეგი მონაცემთა დამმუშავებლების, უფლებამოსილი პირებისა და „ავტორიზებული მომხმარებლების“ რაოდენობის ზრდა და სხვადასხვა მონაცემთა ბაზებთან მათი წვდომის გაზრდილი შესაძლებლობებია. ეს წარმოშობს მონაცემთა არამართლზომიერი გამოყენების საფრთხეს და ართულებს მათი უკანონო მოპოვებისა და გასაჯაროების ფაქტების გამოვლენას.

კანონი არეგულირებს მონაცემთა დამმუშავებლისა[3] და უფლებამოსილი პირის[4] ურთიერთობას და აწესებს მთელ რიგ მოთხოვნებს, კერძოდ: უფლებამოსილ პირს პერსონალურ მონაცემთა დამუშავება შეუძლია მხოლოდ სამართლებრივი აქტის ან მონაცემთა დამმუშავებელთან დადებული წერილობითი ხელშეკრულების საფუძველზე, რომელიც დეტალურად უნდა განსაზღვრავდეს მონაცემთა დამუშავების მიზნებსა და ფარგლებს, მხარეთა უფლება-მოვალეობებს, მონაცემთა უსაფრთხოების საკითხებს.

> ციფრული ტექნოლოგიების ეპოქა, რომელშიც ჩვენ ვცხოვრობთ, გამოირჩევა კრეატიული და ინოვაციური მიდგომებით. შეუძლებელი და მიზანშეუწონელია კანონით „ინოვაციის“ რეგულირება. თუმცა, კანონმა აუცილებელად უნდა შექმნას ადამიანის უფლებების რეალიზების საშუალებები და განსაზღვროს მონაცემთა დამმუშავებლების პასუხისმგებლობა.
>
> **პიტერ ჰუსტინქსი,**
> ევროპის მონაცემთა დაცვის ზედამხედველი

კანონით **აკრძალულია უფლებამოსილი პირის მიერ დამუშავების უფლების გადაცემა სხვა პირისათვის მონაცემთა დამმუშავებლის თანხმობის გარეშე**. დაუშვებელია უფლებამოსილი პირის მიერ ნებისმიერი სხვა მიზნით მონაცემთა შემდგომი დამუშავება, თუმცა პრაქტიკაში ყველაზე ხშირად სწორედ ეს ვალდებულება ირღვევა. **უფლებამოსილი პირები მონაცემთა დამმუშავებლის მიერ მიწოდებულ ინფორმაციას ინახავენ და სხვა მიზნით იყენებენ სახელშეკრულებო ურთიერთობის დასრულების შემდგომაც.** ეს პრობლემა ყველაზე ნათლად წარმოჩინდა მომხმარებელთა ტელეფონის ნომრებზე სხვადასხვა ხასიათის სარეკლამო შეტყობინების მასიური დაგზავნის პროცესზე დაკვირვებისას.

ამავე დროს, დაუშვებელია მონაცემთა დამუშავების შესახებ ხელშეკრულების დადება, თუ უფლებამოსილი პირის საქმიანობიდან ან/და მიზნებიდან გამომდინარე, არსებობს მონაცემთა არამიზნობრივი დამუშავების საფრთხე. **უფლებამოსილი პირი ვალდებულია, უზრუნველყოს მონაცემთა უსაფრთხოება და ამ მხრივ გაატაროს შესაბამისი ორგანიზაციულ-ტექნიკური ზომები.** დამმუშავებელი ვალდებულია, მონიტორინგი გაუწიოს უფლებამოსილი პირის მიერ მონაცემთა დამუშავებას და მიიღოს შესაბამისი ზომები მონაცემთა შემთხვევითი ან უკანონო გამჟღავნების, მოპოვების, შეცვლის, განადგურების, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და დაკარგვის თავიდან ასაცილებლად.

სამწუხაროდ, საანგარიშო პერიოდში ჩვენ მიერ განხილულ ხელშეკრულებებსა და სამართლებრივ აქტებში, რომელთა საფუძველზეც ხდებოდა მონაცემთა დამუშავება, დეტალურად არ იყო ასახული კანონით დადგენილი მოთხოვნების დიდი ნაწილი და არც დამმუშავებლების მიერ უფლებამოსილი პირის კონტროლი ხორციელდებოდა სათანადო დონეზე. პრაქტიკაში უწყების მიერ უფლებამოსილი პირების მონიტორინგის მხოლოდ ერთი შემთხვევა შეგვხვდა, რომელიც აღმოჩენილ დარღვევაზე სახელშეკრულებო სანქციის გამოყენებით დასრულდა. უნდა აღინიშნოს, რომ მონიტორინგის ერთეული ფაქტები, ეფექტური პრევენციული ზომების გარეშე, ვერ იქნება საკმარისი მონაცემთა დაცვის სათანადო ხარისხის უზრუნველსაყოფად.

პოზიტიურ შეფასებას იმსახურებს ის გარემოება, რომ ინსპექტორის აპარატთან კონსულტაციების შედეგად საქართველოს მთავრობის კანცელარიამ, საქართველოს იუსტიციის, შინაგან საქმეთა, სასჯელაღსრულებისა და პრობაციის, ოკუპირებული ტერიტორიებიდან იძულებით გადაადგილებულ პირთა, განსახლებისა და ლტოლვილთა სამინისტროებმა, სსიპ საჯარო სამსახურის ბიურომ, სსიპ სახელმწიფო სერვისების განვითარების სააგენტომ, სსიპ სოციალური მომსახურების სააგენტომ განსაზღვრეს მონაცემთა დამუშავების კონკრეტული საფუძვლები, ასევე რამდენიმე მათგანმა დახვეწა და კანონთან შესაბამისობაში მოიყვანა ელექტრონული სისტემის მეშვეობით მონაცემთა დამუშავების პროცესი.

3 მონაცემთა დამმუშავებელი არის საჯარო დაწესებულება, ფიზიკური ან იურიდიული პირი, რომელიც ინდივიდუალურად ან სხვებთან ერთად განსაზღვრავს პერსონალური მონაცემთა დამუშავების მიზნებსა და საშუალებებს, უშუალოდ ან უფლებამოსილი პირის მეშვეობით ახორციელებს მონაცემთა დამუშავებას.

4 უფლებამოსილი პირი არის ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც ამუშავებს მონაცემებს მონაცემთა დამმუშავებლისათვის ან მისი სახელით.

ჯანმრთელობის, პოლიტიკური შეხედულებების, ნასამართლობის და სხვა განსაკუთრებული კატეგორიის მონაცემთა შეგროვება, შენახვა, გამჟღავნება და სხვაგვარი დამუშავება

საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ სპეციალურ გარანტიებს ადგენს ისეთი მონაცემების მიმართ, რომლებიც დაკავშირებულია პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიული ორგანიზაციის წევრობასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან ან ნასამართლობასთან. ეს მონაცემები, ისევე როგორც გარკვეული სახის ბიომეტრული მონაცემები, სენსიტიური ხასიათიდან გამომდინარე, განეკუთვნება განსაკუთრებულ კატეგორიას, ვინაიდან ამ ტიპის მონაცემთა უკანონოდ შეგროვება, შენახვა ან გავრცელება შესაძლოა ქმნიდეს პირადი ცხოვრების ხელყოფის, ადამიანის დევნის, შევიწროების ან სხვაგვარი დისკრიმინაციის საფრთხეს.

კანონი კრძალავს განსაკუთრებული კატეგორიის მონაცემთა დამუშავებას, გარდა იმ შემთხვევისა, როცა:

- მონაცემთა სუბიექტმა გამოხატა წერილობითი თანხმობა მისი განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე;
- სუბიექტმა გაასაჯაროა მის შესახებ მონაცემები, მათი გამოყენების აშკარა აკრძალვის გარეშე;
- მონაცემთა დამუშავება აუცილებელია შრომითი ვალდებულების შესრულებისა ან მასთან დაკავშირებული უფლების განხორციელებისათვის;
- მონაცემთა დამუშავება აუცილებელია სუბიექტის ან მესამე პირის სასიცოცხლო ინტერესის დასაცავად და მონაცემთა სუბიექტს ფიზიკურად ან სამართლებრივად არ აქვს უნარი, განაცხადოს თანხმობა მონაცემთა დამუშავებაზე;
- მონაცემთა დამუშავება ხორციელდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნებისათვის, აგრეთვე, თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისთვის და ფუნქციონირებისათვის;
- მონაცემთა დამუშავება ხორციელდება ლეგიტიმური საქმიანობის განხორციელებისას პოლიტიკური, ფილოსოფიური, რელიგიური ან სავაჭრო გაერთიანების, ასოციაციის ან სხვა არაკომერციული ორგანიზაციის მიერ. ასეთ შემთხვევაში მონაცემთა დამუშავება შეიძლება დაკავშირებული იყოს მხოლოდ ამ ორგანიზაციის წევრებთან ან პირებთან, რომლებსაც მუდმივი კავშირი აქვთ ამ ორგანიზაციასთან. ამ შემთხვევაში ინფორმაციის მესამე პირისათვის გამჟღავნება დაუშვებელია მონაცემთა სუბიექტის თანხმობის გარეშე.

პრაქტიკაში განსაკუთრებული კატეგორიის მონაცემთა დამუშავება უმეტესწილად სუბიექტის წერილობითი თანხმობით ხორციელდება. თუმცა, დამმუშავებლები ხშირად ვერ უზრუნველყოფენ თანხმობის ამსახველი დოკუმენტის წარმოდგენას, რომელშიც მკაფიოდ და ნათლად იქნებოდა გამოხატული სუბიექტის ნება. უფრო მეტიც, **დამმუშავებლები არ არიან ინფორმირებულნი მათ მიერ დამუშავებული მონაცემების სენსიტიური ხასიათისა და კანონის მიერ დადგენილი მოთხოვნების შესახებ,** რის გამოც უზრუნველყოფილი არ არის მონაცემთა უსაფრთხოების მინიმალური სტანდარტი.

მოქალაქეთა დიდი ნაწილი გამოთქვამს უკმაყოფილებას განსაკუთრებული კატეგორიის მონაცემთა გამჟღავნების გამო, რაც ძირითადად შეეხება ჯანმრთელობის მდგომარეობასთან და ნასამართლობასთან დაკავშირებული მონაცემების უკანონო გასაჯაროებას.

საანგარიშო პერიოდში დაფიქსირდა თანხმობის გარეშე პაციენტის სამედიცინო ისტორიის მედია საშუალებებით გავრცელების შემთხვევა. ასევე ერთ-ერთ სატელევიზიო გადაცემაში მოხდა ნარკოტიკულ საშუალებებზე დამოკიდებულებისა და ნასამართლობის შესახებ მონაცემების უკანონო გასაჯაროება.

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

2013 წლის აგვისტო-სექტემბერში, ეროვნული უშიშროების საბჭოს მდივნის მომართვის საფუძველზე, ინსპექტორმა შეისწავლა წინასაარჩევნო პერიოდში ერთ-ერთი უნივერსიტეტის კვლევის ფარგლებში მთავრობის კანცელარიის კოორდინირებით 12 სამინისტროში მოხელეთა პოლიტიკური შეხედულებების შესახებ მონაცემთა დამუშავების საკითხი. დადგინდა, რომ კვლევის მიზანს წარმოადგენდა საჯარო სექტორში მოქალაქეთა დასაქმების განმაპირობებელი ფაქტორების გამოვლენა. მთავრობის კანცელარია კოორდინაციას უწევდა სამინისტროების მონაწილეობას კვლევაში და არ წარმოადგენდა მონაცემთა დამმუშავებელს. საჯარო მოსამსახურეებისთვის დარიგებული კითხვარები იყო ანონიმური, მათი შევსება არ ატარებდა სავალდებულო ხასიათს, თუმცა კითხვარს არ ახლდა შესაბამისი განმარტება და დასმული კითხვების ერთობლიობა იძლეოდა კვლევაში მონაწილე მოხელეთა იდენტიფიცირების შესაძლებლობას. შევსებული კითხვარების შეგროვება ხდებოდა თითოეულ უწყებაში სპეციალურად განსაზღვრულ პირთან. მიუხედავად იმისა, რომ საკითხის შესწავლის დროისთვის მთავრობის კანცელარიის ინიციატივით კვლევა შეწყდა, არსებობდა პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-4, მე-5 და მე-6 მუხლების დარღვევის საფრთხე. ამიტომ პერსონალურ მონაცემთა დაცვის ინსპექტორის მიმართვის საფუძველზე შევსებული კითხვარები განადგურდა.

აღსანიშნავია, რომ საანგარიშო პერიოდში ჩატარებული ტრენინგებისა და კონსულტაციების შედეგად არაერთმა საჯარო დაწესებულებამ დაიწყო მათ მიერ დამუშავებული მონაცემების პროპორციულობისა და კანონიერების შეფასება, თანამშრომელთა პირადი საქმეებისა და ადამიანური რესურსების მართვის სისტემების კანონთან შესაბამისობაში მოყვანა.

კერძო სექტორში განსაკუთრებული კატეგორიის მონაცემების დამუშავებისას ხშირად ხდება კანონით განსაზღვრული საფუძვლების ფართოდ ინტერპრეტაცია.

მაგალითად, ერთ-ერთი დამსაქმებელი კონკურსის წესით შერჩეული კანდიდატისგან განათლებისა და სამუშაო გამოცდილების, სახელფასო ისტორიისა და შემოსავლის შესახებ ინფორმაციის გარდა, სავალდებულო წესით ითხოვდა მისი და ოჯახის წევრების ჯანმრთელობის მდგომარეობის, სისხლის სამართლის საქმეში ნებისმიერი სტატუსით მონაწილეობის, ეთნიკური წარმომავლობის და რელიგიური შეხედულებების შესახებ ინფორმაციას. დასაქმების კანდიდატი იძულებული გახდა წარედგინა ეს მონაცემები, ვინაიდან წარუდგენლობა გამოიწვევდა სამსახურში მის მიღებაზე უარის თქმას.

საანგარიშო პერიოდში ჩატარებული ტრენინგებისა და საკონსულტაციო შეხვედრების შედეგად რამდენიმე კომპანიამ დაიწყო ზრუნვა კანონის შესაბამისად განსაკუთრებული კატეგორიის მონაცემთა დამუშავებაზე. თუმცა, 2016 წლამდე კერძო სექტორის მიმართ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის შეზღუდული მოქმედების გამო, დამმუშავებლების დიდი ნაწილისთვის პერსონალური მონაცემების დაცვა პრიორიტეტს არ წარმოადგენს.

ბიომეტრული მონაცემების დამუშავება

მაღალი საზოგადოებრივი ინტერესიდან გამომდინარე, პერსონალურ მონაცემთა დაცვის მდგომარეობის შეფასებისას, აუცილებელია ბიომეტრულ მონაცემთა დამუშავების საკითხის ცალკე განხილვა. ბიომეტრული მონაცემი არის ნებისმიერი ფიზიკური, ფსიქიკური ან ქცევის მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდი, თვალის ფერადი გარსი, დნმ-ის კოდი და სხვა). სწორედ ამ მონაცემების უნიკალურობამ და მათი საშუალებით პირის უტყუარი იდენტიფიცირების შესაძლებლობამ განაპირობა მსგავსი კატეგორიის მონაცემების დამუშავების განსხვავებული რეგულირება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით.

ბიომეტრული მონაცემების დამუშავება დასაშვებია მხოლოდ პირის უსაფრთხოებისა და საკუთრების დაცვის, ასევე საიდუმლო ინფორმაციის გამჟღავნების თავიდან აცილების მიზნით. იმავდროულად, ამ მიზნების მიღწევა სხვა საშუალებით უნდა იყოს შეუძლებელი ან უკავშირდებოდეს არაპროპორციულად დიდ ძალისხმევას.

გარდა აღნიშნულისა, საჯარო დაწესებულებებს ბიომეტრული მონაცემების დამუშავება შეუძლიათ კანონით დადგენილი წესით პირადობის დამადასტურებელი დოკუმენტის გაცემის ან სახელმწიფო საზღვრის გადამკვეთი პირის იდენტიფიკაციის მიზნებისათვის, ხოლო კერძო ორგანიზაციებს - საქმიანობის განხორციელების მიზნებისათვის.

საანგარიშო პერიოდში საჯარო დაწესებულებების მიერ ბიომეტრულ მონაცემების დამუშავებასთან დაკავშირებით გამოიკვეთა პრობლემა, რომელიც უკავშირდება ერთი უწყების მონაცემთა ბაზაში დაცულ ბიომეტრულ ფოტოზე სხვა უწყების წვდომას, მაშინ, როცა მონაცემთა მიმღებს არა აქვს ამ სახის მონაცემების მიღების სამართლებრივი საფუძველი.

საჯარო დაწესებულებებისგან განსხვავებით, კერძო ორგანიზაციები ბიომეტრული მონაცემების გამოყენებამდე ვალდებულნი არიან პერსონალურ მონაცემთა დაცვის ინსპექტორს მიაწოდონ დეტალური ინფორმაცია ასეთი მონაცემების დამუშავების შესახებ. ერთიანი სტანდარტის დადგენის მიზნით, ინსპექტორის აპარატმა შეიმუშავა ბიომეტრული მონაცემების დამუშავების შესახებ კერძო ორგანიზაციების მიერ წარსადგენი ფორმა და შესაბამისი ინსტრუქცია. თუმცა, **დღემდე ოფიციალური შეტყობინება ინსპექტორის აპარატში არ შემოსულა.**

მოქალაქეთა განცხადებებისა და კონსულტაციების საფუძველზე იკვეთება, რომ ადგილი აქვს ბიომეტრული მონაცემების დამუშავებას და გამოყენებას არსებული საკანონმდებლო მოთხოვნების შეუსაბამოდ.

მაგალითად, როგორც მოქალაქეები უთითებენ, რამდენიმე ორგანიზაციის, მათ შორის საგანმანათლებლო დაწესებულების მიერ, თითის ანაბეჭდები გამოიყენება დასაქმებულთა შრომითი ანაზღაურების გადახდისა და სამსახურში გამოცხადების აღრიცხვის მიზნით. ორგანიზაციის საქმიანობის ხასიათი არ ადასტურებს ასეთი მონაცემების გამოყენების საჭიროებას, არც ორგანიზაციის შინაგანაწესშია განსაზღვრული თითის ანაბეჭდების დამუშავების მიზანი. თანამშრომლებს არ გამოუხატავთ თანხმობა ბიომეტრული მონაცემების დამუშავებაზე და არც სხვა კანონიერი საფუძველია სახეზე. აღნიშნულ შემთხვევაში ორგანიზაციას შეეძლო ანაზღაურების ან სამსახურში გამოცხადების კონტროლი სხვა საშუალებით, მაგალითად ტაბელით, აღრიცხვის ჟურნალით ან ბარათით.

ფარული მიყურადებისა და მოსმენების კუთხით არსებული გამოწვევები

ადამიანის პირადი ცხოვრების ხელშეუხებლობის თვალსაზრისით განსაკუთრებით აქტუალურია სამართალდამცავი ორგანოების მიერ სატელეკომუნიკაციო კომპანიების მონაცემთა ბაზებში არსებულ (მათ შორის სატელეფონო კომუნიკაციისა და პირის ადგილმდებარეობის შესახებ) ინფორმაციასთან პირდაპირი წვდომა, ფარული მიყურადებისა და თვალთვალის განხორციელება, რაც განპირობებულია მათი უფლებამოსილებით, დანაშაულის გამოძიების მიზნებისთვის აწარმოონ ფარული ვიდეო და აუდიოჩაწერა, ფოტოგადაღება, სატელეფონო საუბრის მოსმენა და სხვა.

ფარული მიყურადებისა და თვალთვალის საკითხი განსაკუთრებული სიმწვავით წარმოჩნდა 2013 წლის გაზაფხულზე, როდესაც შინაგან საქმეთა სამინისტრომ გაავრცელა ინფორმაცია 2005-2012 წლებში შექმნილი ათასობით **ფარული აუდიო და ვიდეო ჩანაწერის შესახებ, რომელთა საერთო მოცულობა 260 678 მეგაბაიტი იყო, ხოლო ჩანაწერების ხანგრძლივობა 1760 საათს აჭარბებდა.**

ამ საკითხზე საქართველოს მთავრობის გადაწყვეტილებით შეიქმნა **უკანონო მიყურადებისა და ფარული ჩანაწერების საკითხებზე მომუშავე დროებითი კომისია,** რომლის შემადგენლობაშიც შედიოდნენ საქართველოს შინაგან საქმეთა მინისტრი (კომისიის თავმჯდომარე), საქართველოს იუსტიციის მინისტრი, საქართველოს მთავარი პროკურორი, საქართველოს სახალხო დამცველი, პერსონალურ მონაცემთა დაცვის ინსპექტორი, თბილისის სააპელაციო სასამართლოს მოსამართლე, გაზეთ „რეზონანსის“ მთავარი რედაქტორი, საარჩევნო და პოლიტიკური ტექნოლოგიების კვლევის ცენტრის ხელმძღვანელი და საერთაშორისო გამჭვირვალობა - საქართველოს აღმასრულებელი დირექტორი.

> არაიდენტიფიცირებადი ფორმით, სწრაფი გადახვევის რეჟიმში სამიოდე ჩანაწერის თითო წუთის ნახვაც კი საკმარისია იმის გასაცნობიერებლად, თუ რამდენად უსუსური, დაუცველი და უუფლებოა ადამიანი, როცა „აზრის პოლიციას შეუძლია ყველა კაბელს მიუერთდეს“, ფარული კამერები დაამონტაჟოს საცხოვრებელ სახლსა თუ სასტუმროს ნომერში, სამსახურსა თუ რესტორანში, უხეშად ჩაერიოს ადამიანის პირად ცხოვრებაში.
>
> **თამარ ქალდანი,**
> პერსონალურ მონაცემთა დაცვის ინსპექტორი

აღმოჩენილი მასალა მოიცავდა პოლიტიკოსების, ბიზნესის და სამოქალაქო საზოგადოების წარმომადგენლების პირადი ცხოვრების ამსახველ კადრებს, აუდიო ჩანაწერებსა და ფოტოებს. რამდენიმე ჩანაწერზე ასახული იყო პატიმართა წამების ფაქტები. კომისიამ მუშაობის **პროცესში ვერ მოიძია პირადი ცხოვრების ამსახველი ვიდეო და აუდიო მასალის კანონიერად მოპოვების დამადასტურებელი ოფიციალური დოკუმენტი.** პერსონალურ მონაცემთა დაცვის ინსპექტორის რეკომენდაციით, კომისიამ შეიმუშავა ინტიმური ცხოვრების ამსახველი მასალის აღრიცხვის, უსაფრთხოებისა და განადგურების მეთოდოლოგია, რის შედეგადაც **განადგურდა ინფორმაციის 112 ელექტრონული მატარებელი,** ხოლო ძირითადი მასალა (633 ელექტრონული მატარებელი) გამოძიების მიზნით გადაეცა მთავარ პროკურატურას.

> სახელმწიფოს ზოგადად ეკრძალება, გაეცნოს სატელეფონო და სხვა სახის ტექნიკური საშუალებით წარმოებული საუბრებისა და შეტყობინებების შინაარსს, აგრეთვე, დააწესოს კონტროლი, ვისთან და რა ინტენსივობით შედგა ასეთი ურთიერთობები.
>
> **საქართველოს საკონსტიტუციო სასამართლო**[6]

რამდენადაც სისხლის სამართლის მოქმედი კანონმდებლობა სათანადოდ ვერ უზრუნველყოფდა პირადი ცხოვრების ხელშეუხებლობის უფლებების დაცვას და დარღვევის გამოვლენის შემთხვევაში ადეკვატური პასუხისმგებლობის დაკისრებას, კომისიამ შეიმუშავა და საქართველოს პარლამენტს წარედგინა კანონპროექტი, რომელიც ითვალისწინებს სისხლის სამართლის კოდექსის 157-159 მუხლებით[5] განსაზღვრული სანქციების გამკაცრებას, ასევე დანაშაულის შემადგენლობის გადასინჯვასა და პერსონალურ მონაცემთა უკანონოდ მოპოვების, შენახვის, გამოყენებისა და გავრცელების კრიმინალიზაციას.

2013 წლის მეორე ნახევარში **გაუმჯობესდა სასამართლოს კონტროლი სატელეფონო საუბრების ფარულ მიყურადებასა და ჩაწერაზე,** ტექნიკური საშუალებებით თვალყურის დევნებაზე. უზენაესი სასამართლოს სტატისტიკური მონაცემების თანახმად, 2012 წელს სასამართლოს მიერ არ დაკმაყოფილდა განხილული შუამდგომლობების მხოლოდ 0.25%, ხოლო 2013 წელს - 7.56%.[7] შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაციის თანახმად, დაიხვეწა და **გამკაცრდა შიდა მონიტორინგი ოპერატიულ-სამძებრო საქმიანობის განხორციელების პროცესზე.** კონტროლის გამკაცრებისა და ინფორმაციის არამართლზომიერი მოპოვების შესაძლებლობების აღმოფხვრის მიზნით, შინაგან საქმეთა სამინისტრომ განახორციელა მთელი რიგი ორგანიზაციული ღონისძიებები, კერძოდ:

1. გაუქმდა სხვადასხვა სამინისტროებში, დეცენტრალიზებული სახით არსებული ფარული მიყურადების სისტემები და ამჟამად აღნიშნული ოპერატიულ-სამძებრო ღონისძიებები ხორციელდება ცენტრალიზებული სახით, ერთი კონკრეტული უწყების მიერ, რაც მნიშვნელოვნად ზღუდავს არამართლზომიერი მიყურადების განხორციელების შესაძლებლობას და იმავდროულად ამარტივებს კონტროლის მექანიზმების გამოყენებას;

2. ფარული მიყურადება ხორციელდება სპეციალურ დაცულ, შეზღუდული დაშვების მქონე ზონებში, სადაც დაიშვებიან მხოლოდ სათანადო უფლებამოსილების მქონე პირები. კონტროლის მიზნებისათვის გამოიყენება სამზღუდიანი, მათ შორის ბიომეტრული კონტროლის სისტემა.

3. შეზღუდული დაშვების მქონე ზონებში გაუმჯობესდა ვიდეომეთვალყურეობის სისტემები, რომელთა მიზანია გამოვლენილ და აღკვეთილ იქნეს ინფორმაციის გაჟონვისა და მოპოვებული მასალის არამართლზომიერი დუბლირების მცდელობათა ფაქტები.

4. ინფორმაციის გაჟონვის თავიდან არიდების მიზნით, ზემოაღნიშნულ არეალებში გამკაცრდა ფოტო და ვიდეო ტექნიკის, მობილური ტელეფონების და ინფორმაციის ჩაწერისა და შენახვისთვის განკუთვნილი სხვა საშუალებების შეტანა.

5. გამკაცრდა უფლებამოსილი პირების სისტემაზე წვდომის ლოგირების ელექტრონული აღრიცხვა.

5 პირადი და ოჯახური საიდუმლოების ხელყოფა (მუხლი 157); კერძო კომუნიკაციის საიდუმლოების დარღვევა (მუხლი 158); პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა (მუხლი 159).

6 საქართველოს საკონსტიტუციო სასამართლოს 2007 წლის 26 დეკემბრის #1/3/407 გადაწყვეტილება საქმეზე „საქართველოს ახალგაზრდა იურისტთა ასოციაცია და საქართველოს მოქალაქე ეკატერინე ლომთათიძე საქართველოს პარლამენტის წინააღმდეგ.“

7 2012 წელს სასამართლოს მიერ განხილულ იქნა 11580 შუამდგომლობა, ხოლო 2013 წელს - 3699.

მნიშვნელოვანია, რომ დანაშაულის გამოძიების მიზნებისათვის სამართალდამცავი ორგანოების მიერ განხორციელებული თვალთვალი, მიყურადება და სატელეკომუნიკაციო კომპანიების მონაცემებზე წვდომა განხორციელდეს ადამიანის უფლებთა ევროპული კონვენციის მე-8 მუხლის მოთხოვნების და საერთაშორისო სტანდარტების შესაბამისად. ადამიანის უფლებათა ევროპული სასამართლოს თანახმად, ეროვნული კანონმდებლობა უნდა ითვალისწინებდეს ჯეროვან გარანტიებს ხელისუფლების ორგანოების მხრიდან უფლებამოსილების ბოროტად ან თვითნებურად გამოყენების წინააღმდეგ.[8] ამ სტანდარტთან შესაბამისობის მიზნით, მიზანშეწონილია, კანონმდებლობის დახვეწა, დამოუკიდებელი და მაღალი ლეგიტიმაციის მქონე კონტროლის მექანიზმის შექმნა, რაც უზრუნველყოფს ბალანსის დაცვას ადამიანის ღირსების, პირადი ცხოვრების ხელშეუხებლობის უფლებასა და საზოგადოებრივი უსაფრთხოების, დანაშაულის გამოძიებისა და პრევენციის ლეგიტიმურ საჯარო ინტერესს შორის.

აღსანიშნავია, რომ საანგარიშო პერიოდში პერსონალურ მონაცემთა დაცვის ინსპექტორს რამდენიმე მოქალაქემ მიმართა, რომელთა ინტერესის ძირითად საგანს წარმოადგენდა მათ მიმართ ფარული თვალთვალის განხორციელების შედეგად სამართალდამცავ ორგანოებში არსებული ინფორმაციის გაცნობის უფლება. ვინაიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება არ ვრცელდება საზოგადოებრივი და სახელმწიფო უსაფრთხოების, ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნებისთვის მონაცემთა დამუშავებაზე, მოქალაქეებს ეზღუდებათ ამ კანონით გარანტირებული უფლებები და ინსპექტორი ვერ ახდენს რეაგირებას ასეთი სახის განცხადებებზე.

ევროპული სტანდარტის თანახმად, პირს უნდა ჰქონდეს შესაძლებლობა, მიიღოს ინფორმაცია მის მიმართ განხორციელებული ოპერატიულ-სამძებრო ღონისძიების შესახებ იმ მომენტიდან, როდესაც მისთვის ინფორმაციის მიწოდება ობიექტურად ზიანს ვეღარ მიაყენებს გამოძიების ინეტერესს.[9] ამ სტანდარტის საქართველოში დანერგვა ხელს შეუწყობს პირადი ცხოვრების ხელშეუხებლობის სათანადო გარანტიების შექმნას და იმ პირებს, ვის მიმართაც განხორციელდა ოპერატიულ-სამძებრო ღონისძიება, გარკვეულ ეტაპზე ექნებათ შესაძლებლობა, გაასაჩივრონ პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევა, თუკი მათ მიმართ ასეთი ღონისძიებები უკანონოდ განხორციელდა.

8 Klass and Others, pp. 25 26, §§ 54 56; mutatis mutandis, Leander v. Sweden, judgment of 26 March 1987, Series A no. 116, pp. 25 27, §§ 60 67; Halford, cited above, p. 1017, § 49; Kopp, cited above, p. 541, § 64; and Weber and Saravia, cited above, § 94.

9 Principle 2.2; Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector.

ვიდეოთვალთვალის განხორციელების მიზანი და კანონიერება

ბოლო პერიოდში სხვადასხვა კერძო და საჯარო დაწესებულებები სულ უფრო ხშირად იყენებენ ვიდეო კონტროლს. მზარდია მოქალაქეთა ინტერესი ქუჩასა თუ საზოგადოებრივი თავშეყრის ადგილებში, შენობებსა და საზოგადოებრივ ტრანსპორტში ვიდეომონიტორინგისა და ჩანაწერების მიმართ.

მოქმედი კანონმდებლობა არეგულირებს ვიდეოთვალთვალის განხორციელების მიზნებსა და წესს ქუჩაში, საჯარო და კერძო დაწესებულებებში, საცხოვრებელ შენობებში. ვიდეოთვალთვალის განხორციელება დასაშვებია მხოლოდ დანაშაულის პრევენციის, პირის უსაფრთხოებისა და საკუთრების, საიდუმლო ინფორმაციის, საზოგადოებრივი წესრიგისა და არასრულწლოვანის მავნე ზეგავლენისაგან დაცვის მიზნით. ამასთან, ვიდეოთვალთვალის სისტემის დაყენების შემთხვევაში, საჯარო და კერძო დაწესებულებები ვალდებულნი არიან, თვალსაჩინო ადგილას განათავსონ შესაბამისი გამაფრთხილებელი ნიშანი.

> 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.
>
> **რიჩარდ ტომასი,**
> დიდი ბრიტანეთის ინფორმაციის კომისარი

ვიდეოთვალთვალის სისტემის მეშვეობით შესაძლებელია, განხორციელდეს მხოლოდ შენობის გარე პერიმეტრისა და შესასვლელის მონიტორინგი. ამასთან, დაუშვებელია ვიდეოთვალთვალის განხორციელება გამოსაცვლელ და ჰიგიენისათვის განკუთვნილ ოთახებში.

როგორც საკითხის შესწავლის დროს გამოიკვეთა, **ვიდეოთვალთვალის სისტემების გამოყენების მიზანი ხშირად სცდება კანონით გათვალისწინებულ ფარგლებს.** ორგანიზაციები ვერ ასაბუთებენ მათ მიერ ვიდეოთვალთვალის განხორციელების შესახებ გადაწყვეტილებას და ვერ ახდენენ კანონით განსაზღვრული მიზნის იდენტიფიცირებას.

განსაკუთრებით უნდა აღინიშნოს იმ საკანონმდებლო მოთხოვნის შეუსრულებლობა, რომელიც კერძო და საჯარო დაწესებულებებს ავალდებულებს, **დასაქმებულ პირებს წერილობითი ფორმით მიაწოდონ ინფორმაცია სამუშაო ადგილზე ვიდეოთვალთვალის განხორციელებისა და მათი უფლებების შესახებ.**

მაგალითად: ერთ-ერთი ორგანიზაციის მიერ ვიდეო მონიტორინგი ხორციელდებოდა დაგვიანების შემთხვევაში დასაქმებულთა მიმართ დისციპლინური პასუხისმგებლობის გამოყენების მიზნით, მაშინ, როდესაც თანამშრომლები არ იყვნენ ინფორმირებულნი ამის შესახებ.

უმეტეს შემთხვევებში, **შენობებსა და გარე პერიმეტრზე არ არის განთავსებული მიმდინარე ვიდეოთვალთვალის შესახებ გამაფრთხილებელი ნიშნები** და მონაცემთა სუბიექტებს არც სხვა ფორმით მიეწოდებათ ინფორმაცია კონტროლის თაობაზე.

კანონი ადგენს მონაცემთა დამმუშავებლის ვალდებულებას, შექმნას **ვიდეოჩანაწერების შენახვისათვის განკუთვნილი ფაილური სისტემა.** ჩანაწერების (სურათები/ხმა) გარდა, სისტემა უნდა შეიცავდეს ინფორმაციას მონაცემთა დამუშავების თარიღის, ადგილისა და დროის შესახებ. ინსპექტორის აპარატის მიერ შესწავლილმა პრაქტიკამ აჩვენა, რომ დამმუშავებლების უმრავლესობა ვერ ახერხებს ჩანაწერების შენახვის ტექნიკური პროცედურებისა და ვადების ერთიანი სტანდარტის დადგენას. **ჩანაწერების შენახვა ხშირად არ ხდება შეგროვების მიზნის პროპორციული ვადით, არც მათი უსაფრთხოების მინიმალური სტანდარტებია დაცული და გაურკვეველია, ვისთვის შეიძლება გახდეს ეს ჩანაწერები ხელმისაწვდომი.**

2013 წლის ოქტომბრის დასაწყისში, ბრალდებულ ბაჩანა ახალაიას საკნის ვიდეო და აუდიო ჩანაწერების მედია საშუალებებით გავრცელების შემდეგ,[10] ინსპექტორმა საკუთარი ინიციატივით დაიწყო სასჯელაღსრულების სისტემაში ვიდეო/აუდიო მონიტორინგის განხორციელებისა და ჩანაწერების წარმოების საკითხის შესწავლა.

მოთხოვნილი ინფორმაციის შესწავლისა და ადგილზე დათვალიერების შედეგად გამოიკვეთა სამართლებრივი, პროცედურული და ინფრასტრუქტურული ცვლილებების განხორციელების საჭიროება, მათ შორის ტექნიკური საშუალებებით მეთვალყურეობის შესახებ საკანონმდებლო ბაზის დახვეწა, დაწესებულების რეჟიმის სპეციფიკის გათვალისწინებით ტექნიკური საშუალებებით მეთვალყურეობის ერთიანი წესის დადგენა, პერსონალურ მონაცემთა დაცვისა და უსაფრთხოების ერთიანი სტანდარტების დამკვიდრება.

ინსპექტორის მიერ შემუშავებული რეკომენდაციები ეხებოდა:

- *აუდიო, ვიდეო, ელექტრონული ან სხვა ტექნიკური საშუალებების გამოყენების შესახებ გადაწყვეტილების მიღების, მისი განხორციელების, ასევე პერსონალური მონაცემების შემცველი და კონფიდენციალური ინფორმაციის შენახვის, წაშლისა და განადგურების საკითხების რეგულირებას;*
- *სასჯელაღსრულების დაწესებულების ადმინისტრაციის მიერ ტექნიკური საშუალებების გამოყენებით კონტროლის განხორციელების შესახებ გადაწყვეტილების დასაბუთებულობასა და მიზნის პროპორციულობის შეფასებას;*
- *სასჯელაღსრულების დაწესებულების შენობაში მიმდინარე ვიდეო/აუდიო კონტროლის თაობაზე გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილას განთავსებას;*
- *დაწესებულებაში მყოფ პირთა ინფორმირებას მათ მიმართ კონტროლის ამა თუ იმ ფორმის გამოყენების შესახებ;*
- *ვიდეო და აუდიო მონიტორინგის განხორციელების პროცესების გამიჯვნას;*
- *სასჯელაღსრულების სისტემაში ინფორმაციული უსაფრთხოების პოლიტიკის, პროცედურებისა და სამუშაო ინსტრუქციების საერთაშორისოდ აღიარებულ სტანდარტებთან შესაბამისობაში მოყვანას;*
- *სასჯელაღსრულების სისტემის თანამშრომელთა გადამზადებას და ინფორმირებას უსაფრთხოების პოლიტიკისა და მონაცემთა დაცვის საკითხებზე.*

10 კახეთის საინფორმაციო ცენტრის მიერ საჯაროდ გავრცელდა ბაჩანა ახალაიას საკანში გადაღებული ვიდეო/აუდიო მასალის ნაწილი, სადაც ისმის როგორც უშუალოდ ბაჩანა ახალაიას, ასევე მასთან საკანში შესულ პირთა ხმაც: http://www.ick.ge/articles/16000-i.html.

აღსანიშნავია, რომ ინსპექტორის 2013 წლის 8 ნოემბრის დასკვნაში მოცემული რეკომენდაციები აისახა სასჯელაღსრულებისა და პრობაციის სამინისტროს მიერ პატიმრობის კოდექსში ინიცირებულ ცვლილებებში. პოზიტიურ შეფასებას იმსახურებს სამინისტროს სასწავლო ცენტრის მიერ პერსონალურ მონაცემთა დაცვის საკითხებზე სპეციალური ტრენინგ-პროგრამის შემუშავება. თუმცა, ინფორმაციული უსაფრთხოების პოლიტიკისთან დაკავშირებული რეკომენდაციები საჭიროებს უფრო გრძელვადიან და კომპლექსურ მიდგომას.

საანგარიშო პერიოდში ადგილი ჰქონდა ქ. თბილისის მასშტაბით მიკროავტობუსებში ვიდეოკამერების დამონტაჟებას. საზოგადოების მაღალი ინტერესიდან გამომდინარე, ინსპექტორმა განცხადება გაავრცელა აღნიშნული საკითხზე და გამაფრთხილებელი ნიშნების გამოყენების რეკომენდაციით მიმართა შესაბამის უწყებას. საკითხის შესწავლის დროს გამოიკვეთა საზოგადოებრივ ტრანსპორტში ვიდეოთვალთვალის საკანონმდებლო დონეზე რეგულირების საჭიროება, ვინაიდან მოქმედი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ არეგულირებს ვიდეოთვალთვალის განხორციელებას მხოლოდ ქუჩაში, დაწესებულებებსა და საცხოვრებელ შენობებში.

სხვა სახელმწიფოსთვის ან/და საერთაშორისო ორგანიზაციისათვის პერსონალურ მონაცემთა გადაცემა

საქართველოს პარლამენტმა 2013 წლის ივლისში მოახდინა „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ კონვენციის“ დამატებითი ოქმის რატიფიცირება, რომელიც არეგულირებს მონაცემთა ტრანსსასაზღვრო გადაცემას.

პერსონალურ მონაცემთა სახელმწიფოს იურისდიქციის ფარგლებს გარეთ გადაცემა გარკვეულ საფრთხეებთან არის დაკავშირებული, ამიტომ პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი არეგულირებს მონაცემთა სხვა სახელმწიფოსათვის ან/და საერთაშორისო ორგანიზაციისთვის გადაცემის საკითხს და ინსპექტორს ანიჭებს უფლებამოსილებას, შეაფასოს სხვა სახელმწიფოში/საერთაშორისო ორგანიზაციაში მონაცემთა დაცვის სათანადო გარანტიები კანონმდებლობისა და პრაქტიკის ანალიზის საფუძველზე.

კანონის თანახმად, მონაცემთა გადაცემა შესაძლებელია, თუ:

- არსებობს მონაცემთა დამუშავების შესაბამისი სამართლებრივი საფუძველი და მიმღებ ქვეყანაში ან/და საერთაშორისო ორგანიზაციაში პერსონალურ მონაცემთა დაცვის სათანადო გარანტიები;
- ეს გათვალისწინებულია საქართველოს საერთაშორისო ხელშეკრულებით და შეთანხმებით;
- მონაცემთა დამმუშავებელსა და მიმღებს შორის დადებული ხელშეკრულებით უზრუნველყოფილია დაცვის სათანადო გარანტიები.

ამ უკანასკნელ შემთხვევაში, მონაცემთა გადაცემა შესაძლებელია ინსპექტორის ნებართვის შემდგომ. თუმცა, ამ დროისთვის, აპარატში შემოსულია მხოლოდ ერთი განცხადება მონაცემთა გერმანიაში გადაცემის ნებართვის მისაღებად.

პრაქტიკის ანალიზის საფუძველზე იკვეთება, რომ **მონაცემთა გადაცემა ხშირად ხორციელდება შესაბამისი სამართლებრივი საფუძვლის გარეშე.** ასევე პრობლემატურია მხარეთა შორის დადებულ ხელშეკრულებებში მონაცემთა დაცვის სათანადო გარანტიების ასახვა. როგორც წესი, საქართველოსა და უცხო ქვეყნის მონაცემთა დამმუშავებლებს შორის არსებული ხელშეკრულებები ან/და სადამფუძნებლო დოკუმენტები არ არეგულირებს მონაცემთა გადაცემასთან და უსაფრთხოების უზრუნველყოფასთან დაკავშირებულ საკითხებს.

საქართველოში შექმნილ პერსონალურ მონაცემთა ბაზებთან ხშირად წვდომა აქვს მონაცემთა დამმუშავებლების უცხოელ აქციონერებსა თუ პარტნიორებს.

საკითხის დაურეგულირებლობის გამო საქართველოს მოქალაქეთა პერსონალური მონაცემები მათი თანხმობის ან სხვა კანონიერი საფუძვლის გარეშე უკონტროლოდ და სისტემატურად გაედინება სხვადასხვა ქვეყნებსა და საერთაშორისო ორგანიზაციებში.

მონაცემთა ტრანსსასაზღვრო გადაცემის საკითხის დარეგულირების მიზნით, ინსპექტორის აპარატი ამჟამად მუშაობს **ე.წ. „თეთრი სიის“ შექმნაზე,** რომელიც საშუალებას მისცემს მონაცემთა დამმუშავებლებს, კანონით განსაზღვრული საფუძვლების არსებობისას, სპეციალური ნებართვის გარეშე გადასცენ მონაცემები იმ ქვეყნის იურიდიულ და ფიზიკურ პირებს, სადაც უზრუნველყოფილია მონაცემთა დაცვის სათანადო გარანტიები.

პირდაპირი მარკეტინგი

ბოლო დროს მოქალაქეებისათვის მოკლე ტექსტური შეტყობინებების გზით სხვადასხვა სახის პროდუქციისა თუ მომსახურების შეთავაზებამ იმდენად მასშტაბური ხასიათი მიიღო, რომ მოქალაქეთა მომართვების ძირითადი ნაწილი სწორედ არასასურველ სარეკლამო შეტყობინებებს და ამ მიზნით მათი მონაცემთა დამუშავებას ეხება. **სუბიექტები ვერ იღებენ ინფორმაციას მათი მონაცემების შეგროვების წყაროსა და დამუშავების შეწყვეტის საშუალებების შესახებ,** ვინაიდან მათთვის უცნობია ვინ არის მონაცემთა დამმუშავებელი - მობილური ოპერატორი, სარეკლამო კომპანია თუ რეკლამის დამკვეთი.

მოქმედი კანონის თანახმად, პირდაპირი მარკეტინგის მიზნებისათვის შეიძლება დამუშავდეს საჯაროდ ხელმისაწვდომი წყაროებიდან მოპოვებული ისეთი მონაცემები, როგორიცაა სახელი, მისამართი, ტელეფონის ან ფაქსის ნომერი, ელ-ფოსტის მისამართი. სხვა კატეგორიის მონაცემთა დასამუშავებლად აუცილებელია **მონაცემთა სუბიექტის თანხმობა. მიუხედავად თანხმობისა, მონაცემთა სუბიექტს უფლება აქვს, ნებისმიერ დროს წერილობითი ფორმით მოითხოვოს მის შესახებ მონაცემთა პირდაპირი მარკეტინგის მიზნებისათვის გამოყენების შეწყვეტა.** დამმუშავებელი ვალდებულია, შეწყვიტოს მონაცემთა დამუშავება სუბიექტის მოთხოვნის მიღებიდან არა უგვიანეს 10 სამუშაო დღისა და, ამასთანავე, განუმარტოს მისი უფლებები. ვინაიდან პირდაპირი მარკეტინგის მიზნებსა და საშუალებების განსაზღვრას ახდენს რეკლამის დამკვეთი კომპანია, სწორედ მას ეკისრება მონაცემთა სუბიექტების ინფორმირებისა და მათ მიერ მონაცემთა დამუშავების შეწყვეტის მოთხოვნის უზრუნველყოფის ვალდებულება. გარდა ამისა, დამმუშავებელი უნდა დარწმუნდეს, რომ მის მიერ დაქირავებულმა სარეკლამო კომპანიამ მონაცემთა დასაცავად მიიღო შესაბამისი ორგანიზაციული და ტექნიკური ზომები. იგი ასევე ვალდებულია, მონიტორინგი გაუწიოს უფლებამოსილი პირის მიერ მონაცემთა დამუშავებას.

ვინაიდან წლების განმავლობაში არ არსებობდა პერსონალური მონაცემების დაცვის შესახებ კანონმდებლობა, ხშირად ხდებოდა სხვადასხვა სახის პერსონალური მონაცემების გასაჯაროება, გაზიარება, გაყიდვა. შესაბამისად, წარმოიქმნა საკმაოდ მოცულობითი ბაზები, რომელთა ლეგიტიმურობისა და წყაროს დადგენა სირთულეებთან არის დაკავშირებული. ამასთანავე, მოქმედი კანონი 2016 წლამდე არ ითვალისწინებს კერძო სექტორის მიმართ ინსპექტირებისა და შესაბამისი სანქციების გამოყენების შესაძლებლობას, რის გამოც ინსპექტორი მოქალაქეთა საჩივრებზე ეფექტურ რეაგირებას ვერ ახდენს. საანგარიშო პერიოდში არაერთ მოქალაქეს გაეწია კონსულტაცია პირდაპირი მარკეტინგის მიზნებისათვის მონაცემთა დამუშავებისას მათი უფლებებისა და ამ უფლებების რეალიზების საშუალებების შესახებ. ასევე, ინსპექტორმა საჯარო განცხადებით მოუწოდა პირდაპირი მარკეტინგის განმახორციელებელ კომპანიებს, დაეცვათ არსებული საკანონმდებლო მოთხოვნები.

აღსანიშნავია, რომ კანონში პირდაპირი მარკეტინგის მარეგულირებელი ნორმა საჭიროებს დახვეწას, რისთვისაც ინსპექტორის აპარატის ინიციატივით მუშავდება კანონპროექტი „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონში ცვლილებებისა და დამატებების შესახებ.

მოქალაქეთა ინფორმირებულობა და უფლებების დაცვა

როგორც პერსონალურ მონაცემთა დაცვაზე 29-ე მუხლის სამუშაო ჯგუფის[11] მე-14 წლიურ ანგარიშშია აღნიშნული, ერთი ადამიანის მონაცემები 250-დან 1000-მდე მონაცემთა ბაზაშია რეგისტრირებული. ფაქტობრივად შეუძლებელია, ადამიანმა აკონტროლოს თითოეულ ბაზაში მისი პერსონალური მონაცემების დამუშავების კანონიერება, რომ არაფერი ითქვას ინფორმაციის მიღების, მონაცემთა გასწორების ან წაშლის მოთხოვნის უფლების განხორციელებაზე. პერსონალურ მონაცემთა დაცვის უფლება ვერ იქნება სათანადოდ უზრუნველყოფილი, თუ ის მხოლოდ მოქალაქის მიერ გარკვეული ქმედებების განხორციელებაზეა დამოკიდებული. სწორედ ამიტომ, მონაცემთა დამმუშავებლებმა უნდა აიღონ პასუხისმგებლობა მონაცემთა დამუშავების კანონიერებაზე.

საქართველოში მსხვილ ორგანიზაციებსაც კი არა აქვთ სრულად გათვითცნობიერებული მათი პასუხისმგებლობა და ვალდებულებები. მიუხედავად იმისა, რომ საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ 2012 წლის მაისში შევიდა ძალაში, პრაქტიკაში მისი დანერგვა მხოლოდ 2013 წლის მეორე ნახევარში - პერსონალურ მონაცემთა დაცვის საზედამხედველო ინსტიტუტის შექმნის შემდგომ დაიწყო.

ტექნოლოგიური პროგრესის პირობებში პერსონალური მონაცემების მოპოვებამ და დამუშავებამ სწრაფი, მასშტაბური და მოცულობითი ხასიათი შეიძინა.

> ევროპელთა 92%-ს აწუხებს მობილური აპლიკაციების გამოყენებისას მათი თანხმობის გარეშე პერსონალური მონაცემების შეგროვების საკითხი, ხოლო 89%-ს აინტერესებს, ვის მიუწვდება ხელი ტელეფონში შენახულ ინფორმაციაზე. ხშირად, ტექნოლოგიური ცვლილებები ადამიანს არჩევანის უფლებას უზღუდავს, რაც იწვევს მათ უნდობლობას. სწორედ ამიტომაა მნიშნელოვანი, მოქალაქეებს დავუბრუნოთ კონტროლი მათ პერსონალურ მონაცემებზე.
>
> **ვივიანა რიდინგი,**
> ევროპის კომისიის ვიცე-პრეზიდენტი

ადამიანები ყოველდღიურ ცხოვრებაში ხედავენ, რამდენად ხშირია მათი მონაცემების შეგროვება, შენახვა, გამჟღავნება ან გავრცელება. მოქალაქეთა გარკვეულ ნაწილს აქვს განცდა, რომ მუდმივი დაკვირვების ქვეშ არიან. შესაბამისად, აინტერესებთ, რა მიზნით და რა ვადით ხდება მათ შესახებ ინფორმაციის შეგროვება, არის თუ არა ეს კანონიერი, ვის მიუწვდება ხელი მათ მონაცემებზე, რა საშუალებები არსებობს მათი დარღვეული უფლებების დასაცავად.

ინფორმირებულობის დაბალი მაჩვენებლის გამო, სამწუხაროდ, მოქალაქეები სოციალური ქსელებით თუ სხვა საშუალებებით ხშირად ასაჯაროებენ საკუთარ პერსონალურ მონაცემებს და ვერ აცნობიერებენ, რა ზიანის მომტანი შეიძლება იყოს მათი ქმედება. ეს პრობლემა აქტუალურია არა მხოლოდ საქართველოში, არამედ სხვა, უფრო განვითარებულ ქვეყნებშიც. ევროპის კავშირის ფუნდამენტურ უფლებათა სააგენტოს მიერ 16 სახელმწიფოში ჩატარებული კვლევის საფუძველზე გამოქვეყნებულ ანგარიშში[12] ხაზგასმულია მოქალაქეთა ცნობიერებისა და ინფორმირებულობის დაბალი დონე. შესაბამისად, მთავარ რეკომენდაციად სწორედ საზოგადოებრივი ცნობიერების ამაღლებაა მითითებული.

11 „The Article 29 Data Protection Working Party“ დაფუძნდა ევროპის საბჭოსა და ევროპის პარლამენტის 1995 წლის 24 ოქტომბრის დირექტივის (95/46/ EC) საფუძველზე.

12 FRA, Access to Data Protection Remedies in EU Member States, Publications Office of the European Union, 2013, p.10

პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატმა, საზოგადოების ინფორმირების მიზნით, მასმედიის საშუალებებით გაავრცელა განცხადებები მოქალაქეთა უფლებების შესახებ, მომზადდა საინფორმაციო მასალა. ვებგვერდზე ინფორმაციასთან ერთად ხელმისაწვდომია უფლებების რეალიზებისთვის საჭირო რამდენიმე განცხადების ნიმუში. ინსპექტორის აპარატი, ასევე, მუშაობს მონაცემთა დამმუშავებლების განათლების დონის ამაღლებაზე, რადგან სწორედ მათ მიერ კანონის მოთხოვნების შესრულებაზეა დამოკიდებული ქვეყანაში მონაცემთა დაცვის უზრუნველყოფა.

პოზიტიურ შეფასებას იმსახურებს მონაცემთა არაერთი მსხვილი დამმუშავებლის, მათ შორის საჯარო დაწესებულებების მზადყოფნა, ქმედითი ნაბიჯები გადადგან კანონით გათვალისწინებული ვალდებულებების შესასრულებლად, რაც უნდა გამოიხატოს მოქალაქეთათვის ინფორმაციის ხელმისაწვდომობის უზრუნველყოფაში, მონაცემთა გასწორების, წაშლის ან განადგურების ეფექტური და მარტივი მექანიზმების შექმნაში.

რეკომენდაციები საქართველოს მთავრობას პერსონალურ მონაცემთა დაცვის მიზნით გასატარებელი ღონისძიებების შესახებ

არსებული საკანონმდებლო ჩარჩოსა და პრაქტიკაში არსებული მდგომარეობის ანალიზის შედეგად იკვეთება, პერსონალურ მონაცემთა დაცვის მაღალი სტანდარტების დანერგვის მიზნით, ქმედითი ნაბიჯების განხორციელების აუცილებლობა, რაც ასევე ევროპის კავშირთან სავიზო რეჟიმის გამარტივების ერთ-ერთ წინაპირობას წარმოადგენს. ამ მიზნით, პერსონალურ მონაცემთა დაცვის ინსპექტორმა შეიმუშავა შემდეგი სახის რეკომენდაციები:

1. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი საჭიროებს ევროპულ სტანდარტებთან[13] სრულ შესაბამისობაში მოყვანას, კერძოდ:

- განსაკუთრებულ კატეგორიას მიკუთვნებულ მონაცემთა ჩამონათვალის გაფართოებას და მათი დამუშავების საფუძვლების დაკონკრეტებას;
- პერსონალურ მონაცემთა სუბიექტის უფლებების შესახებ არსებული ნორმების დახვეწას და დაცვის გარანტიების გაზრდას;
- პირდაპირ მარკეტინგთან დაკავშირებული რეგულაციების დახვეწას;
- კერძო სექტორის მიმართ კანონის ამოქმედების თარიღის გადმოწევას;
- საზოგადოებრივი თავშეყრის ადგილებსა და საზოგადოებრივ ტრანსპორტში ვიდეოთვალთვალის განხორციელების რეგულირებას;
- სხვა სახელმწიფოსთვის/საერთაშორისო ორგანიზაციისათვის მონაცემთა გადაცემის რეგულაციების დახვეწას და კონვენციის დამატებით ოქმთან შესაბამისობაში მოყვანას;
- ინსპექტორის ანგარიშვალდებულების გაზრდას პარლამენტის წინაშე.

2. ვინაიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ კანონის მიღებისას არ მომხდარა საკანონმდებლო ბაზის ძირეული გადასინჯვა (გარდა საქართველოს ზოგად ადმინისტრაციული კოდექსისა), პირველ ეტაპზე, საზედამხედველო ინსტიტუტის მდგრადობისთვის, ცვლილებები უნდა განხორციელდეს „საჯარო სამსახურის შესახებ“ საქართველოს კანონსა და „საჯარო სამსახურში ინტერესთა შეუთავსებლობისა და კორუფციის შესახებ“ საქართველოს კანონში, ასევე რამდენიმე კანონქვემდებარე აქტში. შემდგომ ეტაპზე მნიშვნელოვანია, გაანალიზდეს დარგობრივი კანონმდებლობა (ჯანდაცვა, დაზღვევა, საბანკო-საფინანსო საქმიანობა, განათლება, სოციალური უზრუნველყოფა და სხვა) და, საჭიროების შემთხვევაში, მოხდეს მისი ეტაპობრივი გადასინჯვა.

3. საჯარო დაწესებულებათა მიერ მონაცემთა კანონიერი და პროპორციული დამუშავების უზრუნველსაყოფად, უნდა დარეგულირდეს მონაცემთა შენახვის, არქივირებისა და განადგურების წესი და ვადები. დაუყოვნებლივ უნდა მოხდეს საჯარო დაწესებულებებში კანონიერი საფუძვლის გარეშე მოპოვებული მონაცემების დაბლოკვა, წაშლა ან განადგურება.

13 პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ ევროპის საბჭოს N108 კონვენცია; ასევე პერსონალური მონაცემების დამუშავებისა და გადაცემის დროს ფიზიკური პირების დაცვის შესახებ ევროპის პარლამენტისა და ევროპის საბჭოს დირექტივა (95/46/EC) და ევროპის ქვეყნების საუკეთესო გამოცდილება.

4. უფლებამოსილი პირის მიერ მონაცემთა დამუშავების შემთხვევაში, მონაცემთა დამმუშავებლებმა უნდა უზრუნველყონ:

- უფლებამოსილი პირის მიერ მონაცემთა დამუშავების განხორციელება წერილობითი ხელშეკრულების ან სამართლებრივი აქტის საფუძველზე სათანადო უსაფრთხოების ზომების დაცვით;
- პერიოდული მონიტორინგის ჩატარება მონაცემთა არამიზნობრივი გამოყენების პრევენციისა და აღკვეთის მიზნით.

5. ფარულ მიყურადებასა და მოსმენებთან დაკავშირებულ საკანომდებლო ინიციატივებში მიზანშეწონილია, გათვალისწინებულ იქნას ჯეროვანი გარანტიები ხელისუფლების ორგანოების მხრიდან უფლებამოსილების ბოროტად ან თვითნებურად გამოყენების წინააღმდეგ და მექანიზმები, რომლებიც უზრუნველყოფს ბალანსის დაცვას ადამიანის ღირსების, პირადი ცხოვრების ხელშეუხებლობის უფლებასა და საზოგადოებრივი უსაფრთხოების, დანაშაულის გამოძიებისა და პრევენციის ლეგიტიმურ საჯარო ინტერესს შორის.

6. საერთაშორისო ხელშეკრულებისა და შეთანხმების დადების დროს, გათვალისწინებულ უნდა იქნეს საჯარო დაწესებულებების მიერ სხვა ქვეყნებისა და საერთაშორისო ორგანიზაციებისთვის პერსონალური მონაცემების შემცველი ინფორმაციის მიწოდების საკითხი.

პერსონალურ მონაცემთა დაცვის
ინსპექტორის აპარატი

www.personaldata.ge

www.pdp.ge

(+995 32) 242 1000

აფაქიძის ქ. 15, 0171,
თბილისი, საქართველო

office@pdp.ge