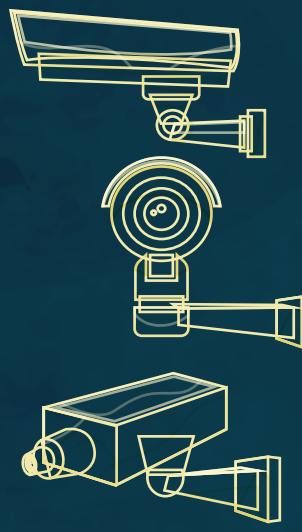
პერსონალურ მონაცემთა
დაცვის სამსახური



რეკომენდაციები ვიდეომონიტორინგის და აუდიომონიტორინგის განხორციელების თაობაზე

HD

00:00:00:00

www.pdps.ge

რეკომენდაციები ემსახურება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ნორმათა განმარტებას, საუკეთესო პრაქტიკის დამკვიდრების ხელშეწყობას, ის არ წარმოადგენს სამართლებრივ აქტს, არის სარეკომენდაციო ხასიათის და არ წარმოშობს დამატებით უფლებებსა და ვალდებულებებს.

შინაარსი

შესავალი

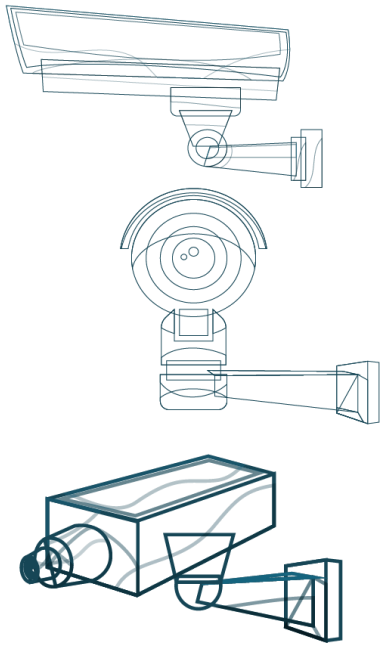
„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, მონაცემთა დამუშავების ერთ-ერთ სახედ, ითვალისწინებს ვიდეომონიტორინგისა და აუდიომონიტორინგის განხორციელებას[1], განსაზღვრავს მათ ცნებებს[2] და ადგენს ხსენებული ფორმებით მონაცემთა დამუშავების სპეციალურ წესებს[3]. უფრო კონკრეტულად, კანონი ადგენს ვიდეომონიტორინგის კონკრეტულ მიზნებს და განსაზღვრავს დასაქმებული პირის სამუშაო პროცესის/სივრცის, ასევე, საცხოვრებელი შენობის, გამოსაცვლელი ოთახების, ჰიგიენისთვის განკუთვნილი ადგილების ან ისეთი სივრცეების ვიდეომონიტორინგთან დაკავშირებულ საკითხებს, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს. გარდა ამისა, კანონი ამომწურავად განსაზღვრავს აუდიომონიტორინგის განხორციელების საფუძვლებს, სუბიექტის ინფორმირებისა და აუდიომონიტორინგის/ვიდეომონიტორინგის გზით მონაცემთა დამუშავების პროცესის მახასიათებლების წერილობით განსაზღვრის ვალდებულებებს.

წინამდებარე რეკომენდაციები მიზნად ისახავს, გაანალიზოს ვიდეომონიტორინგისა და აუდიომონიტორინგის განხორციელების თაობაზე კანონმდებლობით დადგენილი წესები, რათა შესაბამისმა პასუხისმგებელმა სუბიექტებმა სრულყოფილად აღიქვან მათთვის დაკისრებული ვალდებულებების არსი და ფარგლები.

რეკომენდაციები მომზადებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) ნორმატიული შინაარსისა და საუკეთესო ქართული და ევროპული გამოცდილების ანალიზის საფუძველზე.

[1] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის (14/06/2023; №3144-XIმს-Xმპ) მე-3 მუხლის „ვ“ ქვეპუნქტი.
[2] იქვე, მე-3 მუხლის „ღ“ და „ყ“ ქვეპუნქტები.
[3] იქვე, მე-10 და მე-11 მუხლები.

1. ვიდეომონიტორინგი



1.1. ვიდეომონიტორინგის ცნება და მიმართება პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან

თანამედროვე ეპოქაში, მზარდი ტექნოლოგიური განვითარების პირობებში, ვიდეომონიტორინგი მონაცემთა დამუშავების ერთ-ერთ ყველაზე ფართოდ გავრცელებულ ფორმად ჩამოყალიბდა, რომელიც აქტიურად გამოიყენება როგორც საჯარო და კერძო დაწესებულებების, ისე ფიზიკური პირების მიერ.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „ღ“ ქვეპუნქტი ვიდეომონიტორინგს განმარტავს, როგორც საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ვიზუალური გამოსახულების დამუშავებას, კერძოდ, ვიდეოკონტროლს ან/და ვიდეოჩაწერას (გარდა ფარული საგამოძიებო მოქმედებისა).

ხსენებული ვიდეო გადაღების ტექნოლოგიების უმეტესობას გააჩნია პირდაპირ რეჟიმში დაკვირვების, ღამის ხედვის, მანევრირების, შორი მანძილიდან დაკვირვების, დეტალების (მათ შორის, ადამიანის თვალისთვის შეუმჩნეველი) აღმოჩენის, აუდიოჩაწერის, ადამიანის უნიკალური მახასიათებლების (მაგალითად, სახის) ამოცნობის, მათი ქცევის შესწავლისა და გაანალიზების ტექნიკური შესაძლებლობები[4].

ვიდეომონიტორინგის სისტემის მეშვეობით განხორციელებული ჩანაწერი პერსონალურ მონაცემად განიხილება, როდესაც შესაძლებელია მასზე აღბეჭდილი ადამიანის სახის გამოსახულების გარჩევა (პირდაპირი იდენტიფიკაცია), ან ადამიანის სახის ნაკვთების გარჩევა შეუძლებელია, მაგრამ სისტემის მიერ დაფიქსირებული ნივთების ან/და ადამიანის ქცევის მახასიათებლებით, მათი სხვა მონაცემებთან შედარებით შესაძლებელია პირის იდენტიფიცირება (არაპირდაპირი იდენტიფიკაცია). მაგალითად, ავტოსატრანსპორტო საშუალების მძღოლის მიერ სხვა სატრანსპორტო საშუალების დაზიანების შემთხვევაში ვიდეოჩანაწერში დაფიქსირებული სანომრე ნიშანი გამოიყენება იმ მანქანის მფლობელის ვინაობის

[4] „ვიდეოთვალთვალის განხორციელების წესი - რეკომენდაცია“, 2021, 4. იხ. < https://old.pdps.ge/cdn/2021/12/recommendation-video-surveillance.pdf > [20.03.2024].

დასადგენად (ავტოსატრანსპორტო საშუალების მფლობელის შესახებ ინფორმაციის გამოთხოვა), რომლის მიზეზითაც მოხდა დაზიანება[5].

ოპტიკური აუდიო-ვიზუალური საშუალებების გამოყენებით კონკრეტული სივრცის სისტემატური მონიტორინგი, რაც ხშირად განპირობებულია უსაფრთხოების, საკუთრებისა თუ პირის სიცოცხლისა და ჯანმრთელობის დაცვის მიზნით, თანამედროვეობის მნიშვნელოვან გამოწვევად იქცა. ამ ტიპის ტექნოლოგიები, შესაძლოა, საშუალებას იძლეოდეს, შეგროვდეს და შენახულ იქნეს ვიდეოკამერის ხედვის არეალში მოქცეული ყველა იმ პიროვნების პერსონალური მონაცემები, რომლებიც იდენტიფიცირებადი არიან მათი გარეგნობის ან რაიმე სხვა ნიშნის გათვალისწინებით. საყურადღებოა, რომ ამგვარი ტექნოლოგიების არაკეთილსინდისიერი გამოყენების შესაძლებლობიდან გამომდინარე რისკები მზარდია ვიდეომონიტორინგს დაქვემდებარებული ტერიტორიის მასშტაბისა და ამ ადგილით მოსარგებლე მონაცემთა სუბიექტების რაოდენობის გათვალისწინებით[6].

ამდენად, მიუხედავად ვიდეომონიტორინგის საშუალებით უსაფრთხოების უზრუნველყოფის ინტერესისა, აუცილებელია, თავიდან იქნეს აცილებული მონაცემთა ყველა შესაძლო არამიზნობრივი და შესაბამისად, უკანონო დამუშავება. ყოველივე ეს განსაკუთრებით საყურადღებოა იმ ფონზე, რომ ტექნოლოგიურმა განვითარებამ შესაძლებელი გახადა სტანდარტული ვიდეოკამერების აღჭურვა შესაბამისი სისტემური უზრუნველყოფით და მათი ე.წ. „ჭკვიან კამერებად“ ქცევა, რაც დამუშავებული მონაცემთა მასშტაბისა და ტექნოლოგიური შესაძლებლობების გათვალისწინებით, ზრდის მონაცემთა შემდგომი არამიზნობრივი დამუშავების საფრთხეს[7]. აქედან გამომდინარე, ვიდეომონიტორინგის განხორციელების პროცესში, მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის მიერ მკაცრად იქნეს დაცული კანონით დადგენილი ვალდებულებები.

1.2. ვიდეომონიტორინგის განხორციელების მიზნები

ვიდეომონიტორინგის განხორციელებისას, გადამწყვეტი მნიშვნელობა ენიჭება, აქვს თუ არა დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს შესაბამისი მიზანი, რომელთა მისაღწევადაც აუცილებელია ვიდეომონიტორინგის

[5] „რეკომენდაციები ვიდეოთვალთვალის განხორციელების შესახებ“, 2. იხ. < https://old.pdps.ge/cdn/2018/12/video-surviellance-recommendation-final.pdf > [20.03.2024].

[6] *European Data Protection Board (EDPB)*, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §7.

[7] იქვე, §2.

განხორციელება. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლი დეტალურად განსაზღვრავს, თუ რა მიზანს შეიძლება ემსახურებოდეს ვიდეომონიტორინგი და ამ გზით მონაცემთა დამუშავება. კერძოდ, ვიდეომონიტორინგის განხორციელება დასაშვებია, თუ იგი მიზნად ისახავს შემდეგი ამოცანების შესრულებას:

- დანაშაულის თავიდან აცილება ან მისი გამოვლენა;
- საზოგადოებრივი უსაფრთხოება;
- პირის უსაფრთხოებისა და საკუთრების დაცვა;
- არასრულწლოვანის დაცვა (მათ შორის, მავნე ზეგავლენისგან დაცვია);
- საიდუმლო ინფორმაციის დაცვა;
- გამოცდის/ტესტირების მიზნები.

აღსანიშნავია, რომ მოცემული ჩამონათვალი არ არის ამომწურავი და შესაძლოა არსებობდეს სხვა საჯარო ან/და ლეგიტიმური ინტერესი, რომელიც ვიდეომონიტორინგს აუცილებელს გახდის.

მნიშვნელოვანია, რომ უსაფრთხოების, საკუთრების თუ ინფორმაციის დაცვის ზემოხსენებული საჭიროება გამომდინარეობდეს რეალურად მოსალოდნელი საფრთხისაგან[8] და ვიდეომონიტორინგის განხორციელება მონაცემთა დამუშავების მიზნის ადეკვატურ და პროპორციულ საშუალებას წარმოადგენდეს.

1.3. ვიდეომონიტორინგის განხორციელების პროცესის მახასიათებლების წერილობით განსაზღვრის ვალდებულება

კანონის მე-10 მუხლის მე-2 პუნქტი ვიდეომონიტორინგის განსახორციელებლად ადგენს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, კანონის მე-4 მუხლით დადგენილი პრინციპების შესაბამისად, წერილობით განსაზღვროს ვიდეომონიტორინგის მიზანი და მოცულობა, ვიდეომონიტორინგის ხანგრძლივობა და ვიდეოჩანაწერის შენახვის ვადა, ვიდეოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები, გარდა იმ შემთხვევისა, როდესაც ფიზიკური პირი ვიდეომონიტორინგს ახორციელებს საცხოვრებელ შენობაში.

[8] European Data Protection Board (EDPB), Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §20.

ხსენებული მუხლის მიზნებისთვის, ვიდეომონიტორინგის პროცესის შესახებ ინფორმაცია წერილობით შეიძლება განისაზღვროს როგორც დამოუკიდებელი დოკუმენტის სახით, ისე დაწესებულების/ორგანიზაციის სხვა შიდაორგანიზაციული აქტის/დოკუმენტის შემადგენელ ნაწილად.

აღნიშნული ვალდებულების მიზანია, უზრუნველყოს ვიდეომონიტორინგის გზით მონაცემთა დამუშავების პროცესის კანონთან შესაბამისი ფორმით დაგეგმვა და განხორციელება, რაც დამუშავებისთვის პასუხისმგებელ პირს ვიდეომონიტორინგის პროცესის წინასწარი ორგანიზების, ასევე მონაცემთა სუბიექტების უფლებების ხელყოფის თავიდან არიდების შესაძლებლობას მისცემს.

ამასთან, ხსენებულ პუნქტში ჩამოთვლილი ინფორმაციის წინასწარ, წერილობით განსაზღვრის პირობებში, მონაცემთა სუბიექტისთვის ბევრად უფრო მარტივად აღქმადი გახდება მონაცემთა დამუშავების კონკრეტული პროცესის მიზანი და მოცულობა, ასევე, ინფორმაცია ვიდეომონიტორინგის ხანგრძლივობის და ვიდეოჩანაწერის შენახვის ვადისა და ხსენებული დებულებით გათვალისწინებული სხვა საკითხების შესახებ.

1.4. დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი

პერსონალურ მონაცემთა და პირადი ცხოვრების ხელშეუხებლობის უფლებების დაცვა გარანტირებულია როგორც არასამუშაო, ისე სამუშაო დროსა და სივრცეში. ადამიანის უფლებათა ევროპულმა სასამართლომ ერთ-ერთი საქმეზე მკაფიოდ განმარტა[9], რომ პირადი ცხოვრების უფლება თავის თავში მოიაზრებს პირის უფლებას, განავითაროს ურთიერთობები სხვა ადამიანებთან მაშინაც კი, თუ ეს ურთიერთობა სამუშაო პროცესის დროს ხდება. ამასთან, სასამართლო მიუთითებს, რომ სამუშაო გარემოს სპეციფიკის მიუხედავად, დამსაქმებლის ინსტრუქციები სამუშაო ადგილას პირად სოციალურ ცხოვრებას მთლიანად ვერ აღკვეთს. ამდენად, პირადი ცხოვრების ცნება მოიცავს პროფესიული ხასიათის საქმიანობასაც, ვინაიდან ადამიანების უმეტესობას გარე სამყაროსთან კომუნიკაციის საშუალება სწორედ სამსახურებრივი ურთიერთობის ფარგლებში ეძლევა. ზემოაღნიშნულიდან გამომდინარე, სამუშაო ადგილზე ვიდეომონიტორინგის დროს, დაცული უნდა იქნეს კანონით დადგენილი წესები და დასაქმებულთა პირადი ცხოვრების ხელშეუხებლობის უფლება[10].

[9] Antonovic and mirkovic v. Montenegro, 28/11/2017, №70838/13.

[10] „ვიდეოთვალთვალის განხორციელების წესი - რეკომენდაცია“, 2021, 28-29.

ამდენად, სამუშაო სივრცეში ვიდეომონიტორინგის თანმდევი მომეტებული საფრთხეების გათვალისწინებით, კანონის მე-10 მუხლის მე-3 პუნქტმა განსაზღვრა, რომ დასაქმებული პირის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი დასაშვებია მხოლოდ გამონაკლის შემთხვევაში, თუ ამ მუხლის პირველი პუნქტით განსაზღვრული მიზნების მიღწევა სხვა საშუალებით შეუძლებელია ან დაკავშირებულია არაპროპორციულად დიდ ძალისხმევასთან. რაც შეეხება თავად „სამუშაო სივრცის“ ცნების შინაარსს, ასეთად შეიძლება ჩაითვალოს ძირითადი სამსახურებრივი ფუნქციების შესასრულებლად განკუთვნილი სივრცე, სადაც დაწესებულებაში დასაქმებული პირები უშუალოდ ახორციელებენ სამსახურებრივ უფლებამოსილებას (მაგალითად, სამუშაო ოთახი, საპროცედურო ოთახი, სალარო)[11].

დასაქმებულის სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი შეიძლება ჩაითვალოს მომეტებული საფრთხის წყაროდ დასაქმებულის (მონაცემთა სუბიექტის) მიმართ, ვინაიდან აღნიშნული პროცესი შესაძლებელს ხდის დასაქმებულის ქცევის განგრძობად კონტროლს, რამაც კანონით გათვალისწინებული პირობების დაუცველობის შემთხვევაში, სუბიექტის პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევა შეიძლება გამოიწვიოს[12]. ზოგადად, დასაქმებულებზე მონიტორინგის განმახორციელებელი ტექნოლოგიების გამოყენებას, შესაძლოა, ჰქონდეს ე.წ. „მსუსხავი ეფექტი“ დასაქმებულის ფუნდამენტურ უფლებებზე, მათ შორის, ორგანიზების, თანამშრომელთა შეკრებისა და კონფიდენციალური კომუნიკაციის შესაძლებლობაზე. აღნიშნული სისტემების სამუშაო ადგილზე გამოყენება, საჯარო სივრცეში გადამეტებული მასშტაბით განხორციელებული ვიდეომონიტორინგის მსგავსად, შეიძლება იწვევდეს თანამშრომლებზე ირიბ ზეწოლას და მათი ქცევის კონტროლს/კორექტირებას. ამგვარი ტექნოლოგიების შესაძლებლობების გათვალისწინებით, დასაქმებულებისთვის (მონაცემთა სუბიექტებისთვის) შეიძლება უცნობიც კი იყოს, თუ მათი კონკრეტულად რომელი მონაცემი მუშავდება და რა მიზნით. გარდა ამისა, ცალკეულ შემთხვევებში, არსებობს საფრთხე, სუბიექტისთვის უცნობი იყოს, კონკრეტულ გარემოში ამგვარი მონიტორინგის სისტემის არსებობის ფაქტი[13].

სამუშაო სივრცეში ვიდეომონიტორინგის კანონიერებასთან მიმართებით, ადამიანის უფლებათა ევროპული სასამართლო პირდაპირ მიუთითებს, რომ სამუშაო ადგილზე დასაქმებულთა მიმართ განხორციელებული ვიდეომონიტორინგი, მიუხედავად იმისა

[11] „ვიდეოთვალთვალის განხორციელების წესი - რეკომენდაცია“, 2021, 7.

[12] *Article 29 Data Protection Working Party*, Opinion 2/2017 on Data Processing at Work, Adopted on 8 June 2017, 19.

[13] იქვე, 9-10.

ფარულია იგი თუ არა, აღქმულ უნდა იქნას, როგორც მნიშვნელოვანი ჩარევა დასაქმებულის პირადი ცხოვრების უფლებით დაცულ სფეროში[14].

გასათვალისწინებელია, რომ კანონის მე-10 მუხლის მე-8 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი თვალსაჩინოდ განათავსოს, ხოლო სამუშაო პროცესის/სივრცის ვიდეომონიტორინგის შემთხვევაში – დამატებით, დასაქმებული პირი წერილობით გააფრთხილოს ვიდეომონიტორინგის კონკრეტული მიზნ(ებ)ის შესახებ. აღნიშნული მოთხოვნების დაცვის შემთხვევაში, მონაცემთა სუბიექტი მის შესახებ მონაცემთა დამუშავების თაობაზე ინფორმირებულად მიიჩნევა.

ყოველივე ზემოაღნიშნულიდან გამომდინარე, ეჭვგარეშეა, რომ დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის მხრიდან განხორციელებული სამუშაო პროცესის/სივრცის ვიდეომონიტორინგი, ზოგადად, დასაქმებულის (მონაცემთა სუბიექტის) პირადი ცხოვრების ხელშეუხებლობის უფლებაში საკმაოდ ინტენსიურ ჩარევას წარმოადგენს, ამ დროს, მონაცემთა დამმუშავებელს განსაკუთრებული სიფრთხილე და კანონით გათვალისწინებული ნორმების ზედმიწევნით დაცვა მართებს, როგორც ვიდეომონიტორინგის სათანადო საფუძვლისა და მიზნის სწორად იდენტიფიცირების, ისე სუბიექტის ინფორმირების კუთხით. ამასთან, მნიშვნელოვანია აღინიშნოს, რომ ადამიანის უფლებათა ევროპული სასამართლოს განმარტებით, დასაქმებულების სამუშაო პროცესის/სივრცის ვიდეომონიტორინგის თვალსაზრისით, აუცილებელია განვასხვავოთ, მონიტორინგის განხორციელების სხვადასხვა ადგილები, კონფიდენციალურობის დაცულობის იმ მოლოდინის გათვალისწინებით, რომელიც თანამშრომელს კონკრეტული სივრცის მიმართ შეიძლება გააჩნდეს[15].

1.5. ვიდეომონიტორინგი ჰიგიენისთვის განკუთვნილ ადგილებში

საყურადღებოა, რომ კანონის მე-10 მუხლის მე-4 პუნქტი იმპერატიულად კრძალავს ვიდეომონიტორინგის განხორციელებას გამოსაცვლელ ოთახებში, ჰიგიენისთვის განკუთვნილ ადგილებში ან ისეთ სივრცეში, სადაც სუბიექტს პირადი ცხოვრების დაცულობის გონივრული მოლოდინი აქვს ან/და ვიდეომონიტორინგის განხორციელება საყოველთაოდ აღიარებულ ზნეობრივ ნორმებს ეწინააღმდეგება.

[14] Antonovic and mirkovic v. Montenegro, 28/11/2017, №70838/13, §55.

[15] *European Court of Human Rights*, Guide to the Case-Law of the of the European Court of Human Rights - Data protection, Updated on 31 August 2022, §158.

კანონის მიზნებისთვის, გამოსაცვლელ ოთახში იგულისხმება სივრცე, რომელსაც დაწესებულების თანამშრომლები/მომხმარებლები/სტუმრები სისტემატურად იყენებენ სამოსის გამოცვლის მიზნით (მაგალითად, საცურაო აუზის/სპორტული დარბაზის გასახდელი). აქვე, გასათვალისწინებელია ისიც, რომ ცალკეულ შემთხვევებში, როდესაც დაწესებულებას არ აქვს გამოყოფილი სპეციალური გამოსაცვლელი ოთახი, მისი თანამშრომლები, შესაძლოა, სხვა დანიშნულების ოთახს (მაგალითად, სუპერმარკეტის საწყობს) დამატებით იყენებენ გამოსაცვლელ სივრცედ. ამ კუთხით, საყურადღებოა, რომ ვიდეოთვალთვალი დაუშვებელია როგორც გამოსაცვლელად გამოყოფილ სპეციალურ ოთახში, ასევე იმ სივრცეში, რომელსაც თანამშრომლები ამ მიზნით იყენებენ. აქვე, უნდა განიმარტოს, რომ დამუშავებისთვის პასუხისმგებელი პირი თავისუფლდება პასუხისმგებლობისგან იმ შემთხვევაში, თუკი იგი თანამშრომლებს გააფრთხილებს კონკრეტული სივრცის (სადაც მიმდინარეობს ვიდეომინიტორინგი) გამოსაცვლელ ოთახად გამოყენების დაუშვებლობის შესახებ.

რაც შეეხება ჰიგიენისთვის განკუთვნილ სივრცეს, იგი შეიძლება მოიცავდეს როგორც საპირფარეშოს კაბინებს, ასევე ხელსაბან სივრცეს. ამასთან, საყურადღებოა, რომ მე-10 მუხლის მე-4 პუნქტით გათვალისწინებული აკრძალვა არ მოიცავს მხოლოდ უშუალოდ ამგვარი სივრცეების შიდა ტერიტორიაზე განთავსებულ ვიდეო კამერებს, არამედ იგი ასევე გულისხმობს იმგვარ შემთხვევებსაც, როდესაც, მაგ. დერეფანში დაყენებული კამერის ხედვის არეალში შეიძლება მოექცეს ჰიგიენისთვის განკუთვნილი სივრცის კარი, რომლის გაღებისას შესაძლებელი იქნება ამგვარი სივრცის შიდა ტერიტორიის დანახვა.

1.6. ვიდეომონიტორინგი საცხოვრებელ შენობაში

თანამედროვე სამყაროში, ფიზიკური პირების მიერ, სულ უფრო ხშირად ხდება ვიდეომონიტორინგის სისტემები გამოყენება საცხოვრებელ შენობებში ქონების ან/და პირის უსაფრთხოების დაცვის მიზნით.

აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედება არ ვრცელდება ფიზიკური პირის მიერ აშკარად პირადი მიზნით ან/და ოჯახური საქმიანობის ფარგლებში მონაცემთა დამუშავებაზე, რომელიც დაკავშირებული არ არის მის სამეწარმეო ან/და ეკონომიკურ, პროფესიულ საქმიანობასთან ან სამსახურებრივი მოვალეობის შესრულებასთან. მიუხედავად ამისა, არის შემთხვევები, როდესაც ფიზიკური პირის მიერ განხორციელებული ვიდეომონიტორინგი სცდება პირად სივრცეს და მოიცავს საჯარო სივრცეს (თუნდაც ნაწილობრივ) ან/და სხვა პირთა კერძო საკუთრებასაც. მაგალითისთვის შეგვიძლია მოვიყვანოთ შემთხვევა, როდესაც ფიზიკური პირის მიერ ხორციელდება საკუთარი

საცხოვრებელი შენობის გარე პერიმეტრის ვიდეომონიტორინგი, რომლის ხედვის არეალში ექცევა მეზობლის ან მომიჯნავედ მცხოვრები პირის საცხოვრებელი სახლი. ასეთ დროს, ვინაიდან საცხოვრებელი შენობის ვიდეომონიტორინგი სხვის პირად ცხოვრებაში არამართლზომიერი ჩარევის რისკებს ზრდის, ფიზიკურმა პირებმა ვიდეომონიტორინგის განხორციელებისას უნდა გაითვალისწინონ სხვა პირთა უფლებები და ლეგიტიმური ინტერესები, მათ შორის, პირადი ცხოვრების ხელშეუხებლობის უფლება, რომლის თანახმადაც, ნებისმიერ პირს აქვს უფლება თავისუფლად ისარგებლოს საკუთარი საცხოვრებელი სივრცით ისე, რომ არ მოხდეს მის საცხოვრებელ შენობაში მისი გადაადგილების, შემსვლელ და გამომსვლელ პირთა იდენტიფიცირება ან/და შენობაში შესვლა-გასვლის დროის დაფიქსირება[16].

შესაბამისად, როდესაც ფიზიკური პირის მიერ ვიდეომონიტორინგის განხორციელება სცდება პირად მიზნებს და როდესაც, შესაძლოა, ადგილი ჰქონდეს სხვა პირთა ლეგიტიმური ინტერესების შელახვას, ვიდეომონიტორინგის განმახორციელებელმა პირმა უნდა დაიცვას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნები და, საჭიროების შემთხვევაში, მოიპოვოს შესაბამისი თანხმობა. კერძოდ, საცხოვრებელი შენობის საერთო შესასვლელისა და მასში არსებული საერთო სივრცის ვიდეომონიტორინგის განხორციელების შემთხვევაში, აუცილებელია მესაკუთრეთა ნახევარზე მეტის წერილობითი თანხმობა, ხოლო საცხოვრებელ შენობაში არსებული ინდივიდუალური საკუთრების შესასვლელის ვიდეომონიტორინგი დასაშვებია მხოლოდ მისი მესაკუთრის/მფლობელის გადაწყვეტილებით ან მისი წერილობითი თანხმობით იმგვარად, რომ ვიდეომონიტორინგის განხორციელებით არ ილახებოდეს სხვა პირების (მათ შორის, მესაკუთრის, ფართობით კანონიერად მოსარგებლის) ლეგიტიმური ინტერესები.

მნიშვნელოვანია აღინიშნოს, რომ თუ საცხოვრებელ შენობაში ან მის გარე პერიმეტრზე განთავსებულ ვიდეომონიტორინგის სისტემის ხედვის არეალში ექცევა საჯარო ან საერთო სივრცე, ასევე, მომიჯნავედ მცხოვრები პირის საცხოვრებელი სახლი, ვიდეომონიტორინგის განმახორციელებელმა პირმა უნდა განათავსოს გამაფრთხილებელი ნიშანი, რომელიც ვიდეომონიტორინგის სისტემის ხედვის არეალში მოხვედრილი ნებისმიერი ადამიანისთვის თვალსაჩინო და აღქმადი იქნება.

ვინაიდან, გარკვეულ შემთხვევებში, საცხოვრებელ შენობაში (ან გარე პერიმეტრზე) განხორციელებულ ვიდეომონიტორინგზე შესაძლოა გავრცელდეს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნები, მნიშვნელოვანია, რომ ვიდეომონიტორინგის განმახორციელებელმა პირმა:

[16] „ვიდეოთვალთვალის განხორციელების წესი - რეკომენდაცია“, 2021, 61.

- ყურადღება მიაქციოს ვიდეო სათვალთვალო მოწყობილობის მდებარეობას, მის ხედვის არეალს და შეაფასოს ხომ არ არსებობს სხვათა უფლებების შელახვის რისკები;
- შეაფასოს ვიდეომონიტორინგის განხორციელების აუცილებლობა და პროპორციულობა;
- საჭიროების შემთხვევაში, შესაბამისი პირებისგან მოიპოვოს თანხმობა;
- გამოიყენოს დაცული ვიდეომონიტორინგის სისტემები;
- განსაზღვროს, თუ რა ვადით ხდება შესაბამისი ჩანაწერების შენახვა და მათზე წვდომა;
- თვალსაჩინო ადგილას განათავსოს მარტივად აღქმადი გამაფრთხილებელი ნიშანი.

დამატებით უნდა აღინიშნოს, რომ პრაქტიკაში არსებობს შემთხვევები, როდესაც ფიზიკური პირების მხრიდან ხდება უფუნქციო ვიდეომონიტორინგის სისტემის დაყენება, რა დროსაც რეალურად არ ხდება ვიდეომონიტორინგი, რაც მოქალაქეებს არასწორ წარმოადგენს უქმნის მონაცემთა დამუშავების პროცესთან დაკავშირებით, მონაცემთა სუბიექტების შეცდომაში შეყვანის თავიდან აცილების მიზნით, მიზანშეწონილია, მსგავსი ვიდეომონიტორინგის კამერები არ განთავსდეს[17].

1.7. ვიდეომონიტორინგს დაქვემდებარებული მონაცემთა სუბიექტის ინფორმირებულობა

მონაცემთა სუბიექტის ერთ-ერთ ფუნდამენტურ უფლებად კანონი განიხილავს მონაცემთა დამუშავების შესახებ ინფორმაციის მიღების უფლებას, რომელიც დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს ავალდებულებს, მონაცემთა სუბიექტს მიაწოდოს შესაბამისი ინფორმაცია მონაცემთა დამუშავების პროცესის შესახებ (გარდა კანონით გათვალისწინებული გამონაკლისი შემთხვევებისა). აღნიშნული უფლება ვრცელდება ასევე ვიდეომონიტორინგის განხორციელების დროსაც. კერძოდ, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია განათავსოს ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი, რომლის განთავსების ადგილი და მასზე დატანილი წარწერა და გამოსახულება აღქმადი უნდა იყოს კონტროლის სივრცეში მოხვედრილი ნებისმიერი ადამიანისთვის. ამასთან, ნიშანი უნდა განთავსდეს შენობის ყველა იმ სივრცეში, სადაც უშუალოდ მიმდინარეობს ვიდეომონიტორინგი.

[17] „ვიდეოთვალთვალის განხორციელების წესი - რეკომენდაცია", 2021, 66.

მონაცემთა სუბიექტების ინფორმირებულობის თვალსაზრისით, გამაფრთხილებელი ნიშნის თვალსაჩინო ადგილას განთავსების გარდა, მნიშვნელოვანია, იგი იყოს მარტივად აღქმადი (მაგალითად, გასათვალისწინებელია წარწერის ზომა, ფერი, განთავსების ადგილი) და შეიცავდეს კანონით გათვალისწინებულ ინფორმაციას. კერძოდ, ვიდეომონიტორინგის მიმდინარეობის შესახებ გამაფრთხილებელი ნიშანი უნდა შეიცავდეს[18]:

- მარტივად აღქმად წარწერას და გამოსახულებას ვიდეომონიტორინგის მიმდინარეობის თაობაზე;
- დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებას;
- დამუშავებისთვის პასუხისმგებელი პირის საკონტაქტო მონაცემებს.

დამატებით, მიზანშეწონილია, დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის მიერ არ განთავსდეს გამაფრთხილებელი ნიშნები იმ სივრცეში, სადაც ვიდეომონიტორინგი რეალურად არ ხორციელდება, რათა თავიდან იქნეს აცილებული მონაცემთა სუბიექტების შეცდომაში შეყვანისა და მათი პირადი ცხოვრების უფლებაზე ზემოქმედების ირიბი საფრთხე.

აქვე უნდა აღინიშნოს, რომ თუ დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს გამაფრთხილებელი ნიშნები განთავსებული ჰქონდა 2024 წლის პირველ მარტამდე, იგი თავისუფლდება ვალდებულებისგან, შეცვალოს გამაფრთხილებელი ნიშნები და მასზე დამატებით განათავსოს ინფორმაცია, დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებისა და მისი საკონტაქტო მონაცემების თაობაზე. რაც შეეხება 2024 წლის პირველი მარტის შემდეგ განთავსებულ გამაფრთხილებელ ნიშნებს, კანონის მე-10 მუხლის მე-9 პუნქტით გათვალისწინებული პირობები სტანდარტულად გავრცელდება ყველა მათგანზე.

[18] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-9 პუნქტი.

2. აუდიომონიტორინგი

2.1. აუდიომონიტორინგის ცნება

ტექნოლოგიური განვითარების კვალდაკვალ, სულ უფრო მარტივი ხდება ფიზიკური პირების მიერ მონაცემთა დამუშავება ისეთი მოწყობილობების გამოყენებითაც, რომლებიც მონაცემთა სუბიექტის საუბრის აუდიომონიტორინგის შესაძლებლობას იძლევა. აუდიომონიტორინგის ფარგლებში მონაცემთა დამუშავება შესაძლოა საკმაოდ სენსიტიური იყოს მონაცემთა სუბიექტისათვის და იწვევდეს მის პირადი ცხოვრების ხელშეუხებლობით დაცულ სფეროში უკანონო ჩარევას, შესაბამისად, მნიშვნელოვანია, რომ დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა მკაცრად დაიცვას აუდიომონიტორინგის განხორციელების წესები.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი მე-3 მუხლის „ყ“ ქვეპუნქტის თანახმად, აუდიომონიტორინგი განიმარტება, როგორც საჯარო ან კერძო სივრცეში განთავსებული/დამონტაჟებული ტექნიკური საშუალებების გამოყენებით ხმოვანი სიგნალის მონაცემთა დამუშავება. კერძოდ, აუდიოკონტროლი ან/და აუდიოჩაწერა (გარდა ფარული საგამოძიებო მოქმედებისა).

კანონი საკმაოდ ფართოდ განმარტავს აუდიომონიტორინგის ცნებას, შესაბამისად, მასში მოიაზრება, როგორც ვიდეომონიტორინგის სისტემა, რომელიც აღჭურვილია აუდიოკონტროლის მექანიზმით, ისე ცალკე აღებული ტექნიკური საშუალება, მათ შორის პორტატული ხმის ჩამწერი მოწყობილობა, რომელიც მხოლოდ და მხოლოდ აუდიოჩაწერას ახდენს.

2.2. აუდიომონიტორინგის განხორციელების საფუძვლები

ვიდეომონიტორინგის განხორციელების წესისგან განსხვავებით, რომელიც მონაცემთა დამუშავების დასაშვებობას მის მიზნებს უკავშირებს (მაგ., დანაშაულის თავიდან აცილება, მისი გამოვლენა, საზოგადოებრივი უსაფრთხოების, პირის უსაფრთხოებისა და საკუთრების დაცვა და სხვა), აუდიომონიტორინგთან მიმართებით, კანონის მე-11 მუხლი ამომწურავად ჩამოთვლის მონაცემთა ამ ფორმით დამუშავების კონკრეტულ საფუძვლებს. კერძოდ, ხსენებული მუხლის პირველი პუნქტის თანახმად, აუდიომონიტორინგის განხორციელება დასაშვებია მხოლოდ და მხოლოდ:

- მონაცემთა სუბიექტის თანხმობით;
- საოქმო ჩანაწერის საწარმოებლად;
- დამუშავებისთვის პასუხისმგებელი პირის მნიშვნელოვანი ლეგიტიმური ინტერესის დასაცავად, თუ განსაზღვრულია სათანადო და კონკრეტული ღონისძიებები მონაცემთა სუბიექტის უფლებებისა და ინტერესების დასაცავად;
- საქართველოს კანონმდებლობით პირდაპირ გათვალისწინებულ სხვა შემთხვევებში.

აღსანიშნავია, რომ მონაცემთა სუბიექტის თანხმობასთან დაკავშირებით კანონი საკმაოდ მაღალ სტანდარტს ადგენს. კერძოდ, კანონი მონაცემთა სუბიექტის თანხმობას განმარტავს, როგორც მონაცემთა სუბიექტის მიერ შესაბამისი ინფორმაციის მიღების შემდეგ, მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე აქტიური მოქმედებით, წერილობით (მათ შორის, ელექტრონულად) ან ზეპირად, თავისუფლად და მკაფიოდ გამოხატულ ნებას. რაც შეეხება წერილობითი თანხმობას, იგი განმარტებულია, როგორც თანხმობა, რომელსაც მონაცემთა სუბიექტმა ხელი მოაწერა ან რომელიც მან სხვაგვარად გამოხატა წერილობით (მათ შორის, ელექტრონულად) მის შესახებ მონაცემთა კონკრეტული მიზნით დამუშავებაზე შესაბამისი ინფორმაციის მიღების შემდეგ[19]. ამდენად, მე-11 მუხლის მიზნებისათვის, მონაცემთა სუბიექტის თანხმობა, აუცილებელია, აკმაყოფილებდეს ნებაყოფლობითობისა და ინფორმირებულობის კრიტერიუმებს, გამოხატული იყოს აქტიური მოქმედებით და მიემართებოდეს მონაცემთა დამუშავების კონკრეტულ მიზანს.

ამასთან, საყურადღებოა, რომ გარდა მე-11 მუხლის პირველი პუნქტით გათვალისიწინებული აუდიომონიტორინგის განხორციელების საფუძვლებისა, ყოველი კონკრეტული დამუშავების პროცესში, აუცილებელია, ზედმიწევნით იყოს დაცული კანონის მე-4 მუხლით გათვალისწინებული პრინციპები, რამდენადაც ერთ-ერთი მათგანის დარღვევაც კი, მონაცემთა დამუშავების პროცესს უკანონოდ აქცევს.

2.3. აუდიომონიტორინგის განხორციელების პროცესის მახასიათებლების წერილობით განსაზღვრის ვალდებულება

ვიდეომონიტორინგის მსგავსად, კანონის მე-11 მუხლის მე-2 პუნქტი აუდიომონიტორინგის განსახორციელებლადაც ადგენს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, კანონის მე-4 მუხლით გათვალისწინებული

[19] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-3 მუხლის „მ“ და „ნ“ ქვეპუნქტები.

პრინციპების შესაბამისად, წერილობით, წინასწარ განსაზღვროს აუდიომონიტორინგის მიზანი და მოცულობა, აუდიომონიტორინგის ხანგრძლივობა, აუდიოჩანაწერზე წვდომის, მისი შენახვისა და განადგურების წესი და პირობები, ასევე, მონაცემთა სუბიექტის უფლებების დაცვის მექანიზმები.

აუდიომონიტორინგის განხორციელების პროცესის მახასიათებლების წერილობით განსაზღვრის ვალდებულებასთან დაკავშირებული მოთხოვნა არსებითად იდენტურია ვიდეომონიტორინგთან დაკავშირებული შესაბამისი რეგულაციისა. ამდენად, შეიძლება ითქვას, რომ წინამდებარე რეკომენდაციების 1.3 ქვეთავში წარმოდგენილი მითითებები თანაბრად მიემართება აუდიომონიტორინგის განხორციელების პროცესის მახასიათებლების წერილობით განსაზღვრის ვალდებულების საკითხსაც.

2.4. აუდიომონიტორინგს დაქვემდებარებული მონაცემთა სუბიექტის ინფორმირებულობა

პერსონალურ მონაცემთა დაცვის სამართალში მონაცემთა დამუშავების თაობაზე სუბიექტის ინფორმირებულობა, როგორც არაერთგზის აღინიშნა, უმნიშვნელოვანესი და ერთ-ერთი ფუნდამენტური უფლებაა. ისევე, როგორც ვიდეომონიტორინგის შემთხვევაში, აუდიომონიტორინგის განხორციელების დროსაც, სავალდებულოა, რომ დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა მონაცემთა სუბიექტს მკაფიოდ და ნათლად განუმარტოს, რომ მიმდინარეობს აუდიოკონტროლი.

განსაკუთრებით მგრძნობიარე ხასიათისა და სპეციფიკიდან გამომდინარე, აუდიომონიტორინგის განხორციელებისას მონაცემთა სუბიექტის ინფორმირებასთან დაკავშირებით სპეციალური რეგულირება მოქმედებს. კერძოდ, კანონის მე-11 მუხლის მე-3 პუნქტის თანახმად, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ ან აუდიომონიტორინგის დაწყებისთანავე გააფრთხილოს მონაცემთა სუბიექტი აუდიომონიტორინგის განხორციელების შესახებ და განუმარტოს უარის თქმის თაობაზე მისი უფლება (ასეთის არსებობის შემთხვევაში). აუდიომონიტორინგის განხორციელების შესახებ ინფორმაციის მიწოდებისას, სუბიექტს ასევე უნდა ეცნობოს თუ კონკრეტულად რა მიზნით ხდება მონაცემთა დამუშავება, რაც სუბიექტის ინფორმირების მნიშვნელოვან ასპექტს წარმოადგენს.

მნიშვნელოვანია, რომ აუდიომონიტორინგის შესახებ გაფრთხილება მოხდეს წინასწარ. მაგალითად იმ შემთხვევაში თუკი აუდიოკონტროლი ხორციელდება საზოგადოებრივი თავშეყრის ადგილებში, აუცილებელია, რომ მონაცემთა

სუბიექტებს ჰქონდეთ აღნიშნული დამუშავების პროცესის შესახებ ინფორმაცია. ამასთან, პრაქტიკის მრავალფეროვნებიდან გამომდინარე, ხშირია შემთხვევა, როდესაც მონაცემთა სუბიექტების წინასწარი გაფრთხილება შეუძლებელია, მაგალითად, იმ შემთხვევაში თუკი ცხელი ხაზის ნომრებზე ზარის განხორციელების პროცესში მიმდინარეობს აუდიოჩაწერა, შეუძლებელია მონაცემთა სუბიექტის გაფრთხილება მოხდეს წინასწარ. სწორედ ამიტომ კანონი ქმნის ერთგვარ ალტერნატიულ შესაძლებლობას, კერძოდ დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს აქვს უფლება, მონაცემთა სუბიექტი აუდიომონიტორინგის შესახებ გააფრთხილოს უშუალოდ აუდიოჩაწერის დაწყებისთანავე. ამ კუთხით, მნიშვნელოვანია, რომ მონაცემთა სუბიექტის ინფორმირების უფლების რეალიზებისთვის, დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა ცხელი ხაზის ნომერზე მომხმარებლის მხრიდან ზარის განხორციელებისას ავტომოპასუხის ფუნქციის დაწყებისთანავე (სხვადასხვა ღილაკების მეშვეობით სხვადასხვა მომსახურების შეთავაზებამდე), ავტომატურ რეჟიმში გააფრთხილოს მონაცემთა სუბიექტი აუდიომონიტორინგის განხორციელების თაობაზე[20] და არ იყოს საჭირო შესაბამისი ინფორმაციის მისაღებად ავტომოპასუხის ბოლომდე მოსმენა. სწორედ აღნიშნული პრინციპი უნდა იქნეს გამოყენებული სხვა ყველა იმ შემთხვევაში, როდესაც სუბიექტის წინასწარი გაფრთხილება შეუძლებელია.

აქვე უნდა აღინიშნო, რომ მონაცემთა სუბიექტის ინფორმირების მტკიცების ტვირთი ეკისრება დამუშავებისთვის პასუხისმგებელ პირს/დამუშავებაზე უფლებამოსილ პირს. აქედან გამომდინარე, დავის არსებობის შემთხვევაში, სწორედ ხსენებული პირი იქნება ვალდებული, ამტკიცოს, რომ მონაცემთა სუბიექტი კანონმდებლობით გათვალისწინებული სტანდარტის შესაბამისად იყო ინფორმირებული აუდიომონიტორინგის განხორციელების შესახებ.

აუდიომონიტორინგის შესახებ მონაცემთა სუბიექტის წინასწარი ინფორმირებულობა ასევე მოიცავს დამუშავებისთვის პასუხისმგებელი პირის/დამუშავებაზე უფლებამოსილი პირის ვალდებულებას, განათავსოს შესაბამისი გამაფრთხილებელი ნიშნები. კერძოდ, თუკი აუდიომონიტორინგი, თავისი სპეციფიკიდან გამომდინარე, იძლევა შესაძლებლობას, რომ მონაცემთა სუბიექტების ინფორმირებულობა მოხდეს წინასწარ, დამუშავებისთვის პასუხისმგებელი პირი/დამუშავებაზე უფლებამოსილი პირი ვალდებულია, ვიდეომონიტორინგის მსგავსად, განათავსოს შესაბამისი გამაფრთხილებელი ნიშანი, რომელიც უნდა შეიცავდეს შესაბამის წარწერას, მარტივად აღქმად გამოსახულებას აუდიომონიტორინგის მიმდინარეობის შესახებ და

[20] იხ. პერსონალურ მონაცემთა დაცვის სამსახურის 2023 წლის 8 დეკემბრის გადაწყვეტილება №-1/297/2023, გვ 30.

დამუშავებისთვის პასუხისმგებელი პირის სახელწოდებასა და მის საკონტაქტო მონაცემებს[21].

3. მონაცემთა უსაფრთხოების დაცვის ტექნიკური და ორგანიზაციული ზომები

ვიდეომონიტორინგის და აუდიომონიტორინგის გზით მონაცემთა დამუშავებისას, მნიშვნელოვანია არა მხოლოდ შესაბამისი მიზნისა და საფუძვლების არსებობა, არამედ უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების უზრუნველყოფა, „რომელიც უნდა იყოს ადამიანის ძირითად უფლებათა და თავისუფლებათა შესაძლო შელახვის რისკების პროპორციული“[22]. შესაბამისად, „მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას, დამუშავებისთვის პასუხისმგებელი პირი და დამუშავებაზე უფლებამოსილი პირი ვალდებული არიან, გაითვალისწინონ დასამუშავებელ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები, აგრეთვე პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველსაყოფად მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დასაცავად ადეკვატური ზომების მიღება ან/და არსებულის განახლება“[23].

ამასთან, უსაფრთხოების ტექნიკური და ორგანიზაციული ზომები უნდა დაინერგოს ვიდეომონიტორინგის/აუდიომონიტორინგის დაწყებისთანავე და დაცულ უნდა იქნეს მონაცემთა დამუშავების სრული პროცესის განმავლობაში, რა დროსაც, ამგვარი ზომები უნდა უზრუნველყოფდეს ინფორმაციული უსაფრთხოების საერთაშორისოდ აღიარებულ პრინციპების დაცვას:

- **კონფიდენციალურობას** - მონაცემებზე წვდომა უნდა ჰქონდეს მხოლოდ ასეთი უფლების მქონე პირებს;
- **მთლიანობას** - მონაცემთა დაკარგვის, ან მათზე რაიმე მანიპულაციის პრევენციისთვის მიღებულ უნდა იქნეს შესაბამისი ზომები;
- **ხელმისაწვდომობას** - მონაცემებზე წვდომა უნდა ხდებოდეს მხოლოდ საჭიროების შემთხვევაში[24].

[21] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-4 პუნქტი.
[22] *European Data Protection Board (EDPB)*, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §123.
[23] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 27-ე მუხლის მე-3 პუნქტი.
[24] *European Data Protection Board (EDPB)*, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §132.

უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების განსაზღვრისას, დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა ყურადღება უნდა მიაქციოს ვიდეო თუ აუდიო ჩანაწერებზე წვდომის აღრიცხვის შესაძლებლობას. ამ კუთხით, ვიდეომონიტორინგის/აუდიომონიტორინგის განხორციელების პროცესში, უსაფრთხოების უზრუნველყოფის მნიშვნელოვან მექანიზმად შეიძლება ჩაითვალოს ე.წ. „ლოგირების“ სისტემა, რომელიც ვიდეო თუ აუდიო ჩანაწერებზე წვდომის თითოეული შემთხვევის აღრიცხვის, მათ შორის, წვდომის დროისა და მომხმარებლის სახელის აღრიცხვის შესაძლებლობას იძლევა[25].

ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა უნდა მიიღოს შესაბამისი ინფორმაციული უსაფრთხოების ზომები, რომელიც ინტერნეტიდან და კომპიუტერული ქსელიდან სისტემაში უკანონო შეღწევის თავიდან არიდებას უზრუნველყოფს.

დამატებით, უნდა განიმარტოს, რომ მონაცემთა უსაფრთხოება არ მიიღწევა მხოლოდ სწორი აღჭურვილობის, კერძოდ, ტექნოლოგიური და პროგრამული მხარდაჭერის დანერგვით. იგი, ასევე, მოითხოვს შესაბამისი შიდა ორგანიზაციული წესების დადგენას[26] და, მათ შორის, მონაცემთა ფიზიკური უსაფრთხოების უზრუნველყოფას. ამ კუთხით, მნიშვნელოვანია, დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა:

- დამუშავებულ მონაცემებზე წვდომა მიანიჭოს პირთა განსაზღვრულ წრეს, რა დროსაც, მხედველობაში უნდა იქნეს მიღებული თანამშრომელთა ფუნქციები და ჩანაწერებზე მათი წვდომის საჭიროება;
- უზრუნველყოს, რომ ვიდეომონიტორინგის/აუდიომონიტორინგის სიტემაზე დაშვება მოხდეს მხოლოდ უფლებამოსილი პირების განპიროვნებული მომხმარებლის სახელითა და ინდივიდუალური პაროლის გამოყენებით;
- ვიდეომონიტორინგის და აუდიომონიტორინგის სისტემები განათავსოს დაცულ ოთახში, სადაც დაიშვებიან მხოლოდ შესაბამისი უფლებამოსილების მქონე პირები;
- შეიმუშაოს შიდა დოკუმენტი, სადაც დეტალურად იქნება გაწერილი ვიდეომონიტორინგის/აუდიომონიტორინგის პროცესი და წესები, ასევე სისტემის ფუქნციონირების, მასზე წვდომის საკითხები და ა.შ.;
- პერიოდულად შეამოწმოს სისტემის ფუნქციონირება, წვდომის შემთხვევები და რეაგირება მოახდინოს არასანქცირებული წვდომის ან/და რაიმე სხვა დარღვევის ფაქტებზე.

[25] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-10 მუხლის მე-5 პუნქტი.

[26] მონაცემთა დაცვის ევროპული სამართალის სახელმძღვანელო (თარგმანი), გამომცემლობა „იურისტების სამყარო“, თბილისი, 2015, 121.

4. მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების საჭიროება

კანონის 31-ე მუხლი ითვალისწინებს დამუშავებისთვის პასუხისმგებელი პირის ვალდებულებას, წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე[27]. გარდა ამისა, მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელება სავალდებულოა, თუ დამუშავებისთვის პასუხისმგებელი პირი:

- მონაცემთა სუბიექტისთვის სამართლებრივი, ფინანსური ან სხვა სახის არსებითი მნიშვნელობის შედეგის მქონე გადაწყვეტილებას იღებს სრულად ავტომატიზებულად, მათ შორის, პროფაილინგის საფუძველზე;
- ამუშავებს დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემებს;
- ახორციელებს მონაცემთა სუბიექტების ქცევის სისტემატურ და მასშტაბურ მონიტორინგს საზოგადოებრივი თავშეყრის ადგილებში[28].

დამატებით, აღსანიშნავია, რომ „მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულების წარმომშობი გარემოებების დადგენის კრიტერიუმებისა და შეფასების წესი“ დამტკიცებულია პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის შესაბამისი ბრძანებით, რომელიც დეტალურად აწესრიგებს ხსენებულ საკითხებს.

საყურადღებოა, რომ ვიდეომონიტორინგის განხორციელების სტანდარტული მიზნების გათვალისწინებით (დანაშაულის თავიდან აცილება, მისი გამოვლენა, საზოგადოებრივი უსაფრთხოება, პირის უსაფრთხოება და საკუთრების დაცვა, არასრულწლოვანის დაცვის (მათ შორის, მავნე ზეგავლენისგან დაცვის), საიდუმლო ინფორმაციის დაცვა და სხვა), სავარაუდოა, რომ მისი არაერთი პროცესი დაექვემდებარება მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულებას[29]. აქედან გამომდინარე, ვიდეომონიტორინგის განმახორციელებელ დამუშავებისთვის პასუხისმგებელ პირებს მართებთ, სათანადოდ შეაფასონ მონაცემთა დამუშავების პროცესის შესაძლო გავლენა ადამიანის ძირითად უფლებებსა და თავისუფლებებზე

[27] იხ. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის 31-ე მუხლის პირველი პუნქტი.
[28] იქვე, 31-ე მუხლის მე-2 პუნქტი.
[29] *European Data Protection Board (EDPB)*, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §137.

და საჭიროების შემთხვევაში, განახორციელონ მონაცემთა დაცვაზე ზეგავლენის შეფასება.

მაგალითად, მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება შესაძლოა არსებობდეს მაშინ, როდესაც, გამოიყენება ე.წ. „ჭკვიანი კამერა“ საგზაო მოძრაობის უსაფრთხოების უზრუნველსაყოფად, რა დროსაც, ხორციელდება მძღოლების ქცევის სისტემატური და მასშტაბური მონიტორინგი[30].

დამატებით, აღსანიშნავია, რომ შინაარსით, მასშტაბითა და კონტექსტით ერთმანეთთან დაკავშირებული მონაცემთა დამუშავების რამდენიმე პროცესის მიმართ შეიძლება მომზადდეს ერთი ზეგავლენის შეფასების დოკუმენტი. მაგალითად, რამდენიმე მუნიციპალურ ორგანოს, რომელიც ერთი და იმავე მიზნით ამონტაჟებს ერთი და იმავე ვიდეომონიტორინგის სიტემას, ზეგავლენის შეფასების ცალ-ცალკე განხორციელების ნაცვლად, შეუძლია მოამზადოს ზეგავლენის შეფასების ერთიანი დოკუმენტი, რომელიც სხვადასხვა დამუშავებისთვის პასუხისმგებელი პირის მიერ დაგეგმილ მსგავს მონაცემთა დამუშავების პროცეს ერთობლივად შეაფასებს. იგივე შეიძლება ითქვას, მაგ., რკინიგზის სისტემის ოპერატორზე, რომელსაც შეუძლია რკინიგზის ყველა სადგურზე განხორციელებული ვიდეომონიტორინგის პროცესი მოაქციოს მონაცემთა დაცვაზე ზეგავლენის შეფასების ერთიან დოკუმენტში და სხვა[31].

აღსანიშნავია, რომ აუდიომონიტორინგს დაქვემდებარებული მონაცემთა სუბიექტებისა და დამუშავებული მონაცემების კატეგორიების სიმრავლის, ასევე, მათი რაოდენობრივი მასშტაბის გათვალისწინებით, შესაძლოა, იქმნებოდეს დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების ვალდებულება, რაც აუდიომონიტორინგის სისტემის დანერგვამდე, ყოველ კონკრეტულ შემთხვევაში დამოუკიდებლად უნდა შეფასდეს.

მონაცემთა დაცვაზე ზეგავლენის შეფასების განხორციელების ვალდებულებასთან დაკავშირებით, საყურადღებოა, რომ კანონის 90-ე მუხლის მე-3 პუნქტი კანონის 31-ე მუხლის ამოქმედების თარიღად 2024 წლის 1 ივნისს განსაზღვრავს.

[30] *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP248 rev.01, Adopted on 4 April 2017, 11.

[31] იქვე, 7.

ნატო ვაჩნაძის ქუჩა N° 7, თბილისი

ბაქოს ქუჩა N° 48, ბათუმი

(+995 32) 242 1000

office@pdps.ge