ჭკვიანი კამერების სისტემაში პერსონალურ მონაცემთა დაცვის მონიტორინგი

ანგარიში

ანგარიში შექმნილია ნიდერლანდების საელჩოს მხარდაჭერილი პროექტის ფარგლებში. მის შინაარსზე სრულად პასუხისმგებელია „ინოვაციებისა და რეფორმების ცენტრის“ მკვლევართა ჯგუფი და არ ნიშნავს რომ იგი ასახავს ნიდერლანდების საელჩოს შეხედულებებს.

2020

შესავალი

დღეისათვის ფიზიკურ პირთა პერსონალური მონაცემების მოუწესრიგებელი და უკონტროლო დამუშავებდან მომდინარე საფრთხეების მნიშვნლეობა სცდება ადამიანისთვის მიყენებულ ფსიქოლოგიურ ტკივილსა და დისკომფორტს, რაც შეიძლება გამოიწვიოს ცალკეული პირადი მონაცემების გამჟღავნებამ. პერსონალურ მონაცემთა გადაჭარბებული და უკონტროლო დამუშავება ადამიანის სხვა უფლებებისა და თავისუფლებების შეზღუდვის არსებით რისკებს შეიცავს, რაც დაკავშირებულია ადმიანის ქცევის პროგნოზირებასა და მასზე მანიპულაციის შესაძლებლობასთან, ეს კი თავის მხრივ ასევე საფრთხეს უქმნის თანამედროვე დემოკრატიული წესრიგის არსებობას.

უკანასკნელი ორი ათწლეულის განმავლობაში, ციფრული ტექნოლოგიების განვითარების კვალდაკვალ, სულ უფრო მეტ მნიშვნელობას იძენს ადამიანების და მათი ქცევის შესახებ მონაცემების შეგროვება და დამუშავება. ადამიანის ქცევის შესახებ მონაცემთა ანალიზისა და შესაბამისი პროფილირების საფუძველზე მრავალი მმართველობითი თუ ბიზნეს ამოცანის გადაწყვეტა შეიძლება, თუმცა ამავე დროს იქმნება მომეტებული რისკები ადმიანის პირად ცხოვრებაში და თავისუფლებაში გაუმართლებელი ჩარევისთვის.

შესაბამისად, პერსონალურ მონაცემთა დაცვას, როგორც ადამიანის ერთ-ერთ ფუნდამენტურ უფლებას მზარდი მნიშვნელობა ენიჭება და დემოკრატიული სახელმწიფოები ახლებურ მიდგომებსა და სამართლებრივ მექანიზმებს ავითარებენ მზარდ გამოწვევებზე საპასუხოდ. თანამედროვე სამყაროში არსებულ გამოწვევებთან გასამკლავებლად აღარ არის საკმარისი საკანონმდებლო დონეზე მხოლოდ მონაცემთა დაცვის პრინციპების განსაზღრა და მონაცემთა დაცვის ადეკვატური დონის მისაღწევად სახელმწიფოები უფრო დეტალური, კომპლექსური რეგულაციების შექმნაზე არიან ორინტირებულნი, რომელიც სამართლებრივი პრინციპების და კონცეფციების განსაზღვრასთან ერთად ორგანიზაციული და ტექნოლოგიური გადაწყვეტების სავალდებულოობასაც გულისხმობს.

საქართველოში მრავალი საჯარო თუ კერძო დაწესებულებისთვის პერსონალურ მონაცემთა დაცვის საკითხი ჯერ კიდევ „სიახლედ“ ითვლება, მიუხედავად იმისა, რომ შესაბამისი კანონის ძალაში შესვლიდან 8 წელზე მატი გავიდა. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი 2012 წლიდან მოქმედებს, თუმცა ამ დროის მანძილზეც საკითხის ცნობადობა და მისი მნიშვნელობის აღქმა მონაცემთა დამმუშავებელთა უმრავლესობისთვის ვერ გასცდა ზოგად შემეცნებით დონეს. საქართველოში ის საჯარო დაწესებულებებიც კი, რომლებიც შეიძლება „სანიმუშოდ“ ითვლებიან მონაცემთა დაცვის სფეროში, ხშირად შორს არიან მონაცემთა დაცვის მაღალი სტანდარტისგან და მხოლოდ კანონის მოთხოვნების ფორმალური დაცვით და ზედაპირზე არსებული პრობლემების მოგვარებით შემოიფარგლებიან.

საქართველოში პერსონალურ მონაცემთა დაცვის საკითხს ზედამხედველობას უწევს დამოუკიდებელი საზედამხედველო ორგანო - სახელმწიფო ინსპექტორის სამსახური. იმის გათვალისწინებით, რომ ინსპექტორის სამსახურის რესურსები შეზღუდულია და ამ შეზღუდული რესურსების მნიშვნელოვანი ნაწილი მიემართება საკითხის ცნობადობის ამაღლებისთვის მიძღვნილ ღონისძიებებზე თუ კონკრეტულ განცხადებება-საჩივრებზე რეაგირებაზე, ზოგჯერ ფოკუსს მიღმა რჩება რიგი კომპლექსური და კრიტიკული საკითხები.

არსებული რეალობისა და იმის გათვალისწინებით, რომ ჩვენს რეალობაში პერსონალურ მონაცემთა დაცვის თემაზე თითქმის არ ისმის ალტერნატიული შეფასებები და საექსპერტო მოსაზრებები, სამოქალაქო მონიტორინგის გზით და შესაბამისი ანგარიშებით გვსურს გამოვკვეთოთ რეალურად არსებული პრობლემური არეები და საზოგადოების ყურადღება მივაპყროთ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებაში ჩარევის თვალსაზრისით მაღალი რისკების შემცველ სისტემებზე, რომლებიც კომპლექსურ მიდგომასა და მოწესრიგებას საჭიროებს.

1. კონტექსტი

როგორც ადგილობრივი ისე საერთაშირისო კონტექსტის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის საკითხი სულ უფრო აქტუალური ხდება საქართველოშიც, მითუმეტეს, რომ ქვეყანას აღებული აქვს საერთაშორისო ვალდებულებები პერსონალურ მონაცემთა დაცვის საკითხის ევროპული სტადარტების შესაბამისად მოწესრიგებაზე. 2016 წლამდე პერსონალურ მონაცემთა დაცვის საკითხი საქართველოს მთვარობისთვის აქტუალური იყო, ევროკავშირთან სავიზო რეჟიმის ლიბერალიზაციისა და ასოცირების ხელშეკრულების კონტექსტში - საქართველოს მთვარობას ნაკისრი ჰქონდა ვალდებულება გაეუმჯობესებინა პერსონალურ მონაცემთა დაცვის კანონმდებლობა და პრატქიკა. ასევე, აღსანიშნავია, რომ საქართველო მიერთებულია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ 108-ე კონვენციას და მის დამატებით ოქმს.

ბოლო წლების განმავლობაში საქართველოში, როგორ სახელმწიფო, ასევე კერძო სექტორში იდგმება ცალკეული ნაბიჯები პერსონალურ მონაცემთა დაცვის საკითხის მოწესრიგებისკენ. თუმცა მიგვაჩნია, რომ გატარებული ღონისძიებები არ არის საკმარისი და არსებული გამოწვევების ადეკვატური. როგორც უკვე აღინიშნა, პერსონალურ მონაცემთა დაცვის საკითხის საკანონმდებლო მოწესრიგებას საქართველოში მხოლოდ 8-9 წლიანი ისტორია აქვს. საჯარო თუ კერძო სექტორში კი მრავალი მიმართულებით რეფორმები ისე გატარდა და მონაცემთა დამუშავების სისტემები ისე განვითარდა რომ პერსონალურ მონაცემთა დაცვის საკითხი საერთოდ არ იყო მხედველობაში მიღებული ან ნაკლები ყურადღება ეთმობოდა. აღნიშნული პრაქტიკა ნაწილობრივ დღემდე გრძელდება, რის შედეგადაც სახეზე გვაქვს

მრავალი საინფორმაციო სისტემა და ინსტრუმენტი, რომელიც დიდი მოცულობით პერსონალურ მონაცემებს ამუშავებს, თუმცა შეუსაბამოა მოქმედ კანონმდებლობასთან, მათი ადაპტირება კი დიდ დანახარჯებთანაა დაკავშირებული, რომლის გაღების საკმარისი მოტივაცია მონაცემთა დამმუშვებელ ორგანიზაციებს არ აქვთ. ამას ნაწილობრივ ისიც განაპირობებს, რომ საქართველოს კანონმდებლობით გათვალისწინებულია ჯარიმების არაადეკვატურად მცირე ოდენობა.

კანონის შემოღებიდან მეცხრე და ინსპექტორის აპარატის დაარსებიდან მეშვიდე წელს პრაქტიკაში ჯერ კიდევ ვხვდებით მონაცემთა დაცვის ძირეული ასპექტების არასწორ გაგებას თუ იგნორირებას. მონაცემთა მსხვილ დამმუშავებელთა ნაწილს, როგორებიცაა მსხვილი ბანკები, სახელმწიფო დასაწესებულებები, სადაზღვევო თუ სატელეკომუნიკაციო კომპანიები და ა.შ. ამდენი ხნის მანძილზე ჯერ კიდევ არ მოუხდენიათ თავიანთი სისტემების ინვენტარიზაცია და რევიზია მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის დადგენის მიზნი. მეტიც, გასულ წელს ისე დაინერგა ჯანდაცვის ელექტრონული ჩანაწერების (ehr) სისტემა, რომ მონაცემთა დაცვაზე გავლენის სიღრმისეული წინასწარი ანალიზი არ მომხდარა და არ იძებნება ინფორმაცია ამ სისტემაში მონაცემთა დაცვის უზრუნველსაყოფად გატარებული ღონისძიებების - მიღებული ორგანიზაციულ-ტექნიკური ზომების შესახებ.

ასეთ გარემოში უაღრესად მნიშვნელოვანად მიგვაჩია სამოქალაქო საზოგადოების და დამოუკიდებელი ექსპერტების/აქტივისტების როლი, რომლებიც გარედან, ობიექტური დამკვირვებლის თვალით აფასებენ პერსონალური მონაცემების დაცვის თვალსაზრისით ქვეყანაში არსებულ გარემოს და შესაბამისი ცოდნის და გამოცდილების გაზიარებით ხელს უწყობენ სფეროს შემდგომ განვითარებას.

2. კვლევის ამოცანები

ინოვაციებისა და რეფორმების ცენტრმა შეარჩია ისეთი სისტემები, რომლებიც დამუშავებული მონაცემების კატეგორიის, მონაცემთა სუბიექტების სიმრავლისა და ასევე დამუშავების პროცესში გამოყენებული ტექნიკური საშუალებებისა და მათი შესაძლებლობების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის თვალსაზრისით მაღალი რისკის მატარებელს წარმოადგენს.

მნიშვნელოვანია, მსგავს სისტემებში პერსონალურ მონაცემთა დამუშავების საკითხის დეტალური სამართლებრივი რეგლამენტაცია, მონიტორინგის ეფექტიანი და ქმედითი მექანიზმების არსებობა და სისტემის მაქსიმალური გამჭვირვალობა.

იმისათვის, რომ მსგავს მაღალი რისკის შემცველ სისტემებში მინიმუმამდე იქნას დაყვანილი პერსონალურ მონაცემთა უკანონო დამუშავების და მათი არადანიშნულებისამებრ გამოყენების რისკები, აუცილებელია, გატარებული იქნას სამართლებრივი, ორგანიზაციული და ტექნიკური ღონისძიებების ერთობლიობა.

ამგვარი ღონისძიებები შეიძლება იყოს, მათ შორის მონაცემთა დამუშავების საკითხის დეტალური რეგლამენტაცია და გამჭვირვალობის მაღალი ხარისხის უზრუნველყოფა, მონაცემთა დამუშავების პროცესების დოკუმენტირება, ჩანაწერების შენახვის ვადების განსაზღვრა, მონაცემებზე წვდომის კონტროლი, სისტემის დანერგვისას ისეთი პრინციპების უზრუნველყოფა, როგორიცაა მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“), მონაცემთა დამუშავების ზეგავლენის შეფასება (DPIA) და ა.შ.

კვლევის ამოცანას წარმოადგენდა იმის დადგენა, თუ რამდენად არის უზრუნველყოფილი პერსონალურ მონაცემთა დაცვა შერჩეულ სისტემებში და რამდენად სერიოზულად ეკიდებიან საჯარო უწყებები მონაცემთა დაცვის საკითხს მონაცემთა დამუშავების მასშტაბურ, რისკების შემცველ სისტემაში და გატარებულია თუ არა შესაბამისი ორგანიზაციული და ტექნიკური ზომები. უფრო კონკრეტულად კი გვინდოდა პასუხი გაგვეცა შემდეგ კითხვებზე:

- განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების კონკრეტული მიზნები, შესაბამისად, განჭვრეტადია თუ არა მონაცემთა დამუშავების პროცესი მონაცემთა სუბიექტისთვის;
- შეფასებულია თუ არა სისტემაში მონაცემთა დამუშავების ზეგავლენა ან ჩატარდა თუ არა სხვა ტიპის ანალიზი იმის დასადგენად, თუ რა გავლენა აქვს აღნიშნულ სისტემას ფიზიკურ პირთა პერსონალურ მონაცემთა დაცვაზე, რა რისკებს შეიცავს და რამდენად შესაბამისობაშია მოქმედ კანონმდებლობასთან;
- განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების საფუძვლები და ვადები, დაცულია თუ არა მონაცემთა დამუშავების პრინციპები;
- ნათელი და ხელმისაწვდომია თუ არა ინფორმაცია მონაცემთა სუბიექტისათვის, რა მონაცემები შეიძლება დამუშავდეს მის შესახებ ამ სისტემის მეშვეობით;
- რეგულირებულია თუ არა სისტემაში დამუშავებულ მონაცემებზე წვდომის წესები და დონეები;
- რეგულირებული და განჭვრეტადია თუ არა მონაცემთა სუბიექტისთვის სისტემიდან მონაცემების მესამე პირებისათვის გადაცემის საკითხი;
- აქვს თუ არა მონაცემთა დამმუშვებელს მიღებული ადეკვატური ორგანიზაციული და ტექნიკური ზომები სისტემაში მონაცემთა უსაფრთხოების უზრუნველსაყოფად;

კვლევითი ამოცანების შესაბამისად, ინოვაციებისა და რეფორმების ცენტრმა შეიმუშავა კითხვარი და შერჩეული უწყებებიდან გამოითხოვა.

ასევე დამუშავებული იქნა უკვე გამოქვეყნებული/ხელმისაწვდომი ინფორმაცია ნორმატიული აქტებისა და სხვა ინფორმაციის სახით, მათ შორის პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილებები.

3. ძირითადი მიგნებები

შერჩეული სისტემების მონიტორინგის საფუძველზე რამდენიმე ზოგადი მახასიათებელი გამოიკვეთა. პირველ რიგში, უნდა ითქვას, რომ პერსონალურ მონაცემთა დაცვის მნიშვნელობა მონაცემთა მსხვილი დამმუშავებლების მიერ არასათანადოდაა შეფასებული და გათვალისწინებული. შეფასებული უწყებებისთვის არ ჩანს პერსონალურ მონაცემთა დაცვის საკითხის პრიორიტეტულობა და მისი გათვალისწინება ყოველდღიურ საქმიანობაში, ათასობით მოქალაქის პერსონალურ მონაცემებთან ურთიერთობისას.

მონაცემთა დაცვის საკითხისადმი სისტემური მიდგომა არ არსებობს ისეთ მნიშვნელოვან და მსხვილ დამმუშავებლებშიც, როგორიცაა მაგ. შინაგან საქმეთა სამინისტრო, საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო.

გასათვალისწინებელია, რომ არცერთი შემოწმებული სისტემისათვის, მათ შორის, ისეთი სენსიტიური სისტემებისთვისაც კი, როგორიცაა ჯანმრთელობის შესახებ ჩანაწერების ელექტრონული სისტემა, ჭკვიანი კამერების სისტემა, მშვილებელთა რეესტრი და ა.შ, არ არის შეფასებული მონაცემთა დამუშავების ზეგავლენა და მონაცემთა დამუშავებასთან დაკავშირებული შესაბამისი რისკები.

მონიტორინგის ფარგლებში არცერთ უწყებაში არ აღმოჩნდა მონაცემთა დამუშავების წესების მარეგულირებელი ისეთი დოკუმენტაცია, რომელიც კონკრეტულად უწყებისა თუ სისტემის გათვალისწინებით მოაწესრიგებდა მონაცემთა დამუშავების სპეციფიკურ საკითხებს.

რიგ შემთხვევებში არ არის იდენტიფიცირებული და რეგლამენტირებული მონაცემთა დამუშავების მიზნები და საფუძვლები.

უმეტეს შემთხვევაში პრობლემურია მონაცემთა სუბიექტის უფლების რეალიზების მექანიზმები, რაც გამოიხატება არა იმდენად კონკრეტულ ფაქტებში, როდესაც სუბიექტს შეეზღუდა მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებები, არამედ სისტემურ სურათში, როდესაც ეფექტიანი მექანიზმების არარსებობა, მონაცემთა წვდომების

არასათანადო აღრიცხვა და ა.შ. ქმნის საფრთხეს მონაცემთა სუბიექტის მოთხოვნა ვერ დაკმაყოფილდეს ან მხოლოდ ნაწილობრივ დაკმაყოფილდეს.

პრობლემურია მონაცემთა შენახვის ვადებთან დაკავშირებული საკითხი, რადგან უმეტესი მონაცემებისა და სისტემებისათვის არ არის განსაზღვრული კონკრეტული, კანონიერ მიზანთან შესაბამისი ვადები. ასევე, არ არსებობს მონაცემთა განდაგურებისა თუ დაარქივების სათანადო წესები.

მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული მონაცემთა უსაფრთხოების უზრუნველსაყოფად მისაღები ორგანიზაციული და ტექნიკური ზომები უწყებების მიერ ძალიან ფრაგმენტულად არის მიღებული. ზოგიერთ უწყებაში გათვალისწინებულია მონაცემთა ბაზებზე წვდომის ავტორიზაცია, ზოგიერთი დამმუშავებელი ახდენს მონაცემთა მიმართ შესრულებული ქმედებების ლოგირებას და ა.შ, თუმცა არცერთ უწყებაში არ აქვს ადგილი სიტუაციის დეტალურ ანალიზს, სათანადო შეფასებას და დამუშავებული მონაცემების ადეკვატური ზომების მიღებას.

4. ჭკვიანი კამერების სისტემა

4.1 სისტემის აღწერა

2019 წლიდან საქართველოში მთელი ქვეყნის მასშტაბით დაიწყო ე.წ. ჭკვიანი კამერების დაყენება. 2019 წლის ნოემბრის მდგომარეობით უკვე 4 318 ე.წ. ჭკვიანი კამერა[1] განთავსდა როგორც დედაქალაქსა და დიდ ქალაქებში, ასევე ცენტრალურ მაგისტრალებსა და საავტომობილო გზებზე. Avigilon ბრენდის (სავარაუდოდ 2.0C-H4A-B3 მოდელის) კამერები დღე-ღამის ნებისმიერ მონაკვეთში მაღალი გარჩევადობის მქონე ქსელური ტიპის ვიდეოსამეთვალყურეო კამერებია. ზოგადი ხედვის კამერებისაგან განსხვავებით, ჭკვიანი კამერების საშუალებით ადმინისტრაციული სამართალდარღვევის დაფიქსირება ხდება ავტომატური ფიქსაციის გზით, კერძოდ, ვიდეო ანალიტიკური პროგრამა ავტომატურად ახდენს ჩადენილი სამართალდარღვევის ფაქტებისა და ავტომანქანის სანომრე ნიშნის დაფიქსირებას.[2] მიუხედავად იმისა, რომ სტანდარტულ, ზოგადი ხედვის კამერების სისტემას საქართველოს შინაგან საქმეთა სამინისტრო მანამდეც იყენებდა, ე.წ „ჭკვიანი კამერების“ სისტემა გაცილებით ფართომასშტაბიანია და არსებითად განსხვავებულ რეალობასა და გამოწვევებს ქმნის პერსონალურ მონაცემთა დაცვის თვალსაზრისით.

ე.წ „ჭკვიანი კამერა“ აღჭურვილია ისეთი ფუნქციებით, როგორიცაა სატრანსპორტო საშუალების ნომრის ამოცნობა, საგზაო მოძრაობის წესების დარღვევების ამოცნობა და როგორც ადამიანის ქცევის, ისე სხვა სახის მოძრაობის - აქტიური თუ პასიური ქმედების დეტექციის ფუნქცია. ინტეგრირებული ანალიტიკის საშუალებით მას შეუძლია მოძრავი ობიექტის დადგენა, მის ავტომობილად და ადამიანად კლასიფიკაცია და შესაბამისი განგაშის სიგნალის აქტივირება. კამერები საქართველოს შინაგან საქმეთა სამინისტროს სტრუქტურული ქვედანაყოფის ერთობლივი ოპერაციების ცენტრის (შემდგომში - ცენტრი) ტერიტორიაზე განთავსებულ ცენტრალურ ვიდეო სერვერებთან დაკავშირებულია ფიზიკურად გამოყოფილი ოპტიკურ-ბოჭკოვანი არხების საშუალებით, რომლებსაც არ გააჩნიათ წვდომა ინტერნეტთან. ცენტრალურ სერვერებთან დაკავშირების მიზნით გამოყენებული ქსელური კავშირისა და უსაფრთხოების აპარატურის ტექნიკურ მომსახურებას უზრუნველყოფს სსიპ ოპერატიულ-ტექნიკური სააგენტო (შემდგომში - სააგენტო), ხოლო ცენტრალური ვიდეო სერვერები, რომელზეც ინახება ჭკვიანი კამერების საშუალებით მოპოვებული უწყვეტი ვიდეოჩანაწერები, განთავსებულია ცენტრის ტერიტორიაზე და მათ ტექნიკურ მხარდაჭერას ახორციელებს ცენტრი.

---

[1] https://police.ge/ge/shinagan-saqmeta-saministrom-sagzao-usafrtkhoebis-kampaniis-akhali-etapi-daitsko/13112

[2] სისტემის აღწერა მოცემულია საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილების მიხედვით

პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ 2019 წლის 20 თებერვლიდან ამავე წლის 20 მაისის ჩათვლით განხორციელებული ინსპექტირების შედეგად დგინდება, რომ ჭკვიანი კამერების ფუნქციონირება ხორციელდება სახელმწიფო სანომრე ნიშნის ამომცნობი ვიდეო ანალიტიკური პროგრამის - ISS Secur OS (შემდგომში - ვიდეო ანალიტიკური პროგრამა) მეშვეობით. ჭკვიანი კამერების საშუალებით ვიდეო ანალიტიკური პროგრამის მიერ ავტომატურად ხორციელდება ავტოსატრანსპორტო საშუალებების მიერ ჩადენილი შემდეგი ადმინისტრაციული სამართალდარღვევის ფაქტების დაფიქსირება: 1. მოძრაობის დადგენილი სიჩქარის გადაჭარბება, 2. საგზაო მონიშვნის მოთხოვნათა უგულებელყოფა, 3. იმ ავტოსატრანსპორტო საშუალების მართვა, რომელსაც დადგენილი წესით არ გაუვლია პერიოდული ტექნიკური ინსპექტირება, 4. შუქნიშნის ამკრძალავ წითელ ფერზე გავლის წესების დარღვევა.

აღნიშნული კამერები მუშაობენ მანქანური სწავლების მექანიზმზე ანუ კამერის ხელოვნურ ინტელექტს აქვს დასწავლილი ქმედების აღქმისა და იდენტიფიცირების უნარი. ის, თუ რა ქმედებასა და ქცევით მახასიათებელს „ასწავლის“ სისტემას, ანუ რისი ამოცნობისა და რაზე რეაგირების ფუნქცია ექმნება მას, სრულადაა დამოკიდებული სისტემის მაკონტროლებელზე (მფლობელზე).

კვლევის ფარგლებში ინოვაციებისა და რეფორმების ცენტრმა ვერ მოიპოვა დამატებითი ინფორმაცია, გარდა ზემოთ აღნიშნული 4 ფუნქციისა, კიდევ რა ტიპის ქცევას აღიქვამს აღნიშნული სისტემა და რას მიიჩნევს სავარაუდო გადაცდომად.

ჭკვიანი კამერების სისტემის სამართლებრივ საფუძვლებს ქმნის რამდენიმე სამართლებრივი აქტი:

- საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსი;
- საქართველოს კანონი „პოლიციის შესახებ“;
- საქართველოს შინაგან საქმეთა სამინისტროს ფაილური სისტემებისა და მათში არსებული მონაცემების შენახვის ვადების განსაზღვრის შესახებ საქართველოს შინაგან საქმეთა მინისტრის 2015 წლის 23 იანვრის N53 ბრძანება;
- საქართველოს შინაგან საქმეთა მინისტრის 2016 წლის 3 ოქტომბრის N558 ბრძანებით დამტკიცებული საქართველოს შინაგან საქმეთა სამინისტროს ერთობლივი ოპერაციების ცენტრის (დეპარტამენტი) დებულება;

და მის დეკლარირებულ მიზანს წარმოადგენს დანაშაულის პრევენცია, მასზე ეფექტიანი რეაგირება და გამოძიების ხარისხის გაუმჯობესება, საგზაო მოძრაობის უსაფრთხოების

უზრუნველყოფა და ადმინისტრირების გაუმჯობესება, საგანგებო სიტუაციების ეფექტიანი მართვა და პოლიციის ტექნოლოგიური რეფორმა.[3]

4.2 კვლევის ამოცანები

ჭკვიანი კამერების სისტემისთვის მონაცემთა სუბიექტს პოტენციურად წარმოადგენს საქართველოს ტერიტორიაზე მყოფი ნებისმიერი პირი, რომელიც ექცევა კამერების ხედვის არეალში, მიუხედავად იმისა ფლობს თუ არა ის ავტოსატრანსპორტო საშუალებას.

აღნიშნული სისტემა, მასში დამუშავებული მონაცემების კატეგორიის, მონაცემთა სუბიექტების სიმრავლისა და ასევე დამუშავების პროცესში გამოყენებული ტექნიკური საშუალებებისა და მათი შესაძლებლობების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის თვალსაზრისით წარმოადგენს მაღალი რისკის სისტემას.

სისტემის ზემოთ ჩამოთვლილი ტექნიკური/ფუნქციონალური მახასიათებლები ადამიანის იდენტიფიცირების, მასზე დაკვირვების და მისი ქცევის ანალიზის საშუალებას იძლევა, რაც შეიძლება მოძრაობის წესების დაცვისა და დანაშაულის პრევენციის მიზნების გარდა, გამოყენებული იქნას ადამიანების მიმართ თვალთვალის განხორციელების მიზნებითაც.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, მნიშვნელოვანია, მსგავს სისტემებში პერსონალურ მონაცემთა დამუშავების საკითხის დეტალური სამართლებრივი რეგლამენტაცია, მონიტორინგის ეფექტიანი და ქმედითი მექანიზმების არსებობა და სისტემის მაქსიმალური გამჭვირვალობა, მითუმეტეს იმ რეალობაში, სადაც სამართალდამცავი სისტემისადმი საზოგადოების ნდობა ჯერ კიდევ გამოწვევად რჩება.

იმისათვის, რომ მსგავს სისტემებში მინიმუმამდე იქნას დაყვანილი პერსონალურ მონაცემთა უკანონო დამუშავების და მათი არადანიშნულებისამებრ გამოყენების რისკები, აუცილებელია, გატარებული იქნას სამართლებრივი, ორგანიზაციული და ტექნიკური ღონისძიებების ერთობლიობა.

ამგვარი ღონისძიებები შეიძლება იყოს, მათშორის მონაცემთა დამუშავების საკითხის დეტალური რეგლამენტაცია და გამჭვირვალობის მაღალი ხარისხის უზრუნველყოფა, მონაცემთა დამუშავების პროცესების დოკუმენტირება, ჩანაწერების შენახვის ვადების განსაზღვრა, მონაცემებზე წვდომის კონტროლი, სისტემის დანერგვისას ისეთი პრინციპების უზრუნველყოფა, როგორიცაა მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი

[3] საქართველოს შინაგან საქმეთა მინისტრის 2017 წლის პირველი მაისის N233 ბრძანებით დამტკიცებული საქართველოს შინაგან საქმეთა სამინისტროს პროექტი „უსაფრთხო ქალაქი, უსაფრთხო რეგიონი, უსაფრთხო ქვეყანა“

პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“), მონაცემთა დამუშავების ზეგავლენის შეფასება (DPIA) და ა.შ.

კვლევის ამოცანას წარმოადგენდა იმის დადგენა, თუ რამდენად არის უზრუნველყოფილი პერსონალურ მონაცემთა დაცვა ჭკვიანი კამერების სისტემაში - რამდენად სერიოზულად და გულისხმიერად ეკიდება შინაგან საქმეთა სამინისტრო პერსონალურ მონაცემთა დაცვის საკითხს მონაცემთა დამუშავების ასეთი მასშტაბურ, რისკების შემცველ სისტემაში და გატარებულია თუ არა შესაბამისი ორგანიზაციული და ტექნიკური ზომები. უფრო კონკრეტულად კი გვინდოდა პასუხი გაგვეცა შემდეგ კითხვებზე:

განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების კონკრეტული მიზნები, შესაბამისად, განჭვრეტადია თუ არა მონაცემთა დამუშავების პროცესი მონაცემთა სუბიექტისთვის;

რა ტექნიკური შესაძლებლობები აქვს სისტემას, ამ ეტაპზე რა ფუნქციებია გააქტიურებული და კონკრეტულად რა მონაცემთა დამუშავება ხდება;

შეფასებულია თუ არა სისტემაში მონაცემთა დამუშავების ზეგავლენა ან ჩატარდა თუ არა სხვა ტიპის ანალიზი იმის დასადგენად, თუ რა გავლენა აქვს აღნიშნულ სისტემას ფიზიკურ პირთა პერსონალურ მონაცემთა დაცვაზე, რა რისკებს შეიცავს და რამდენად შესაბამისობაშია მოქმედ კანონმდებლობასთან;

განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების საფუძვლები და ვადები, დაცულია თუ არა მონაცემთა დამუშავების პრინციპები;

ნათელი და ხელმისაწვდომია თუ არა ინფორმაცია მონაცემთა სუბიექტისათვის, რა მონაცემები შეიძლება დამუშავდეს მის შესახებ ამ სისტემის მეშვეობით;

რეგულირებულია თუ არა სისტემაში დამუშავებულ მონაცემებზე წვდომის წესები და დონეები;

რეგულირებული და განჭვრეტადია თუ არა მონაცემთა სუბიექტისთვის სისტემიდან მონაცემების მესამე პირებისათვის გადაცემის საკითხი, მაგ. სისტემაში დამუშავებულ მონაცემთა გამოყენება სხვა სახელმწიფო ორგანოების მიერ ან სხვა მიზნებით, გარდა ადმინისტრაციული სამართალდარღვევის აღმოფხვრისა;

აქვს თუ არა სამინისტროს მიღებული ადეკვატური ორგანიზაციული და ტექნიკური ზომები სისტემაში მონაცემთა უსაფრთხოების უზრუნველსაყოფად;

კვლევითი ამოცანების შესაბამისად, ინოვაციებისა და რეფორმების ცენტრმა შეიმუშავა კითხვარი და საქართველოს შინაგან საქმეთა სამინისტროსგან გამოითხოვა საჯარო ინფორმაცია.

ასევე დამუშავებული იქნა უკვე გამოქვეყნებული/ხელმისაწვდომი ინფორმაცია ნორმატიული აქტებისა და სხვა ინფორმაციის სახით, მათ შორის პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილება.

4.3 კვლევის შედეგები

კვლევის ფარგლებში გამოთხოვილი საჯარო ინფორმაციის[4], საჯაროდ ხელმისაწვდომი სამართლებრივი აქტებისა და სხვა ინფორმაციის, მათ შორის საქართველოს შინაგან საქმეთა სამინისტროს შემოწმების დასრულების შესახებ საქართველოს პერსონალურ მონაცემთა დაცვის ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილების ანალიზის საფუძველზე, გამოიკვეთა შემდეგი პრობლემური საკითხები:

<u>მონაცემთა დამუშავების მიზნები</u>

<u>უშუალოდ ჭკვიანი კამერების სისტემის საშუალებით მონაცემთა დამუშავების ყველა მიზანი სათანადოდ კონკრეტიზებული და და რეგლამენტირებული არ არის</u>

სამინისტროს მოწოდებული და/ან მითითებული არცერთი დოკუმენტი არ შეეხება უშუალოდ ჭკვიანი კამერების სისტემას, ცალსახად არ განსაზღვრავს მონაცემთა დამუშავების კონკრეტულ მიზნებს.

სამინისტრო მიუთითებს ორ დოკუმენტზე - „პოლიციის შესახებ საქართველოს კანონზე (მუხლი 27), და საქართველოს შინაგან საქმეთა მინისტრის 2017 წლის პირველი მაისის N233 ბრძანებით დამტკიცებულ საქართველოს შინაგან საქმეთა სამინისტროს პროექტზე - „უსაფრთხო ქალაქი, უსაფრთხო რეგიონი, უსაფრთხო ქვეყანა“.

მითითებული დოკუმენტები ქმნიან ჭკვიანი კამერების სისტემის მეშვეობით მონაცემთა დამუშავების ზოგად საფუძველს. კერძოდ „პოლიციის შესახებ“ საქართველოს კანონის 27-ე მუხლი ადგენს, რომ სისტემის გამოყენება შესაძლებელია დანაშაულის პრევენციის, პირის უსაფრთხოებისა და საკუთრების, საზოგადოებრივი წესრიგის დაცვის მიზნით, საგზაო მოძრაობის წესების დაცვის უზრუნველსაყოფად, იმავეს იმეორებს მინისტრის ბრძანებით

[4] გარდა საჯარო ინფორმაციის გამოთხოვის განაცხადისა, ინფორმაციის სრულყოფილად მიღებისა და მიღებული ინფორმაციის არასწორი ინტერპრეტაციის თავიდან აცილების მიზნით, შინაგან საქმეთა სამინისტროს ასევე შევთავაზეთ ზეპირი ინტერვიუს ჩატარება, თუმცა შეხვედრა ვერ მოხერხდა

დამტკიცებული პროექტი, თუმცა ეს უკანასკნელი დამატებით ადგენს ზოგად და სამომავლო მიზნებსა და გეგმებს ერთიანი სათვალთვალო სისტემის შექმნისათვის (მაგ. კერძო სუბიექტების სარგებლობაში არსებული სათვალთვალო სისტემების ინტეგრირება, სტიქიური უბედურებების დეტექცია და ა.შ.), რაც ჯერ სრულად არ განხორციელებულა.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლი ადგენს მონაცემთა დამუშავების პრინციპებს, რომელთა თანახმადაც პერსონალური მონაცემები შეიძლება დამუშავდეს კანონიერად და სამართლიანად და მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული მიზნის მისაღწევად, ამასთან დამუშავებული მონაცემები და მათი მოცულობა კანონიერი მიზნის პროპორციული და ადეკვატური უნდა იყოს. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის მსგავსად, თავდაპირველ მიზანთან შეუთავსებელი მიზნით მონაცემთა დამუშავებას კრძალავს „საქართველოს შინაგან საქმეთა სამინისტროში პერსონალური მონაცემების დამუშავებისა და დაცვის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს შინაგან საქმეთა მინისტრის 2015 წლის 30 მაისის N387 ბრძანების მე-4 მუხლიც.

იმისათვის რომ მონაცემთა დამუშავება სრულ შესაბამისობაში იყოს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოთხოვნებთან, შინაგან საქმეთა სამინისტროს მაქსიმალურად უნდა ჰქოდეს დაკონკრეტებული ჭკვიანი კამერების სისტემით მონაცემთა დამუშავების მიზნები. ამჟამად განსაზღვრული მიზნების ნაწილი, როგორიცაა დანაშაულის პრევენცია, გამოძიების ხარისხის გაუმჯობესება, პოლიციის ტექნოლოგიური რეფორმა ძალიან ფართო და ზოგადი ხასიათისაა. შესაბამისად, აუცილებელია მათი დეტალიზაცია და მონაცემთა სუბიექტისთვის განჭვრეტადად, მკაფიოდ და კონკრეტულად ჩამოყალიბება.

მიზნების ასეთი ფართო ფორმულირება, რისკის შემცველია, ვინაიდან არა მხოლოდ მონაცემთა სუბიექტსა და სამოქალაქო საზოგადოების ორგანიზაციებს, არამედ საზედამხედველო ორგანოსაც კი შეიძლება გაუჭირდეს მინიმიზაციის, პროპორციულობისა და მიზნების თავსებადობის პრინციპების დაცულობის შეფასება. ამასთან ასეთი ზოგადი მიზნები, სამინისტროს აძლევს ინტერპრეტირების ფართო არეალსა და შესაძლებლობას.

<u>მონაცემთა დამუშავების ვადები</u>

არ არის დადგენილი მონაცემთა დამუშავების კონკრეტული ვადები

„საქართველოს შინაგან საქმეთა სამინისტროს ფაილური სისტემებისა და მათში არსებული მონაცემების შენახვის ვადების განსაზღვრის შესახებ“ საქართველოს შინაგან საქმეთა მინისტრის 2015 წლის 23 იანვრის ბრძანებით დამტკიცებული დანართის მე-5 პუნქტის თანახმად ვიდეო-მეთვალყურეობის სისტემის მიერ დამუშავებული მონაცემების შენახვის

ვადა დამოკიდებულია სისტემის მახასიათებლებზე, მაგრამ არ უნდა აღემატებოდეს 3 წელს. ამასთან, სამინისტროს განმარტებით[5], ყველა ტიპის ვიდეომონიტორინგის სისტემის ინფორმაცია, როგორც წესი, ინახება 30 დღის ვადით[6].

პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ 2019 წელს ჩატარებული შემოწმების შედეგად დადგინდა, რომ ჭკვიანი და ზოგადი ხედვის კამერების მიერ დაფიქსირებული ყველა უწყვეტი ვიდეოჩანაწერების შენახვა ხორციელდება ცენტრალურ ვიდეო სერვერებზე. სამინისტროს განმარტებით, აღნიშნულ სერვერებზე ჩანაწერები ავტომატურად იშლება 60 დღის შემდეგ. ადგილზე შემოწმებამ კი გამოავლინა, რომ მიუხედავად იმისა, რომ ცენტრალურ ვიდეო სერვერებზე თითოეული კამერის პარამეტრში შესაძლებელია ჩანაწერთა ავტომატურად წაშლის პერიოდის მითითება, პრაქტიკაში ზოგიერთ კამერასთან მიმართებით აღნიშნული პარამეტრი არ იყო განსაზღვრული. შესაბამისად, ჩანაწერების შენახვა მიმდინარეობდა ცენტრალური ვიდეო სერვერების რესურსის ამოწურვამდე. შემოწმების შედეგად დადგინდა, რომ ცენტრალურ ვიდეო სერვერებზე განთავსებულ ყველაზე ძველი ვიდეო ჩანაწერი დათარიღებული იყო - 2018 წლის 8 ნოემბერით;

ინსპექტირების შედეგად ასევე დადგინდა, რომ ვიდეო ანალიტიკური პროგრამის მიერ დაფიქსირებული ადმინისტრაციული სამართალდარღვევის ფაქტის ამსახველი მონაცემების ამავე პროგრამის მიერ შენახვის ვადაც არ იყო განსაზღვრული. შემოწმების პერიოდისთვის პროგრამაში შენახული ყველაზე ძველი ადმინისტრაციული სამართალდარღვევის ფაქტი დათარიღებული იყო - 2017 წლის 31 ოქტომბერით;

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს მონაცემთა შენახვის ვადის შეზღუდვის პრინციპს, რომლის თანახმადაც მონაცემები შენახულ უნდა იქნას მხოლოდ იმ ვადით, რაც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად.

სამინისტროს მიერ ამგვარი ფართო დიაპაზონის ვადების გამოყენება (30 დღე - 3 წელი), ერთი მხრივ, მოწმობს იმას, რომ სისტემის დანერგვისას არ არის შეფასებული და გაანალიზებული მასში დამუშავებული თითოეული მონაცემის დამუშავების მიზანი და არ არის განსაზღვრული მიზნის ადეკვატური შენახვის ვადა. ასევე, პრობლემურია ის საკითხიც, რომ მონაცემთა სუბიექტისათვის არ არის განჭვრეტადი მის შესახებ რომელი მონაცემები შეიძლება შენახული იქნას 3 წლის განმავლობაში და რომელი მონაცემები წაიშლება 30 დღის შემდეგ, რაც სამინისტროს აძლევს იმის შესაძლებლობას, რომ საკუთარი შეხედულებისამებრ გადაწყვიტოს რა მონაცემს რა ვადით შეინახავს.

---

[5] 2019 წლის 15 ნოემბრის MIA 6 19 03068770 წერილი

[6] აღსანიშნავია, რომ განსხვავებული ვადებია მითითებული საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილებაში, ასევე 2019 წლის 18 სექტემბრის MIA 7 19 02478506 წერილში

ასეთი მიდგომა კი ქმნის შესაძლებლობას 3 წლის განმავლობაში შენახული და გამოყენებული იქნას იმ მძღოლის/სატრანსპორტო საშუალების კონკრეტულ ადგილას ყოფნის ამსახველი მონაცემებიც, რომელსაც მოძრაობის წესებიც კი არ დაურღვევია და უბრალოდ, კამერის თვალთახედვის არეალში მოხვდა, რაც, თავის მხრივ, ადამიანის პირად ცხოვრებაში გაუმართლებელი და არათანაზომიერი ჩარევაა.[7]

ამასთან აღსანიშნავია, რომ საქართველოს შინაგან საქმეთა სამინისტროს შემოწმების დასრულების შესახებ საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილების მიხედვით სამინისტროს დაევალა „გზასა და შენობის გარე პერიმეტრზე დამონტაჟებული/განთავსებული ... ვიდეოტექნიკის საშუალებით ... დამუშავებული მონაცემების შენახვის ვადების განსაზღვრა“. სამინისტროსაგან და სახელმწიფო ინსპექტორის სამსახურისგან მიღებული ინფორმაციის[8] ანალიზის საფუძველზე, არ არსებობს იმის მტკიცებულება, რომ აღნიშნული შესრულდა ან შესრულების პროცესშია.

<u>მონაცემთა მოცულობა</u>

<u>არ არის განსაზღვრული დამუშავებული მონაცემების მოცულობა</u>

საქართველოს შინაგან საქმეთა სამინისტროს მიერ მოწოდებული არცერთი დოკუმენტი არ ითვალისწინებს იმ მონაცემთა (მონაცემთა კატეგორიების) კონკრეტულ ჩამონათვალს, რომელთა დამუშავებაც ხდება ჭკვიანი კამერების სისტემით.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის თანახმად მონაცემთა სუბიექტს აქვს უფლება იცოდეს მის შესახებ რომელი მონაცემი მუშავდება, რა მიზნით, რა საფუძვლით, ვისზე გაიცა ეს მონაცემები და ა.შ. კანონი მონაცემთა დამმუშავებელს ავალდებულებს აღნიშნული ინფორმაციის მონაცემთა სუბიექტისთვის მიწოდებას, ასევე, მის ფაილური სისტემის კატალოგში ასახვას.

როგორც უკვე აღინიშნა, „ჭკვიან კამერებს“ შეუძლიათ ამოიცნონ და რეაგირება მოახდინონ იმ ქცევაზე, რომელსაც მაკონტროლებელი ‘დაასწავლის’, თუმცა რადგან სამინისტროს მიერ დასახელებული არცერთი აქტით არ არის განსაზღვრული თუ რა მონაცემები მუშავდება

---

[7] აღნიშნულ მსჯელობას ამყარებს ის ფაქტიც, რომ „საქართველოს შინაგან საქმეთა სამინისტროში ადმინისტრაციულ სამართალდარღვევათა ერთიანი აღრიცხვის, საინფორმაციო ბანკის ფუნქციონირებისა და სააღრიცხვო-ანალიტიკური საქმიანობის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს შინაგან საქმეთა მინისტრის 2006 წლის 1 მარტის N271 ბრძანების თანახმად, სამინისტროს მიერ გამოვლენილი ადმინისტრაციული სამართალდარღვევები ცალკე აღირიცხება და ინახება.

[8] საქართველოს შინაგან საქმეთა სამინისტროს 2019 წლის 18 სექტემბრის MIA 7 19 02478506 და 15 ნოემბრის MIA 6 19 03068770 წერილები, საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილება

რეალურად აღნიშული სისტემის მიერ, მონაცემთა სუბიექტს არ შეუძლია განჭვრიტოს მის შესახებ რა მონაცემები აისახება სისტემაში და რა მიზნების მისაღწევად შეიძლება იქნას გამოყენებული ეს მონაცემები მაგ. შესაძლებელია თუ არა ან აქვს თუ არა გამოყენებულ სისტემას შესაძლებლობა მოახდინოს ავტომანქანის არა მხოლოდ სანომრე ნიშნების, არამედ მძღოლისა და მგზავრების იდენტიფიცირებაც, შესაძლებელია თუ არა ქვეითის კონკრეტული ქმედების იდენტიფიცირება და ა.შ. ეს მდგომარეობა ხელს შეუშლის მონაცემთა სუბიექტის უფლების რეალიზებას, იცოდეს მის შესახებ რომელი მონაცემი მუშავდება და რა მიზნით ხდება მათი გამოყენება.

„უსაფრთხო ქალაქი, უსაფრთხო რეგიონი, უსაფრთხო ქვეყანა“ პროექტში[9] საუბარია მომოვალ დროში, ანუ შემოთავაზებულია იმ დროისთვის (2017 წელი) სამომავლო კონცეფცია რომლის თანახმად, ვიდეომეთვალყურეობის კამერები დანიშნულების **შესაბამისად იქნება აღჭურვილი სხვადასხვა ტიპის ანალიტიკური პროგრამებით, მათ შორის, სახის ამოცნობის, ნომრის ამოცნობის, საგზაო დარღვევების ამოცნობისა და ადამიანის ქცევის დეტექციის ფუნქციებით.** ისინი ჩართული იქნება პოლიციის ერთიან ქსელში და მათი უწყვეტი მონიტორინგი რეალურ დროში განხორციელდება შინაგან საქმეთა სამინისტროს ერთობლივი ოპერაციების ცენტრის მიერ, რომელსაც პირდაპირი წვდომა ექნება ყველა კამერაზე და უზრუნველყოფს მუდმივ მონიტორინგსა და დარღვევებზე მყისიერ რეაგირებას, თუმცა არც სამინისტროსაგან მიღებული ინფორმაციის და არც ხელმისაწვდომი სამართლებრივი აქტების ანალიზის საფუძველზე არ დგინდება აღნიშნული (პოტენციურად შესაძლებელი) ფუნქციებიდან რეალურად რომელს, რა ფორმით და რა მიზნებისთვის იყენებს სამინისტრო ამ ეტაპზე.

<u>მონაცემებზე წვდომა</u>

ჭკვიანი კამერების სისტემაში წვდომის დონეები დოკუმენტირებული არ არის

შინაგან საქმეთა სამინისტროსგან მიღებული ინფორმაციის თანახმად, მონაცემებზე საკუთარი უფლებამოსილების ფარგლებში წვდომის უფლება აქვთ სამინისტროს საპატრულო პოლიციის დეპარტამენტის, სამინისტროს ერთობლივი ოპერაციების ცენტრისა და საინფორმაციო-ანალიტიკური დეპარტამენტის თანამშრომლებს. თუმცა სამინისტროს მიერ ამ საკითხთან დაკავშირებით მითითებული აქტები მხოლოდ სამინისტროს შესაბამისი დეპარტამენტების უფლებამოსილებებს განსაზღვრავს, მათ შორის, „საქართველოს შინაგან საქმეთა სამინისტროში პერსონალური მონაცემების დამუშავებისა და დაცვის შესახებ

[9] საქართველოს შინაგან საქმეთა მინისტრის 2017 წლის პირველი მაისის N233 ბრძანებით დამტკიცებული საქართველოს შინაგან საქმეთა სამინისტროს პროექტი „უსაფრთხო ქალაქი, უსაფრთხო რეგიონი, უსაფრთხო ქვეყანა“

ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს შინაგან საქმეთა მინისტრის 2015 წლის 30 მაისის N387 ბრძანების მე-16 მუხლიც მხოლოდ ინფორმაციულ რესურსებთან თანამშრომლების დაშვების უფლების მინიჭების წესს განსაზღვრავს, თუმცა არცერთი აღნიშნული აქტი არ არეგულირებს თუნდაც უფლებამოსილებების მიხედვით მონაცემებზე წვდომისა და სისტემაში განსახორციელებელი ქმედებების ფარგლებს.

ამავდროულად, საქართველოს შინაგან საქმეთა სამინისტროს შემოწმების დასრულების შესახებ საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილების თანახმად „განხორციელებული ადგილზე შემოწმების შედეგად დადგინდა, რომ.... ვიდეო ანალიტიკურ პროგრამაში არსებობს ორი ტიპის მომხმარებელი - ადმინისტრატორი და ოპერატორი“. ამათგან, ადმინისტრატორს აქვს ჩანაწერების დათვალიერების, გადმოწერის, სისტემის და კამერების ტექნიკური პარამეტრების მითითების უფლება, ხოლო ოპერატორს კი მხოლოდ დათვალიერების და გადმოწერის უფლება.

ყოველივე აღნიშნულიდან გამომდინარე, შეიძლება ითქვას, რომ სამინსიტროს სისტემაში დამუშავებულ პერსონალურ მონაცემებზე წვდომის საკითხი არ აქვს დოკუმენტირებული და შესაბამისად რეგლამენტირებული. პრაქტიკულად სისტემაში არსებობს მომხმარებელთა განსხვავებული ტიპები, თუმცა არ არსებობს დოკუმენტი, რომელიც დაადგენს მაგალითად სამინისტროს ერთობლივი ოპერაციების ცენტრის თანამშრომელს თავისი რომელი უფლებამოსილების ფარგლებში რა მონაცემებზე შეიძლება ჰქონდეს წვდომა და რა მოქმედებების განხორციელება შეუძლია ამ წვდომის ფარგლებში.

ვინაიდან კამერების სერვერთან დაკავშირების მიზნით გამოყენებული ქსელური კავშირისა და უსაფრთხოების აპარატურის ტექნიკურ მომსახურებას უზრუნველყოფს სსიპ ოპერატიულ-ტექნიკური სააგენტო, რომელიც თავის მხრივ, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემვალი საჯარო სამართლის იურიდიული პირია, საინტერესოა, აქვს თუ არა სააგენტოს წვდომა უშუალოდ პერსონალურ მონაცემებზე.

<u>მონაცემთა გადაცემა</u>

მონაცემთა გადაცემის შესახებ ინფორმაცია არ მოიპოვება

სამინისტროდან მიღებული საჯარო ინფორმაციის საფუძველზე არ ირკვევა თუ როგორ არის მოწესრიგებული ჭკვიანი კამერების სისტემის მიერ დამუშავებული მონაცემების მესამე პირებისთვის/ ორგანიზაციებისთვის გადაცემის საკითხი. მიუხედავად, იმისა, რომ გაგზავნილ წერილში[10] პირდაპირი ფორმულირებით იყო დასმული კითხვა მონაცემთა

[10] ინოვაციებისა და რეფორმების ცენტრის 2019 წლის 16 აგვისტოს N10.08.19 წერილი

გადაცემის თაობაზე, საქართველოს შინაგან საქმეთა სამინისტროს არცერთ წერილში არ არის პასუხი აღნიშნულ კითხვაზე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი (მუხლი 21) მონაცემთა სუბიექტს ანიჭებს უფლებას იცოდეს ვისზე გაიცა მის შესახებ მონაცემები, მონაცემთა გაცემის საფუძველი და მიზანი. ამ უფლების რეალიზებისათვის საჭიროა, მონაცემთა დამმუშავებელს აღრიცხული ჰქონდეს მონაცემთა თითოეული გადაცემის ფაქტი.

ასევე, „საქართველოს შინაგან საქმეთა სამინისტროში პერსონალური მონაცემების დამუშავებისა და დაცვის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს შინაგან საქმეთა მინისტრის 2015 წლის 30 მაისის N387 ბრძანების მე-5 თავი მონაცემთა გაცემის საკითხს არეგულირებს და სამინისტროს ავალდებულებს მონაცემთა გაცემისას მათ რეგისტრაციას.

აღნიშნულ კითხვაზე პასუხის გაუცემლობა გვაძლევს საფუძველს ვივარაუდოთ, რომ საქართველოს შინაგან საქმეთა სამინისტროს არ აქვს აღრიცხული სისტემიდან მონაცემთა გადაცემის ფაქტები და, შესაბამისად, ვერ უზრუნველყოფს მონაცემთა სუბიექტის უფლებების სათანადო რეალიზებას.

მონაცემთა უსაფრთხოების ორგანიზაციულ-ტექნიკური ზომები და ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული მოქმედების აღრიცხვა

გამოთხოვილი საჯარო ინფორმაციის ფარგლებში ვერ მივიღეთ ინფორმაცია ჭკვიანი კამერების სისტემის უსაფრთხოებისთვის შინაგან საქმეთა სამინისტროს მიერ გატარებული ორგანიზაციული თუ ტექნიკური ზომების შესახებ. მიუხედავად, იმისა, რომ გაგზავნილ წერილში[11] პირდაპირ იყო მოთხოვნილი ინფორმაცია ლოგირების/ელექტრონული ჟურნალის შესახებ, საქართველოს შინაგან საქმეთა სამინისტროს არცერთ წერილში არ არის მოცემული პასუხი აღნიშნულ კითხვაზე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის მე-2 პუნქტის თანახმად მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.

ასევე, „საქართველოს შინაგან საქმეთა სამინისტროში პერსონალური მონაცემების დამუშავებისა და დაცვის შესახებ ინსტრუქციის დამტკიცების თაობაზე“ საქართველოს

[11] ინოვაციებისა და რეფორმების ცენტრის 2019 წლის 16 აგვისტოს N10.08.19 წერილი

შინაგან საქმეთა მინისტრის 2015 წლის 30 მაისის N387 ბრძანების 27-ე მუხლი ავალდებულებს სამინისტროს სისტემაში განხორციელებული ყველა მოქმედების ლოგირებას.

საქართველოს შინაგან საქმეთა სამინისტროს შემოწმების დასრულების შესახებ პერსონალურ მონაცემთა დაცვის ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილების თანახმად „შემოწმების შედეგად დადგინდა, რომ გზასა და შენობის გარე პერიმეტრზე დამონტაჟებული/განთავსებული ... ვიდეოტექნიკის საშუალებით ... მონაცემთა დამუშავებისას, რიგ შემთხვევებში არ ხორციელდება ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა“, მაგალითად, არ არსებობს ჭკვიანი კამერების მიერ მოპოვებული უწყვეტი ვიდეო ჩანაწერების მიმართ განხორციელებული მოქმედებების აღრიცხვის ჟურნალი, ისევე, როგორც დაფიქსირებული ადმინისტრაციული სამართალდარღვევის ამსახველი მასალის მიმართ განხორციელებული მოქმედებების აღრიცხვის ჟურნალი.

სისტემაში განხორციელებული ქმედებების აღურიცხაობა ქმნის საფრთხეს, შესაბამისი წვდომის უფლების მქონე თანამშრომელმა პირადი ან არაკანონიერი მიზნებით დაათვალიეროს, გადმოწეროს და საკუთარი შეხედულებისამებრ გამოიყენოს სისტემაში არსებული მონაცემები და განახორციელოს უკანონო ვიდეოთვალთვალი ისე, რომ ინსპექტირების ან გამოძიების ჩატარების პირობებშიც კი არ იყოს შესაძლებელი არაკანონიერი წვდომის ფაქტის დადგენა. ვინაიდან, პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-17 მუხლი, ყველა ორგანიზაციას ავალდებულებს მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უსაფრთხოების ზომების მიღებას, მნიშვნელოვანია ე.წ. ინსაიდერული რისკები სათანადოდ იქნას შეფასებული, განისაზღვროს მათი შემცირებისა და გამოვლენის მექანიზმები. ამ თვალსაზრისით გასათვალისწინებელია უახლოესი წარსულის გამოცდილება - მედია საშუალებებით გასაჯაროებულა და ასევე პერსონალურ მონაცემთა დაცვის ინსპექტორის მხრიდანაც გამოვლენილა სამინისტროს თანამშრომელთა მიერ პირადი მიზნებით მონაცემებზე (მათ შორის ვიდეო ჩანაწერებზე) წვდომის ფაქტები.

2019 წლის 27 ივნისის გადაწყვეტილებით საქართველოს შინაგან საქმეთა სამინისტროს დაევალა გადაწყვეტილების ჩაბარებიდან 6 თვის ვადაში უზრუნველეყო სისტემაში განხორციელებული ყველა მოქმედების აღრიცხვა. საქართველოს შინაგან საქმეთა სამინისტროსაგან და სახელმწიფო ინსპექტორის სამსახურისგან მიღებული ინფორმაციის[12] ანალიზის საფუძველზე, არ არსებობს იმის დასტური/მტკიცებულება, რომ დარღვევა აღმოიფხვრა.

[12] საქართველოს შინაგან საქმეთა სამინისტროს 2019 წლის 18 სექტემბრის MIA 7 19 02478506 და 15 ნოემბრის MIA 6 19 03068770 წერილები, საქართველოს სახელმწიფო ინსპექტორის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილება

<u>მონაცემთა დამუშავების ზეგავლენის შეფასება</u>

მიუხედავად იმისა, რომ მოქმედი კანონმდებლობა (განსხვავებით საქართველოს პარლამენტში განხილვის ეტაპზე მყოფი პროექტისა) პირდაპირ არ ადგენს მონაცემთა დამუშავების ზეგავლენის შეფასების ვალდებულებას, ე.წ. ჭკვიანი კამერების სისტემის თავისებურების, საუკეთესო ევროპული პრაქტიკისა და საქართველოს ევროპული ინტეგრაციის (მათ შორის ევროპოლთან თანამშრომლობისა და ასოცირების შეთანხმების) გათვალისწინებით მიზანშეწონილია მონაცემთა უსაფრთხოებისთვის და ლეგიტიმური დამუშავებისთვის დამატებითი ზომების მიღება.

ჭკვიანი კამერების სისტემასთან დაკავშირებით მონაცემთა დამუშავების ზეგავლენის შეფასება არ ჩატარებულა

შინაგან საქმეთა სამინისტროს ცნობით, სამინისტროში მოქმედებს პერსონალურ მონაცემთა დაცვაზე ზედამხედველობის ჯგუფი, რომელსაც წინასწარ ეცნობება ახალი სისტემის დანერგვის შესახებ და სწორედ ეს ჯუფი აფასებს სისტემებს პერსონალურ მონაცემთა დაცვის კუთხით.

თუმცა ჭკვიანი კამერების სისტემასთან დაკავშირებით ასეთი შეფასების შედეგები ან რამე ტიპის დასკვნა ჩვენთვის სამინისტროს არ მოუწოდებია. შინაგან საქმეთა სამინისტროს ასევე არ მიუთითებია პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ აღნიშნული სისტემის შემოწმების შესახებაც.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს მონაცემთა უსაფრთხოებისათვის შესაბამისი ორგანიზაციული და ტექნიკური ზომები და ეს ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

პერსონალურ მონაცემთა დამუშავების ზეგავლენის ანალიზი კი ევროპულ კანონმდებლობით კარგად დანერგილი და ფართოდ გავრცელებული პრაქტიკაა და მნიშვნელოვანია იმდენად, რამდენადაც მონაცემთა დამმუშავებელს აძლევს საშუალებას სისტემურად და სიღრმისეულად გაიაზროს მონაცემთა დამუშავების პროცესი, შეაფასოს და გამოავლინოს კანონმდებლობის მოთხოვნებთან შესაბამისობის საკითხი, მონაცემთა სუბიექტის უფლებების რეალიზების შესაძლებლობები, წინასწარ დეტალურად შეაფასოს მოსალოდნელი რისკები და დროულად მიიღოს სათანადო ორგანიზაციული თუ ტექნიკური ზომები.

4.4 ძირითადი მიგნებები

როგორც უკვე აღინიშნა, ჭკვიანი კამერების სისტემა კომპლექსურია. ასეთ სისტემაში პერსონალურ მონაცემთა დაცვის საკითხი კრიტიკულად მნიშვნელოვანი და აქტუალურია სისტემის ტექნოლოგიური პოტენციალის, მონაცემთა სუბიექტების სიმრავლისა თუ მონაცემთა გამოყენების ფართო არეალის გათვალისწინებით.

მიუხედავად იმისა რომ შინაგან საქმეთა სამინისტრომ უარი განაცხადა მონიტორინგის მიგნებების განხილვაზე ერთობლივი შეხვედრის ფორმატში, რათა მომხდარიყო საკითხების დაზუსტება/ვერიფიკაცია, ასევე კონკრეტულ კითხვათა ნაწილზე პასუხი საერთოდ არ გაგვცა ან არასრულყოფილად გვიპასუხა, საჯაროდ ხელმისაწვდომი ინფორმაციის და სამინისტროსაგან ნაწილობრივ მიღებული პასუხების საფუძვლეზე, მაინც შევძელით ანგარიშის მომზადება და შემდეგი დასკვნების გამოტანა:

- ჭკვიანი კამერების სისტემის ფუნქციონირება და მასში მონაცემთა დაცვის საკითხი არასაკმარისად/არაპროპორციულადაა რეგლამენტირებული, იმ რისკებისა და მონაცემთა დამუშავების პოტენციალის ფონზე რაც ამ სისტემას გააჩნია;
- სისტემის შექმნამდე ან მისი ამოქმედების შემდეგ სამინისტროს მხრიდან არ მომხდარა მისი კომპლექსური ანალიზი პერსონალურ მონაცემთა დაცვაზე გავლენის შესაფასებლად;
- სამონისტრო არ ახდენს მის მიერ ჭკვიანი კამერების სისტემაში დამუშავებულ პერსონალურ მონაცემებზე შესრულებული იმ მოქმედებების აღრიცხვას/ლოგირებას, რაც პირდაპირ ევალება კანონით;
- ჭკვიანი კამერების სისტემაში მონაცემთა დამუშავების მიზნები განსაზღვრულია კანონით თუმცა სასურველია მეტი კონკრეტიზაცია და სიცხადე რათა მინიმიზებული იქნეს მონაცემთა გადაჭარბებული გამოყენებისრისკები;
- სამინისტროს არ აქვს კონკრტეულად განსაზღვრული სისტემაში დამუშავებული მონაცემთა კატეგორიები/მოცულობა, რომლის შესახებ ინფორმაცია ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტებისთვის. ზოგადად ცნობილია თუ მონაცემთა დამუშავების რა პოტენციალი აქვს სისტემას, თუმცა ამ ტექნიკური პოტენციალიდან რა ნაწილია რეალიზებული ბუნდოვანია- არ არსებობს მარეგლამენტირებელი აქტი რომელიც კონკრტულად აწესრიგებს ამ საკიტხს;
- სამინისტროს არა აქვს განსაზღვრული ის კონკრეტული ვადები, რომლებიც აუცილებელია მონაცემთა დამუშავების სხვადასხვა მიზნის მისაღწევად და რა ვადითაც მოხდება მონაცემების დამუშავება. სამართლებრივი აქტით დადგენილია მხოლოდ მაქსიმალური ვადა, ხოლო ამ სფეროში არსებული პრაქტიკული მდგომარეობის შესახებ სამინისტროსგან IRC-თვის მოწოდებული ინფორმაცია შეუსაბამოა სახელმწიფო ინსპექტორის მიერ, ადგილზე შემოწმების შედეგად გაკეთებულ ფაინდინგებთან;

- სამინიტროს არ აქვს შესწავლილი და იდენტიფიცირებული ყველა რისკი, მათ შორის ინსაიდერული, ხოლო ინფორმაცია მონაცემთა დასაცავად მიღებული ორგანიზაციულ-ტექნიკური ზომების (თუნდაც ზოგადი აღწერა) შესახებ გაუმჭვირვალეა.
- გასაუმჯობესებელია მონაცემთა სუბიექტის უფლებების რეალიზების მექანიზმები - სამინისტროს უნდა შეეძლოს მონაცემთა სუბიექტს კანონით განსაზღვრულ ვადებში სრულად მიაწოდოს მის მიერ მოთხოვნილი ინფორმაცია (ზუსტად რას ამუშავებს კონკრეტულ პირზე, რა საფუძვლით, ვის გადაეცემამონაცემი და ა.შ.), თუმცა აღნიშნულის უფლების რეალიზაცია შეუძლებელია სულ ცოტა იმ მიზეზის გამო რომ სამონისტრო არ ახდენს პერსონალურ მონაცემებზე შესრულებული იმ მოქმედებების აღრიცხვას/ლოგირებას, რაც პირდაპირ ევალება კანონით.