პერსონალურ მონაცემთა
დაცვის სამსახური

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

N2, 2023

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალი

№2, 2023

პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის მეორე გამოცემა ეძღვნება
საქართველოს პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს
10 წლის იუბილეს

P-ISSN 2720-8753

E-ISSN 2720-8761

სარჩევი

მთავარი რედაქტორისაგან

პერსონალურ მონაცემთა დაცვის ჟურნალის წინამდებარე ნომერი ეძღვნება პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს შექმნის ათი წლის იუბილეს.

ამ ღირსშესანიშნავ თარიღს პერსონალურ მონაცემთა დაცვის სამსახური არაერთი სიახლით ხვდება.

2023 წლის 20 ივნისს, „მონაცემთა დაცვის ევროპული საბჭოს“ (EDPB) გადაწყვეტილებით, პერსონალურ მონაცემთა დაცვის სამსახურს მიენიჭა საბჭოს საქმიანობის დამკვირვებლის სტატუსი. მონაცემთა დაცვის ევროპული საბჭო, როგორც ევროკავშირის ორგანო, შექმნილია „მონაცემთა დაცვის ძირითადი რეგულაციის“ (GDPR) საფუძველზე და შედგება ევროკავშირის თითოეული წევრი სახელმწიფოს მონაცემთა დაცვის საზედამხედველო ორგანოს, ევროკომისიისა და „ევროპის მონაცემთა დაცვის ზედამხედველის“ (EDPS) წარმომადგენლებისაგან. იგი არსებით როლს ასრულებს ევროკავშირის მასშტაბით პერსონალურ მონაცემთა დაცვის რეგულაციების ეფექტიან უზრუნველყოფასა და მონაცემთა დაცვის საზედამხედველო ორგანოთა თანმიმდევრული, ერთგვაროვანი და საუკეთესო პრაქტიკის ჩამოყალიბებაში.

საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურისთვის დამკვირვებლის სტატუსის მინიჭებაზე საბჭომ გადაწყვეტილება რამდენიმე კრიტერიუმის გათვალისწინებით მიიღო: სამსახურის საქმიანობა და დამოუკიდებლობის ხარისხი, საკანონმდებლო რეგულაციები და სახელმწიფოს მიერ გაცხადებული ნება - ევროკავშირში გაწევრიანების მიზნით აღებული საერთაშორისო ვალდებულება, რომ მონაცემთა დაცვის ეროვნული კანონმდებლობა სრულად შეუსაბამოს ევროკავშირში მოქმედ წესებს. აგრეთვე, აღსანიშნავია, რომ გადაწყვეტილებასთან დაკავშირებით საბჭოს მიერ გავლილ იქნა კონსულტაციები ევროკომისიასთან და ევროკავშირის სხვადასხვა ინსტიტუტებთან ჰომოგენურობის მიზნით.

ეს მეტად მნიშვნელოვანი გადაწყვეტილებაა, რაც გულისხმობს პერსონალურ მონაცემთა დაცვის სამსახურის მონაცემთა დაცვის კოლეგა ორგანოთა ევროპული ოჯახის ღირსეულ წევრობას, რომელიც, ერთი მხრივ, დიდი მიღწევაა ჩვენთვის, ხოლო მეორე მხრივ - უაღრესად დიდი პასუხისმგებლობა, რაც სამსახურის თითოეულ თანამშრომელს გათვითცნობიერებული გვაქვს.

ევროინტეგრაციის გზაზე პერსონალურ მონაცემთა დაცვის სამსახურის გაძლიერებისათვის და ქვეყანაში მონაცემთა დაცვის უფლების მაღალი სტანდარტის უზრუნველყოფისათვის 2023 წლის 14 ივნისს მიღებულ იქნა „პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონი, რომელიც მნიშვნელოვანი წინ გადადგმული ნაბიჯია საქართველოს პერსონალურ მონაცემთა დაცვის სამართლის განვითარებისათვის. კანონის მიღება განპირობებული იყო პერსონალურ მონაცემთა დაცვის სფეროში არსებული კანონმდებლობის ევროპულ სტანდარტებთან დაახლოების, საქართველოს მიერ ნაკისრი საერთაშორისო ვალდებულებების შესრულებისა და საერთაშორისოდ აღიარებული პრინციპებისა და საუკეთესო პრაქტიკის დამკვიდრების საჭიროებით.

მნიშვნელოვანია პერსონალურ მონაცემთა დაცვის შესახებ კანონმდებლობის ჰარმონიზაცია ევროკავშირის კანონმდებლობასთან და შესაბამისად, ახალი სტანდარტების იმპლემენტაცია ეროვნულ დონეზე.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით შემოთავაზებულია ისეთი მნიშვნელოვანი ცვლილებები, როგორიცაა უკვე არსებული ტერმინოლოგიის დახვეწა ანდა სრულიად ახალი ცნებების დამკვიდრება პერსონალურ მონაცემთა დაცვის სფეროში.

კანონი ახლებურად განმარტავს ტერმინს „მონაცემთა სუბიექტის თანხმობა“, „აუდიომონიტორინგი,“ ფართოდ ყალიბდება „პირდაპირი მარკეტინგის“ განმარტება, ამკვიდრებს ისეთ მნიშვნელოვან ახალ ტერმინს, როგორიცაა „პროფაილინგი“. ამასთან, ერთ-ერთ მნიშვნელოვან საკითხს მონაცემთა „ფსევდონიმიზაცია“ წარმოადგენს.

გარდა ტერმინოლოგიური სიახლეებისა, ახალი კანონი პრინციპის დონეზე განსაზღვრავს მონაცემთა დამუშავების „გამჭვირვალობას“. აღნიშნულ პრინციპს უდიდესი მნიშვნელობა აქვს უფლების დაცვისა და რეალიზაციის თვალსაზრისით მონაცემთა სუბიექტისთვის. ფიზიკური პირისთვის ნათელი და გამჭვირვალე უნდა იყოს, რომ მუშავდება ან იგეგმება მისი მონაცემების დამუშავება. გამჭვირვალობის პრინციპი მოითხოვს, რომ მონაცემთა სუბიექტებისათვის ხელმისაწვდომი იყოს ინფორმაცია მათი პერსონალური მონაცემების დამუშავების შესახებ.

ახალი კანონი აფართოებს მონაცემთა სუბიექტის უფლებებს და ამყარებს აღნიშნულ უფლებათა დაცვის გარანტიებს. ერთ-ერთი ახალი უფლება, რასაც ახალი კანონი მონაცემთა სუბიექტებს ანიჭებს, მონაცემთა გადატანის, ე.წ. „პორტირების“ უფლებაა. მონაცემთა გადატანის უფლება მონაცემთა სუბიექტებს გაუმარტივებს გარკვეული სერვისებით სარგებლობას. თავის მხრივ, მნიშვნელოვანია, კომპანიებმა უზრუნველყონ შესაბამისი ტექნიკური საშუალებების დანერგვა, რათა შესაძლებელი გახადონ პერსონალურ მონაცემთა გადატანა ინფორმაციული ტექნოლოგიების ერთი გარემოდან მეორეში და რაც ყველაზე მთავარია, აღნიშნულის განხორციელებისას გაატარონ შესაბამისი უსაფრთხოების ზომები.

უმნიშვნელოვანესია ასევე ახალი კანონით გათვალისწინებული, მონაცემთა დაცვაზე ზეგავლენის შეფასების მექანიზმიც, რაც პერსონალურ მონაცემთა დაცვის ქართული კანონმდებლობისთვის სიახლეს წარმოადგენს და ახალი ტექნოლოგიების უსწრაფესი ტემპით განვითარების პირობებში, ადამიანის უფლებების დარღვევის მომეტებული საფრთხეების შემცირებას ისახავს მიზნად.

ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ ახლებურად აყალიბებს პირდაპირ მარკეტინგთან დაკავშირებულ საკითხებს. საყურადღებოა, რომ ახალი კანონის მიხედვით, მიუხედავად მონაცემთა შეგროვების/მოპოვების საფუძვლისა და მათი ხელმისაწვდომობისა, პირდაპირი მარკეტინგის მიზნით მონაცემთა დამუშავება შესაძლებელი იქნება მხოლოდ მონაცემთა სუბიექტის თანხმობით, განსხვავებით დღეს მოქმედი ნორმისგან. მონაცემთა სუბიექტის სახელის, გვარის, მისამართის, ტელეფონის ნომრისა და ელექტრონული ფოსტის მისამართის გარდა, პირდაპირი მარკეტინგის მიზნით სხვა მონაცემთა დამუშავებისთვის აუცილებელი იქნება მონაცემთა სუბიექტის წერილობითი თანხმობა. აღსანიშნავია ისიც, რომ მონაცემთა

სუბიექტის თანხმობის მიღებამდე და პირდაპირი მარკეტინგის განხორციელებისას დამუშავებისთვის პასუხისმგებელმა პირმა/დამუშავებაზე უფლებამოსილმა პირმა მონაცემთა სუბიექტს ნათლად, მარტივ და მისთვის გასაგებ ენაზე უნდა განუმარტოს მის მიერ თანხმობის ნებისმიერ დროს გამოხმობის უფლება და ამ უფლების განხორციელების მექანიზმი, წესი.

ახალი კანონით გათვალისწინებული სიახლეებიდან მნიშვნელოვანია საჯარო და რიგ კერძო დაწესებულებებში პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნის ვალდებულება.

კანონის მიხედვით, მონაცემთა დაცვის ოფიცერი უზრუნველყოფს:

- მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარების გაწევას;
- მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობას, აგრეთვე დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს;
- მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;
- პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას სამსახურთან ურთიერთობაში;
- მონაცემთა სუბიექტის მიმართვის შემთხვევაში, მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;
- ასევე, პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას.

ოფიცრის დანიშვნის ან განსაზღვრის ვალდებულება ეკისრებათ საჯარო დაწესებულებებს, სადაზღვევო ორგანიზაციებს, კომერციულ ბანკებს, მიკროსაფინანსო ორგანიზაციებს, საკრედიტო ბიუროებს, ელექტრონული კომუნიკაციის კომპანიებს, ავიაკომპანიებს, აეროპორტებს, სამედიცინო დაწესებულებებს, აგრეთვე დამუშავებისთვის პასუხისმგებელ და დამუშავებაზე უფლებამოსილ იმ პირებს, რომელიც ამუშავებენ დიდი რაოდენობით მონაცემთა სუბიექტების მონაცემებს ან ახორციელებენ მათი ქცევის სისტემატურ და მასშტაბურ მონიტორინგს. ამასთან, პირთა წრე, რომლებსაც არ აქვთ ვალდებულება, დანიშნონ ან განსაზღვრონ პერსონალურ მონაცემთა დაცვის ოფიცერი, განისაზღვრება პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით.

მართალია, კანონი ოფიცრის დანიშვნის ვალდებულებას მხოლოდ ზემოთ ჩამოთვლილ სუბიექტებს აკისრებს, თუმცა დამუშავებისთვის პასუხისმგებელ სხვა პირებს, საკუთარი შეხედულებისამებრ, უფლება აქვთ, დანიშნონ ან განსაზღვრონ

პერსონალურ მონაცემთა დაცვის ოფიცერი. კანონის თანახმად, პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში. ამასთან, დამუშავებისთვის პასუხისმგებელ პირსა და დამუშავებაზე უფლებამოსილ პირს მოეთხოვებათ, უზრუნველყონ ოფიცერი შესაბამისი რესურსებითა და დამოუკიდებლობით საქმიანობის განხორციელების პროცესში. გარდა ამისა, მათ ეკისრებათ ვალდებულება, ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია პროაქტიულად გამოაქვეყნონ ვებგვერდზე (ასეთის არსებობის შემთხვევაში) ან სხვა ხელმისაწვდომი საშუალებით.

მონაცემთა დაცვის ოფიცრის ინსტიტუტის შემოღება განსაკუთრებით მნიშვნელოვანია, ვინაიდან იგი პერსონალურ მონაცემთა დაცვის ქართულ კანონმდებლობას აახლოებს ევროპულ სტანდარტებთან და მნიშვნელოვნად აძლიერებს მონაცემთა სუბიექტების უფლებების დაცვის გარანტიებს. დანამდვილებით შეიძლება ითქვას, რომ მონაცემთა დაცვის ოფიცრის ინსტიტუტის რეალური იმპლემენტაცია მნიშვნელოვან პრევენციულ ეფექტს გამოიწვევს და თვისობრივად შეუწყობს ხელს მონაცემთა დამუშავების პროცესის კანონიერების განმტკიცებას.

ერთ-ერთი საკითხი, რომელიც მნიშვნელოვნად იცვლება, ადმინისტრაციული სახდელებია. ახალი კანონი აწესებს გაფრთხილებას ან ჯარიმას „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით განსაზღვრული ნებისმიერი ვალდებულების ან წესის დარღვევისათვის. მაგალითისთვის, მონაცემთა დამუშავებისთვის პასუხისმგებელ პირს შესაძლოა, პასუხისმგებლობა დაეკისროს მონაცემთა დამუშავების პრინციპების ან საფუძვლების დარღვევისთვის, პირდაპირი მარკეტინგის მოთხოვნების გვერდის ავლით განხორციელებისთვის, აუდიომონიტორინგის ან ვიდეომონიტორინგის კანონშეუსაბამოდ განხორციელებისთვის, მონაცემთა დაცვის ოფიცრის არყოლისათვის, მაშინ, როდესაც კანონის ამას ავალდებულებს და ა.შ.

ახალი კანონი ასევე აფართოებს ადმინისტრაციული სამართალდარღვევებისთვის გათვალისწინებულ ადმინისტრაციული პასუხისმგებლობის მასშტაბს და ზრდის პასუხისმგებლობის ზომებს.

მოქმედი კანონის მსგავსად, ახალი კანონი კვლავ ფიქსირებული ჯარიმის ოდენობებს განსაზღვრავს, თუმცა საგრძნობლად გაზრდილია მათი ოდენობა. კერძოდ, ჯარიმის ოდენობა დაუკავშირდა სამართალდამრღვევის ორგანიზაციულ ფორმასა და მის წლიურ ბრუნვას. მაგალითად კანონით გათვალისწინებული მონაცემთა დამუშავების რომელიმე პრინციპის დარღვევა გამოიწვევს ფიზიკური პირის, საჯარო დაწესებულების, არასამეწარმეო (არაკომერციული) იურიდიული პირის, აგრეთვე იურიდიული პირის, უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს არ აღემატება, გაფრთხილებას ან დაჯარიმებას 1 000 ლარის ოდენობით. ხოლო იგივე ქმედების ჩადენა იურიდიული პირის (გარდა არასამეწარმეო (არაკომერციული) იურიდიული პირისა), უცხო ქვეყნის საწარმოს ფილიალისა და ინდივიდუალური მეწარმის, რომელთა წლიური ბრუნვა 500 000 ლარს აღემატება, გამოიწვევს მათ გაფრთხილებას ან დაჯარიმებას 2 000 ლარის ოდენობით.

სიახლეა პასუხისმგებლობის შემამსუბუქებელი და დამამძიმებელი გარემოებების განსაზღვრაც. ასევე, პერსონალურ მონაცემთა დაცვის სამსახურის კანონიერი მოთხოვნის შეუსრულებლობის ადმინისტრაციულ სამართალდარღვევად მიჩნევა, რისთვისაც გათვალისწინებული ჯარიმის ოდენობა შეადგენს 1000 – 2000 ლარს. აღნიშნული ცვლილება ხელს შეუწყობს პერსონალურ მონაცემთა დაცვის სამსახურის მიერ მიღებული გადაწყვეტილებების ეფექტიან აღსრულებას და მნიშვნელოვან გავლენას იქონიებს ქვეყანაში პერსონალურ მონაცემთა დაცვის საერთო მდგომარეობის გაუმჯობესებაზე.

მნიშვნელოვანია აღინიშნოს, რომ ახალი კანონით გათვალისწინებული ადმინისტრაციული სამართალდარღვევებისთვის პასუხისმგებლობის ხანდაზმულობის ვადა 4 თვემდეა გაზრდილი ნაცვლად არსებული 3 თვისა, რაც ასევე მნიშვნელოვან პრევენციულ და სრულყოფილი ზედამხედველობის ხელშემწყობ ზომად შეიძლება მივიჩნიოთ.

ახალი კანონის მიხედვით, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება.

ისეთ შემთხვევებში, როცა ზეგავლენის შეფასების შედეგად გამოვლინდება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის მაღალი საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია მიიღოს ყველა აუცილებელი ზომა საფრთხეების არსებითად შესამცირებლად. ასევე, საჭიროების შემთხვევაში, იგი უფლებამოსილია კონსულტაციის მიზნით მიმართოს პერსონალურ მონაცემთა დაცვის სამსახურს. აღსანიშნავია, რომ თუ დამატებითი ორგანიზაციულ-ტექნიკური ზომებით შეუძლებელია ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხის არსებითად შემცირება, მონაცემთა დამუშავება არ უნდა განხორციელდეს.

ახალი კანონი საზედამხედველო ორგანოსთვის ინციდენტის შეტყობინების ვალდებულებას ითვალისწინებს, როდესაც ინციდენტი მნიშვნელოვან საფრთხეს უქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს. დამატებით უნდა აღვნიშნო, რომ ადამიანის ძირითადი უფლებებისა და თავისუფლებებისთვის მნიშვნელოვანი საფრთხის შემცველი ინციდენტის განსაზღვრის კრიტერიუმები და პერსონალურ მონაცემთა დაცვის სამსახურისთვის ამ ინციდენტის შეტყობინების წესი, ახალი კანონის მიხედვით, უნდა დადგინდეს პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ნორმატიული აქტით. უფრო მეტიც, ახალი კანონი ითვალისწინებს ინციდენტის შესახებ მონაცემთა სუბიექტის ინფორმირების ვალდებულებას.

„პერსონალურ მონაცემთა დაცვის შესახებ“ ახალი კანონის ძირითადი ნაწილი ამოქმედდება 2024 წლის 1 მარტიდან, ხოლო მონაცემთა დაცვის ოფიცრის ინსტიტუტი, მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულება და მათთან დაკავშირებული ადმინისტრაციული სამართალდარღვევების მარეგულირებელი ნორმები ძალაში შევა 2024 წლის 1 ივნისიდან.

ახალი კანონის იმპლემენტაცია არსებითად გააუმჯობესებს პერსონალურ მონაცემთა დამუშავების პროცესს. იგი ერთის მხრივ, შეამცირებს კანონის დარღვევის შემთხვევებს და შესაბამისად გაძლიერდება პრევენციული ეფექტი, ხოლო მეორეს მხრივ, პერსონალურ მონაცემთა დაცვის სამსახურს უფრო ეფექტური ზედამხედველობისა და რეაგირების შესაძლებლობას მისცემს.

ვემსახურებით პერსონალურ მონაცემთა დაცვის ევროპული იდეის, ღირებულებებისა და პრინციპების განხორციელებას საქართველოში!

ლელა ჯანაშვილი

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსი

ივ. ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის
ასოცირებული პროფესორი

ბარსელონის ავტონომიური უნივერსიტეტის მოწვეული პროფესორი

ლევან იოსელიანის მისასალმებელი წერილი

ძვირფასო მკითხველო,

მოხარული ვარ, რომ მეძლევა შესაძლებლობა მოგმართოთ პერსონალურ მონაცემთა დაცვის ჟურნალის ფარგლებში. როგორც საქართველოს სახალხო დამცველი მივესალმები და პოზიტიურად ვაფასებ პერსონალურ მონაცემთა დაცვის სამსახურის ინიციატივას ამ დარგში სამართლებრივი ჟურნალის გამოცემის თაობაზე.

თანამედროვე ტექნოლოგიების და ციფრული ტრანსფორმაციის ეპოქაში, როცა პროგრესი, ყოველდღიურად სხვადასხვა ფორმით, იქნება ეს კომპიუტერული პროგრამები, სოციალური ქსელები, აპლიკაციები თუ ხელოვნური ინტელექტი სულ უფრო მეტი დოზით იჭრება ჩვენს პირად სივრცეში, პერსონალური მონაცემების დამუშავების სამართლებრივ ასპექტებზე ცოცხალი დისკუსიის წარმართვა და დამატებითი ფორუმის შექმნა, რომლის ფარგლებშიც დარგის სპეციალისტებს თუ სამეცნიერო წრეების წარმომადგენლებს საშუალება მიეცემათ იმსჯელონ პირადი ცხოვრებისა და პერსონალური მონაცემების დაცვის თაობაზე, ნამდვილად ღირებულია.

ეს საჭიროება ასევე განპირობებულია იმითაც, რომ არც თუ ისე შორეულ წარსულში მონაცემთა დაცვის ძირითადი ევროპული რეგულაცია ამოქმედდა და საქართველოშიც შიდა ეროვნულ დონეზე ახალი საკანონმდებლო რეგულაცია იქნა მიღებული. ამ ყოველივემ საქართველოში კიდევ უფრო მეტად გახადა აუცილებელი მუდმივად მიმდინარეობდეს აკადემიური მსჯელობა და განხილვა პერსონალური მონაცემების დაცვის საკითხებზე, რაც სამართლის ამ დარგის განვითარებისათვის სასიცოცხლოდ მნიშვნელოვანია.

ამავე დროს აღსანიშნავია, რომ სახალხო დამცველი ბოლო წლებია საპარლამენტო ანგარიშებში აქტიურად მიუთითებს, რომ ქვეყანაში საჯარო ინფორმაციის ხელმისაწვდომობის კუთხით, დიდ გამოწვევად იქცა ღია ინფორმაციის პერსონალური მონაცემების შემცველობის საფუძვლით დახურვა და გასაჯაროების მიმართ არსებული საჯარო ინტერესების უგულებელყოფა, რაც პრობლემაა როგორც საჯარო ინფორმაციის მიღების მსურველი პირების, ისე საჯარო დაწესებულებებისათვის, მათი საქმიანობის ეფექტიანად წარმართვისთვის. ქვეყანაში ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და პერსონალური მონაცემების დაცვაზე საზედამხედველო ინსტიტუტის არსებობის პირობებში, თვალშისაცემია საჯარო ინფორმაციის ხელმისაწვდომობის უფლებასა და პირადი ცხოვრების უფლების დაცვის მექანიზმებს შორის არსებული დისბალანსი. ამასთანავე, სახალხო დამცვლის შეფასებით, ამდაგვარი ნეგატიური პრაქტიკა ძირითადად განპირობებულია მონაცემთა დამმუშავებელთა მხრიდან „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის არასწორი ინტერპრეტაციით. მაგალითად, სახელმწიფო დაწესებულებები უარს ამბობენ პერსონალური მონაცემების შემცველი ინფორმაციის გაცემაზე იმ საფუძვლით, რომ არ არის წარმოდგენილი შესაბამისი სუბიექტის თანხმობა. არ ექცევა ყურადღება იმ გარემოებას, რომ კანონმდებლობა იცნობს ასეთი ინფორმაციის გაცემის სხვა

საფუძვლებსაც, რომელიც საერთოდ არ არის დაკავშირებული მონაცემთა სუბიექტის მიერ თანხმობის გაცემასთან.

დარწმუნებული ვარ, პერსონალური მონაცემების დაცვის სამეცნიერო ჟურნალის პერიოდული გამოცემა და მასში პრობლემური საკითხების განმარტებების თუ აკადემიური შეფასებების ასახვა, პრაქტიკის სწორად განვითარებისათვის ძალიან ღირებული იქნება.

კიდევ ერთხელ მადლობას ვუხდი საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურს ამ ინიციატივისათვის და დარწმუნებული ვარ, რომ მსგავსი სამეცნიერო პროდუქტი ხელს შეუწყობს უფლების ეფექტურად დაცვას, სამართლის ამ დარგის განვითარებას და მის თაობაზე ცნობიერების ამაღლებას. ასევე ის გახდება ღირებული სამეცნიერო დისკუსიის ფორუმი.

ლევან იოსელიანი

საქართველოს სახალხო დამცველი

ლეონარდო სერვერა ნავასის მისასალმებელი წერილი

ძვირფასო მკითხველო,

ჩემთვის დიდი პატივია მივესალმო საქართველოს პერსონალურ მონაცემთა დაცვის სამსახურის შესანიშნავ აკადემიურ ინიციატივას - პერსონალურ მონაცემთა დაცვის სამართლის ჟურნალის მეორე ნომრის გამოცემას, რომლის მიზანია მონაცემთა დაცვის სფეროში საგანმანათლებლო წყაროების გამდიდრება და თავისი წვლილის შეტანა, ასევე მონაცემთა დაცვის კულტურის განვითარება.

ჩვენი ეპოქა ხასიათდება სწრაფად და მუდმივადგანვითარებადი ტექნოლოგიური მიღწევებითა და დიგიტალიზაციით, რაც თავის მხრივ იწვევს პერსონალურ მონაცემთა დამუშავების მოცულობის უპრეცედენტო ზრდას. ასეთი მიღწევების თანმხლები შესაძლებლობებიც და რისკებიც დიდ მნიშვნელობას იძენენ და ღირს თითოეული მათგანის დამსახურებისამებრ განხილვა.

ამიტომ, დღევანდელობა უკიდურესად აუცილებელს ხდის მონაცემთა დაცვის ორგანოებისთვის, რომ ერთი მხრივ, უფრო ღრმად გაიაზრონ პირადი ცხოვრებისა და მონაცემთა დაცვის სფეროში არსებული პრაქტიკული სამართლებრივი პრობლემები და მეორე მხრივ, აამაღლონ და გააძლიერონ საზოგადოებრივი ცნობიერება ამ თემებზე პირველი იმედისმომცემი გამოცემის შემდეგ, სადაც გაანალიზებული იყო ისეთი თემები, როგორიცაა მონაცემთა სუბიექტის უფლებები მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით, მონაცემთა დაცვის ოფიცრებისა და ხელოვნური ინტელექტის როლი. მე ღრმად ვარ დარწმუნებული, რომ ეს ჟურნალი კვლავაც იარსებებს როგორც პლატფორმა დისკუსიისთვის, რომელიც მოახერხებს და გასცდება საქართველოს გეოგრაფიულ საზღვრებს.

ისიამოვნეთ ამ გამოცემით, რომელიც, ვიმედოვნებ, თქვენთვის შთამაგონებელი იქნება.

ლეონარდო სერვერა ნავასი

ევროპის მონაცემთა დაცვის ზედამხედველის გენერალური მდივანი

ნორბერტ ბერნსდორფი*

ევროპის კავშირის „მონაცემთა დაცვის სამართალი“**

1. მონაცემთა დაცვა და ევროპის კომისიის 2022 წლის 17 ივნისის მოთხოვნები

ჩემი მოხსენება მინდა დავიწყო შეკითხვით: ევროპული კომისია - ევროკავშირის კომისია - გამოხატავს თუ არა უკმაყოფილებას საქართველოში მონაცემთა დაცვის დეფიციტთან დაკავშირებით? და თუ ეს ასეა, ეს დასაბუთებულია თუ მონაცემთა დაცვის კანონი უბრალოდ დახვეწას საჭიროებს?

2022 წლის 17 ივნისს ევროკავშირის კომისიის მიერ გამოთქმული მოსაზრება წინააღმდეგობრივია: კომისია მოითხოვს - პირველი, „პერსონალურ მონაცემთა დაცვის სერვისის ... აღჭურვას მისი მანდატის შესაბამისი რესურსებით“ და მეორე, „მისი ინსტიტუციური დამოუკიდებლობის უზრუნველყოფას, იგი ადგენს, რომ „პერსონალურ მონაცემთა დაცვის სამსახურმა... ჯერ კიდევ უნდა დაამტკიცოს თავისი ეფექტურობა და დამოუკიდებლობა“. სულ ეს არის მისი მოსაზრება.

ჩემს პირველ მოხსენებაში მე უკვე მივუთითე ე.წ. „კოპენჰაგენის კრიტერიუმზე“, რომელიც განმცხადებელმა ქვეყანამ უნდა შეასრულოს. ერთ-ერთი ამ კრიტერიუმებიდან არის “acquis criterion” („ევროკავშირის კანონმდებლობის კრიტერიუმი“ / ფრანგული სიტყვიდან “acquis communautaire”), რომლის მიხედვით კანდიდატმა სახელმწიფომ უნდა აღიაროს ევროკავშირის წესებისა და რეგულაციების მთელი ნაკრები, რაც გულისხმობს რამდენიმე 10 000 გვერდიანი იურიდიული ტექსტების ეროვნულ სამართალში ინტეგრირებას და დანერგვას შესაბამის ადმინისტრაციულ და სასამართლო სტრუქტურებში. ის, რასაც “acquis” მოიცავს ევროპული მონაცემთა დაცვის კანონის სფეროში, წარმოადგენს 2014 წლის ევროკავშირისა და საქართველოს შორის „ასოცირების ხელშეკრულების“ შედეგს. „ხელშეკრულების“ მე-14 და 327-ე მუხლის დანართში (I / XV-b) არის მითითება ევროსაბჭოს მონაცემთა დაცვის კანონზე და ახლა უკვე მოძველებულ - უკვე არა ვალიდურ - ევროკავშირის კანონზე, რაც იძლევა კიდევ ერთ მიზეზს, რომ დავაკვირდეთ ახლანდელ, სრულიად შეცვლილ სამართლებრივ სიტუაციას ევროკავშირში.

---

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე.

** პუბლიკაცია წარმოადგენს ავტორის მიერ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტისა და ადმინისტრაციულ მეცნიერებათა ინსტიტუტის თანამშრომლობით ჩატარებული საჯარო ლექციების ფარგლებში წარდგენილი მოხსენების ტექსტს. ღონისძიება ეძღვნებოდა ევროკავშირთან საქართველოს დაახლოებისა და ინტეგრაციის საკითხებს.

2. აღიარება, დანერგვა, აღსრულება

უპირველეს ყოვლისა, იმისათვის, რომ საკითხი გასაგები იყოს, საჭიროა მისი დაზუსტება: როცა კანდიდატმა ქვეყანამ უნდა აღიაროს ევროკავშირის წესების კრებული, როგორ ხდება აღნიშნული ტექნიკურად?

ევროკავშირს არ გააჩნია სამართლებრივი საშუალებები რომ მოახდინოს მისი კანონის ინტეგრირება კანდიდატი სახელმწიფოს ეროვნულ სამართალში. მსგავსად გაწევრიანებისა, ესეც ხდება კანდიდატი ქვეყნის სურვილით. ევროკავშირის კანონმდებლობაში ინტეგრირების სამი ეტაპი არსებობს: „აღიარება“, „დანერგვა“ და „აღსრულება“, რაც გულისხმობს „კანონის ცხოვრებაში გატარებას“. პირველი ორი ეტაპისათვის ასევე ფართოდ გამოიყენება ტერმინები „ტრანსპოზიცია“ - რაც გულისხმობს კანონის ტრანსფორმაციას და „გამოყენება“ - რაც ნიშნავს კანონისადმი დამორჩილებას. ევროკავშირის კანონმდებლობის ეროვნულ სამართალში ინტეგრაცია ჩვეულებრივი აპოლიტიკური პროცესია. აქ უფრო ნაკლები იქნება ე.წ. „ვეტოს უფლებით მოთამაშეები“, რადგან კანდიდატ ქვეყნებში პოლიტიკური დებატები ადრევე გაიმართა, კერძოდ, წევრობისათვის განაცხადის წარდგენამდე.

რას ნიშნავს ტერმინი „შესაბამისობა“ ამ კონტექსტში?

„შესაბამისობა“ ან „არაშესაბამისობა“ დაკავშირებულია ევროკავშირში გაწევრიანების შემდგომ ფაზასთან. აქ საუბარია იმაზე, თუ როგორ იცავს წევრი სახელმწიფო მის მიერ აღიარებულ ევროკავშირის კანონმდებლობას - სრულად თუ საერთოდ არ იცავს, მხოლოდ არასრულად თუ დაგვიანებით. ამის მონიტორინგი ხდება ევროკავშირის კომისიის და ევროკავშირის მართლმსაჯულების სასამართლოს (CJEU) მიერ. აქ საკვანძო სიტყვას წარმოადგენს: სამართალდარღვევათა საქმის წარმოება!

წარმოადგენს თუ არა „აღიარება“ და „ტრანსპოზიცია“ ევროკავშირის კანონმდებლობაში ინტეგრაციის პირველი ეტაპს?

დიახ! - ამის ტექნიკურ საშუალებას წარმოადგენს კანდიდატი ქვეყნის „გაწევრიანება“. ეს ხდება ევროკავშირში ყველა სხვა წევრ-სახელმწიფოს გაწევრიანების ხელშეკრულებით (საერთაშორისო სამართლის მიხედვით). გაწევრიანების თარიღიდან კანდიდატი ქვეყანა ევროკავშირის ყველა ხელშეკრულების მოქმედ ვერსიაში ხდება მხარე. ევროკავშირის ყველა კანონი, რომელიც მიღებულია ამ ხელშეკრულებების საფუძველზე გაწევრიანების თარიღამდე, ავტომატურად ხდება დამავალდებულებელი გაწევრიანების პროცესში მყოფი ქვეყნებისთვის. ევროკავშირის კანონმდებლობა უპირატესია ნებისმიერ ეროვნულ კანონმდებლობაზე. ეს ერთმნიშვნელოვნად არის აღიარებული გაწევრიანების ხელშეკრულებაში (საერთაშორისო სამართლის მიხედვით) კანდიდატი ქვეყნის მიერ.

რას ნიშნავს ეს ევროკავშირის მონაცემთა დაცვის სამართლისთვის? – გაწევრიანებით ესეც ასევე იქნება „ათვისებული“, როგორც პრიორიტეტული უფლება ეროვნულ სამართლებრივ სისტემაში!

ამ ლექციაში არ მინდა მონაცემთა დაცვის ქართული და ევროპული სამართლის ერთმანეთთან შედარება. ჩემი მიზანი არ არის წარმატებების ან წარუმატებლობის ძიება მომავალ „აღიარებასა“ თუ „ტრანსპოზიციაში“. არც შემიძლია ამის გაკეთება, რადგან არ მაქვს ე.წ. ანგარიში ჩატარებულ საქმიანობაზე - „ანგარიში ასოცირების პროცესის განხორციელების შესახებ“, რომელიც კეთდება ყოველწლიურად 2016 წლიდან. ეს ხდება ევროკავშირის კომისიის ან საქართველოს კომპეტენტური ორგანოების მიერ; მე კი არც ევროკავშირის თანამშრომელი ვარ და არც წევრ

სახელმწიფოს გერმანიის ოფიციალური წარმომადგენელი. ასეთი შედარების გაკეთება, ევროკავშირის კომისიის „ტექნიკური დახმარებისა და ინფორმაციის გაცვლის“ ჯგუფის (TAIEX) მოვალეობაა, რომელიც გასული წლიდან უნდა არსებობდეს საქართველოში.

რა არის ჩემი ამოცანა დღეს?

მინდა წარმოგიდგინოთ შემდეგი საკითხები:

- პირველი: ევროკავშირის ე.წ. პირველადი კანონმდებლობა და ე.წ. მეორეული კანონმდებლობა, და პირველ რიგში „მონაცემთა დაცვის ძირითადი რეგულაცია“;
- მეორე: ევროკავშირის მონაცემთა დაცვის კანონმდებლობაში არსებული კონფლიქტები;
- მესამე: ახალი სამართლებრივი ცვლილებები და
- მეოთხე: ევროპული კანონმდებლობის მოთხოვნები მონაცემთა დაცვის ეფექტურად კონტროლისადმი.

3. ევროკავშირის პირველადი კანონმდებლობა მონაცემთა დაცვის შესახებ

ევროკავშირის ყველა ქმედება ეფუძნება ევროპულ ხელშეკრულებებს. ამ ხელშეკრულებებში, რომლებიც წევრ სახელმწიფოებს შორის არის დადებული, განსაზღვრულია ევროკავშირის დაწესებულებების ამოცანები და წესები, ასევე გადაწყვეტილების მიღების პროცესი და ევროკავშირსა და მის წევრ-სახელმწიფოებს შორის ურთიერთდამოკიდებულება. ხელშეკრულებები წარმოადგენენ ევროკავშირის კანონმდებლობის საფუძველს და ეწოდებათ ევროკავშირის „პირველადი კანონმდებლობა“. კანონმდებლობას, რომელსაც საფუძვლად უდევს ამ ხელშეკრულებების ნორმები და ამოცანები ეწოდება „მეორეული კანონმდებლობა“ და მოიცავს რეგულაციებს, დირექტივებს, გადაწყვეტილებებს, რეკომენდაციებსა და მოსაზრებებს.

ა. პირველადი და მეორეული კანონმდებლობა

2009 წლიდან, როცა ლისაბონის ხელშეკრულება შევიდა ძალაში, მონაცემთა დაცვის სამართლებრივ ჩარჩოს ევროპული პირველადი კანონმდებლობისთვის წარმოადგენდა ევროკავშირის ქარტია ფუნდამენტური უფლებების შესახებ - ფუნდამენტური უფლებების ევროპული ქარტია, ამ შემთხვევაში მე-8 მუხლი. მიუხედავად იმისა, რომ პირველადი კანონმდებლობა ასევე შეიცავს 1981 წლის ადამიანთა უფლებების შესახებ ევროპული კონვენციისა და ევროპის საბჭოს კონვენციის მე-8 მუხლს, ჩემი მოხსენება ყურადღებას ამახვილებს ფუნდამენტური უფლებების ევროპული ქარტიის მე-8 მუხლზე.

იმისათვის რომ ჩემი ლექცია არ გახდეს არაკონტროლირებადი, შემოვიფარგლები მხოლოდ მონაცემთა დაცვის მეორეული კანონმდებლობის პრეზენტაციით. მიუხედავად იმისა, რომ ახლა ევროკავშირის უამრავი მეორეული რეგულაციები და დირექტივები არსებობს, მე მხოლოდ მონაცემთა ძირითად რეგულაციაზე გავამახვილებ ყურადღებას, რომელიც ძალაშია 2018 წლიდან. იგი წარმოადგენს პერსონალურ მონაცემთა დაცვის ძირითად სამართლებრივ ინსტიტუტს ევროპაში, და შედეგად მოიტანა რადიკალური ცვლილებები მონაცემთა დაცვის ევროკავშირის კანონმდებლობაში.

ბ. ფუნდამენტური უფლებების ევროპული ქარტიის მე-7 და მე-8 მუხლები

პერსონალური მონაცემთა დაცვა პირადი ცხოვრების დაცვის არსებითი ასპექტია. ეს უკანასკნელი რეგულირებულია ძირითადი უფლებების ევროპული ქარტიის მე-7 მუხლით და რადგანაც მას ასეთი დიდი მნიშვნელობა ენიჭება, ევროკავშირმა ცალკე სპეციალური დებულება მიუძღვნა მონაცემთა დაცვას - ამ შემთხვევაში ადამიანის უფლებების ევროპული კონვენციისგან განსხვავებული ფორმით, სახელდობრ, მე-8 მუხლით. მონაცემთა დაცვის ფუნდამენტური უფლება დაცული უნდა იყოს ევროკავშირის ინსტიტუციების, ორგანოებისა და სააგენტოების მიერ, აგრეთვე ევროკავშირის თითოეული წევრ-სახელმწიფოს მიერ ევროპული კანონმდებლობის განხორციელებისას.

რას ნიშნავს „ევროკავშირის კანონის დანერგვა“ ამ კონტექსტში?

უპირველეს ყოვლისა, უნდა აღინიშნოს, რომ ევროკავშირის წევრ-სახელმწიფოები არ არიან შებოჭილები ევროკავშირის ძირითადი უფლებებით, თუ ისინი ექსკლუზიურად იყენებენ თავიანთ ეროვნულ კანონმდებლობას. ამ შემთხვევაში ძალაშია ეროვნული ძირითადი უფლებები. საქმე სხვანაირად არის, როცა ევროკავშირის კანონის მაგალითად ევროპული დირექტივის გამოყენება ხდება. ესეც ევროკავშირის წევრ-სახელმწიფოების ეროვნული „საკანონმდებლო აქტების“ საშუალებით ხდება. თუმცა, ესენი მხოლოდ „შუალედური“ კანონებია და საბოლოოდ, ემსახურებიან ევროკავშირის სუვერენიტეტის „გაფართოებას“. ეროვნულმა სასამართლოებმა უნდა გამოიყენონ ევროპული ფუნდამენტური უფლებები ეროვნულთან ერთად. ეს რთული ჩანს, მაგრამ მარტივია, თუ ჩავუღრმავდებით.

გ. ძირითადი საფუძვლები

არ მინდა დიდხანს გესაუბროთ დოგმატურ ნიუანსებზე. ამიტომ, ამ ეტაპზე მხოლოდ რამდენიმე მინიშნება:

ფუნდამენტური უფლებების ევროპული ქარტიის მე-8 მუხლი წარმოადგენს სარჩელის ძალის მქონე უფლებას. მსგავსად ნებისმიერი კლასიკური ძირითადი უფლებისა, იგი უპირველეს ყოვლისა, წარმოადგენს სახელმწიფოსა და მისი ხელისუფლებისგან დაცვის უფლებას. თუმცა, მე-8 მუხლი ასევე ავალდებულებს კერძო პირებს უზრუნველყონ პერსონალურ მონაცემთა დაცვა. ამრიგად, მონაცემთა დაცვის ძირითად უფლებას ასევე აქვს ე.წ. მესამე მხარის ეფექტი.

მონაცემთა დაცვის სფერო, ძირითადი უფლებების ევროპული ქარტიის მე-8 მუხლი შეიცავს ფორმულირებებს დაცვის ფარგლების შესახებ და თუ როდის არის გამართლებული პერსონალურ მონაცემთა დაცვის უფლებაში ჩარევა; უფრო მეტიც, მე-8 მუხლი მოითხოვს „დამოუკიდებელი ორგანოს“ შექმნას მონაცემთა დაცვის კანონის შესრულების მონიტორინგის მიზნით. საკითხი იმის შესახებ, ფუნდამენტური უფლებების მფლობელები არიან თუ არა იურიდიული პირებიც, ჯერ არ არის გარკვეული ევროკავშირში.

მონაცემთა დაცვის ფუნდამენტურ უფლებას აქვს განსაკუთრებული თვისება - და ეს არის ბოლო რის თქმასაც ვაპირებ: იგი წარმოადგენს „შებრუნებულ ინჟინერიას!“ - გერმანიაში მას მოიხსენიებენ როგორც „ნორმატიულად შექმნილი“.

რას ნიშნავს ეს? - ეს ნიშნავს, რომ მონაცემთა დაცვის ძირითადი უფლება წინასწარ განსაზღვრულია ყველა დონეზე შესაბამისი მოქმედი ევროპული

მეორეული კანონმდებლობით - ამ შემთხვევაში მონაცემთა დაცვის ძირითადი რეგულაციით. მე-8 მუხლის შინაარსი, რომელიც წარმოადგენს ევროკავშირის პირველადი კანონმდებლობის ნაწილს, „ერთი ერთში“ ეფუძნება მეორეული კანონის შინაარსს, რომელიც ბევრად უფრო დაბალ ნორმატიულ დონეზეა. თუ შეიცვლება მეორეული კანონმდებლობა, ასევე შეიცვლება ძირითადი უფლებაც. ეს არის ის შედეგი, რაც სინამდვილეში არ არის შეთავსებადი ე.წ. ნორმატივების იერარქიის პრინციპთან.

რა არის ევროკავშირის მოტივაცია?

პერსონალურ მონაცემთა დამუშავების დარგი დინამიკურად ვითარდება. მისი მიზანი იყო მონაცემთა დაცვის ძირითადი უფლება „გაღებულიყო მომავლისთვის“. მეორეული სამართლის ამ პროცესებთან ადაპტირება უფრო სწრაფად და მარტივად არის შესაძლებელი, ვიდრე პირველადი სამართლის.

4. მეორეული სამართალი: მონაცემთა დაცვის ძირითადი რეგულაცია

2018 წლის მაისის შემდეგ, მონაცემთა დაცვის ძირითადი რეგულაცია - აბრევიატურით “GDPR” - ძალაშია მეორეული კანონმდებლობის დონეზე. მან ჩაანაცვლა ევროპული დირექტივა, ე.წ. მონაცემთა დაცვის დირექტივა (95/46/EC), რომელიც არსებობდა 1995 წლიდან.

ა. განსხვავება ევროკავშირის რეგულაციასა და ევროკავშირის დირექტივას შორის

თუ რა გავლენა აქვს ამას ევროპულ მონაცემთა დაცვაზე ცხადი ხდება მხოლოდ მაშინ, როცა ხედავ განსხვავებას ევროკავშირის რეგულაციასა და ევროკავშირის დირექტივას შორის:

დირექტივები შემოიფარგლებიან ევროკავშირის წევრი სახელმწიფოებისთვის მხოლოდ კონკრეტული შედეგის დადგენით. თუმცა, ამ შედეგების მიღწევა თვითონ წევრი სახელმწიფოების ვალდებულებაა. მათ უნდა მოახდინონ დირექტივების ტრანსფორმირება თავიანთი საკუთარი სამართლებრივი აქტების მეშვეობით კონკრეტულ ვადებში. ამისგან განსხვავებით, ევროკავშირის რეგულაციებს აქვთ პირდაპირი და მყისიერი დამავალდებულებელი ძალა ევროკავშირის ყველა წევრი სახელმწიფოსთვის, და არა მხოლოდ შედეგის მიღწევასთან მიმართებაში, დირექტივის მსგავსად.

რამ აიძულა ევროკავშირი, რომ ყოფილი მონაცემთა დაცვის დირექტივა ჩაენაცვლებინა რეგულაციით?

ყოფილი მონაცემთა დაცვის დირექტივის მიხედვით, ევროკავშირის ყველა წევრ-სახელმწიფო ეყრდნობოდა ერთსა და იმავე სამართლებრივ საფუძველს. თუმცა, მათ შეეძლოთ თვითონ გადაეწყვიტათ მონაცემთა დაცვის განხორციელება. შესაბამისად, ევროკავშირის ინდივიდუალურ წევრ სახელმწიფოებში არსებობდა მნიშვნელოვანი დისბალანსი მონაცემთა დაცვის დონესთან მიმართებით. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) დანერგვით, რომელსაც გააჩნია პირდაპირი და მყისიერი სამართლებრივად სავალდებულო ძალა ყველა წევრ სახელმწიფოში, უნდა აღმოიფხვრას ეს დისბალანსი.

ამასთან დაკავშირებით კიდევ ერთი შენიშვნა! - რადგანაც მე-8 მუხლით განსაზღვრულ მონაცემთა დაცვის ძირითადი უფლებას უფრო სრულყოფილს ხდის ძირითადი რეგულაციის (GDPR) მეორეული კანონი, რაზეც ეს-ესაა მოგახსენეთ,

რეგულაცია ამაღლდა ძირითადი უფლების ხარისხამდე. თუმცა ეს საკითხი სადავოა ევროპის სამართლებრივ დოგმატიკაში.

ბ. მონაცემთა დაცვის ძირითადი რეგულაციის პრინციპები და საკვანძო საკითხები

მინდა გაგაცნოთ მონაცემთა დაცვის ძირითადი რეგულაციის ზოგიერთი ძირითადი დებულება. არ ვამტკიცებ რომ ვიქნები ამომწურავი, თუმცა, უნდა გაირკვეს თუ მონაცემთა დაცვის რა დონისკენ ისწრაფვის ევროკავშირი 2018 წლის მაისიდან.

(1) ერთი მხრივ, არ უნდა შეიზღუდოს მონაცემთა დაცვა სარისკო საინფორმაციო პროცესებამდე

მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) არ ზღუდავს მის გამოყენებას მხოლოდ სარისკო საინფორმაციო პროცესებამდე, როგორიცაა „სკორინგი“ და ე.წ. „ხელოვნური ინტელექტის“ გამოყენება. პირიქით, იგი გამოიყენება ყველგან უნივერსალურად. და ეს სამართლიანია, რადგანაც საყოველთაო გამომთვლელმა ტექნიკამ გზა გაუკვალა „დიდ მონაცემებს“ ყველა დონეზე. სახელმწიფოსა თუ კერძო პირების ხელთ არსებული მონაცემთა დამუშავების ძალა იზრდება. თუმცა, ფიზიკურმა პირებმა უნდა შეინარჩუნონ კონტროლი საკუთარ მონაცემებზე და ამგვარად შეძლონ გამორიცხონ მესამე მხარის მიერ ამ მონაცემის მოპოვება და გამოყენება. მათ უნდა შეეძლოთ მოიპოვონ ინფორმაცია მათი პირადი მონაცემების შეგროვებასთან დაკავშირებით და შეძლონ მათი წაშლა. რადგანაც პერსონალური მონაცემების მოპოვება ყველგან არის შესაძლებელი, ასეთი მონაცემები დაცული უნდა იყოს არა მარტო კრიტიკულ სფეროებში არამედ ყოველდღიურ ცხოვრებაშიც.

(2) მეორე მხრივ: ეკონომიკური განვითარების არავითარი „შეფერხება“

ბოლო ხანებში, გერმანიის ფედერალური სახელმწიფოს მონაცემთა დაცვის კომისარი გადადგა თანამდებობიდან. იგი არის გერმანიის „თავისუფალი დემოკრატიული პარტიის წევრი“, რომელიც თავიდანვე წარმოადგენს ბიზნესისა და ეკონომიკის ინტერესებს. გადადგომის მიზეზად დაასახელა: „ევროპული მონაცემთა დაცვა ეწინააღმდეგება ბიზნესს. საერთაშორისო კონკურენციაში იგი ევროკავშირის ეკონომიკას არამომგებიან მდგომარეობაში აყენებს. მონაცემთა დაცვა ვერ ახერხებს აღიაროს რომ პერსონალურ მონაცემებსაც გააჩნიათ ეკონომიკური პოტენციალი, ეკონომიკური ღირებულება“.

აქ აუცილებელია ფართოდ გავრცელებული ცრურწმენის გაფანტვა!- მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) კი არ კრძალავს ეკონომიკაში მონაცემთა დაცვის გამოყენებას, არამედ იცავს მას. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) პირველი მუხლი ერთმნიშვნელოვნად იცავს „პერსონალურ მონაცემთა თავისუფალ გადაადგილებას“. აქედან გამომდინარე, მონაცემთა დაცვა არ შეიძლება იყოს მისი არც შეზღუდვის და არც სრულად აკრძალვის მიზეზი. ამიტომ, მონაცემთა დაცვა ეკონომიკაში არ არის აკრძალული; მან მხოლოდ უნდა დაიცვას დამუშავების ის პირობები, რომლებიც რეგულირებულია მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) მე-6 მუხლით. იმის უზრუნველსაყოფად, რომ ევროპულმა

მონაცემთა დაცვამ არ „ჩაახშოს“ ეკონომიკის დიგიტალიზაცია - „ფაილზე დაფუძნებული თუ ხელოვნური ინტელექტის აპლიკაციები“, ზედამხედველი ორგანოები და სასამართლოები ევროკავშირში მნიშვნელოვანი ამოცანის წინაშე დგანან: მონაცემთა დაცვაზე არც გადამეტებულად უნდა გამახვილდეს აქცენტი და არც უნდა „გახდეს აბსოლუტური“, არამედ აუცილებელია ეკონომიკური ინტერესების პერსონალურ მონაცემთა დაცვასთან სათანადო ბალანსირება.

აქტუალური მაგალითი: რადგანაც ამ მხრივ მონაცემთა დაცვა მიჩნეულია აბსოლუტურად, მართლმსაჯულების ევროპული სასამართლო კრძალავს ვიდეო კონფერენციის სისტემისათვის პროგრამული უზრუნველყოფის გამოყენებას თუ იგი შემოდის ევროპის გარედან - ამ კონკრეტულ შემთხვევაში, აშშ-დან: Zoom, Microsoft Teams, Cisco Webex, ა.შ. მაგრამ თუ არ არსებობს შესაბამისი ტექნიკური ალტერნატივა ევროპაში, მაშინ ევროპულ ეკონომიკისთვის ისინი საჭიროა.

(3) გამოყენების სფეროები, შექმნის პრინციპი, ბაზრის ადგილის პრინციპი, მონაცემთა გადატანა მესამე ქვეყნებში

სიტუაცია, რომელშიც GDPR გამოიყენება იმართება რეგულაციის მე-2 მუხლით. ეს ფართოდ უნდა იყოს გააზრებული; პრინციპში, ეს გამოყენებადობა ყოვლისმომცველია. GDPR სამართლებრივად დამავალდებულებელია როგორც საჯარო ისე არასაჯარო ორგანიზაციებისთვის და ასევე გულისხმობს კერძო მხარეებს; თუმცა, ეს არ ვრცელდება პოლიციის აქტივობებზე და კანონის ცხოვრებაში გატარებაზე. აქ გამოიყენება ცალკე, მაგრამ ანალოგიურად სტრუქტურირებული დირექტივა.

GDPR უშვებს მონაცემთა ავტომატურ დამუშავებას. ეს ფართოდ უნდა იყოს გააზრებული. ამ მხრივ, მე-2 მუხლი არის „ტექნოლოგიურად - ნეიტრალური“. იგი არ მოიცავს მონაცემთა ზუსტად ანალოგიურ შენახვას და წმინდად ხელით დამუშავებას - ინდექს ბარათებზე, დოკუმენტის ფორმებზე და ა.შ. გამონაკლისს წარმოადგენს მონაცემთა დამუშავება ოჯახურ გარემოში, რაზეც მონაცემთა დამუშავების ძირითადი კანონი არ ვრცელდება და ეწოდება საოჯახო პრივილეგია.

GDPR მხოლოდ ევროკავშირში გამოიყენება თუ მთელ მსოფლიოში, მონაცემთა საზღვრებს გარეთ მათი გლობალური გადინების გამო?

ჩვენს ონლაინ სამყაროში, პერსონალურ მონაცემთა დამუშავებამ არ იცის ტექნიკური საზღვრები. ამიტომ, GDPR -ს გამოყენება ტერიტორიულად შეზღუდული უნდა იყოს. რადგანაც ევროკავშირის ყველა წევრი სახელმწიფო ვალდებულია უზრუნველყოს მონაცემთა ერთი და იგივე დონით დაცვა, იგი, ბუნებრივია, გამოიყენება ევროკავშირის ტერიტორიაზე ყოველგვარი შეზღუდვის გარეშე. თუმცა, განსაკუთრებული სიფრთხილეა საჭირო მონაცემთა არა-ევროპული კომპანიების მიერ დამუშავების შემთხვევაში. ასევე ეჭვს იწვევს მონაცემების გადატანა ევროკავშირის გარეთ ქვეყნებში. იქ მონაცემთა დაცვის დონე ხშირად მნიშვნელოვნად დაბალია. GDPR ამ პრობლემებს გადაჭრის მე-3 მუხლში განსაზღვრული დაფუძნებისა და მოქმედების ტერიტორიული სფეროს პრინციპით. არაევროპული ქვეყნები, რომლებსაც წარმომადგენლობა ჰყავთ ევროკავშირის ტერიტორიაზე, ვალდებულნი არიან დაიცვან რეგულაცია, მაგრამ ამისათვის არ არის საკმარისი უბრალოდ საფოსტო ყუთი ევროკავშირში. თუ ასეთ კომპანიას არ ჰყავს წარმომადგენლობა ევროკავშირის ტერიტორიაზე, იგი მაინც ვალდებულია, დაიცვას GDPR, თუ იგი ფუნქციონირებს ევროკავშირის შიდა ბაზარზე. ამიტომ, Google and Facebook – Meta ექვემდებარებიან ევროპის მონაცემთა დაცვის კანონს.

რა ვუყოთ პერსონალ მონაცემთა ღრუბელს? არსებობს აქ „ამბრაზურა“? - არა! - ეს შემთხვევა დამოკიდებულია იმაზე, თუ სად მდებარეობს სერვერი.

თუ მონაცემები იმპორტირებულია მესამე ქვეყნებში, შესაფერისი დაცვის დონე უნდა იყოს უზრუნველყოფილი. მონაცემთა ევროკავშირის გარეთ დაცვა - ხანდახან მოიხსენიებენ როგორც „მონაცემთა დაცვის ოქროს სტანდარტი“ - ხშირად ვერ ხერხდება. GDPR-ის 45-ე მუხლის მიხედვით, ასეთი მონაცემების გადატანა ნებადართული უნდა იყოს ევროკავშირის კომისიის ე.წ. ადეკვატური გადაწყვეტილებით. მე მონაცემთა დაცვის ხელშეკრულებებს დავუბრუნდები აშშ-სთან ერთად მოგვიანებით.

(4) ძირითადი აკრძალვა ნებართვის, უფლებამოსილებისა და თანხმობის შენარჩუნებით

ევროპულ მონაცემთა დაცვის კანონზე ვრცელდება შემდეგი პრინციპები: ამოსავალ წერტილს წარმოადგენს ზოგადი აკრძალვა ნებართვის შენარჩუნებით.

რას ნიშნავს ეს? პერსონალურ მონაცემთა დამუშავება ზოგადად არის აკრძალული თუ იგი არ არის კანონით დაშვებული ან თუ მონაცემების მფლობელი - მონაცემთა სუბიექტი- წინასწარ იძლევა თავის თანხმობას. ევროკავშირი ამგვარად თანხმდება პრევენციულ მიდგომაზე, რითაც პერსონალურ მონაცემთა დაცვა ხდება უკიდურესად პრიორიტეტული.

GDPR-ს მე-6 მუხლი არეგულირებს, თუ როდის არის პერსონალურ მონაცემთა დაცვა ნებადართული. აქ არ მინდა სიღრმეებში შესვლა; ამიტომ, ძალიან მოკლედ! ხუთი საფუძველი არსებობს ნებართვის გაცემისთვის: მონაცემთა დაცვა კანონიერია, როცა ის დაკავშირებულია კონტრაქტის დადებასთან ან შესრულებასთან; თუმცა, საკონტრაქტო ურთიერთობის დასრულების შემდეგ, პერსონალური მონაცემები უნდა წაიშალოს. მონაცემთა დამუშავება ასევე შეიძლება მოხდეს, თუ მონაცემთა სუბიექტის სასიცოცხლოდ მნიშვნელოვანი ინტერესები ზარალდება, მაგალითად, პანდემია კორონას ან ბუნებრივი უბედურებების წინააღმდეგ ბრძოლის დროს. დამუშავება ასევე ნებადართულია მონაცემთა დამმუშავებელი პირის ლეგიტიმური ინტერესის არსებობის შემთხვევაში. ეს ის შემთხვევაა, როცა „მონაცემთა სუბიექტი“ დამმუშავებლის კლიენტია ბიზნესის საქმისწარმოებებში ან უბრალოდ დასაქმებულია მის მიერ. ასეთი კანონიერი ინტერესია, მაგალითად, „მონაცემთა სუბიექტის მიერ თაღლითობის ჩადენის პრევენცია.“ და ბოლოს, სახელმწიფო დავალებების შესრულება საკმარისი საფუძველია მონაცემთა დამუშავებისთვის. ამ მხრივ, ევროპული პრეცედენტული სამართალი ახლა პრაქტიკულად უმართავია.

როგორც ნებართვის მიცემის ალტერნატივა, მონაცემთა სუბიექტის თანხმობა შეიძლება გახდეს პერსონალურ მონაცემთა დამუშავების საფუძველი. აქაც მხოლოდ რამდენიმე შენიშვნა: თანხმობა უნდა იყოს ნებაყოფლობითი, და შესაბამისმა „მონაცემთა სუბიექტმა“ უნდა იცოდეს თავისი თანხმობის მნიშვნელობა. როგორც წესი, მცირეწლოვნებს 14 წლის ასაკამდე არ შეუძლიათ კანონიერი თანხმობის მიცემა. მონაცემთა დამუშავების შემდგომ გაცემული თანხმობა, რომელსაც „ავტორიზაცია“ ეწოდება იურიდიულ ტერმინოლოგიაში - არ არის საკმარისი დამუშავების გასამართლებლად.

(5) მონაცემთა კლასიფიკაცია

შესაძლებელია პერსონალური მონაცემების კლასიფიცირება. ზოგიერთი მონაცემის მოპოვება შესაძლებელია ზოგადად ხელმისაწვდომი წყაროებიდან - ტელეფონის და მისამართების წიგნიდან, ინტერნეტიდან, სხვა მონაცემების მიღება კი უფრო გართულებული გზით არის შესაძლებელი. ზოგი მონაცემები საჭიროა პიროვნების ინტეგრაციისათვის - ზოგი სენსიტიურია, ზოგი არა. უმეტეს შემთხვევაში, ზოგადად ხელმისაწვდომი და ნაკლებად სენსიტიური მონაცემები ნაკლებად მნიშვნელოვანია მონაცემთა სუბიექტის თვალსაზრისით. რადგანაც GDPR-ის მე-6 მუხლი არ ახდენს კლასიფიცირებას, რეგულაციის მე-9 მუხლი ითვალისწინებს კვალიფიცირებული მონაცემების უფრო საიმედო დაცვას, რომელიც მოიცავს, მაგალითად, ეთნიკურ წარმომავლობასთან, რელიგიურ და პოლიტიკურ რწმენასა, ასევე ჯანმრთელობისა და სექსუალურ ორიენტაციასთან დაკავშირებული მონაცემებს.

რას ითვალისწინებს ევროპული მონაცემთა დაცვა ე. წ. საჯარო პირებისთვის - პოლიტიკოსები, მოსამართლეები, მსახიობები, ა.შ.?

საზოგადოება დიდ ინტერესს ავლენს იმ პიროვნებების მიმართ, რომლებიც გამოჩენილები არიან, ანუ რომლებიც სარგებლობენ გარკვეული ხარისხის ცნობადობით. ე.წ. საზოგადოებრივ სფეროში საჯარო გამოჩენის ან საჯარო განცხადების გაკეთების შემთხვევაში ამ პიროვნებების მონაცემთა დაცვა შეზღუდულია. ამ სფეროში, პერსონალური მონაცემები შეიძლება შეგროვდეს, მაგ. ფოტოსურათების გადაღებით მათი თანხმობის გარეშე. საქმე ეხება ე.წ. პრივატულ ან ინტიმურ სფეროსაც კი შინაური სფერო და ოჯახი-, სადაც ისეთივე დაცვა არსებობს როგორც არაცნობადი პირებისთვის. მაშინ GDPR-ის მე-9 მუხლი გამოიყენება შეზღუდვების გარეშე.

(6) საინფორმაციო ვალდებულებები, წვდომის, შესწორების, წაშლის და დაბლოკვის უფლებები

როგორც სიახლე წინა სამართლებრივი სიტუაციასთან შედარებით, GDPR უზრუნველყოფს მონაცემთა მფლობელებისთვის მთელ რიგ უფლებებს მე-12 და მე-17 მუხლების მეშვეობით. მათი მიზანია დაცვის უფლების მოქმედებაში მოყვანის ხელშეწყობა მონაცემთა დაცვის კანონის მიხედვით. ეს იწყება ინფორმირების ვალდებულებით, რომელიც პერსონალურ მონაცემთა უფლებამოსილი პირის მოვალეობაა და რომელმაც ამგვარად უნდა „გახსნას“ დამუშავების „შავი ყუთი“. ეს ვრცელდება, პირველ რიგში, „მონაცემთა უსაფრთხოების დარღვევის“ ყველა შემთხვევაზე, როცა ხდება მონაცემთა არაკონტროლირებადი გადინება. დაცვის საშუალებები, რომლებიც „მონაცემთა სუბიექტისგან“ მოითხოვენ გამოიჩინონ ინიციატივა, არიან წვდომის უფლება და შესწორების უფლება მონაცემთა უფლებამოსილი პირთან მიმართებით.

განსაკუთრებით აღსანიშნავია მონაცემთა სუბიექტის უფლება საკუთარი მონაცემების წაშლასთან დაკავშირებით, რომელიც უზრუნველყოფილია GDPR-ის მე-17 მუხლით. ბოლო წლებში იგი ცნობილი გახდა როგორც „დავიწყების უფლება“. ევროპის მართლმსაჯულების სასამართლომ განმარტა ეს უფლება თავის ოთხ გადაწყვეტილებაში Google-ის წინააღმდეგ 2014 წლის შემდეგ. თუ არ წაიშლება პერსონალური მონაცემები ისინი უნდა დაიბლოკოს მომხმარებლისთვის.

(7) „წინასწარი“ მონაცემების დაცვა: მონაცემთა დაცვა „მომსახურების შექმნის პროცესში“ (by design) და „პირველად პარამეტრად“ (by default)

ევროპის მონაცემთა დაცვის კანონის ნოვატორული ინოვაციაა აგრეთვე ის, რომ დამმუშავებელმა უნდა მიიღოს პრევენციული ზომები და თავიდან აიცილოს „წინასწარ“ მონაცემთა უსაფრთხოების დარღვევა. დღემდე, ამ სფეროში ერთადერთი ხელმისაწვდომ იურიდიულ საშუალებას წარმოადგენდა რეგულაციები ე.წ. მონაცემთა ეკონომია ან მონაცემთა მინიმიზაცია. ახლა კი, პერსონალურ მონაცემთა ზომიერი გამოყენება უნდა განხორციელდეს ტექნიკური ან ორგანიზაციული სიფრთხილის ზომების გამოყენებით - „მომსახურების შექმნის პროცესში“ (by design) ან - სტანდარტული პარამეტრებით - „პირველად პარამეტრად“ (by default). პირველი სფერო შეიცავს, მაგალითად, ე.წ. „ფსევდონიმიზაციას“, მეორე სფერო კი ე.წ. ნიმუშებს. ამ პრინციპების დარღვევა ისჯება ჯარიმით.

გ. ექსკურსი: საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“

მომზადებისას, მე ძალიან სწრაფად და ზედაპირულად გადავხედე საქართველოს კანონს პერსონალური მონაცემების დაცვის შესახებ, რომელიც ვნახე პერსონალურ მონაცემთა დაცვის სამსახური მთავარ გვერდზე. მე ვფიქრობ, ეს ისევ აქტუალურია. ამისთვის 2016 წლის დეკემბერს კანონში მიღებული ბოლო ცვლილებებიდან, როგორც ჩანს, მოდელად გამოყენებულია ევროპული მონაცემთა დაცვის ყოფილი დირექტივა (95/46/EC). თუმცა, როგორც ეს განვიხილეთ, GDPR ახლა განსაზღვრავს ახალ პრიორიტეტებს. ორმა საკითხმა გამაოცა: ერთის მხრივ, ქართული კანონი მნიშვნელოვანი ხარისხით ათავისუფლებს მედიას მონაცემთა დაცვის კანონის გამოყენებისგან ჟურნალისტური მიზნებისთვის მონაცემების შეგროვებისას. მეორეს მხრივ, კანონი- როგორც მე წავიკითხე - ასევე ვრცელდება ანალოგიურ მონაცემთა დამუშავებაზე- „მონაცემთა დამუშავება არა-ავტომატური საშუალებებით“.

5. კონფლიქტების ახლანდელი სფეროები ევროპის კავშირში

როგორც უკვე აღვნიშნე ჩემს პრეზენტაციაში, პერსონალურ მონაცემთა დაცვის უფლება არ წარმოადგენს „სუპერ ფუნდამენტურ უფლებას“. მისი მინიჭება არ ხდება სრულფასოვნად, შეზღუდვებისა და პირობების გარეშე. მაგალითად, ის შესაძლოა წინააღმდეგობაში მოვიდეს ასევე დაცულ ინტერნეტ მომხმარებლების უფლებასა და მედია კომპანიების უფლებებთან ინფორმაციის მოპოვებასთან დაკავშირებით. მაგრამ იგი ასევე შეიძლება კონფლიქტში მოვიდეს ხელოვნების, მეცნიერების და კვლევის თავისუფლებებთან. ამას ხშირად „მულტიპოლარულ კონფლიქტს“ უწოდებენ. ამ შემთხვევებში, სხვადასხვა ინტერესები უნდა აიწონოს ერთმანეთის საპირწონედ და დაბალანსდეს: ე.წ. პრაქტიკული შესაბამისობა.

ა. მონაცემთა დაცვა და ინფორმაციის თავისუფლება - ინტერნეტის მომხმარებლები და მედია კომპანიები

ევროკავშირში ყოველთვის ემოციური დებატები იმართება მონაცემთა დაცვის კანონსა და ინფორმაციის თავისუფლებას შორის; ეს უკანასკნელი წარმოადგენს

გამოხატვის თავისუფლების მანიფესტაციას. ეს რატომაც ხდება ადვილი ასახსნელია: მონაცემთა სუბიექტს სურს შეინარჩუნოს კონტროლი თავის პერსონალურ მონაცემებზე. როგორც წესი, ინტერნეტის მომხმარებლებსა და მედია კომპანიებს ჩვეულებრივ უნდათ პირად ცხოვრებაში შეჭრა, რამდენადაც ეს შესაძლებელია.

შეკითხვა: შეიცავს GDPR ამ კონფლიქტის გადაჭრის გზებს?

დიახ! - თუმცა, ევროკავშირი თვითონ ვერ აბალანსებს ინტერესების კონფლიქტს. ნაცვლად ამისა, GDPR- ის 85-ე მუხლი ამას ავალებს ევროკავშირის წევრ-სახელმწიფოებს. მათ ამ მიზნით უნდა გამოსცენ საკანონმდებლო დებულებები. 85-ე მუხლი წარმოადგენს ე.წ. შესავალ პუნქტს, რომელიც სთავაზობს წევრ სახელმწიფოებს „მოქმედების თავისუფლებას“. თუმცა, GDPR ასევე იძლევა ერთ მითითებას: ზემოხსენებული დებულების მე-2 პარაგრაფი ავალდებულებს წევრ-სახელმწიფოებს მოახდინონ GDPR-ს „შესუსტება“ და მისგან „გათავისუფლება“ იმ შემთხვევაში, თუ მონაცემთა დამუშავება ემსახურება ჟურნალისტურ მიზნებს. ფონი: ასეთი „მედიის პრივილეგია“ იყო და ახლაც ფართოდაა გავრცელებული ევროკავშირის წევრ-სახელმწიფოების ეროვნულ კანონში

უბრალოდ ინტერესისთვის: რა ზომებს განიხილავენ წევრი სახელმწიფოები ამ შემთხვევაში?

ერთი საშუალება, მაგალითად, არის დაავალდებულო პლატფორმის ოპერატორები დააყენონ ფილტრაციის სისტემები - ე.წ. ფილტრების ჩატვირთვა. თუმცა, ჩატვირთული ფილტრების სისტემამ, რომელიც ძალიან მასშტაბურია და არ გააჩნია კონტურები და რასაც მივყავართ შინაარსის „ზედმეტად ბლოკირებამდე“, რაც არ წარმოადგენს პრობლემას მონაცემთა დაცვის კუთხით, შესაძლებელია დაარღვიოს ინფორმაციის თავისუფლება.

ბ. მონაცემთა შეკავების მუდმივი პრობლემა

საკითხს, რომელიც ამჟამად იპყრობს მედიის ყურადღებას, წარმოადგენს ე.წ. მონაცემთა შეკავება. ეს შეეხება ტელეკომუნიკაციის კომპანიების ვალდებულებას შეინახონ მომხმარებელთა მდებარეობისა და სერვისების მოძრაობის შესახებ მონაცემები კონკრეტული მიზეზის გარეშე და დიდ ხნის განმავლობაში. ამის მიზანია გაუადვილონ უსაფრთხოების ორგანოებს შეებრძოლონ სერიოზულ დანაშაულსა და საერთაშორისო ტერორიზმს.

ე.წ. მონაცემთა შეკავებამ უკვე შექმნა სამართლებრივი ისტორია: თავდაპირველად, ევროპულმა დირექტივამ მოითხოვა ევროკავშირის წევრ-სახელმწიფოებისგან წინასწარ შეინახონ მდებარეობისა და მოძრაობის მონაცემები. ევროპული მართლმსაჯულების სასამართლოს თავდაპირველი თავშეკავების შემდეგ დირექტივა გამოცხადდა არავალიდურად 2014 წელს. მიზეზი: დირექტივა არაპროპორციულად ზღუდავდა პერსონალურ მონაცემთა დაცვას.

მომდევნო პერიოდში მართლმსაჯულების ევროპულმა სასამართლომ ხელახლა განიხილა კანონები ე.წ. მონაცემთა შეკავების შესახებ. შედეგად, იგი დარჩა უცვლელი თავისი საწყისი პოზიციით, რომლის მიხედვით ასეთი შეკავება წარმოადგენს მონაცემთა დაცვის კანონის არაპროპორციულ ხელყოფას. მიუხედავად ამისა, ევროკავშირის წევრი სახელმწიფოები გამუდმებით გამოსცემდნენ რეგულაციებს ე.წ. მონაცემთა შეკავების შესახებ. მთლიანობაში, ევროპულმა მართლმსაჯულების სასამართლომ შვიდი გადაწყვეტილება გამოიტანა გერმანიის, ესტონეთის, საფრანგეთის, ირლანდიის, ავსტრიის და შვედეთის წინააღმდეგ ბოლო ათი წლის განმავლობაში. პოლიტიკურ არენაზე, ახლა განიხილება ე.წ. მონაცემთა

შეკავების საკითხი: ე.წ. სისტემაში შესვლის მახე და ე.წ. „სწრაფი გაყინვის“ პროცედურა. ე.წ. სისტემაში შესვლის (login) მახე იძლევა კრიმინალების IP მისამართების ავტომატური შენახვის საშუალებას მასიური მეთვალყურეობის ჩატარების გარეშე. ე.წ. „სწრაფი გაყინვის“ პროცედურის საშუალებით უსაფრთხოების ორგანოებს შეუძლიათ გაყინონ მდებარეობისა და მოძრაობის შესახებ მონაცემები პროვაიდერთან. ისინი შემდგომში შეძლებენ მიიღონ მათზე წვდომა სასამართლოს გადაწყვეტილებით

გ. ხელოვნური ინტელექტის გამოყენება: ChatGPT

ე.წ. ხელოვნური ინტელექტის გამოყენება პრინციპში არ არის რეგულაციის საგანი GDPR-ის მიხედვით. მიუხედავად ამისა, მან შესაძლოა პრობლემები წარმოშვას მონაცემთა დაცვის კანონის მხრივ.

ერთ-ერთ მაგალითს წარმოადგენს ტექსტ რობოტი "ChatGPT"; “GPT" ნიშნავს „გენერაციულ წინასწარ მომზადებულ ტრანსფორმერს“. იგი ბაზარზეა უკვე 2022 წლის ნოემბრიდან და ამჟამად იპყრობს დიდ ყურადღებას მთელ მსოფლიოში. იმისათვის, რომ მოხდეს მისი კლასიფიცირება მონაცემთა დაცვის კუთხით, საჭიროა ცოდნა იმისა თუ როგორ მუშაობს: "ChatGPT" უნდა შეიმუშაოს ტექსტები მომხმარებლის შენატანის საფუძველზე. ეს დამოკიდებულია ე.წ. ხელოვნურ ინტელექტზე, რომელიც უზარმაზარ მონაცემებზეა მომზადებული. ინდივიდუალურ მომხმარებელს მართლაც შეუძლია დაიცვას თავისი პერსონალური მონაცემები, თუ არ შეიყვანს მათ პროგრამაში. თუმცა, მთავარი მონაცემთა დაცვის პრობლემა სხვაგანაა. ის დაკავშირებულია ტექსტ რობოტის მონაცემთა ბაზაზე. არსებობს რისკი რომ მოსამზადებელი მასალა ასევე შეიცავს პერსონალური ხასიათის მონაცემებს. ეჭვის შემთხვევაში მათმა დამუშავებამ შეიძლება გამოიწვიოს მონაცემთა უსაფრთხოების დარღვევა რაზეც პასუხისმგებლობა ეკისრება მომხმარებელს. GDPR-ით გათვალისწინებული ჯარიმები მაღალია.

დ. პერსონალურ მონაცემთა გადატანა პორტირება (გადატანა) აშშ-ში

მონაცემთა ტრანსსასაზღვრო პორტირება მესამე ქვეყანაში ვაჭრობისა და ბიზნესისთვის აუცილებელია, მაგრამ რისკის ქვეშ აყენებს მონაცემთა დაცვას. GDPR -ის 45-ე მუხლის მიხედვით, ასეთი მონაცემთა გადატანა მოითხოვს ევროკავშირის კომისიის მიერ ე.წ. ადეკვატური გადაწყვეტილების მიღებას. ეს ასევე ეხება მონაცემთა პორტირებას აშშ-ში.

„ედვარდ სნოუდენის“ საქმისა და აშშ დაზვერვის სამსახურების მიერ მასზე განხორციელებული მეთვალყურეობის შემდეგ ამერიკული მონაცემთა დაცვისადმი ნდობა ევროკავშირში მეტ-ნაკლებად დაიკარგა. ევროკავშირის მოქალაქეები ასევე შეიძლება აღმოჩნდნენ მეთვალყურეობის ქვეშ აშშ-ში, მაგალითად, როცა ისინი აგზავნიან შეტყობინებებს ამერიკული Facebook ქსელის- Meta მეშვეობით.

2000 წელს, ევროკავშირის კომისიამ გააფორმა მონაცემთა დაცვის ხელშეკრულება აშშ-თან, რომელსაც ეწოდება „უსაფრთხო ნავსადგური“ (Safe Harbour). იგი არეგულირებდა მონაცემთა დაცვის კანონის შესრულებას, რომელიც მოეთხოვებოდათ ამერიკულ კომპანიებს და გამიზნული იყო აშშ-ში მონაცემთა დაცვის დონის ევროპულამდე აწევაზე. ხუთი წლის შემდეგ, ევროპის მართლმსაჯულების სასამართლომ გამოაცხადა ეს შეთანხმება -„უსაფრთხო

ნავსადგური“ ძალადაკარგულად. სასამართლომ მიუთითა კანონზე USA PATRIOT, რომელიც საშუალებას აძლევდა ამერიკულ დაზვერვის სამსახურებს ჰქონოდათ წვდომა პერსონალურ მონაცემებზე მონაცემთა სუბიექტის თანხმობის გარეშე.

შემდეგ წელს კი, მოლაპარაკება გაიმართა ახალ შეთანხმებაზე აშშ-სთან, „EU-US Privacy Shield“ (შეთანხმება ევროკავშირსა და აშშ შორის „პირადი ცხოვრების ფარი“). მიუხედავად იმისა რომ იგი უზრუნველყოფდა მონაცემთა დაცვის სრულყოფას, მაინც არ იყო საკმარისი ევროპული სასამართლოსთვის. 2020 წელს, სასამართლომ ასევე მიიჩნია ეს ხელშეკრულება და ევროკავშირის კომისიის ე.წ. ადეკვატური გადაწყვეტილება არაკანონიერად. გასაგებია ეს რასაც ნიშნავს: ამჟამად, მონაცემთა დაცვის კანონის შესაბამისად, ჯერ კიდევ არაკანონიერია გარკვეული პერსონალურ მონაცემთა პორტირება ევროკავშირიდან აშშ-ში. ცნობისათვის, ამჟამად ევროკავშირის კომისია ევროკავშირ-აშშ მონაცემთა დაცვის მესამე ხელშეკრულების დამუშავების პროცესშია.

6. მონაცემთა დაცვის კანონის მომავალი განვითარება - ევროპული კომისიის რეგულაციური გააფთრება

ახლა მინდა რამდენიმე სიტყვა გითხრათ სამართლებრივ განვითარების შესახებ ევროკავშირში!

მონაცემები ყველგანაა და სუნთქვაშემკვრელი ტემპით იზრდება. მასთან ასოცირებულ სარგებლობას ბიზნესისთვის, მეცნიერებისა და ადმინისტრირებისთვის ეიფორიულად მიესალმებიან. მონაცემები გახდა საკვანძო უპირატესობა ეკონომიკისთვის. ამავე დროს, ჩივიან ასევე პერსონალურ მონაცემთა დაცვის ნაკლზეც, რაც არის მონაცემთა თავისუფალი გადინების შედეგი. ზოგჯერ ორივე შეხედულება ცალსახად ურთიერთსაწინააღმდეგოა. თუმცა, თანხმდებიან იმაზე, რომ ევროპას ჭირდება სამართლებრივი ბაზა, რომელიც სცილდება მონაცემთა დაცვის ძირითადი რეგულაციის ფარგლებს.

2020 წლიდან ევროკავშირის კომისია მუშაობს ე.წ. ევროპულ სტრატეგიაზე მონაცემების კუთხით; ამით, მას სურს უზრუნველყოს, რომ მონაცემთა ერთიანი ბაზარი რაც შეიძლება თავისუფალი იყოს ევროკავშირის ეკონომიკისა და მისი გლობალური კონკურენტუნარიანობის ინტერესებიდან გამომდინარე. ამ მხრივ, მან წამოაყენა წინადადებები ოთხი ევროპული რეგულაციის შესახებ: პირველი, „მონაცემთა მართვის კანონი“, რომლითაც სურს შექმნას „მონაცემთა შუამავალი სერვისის პროვაიდერი“, რომელიც, როგორც ნეიტრალური ორგანო და რომელსაც არ გააჩნია ეკონომიკური თვით-ინტერესები, შეაგროვებს მონაცემებს და, თუ დააკმაყოფილებს გარკვეულ სამართლებრივ მოთხოვნებს, მიაწოდებს მათ დაინტერესებულ მხარეებს. ამ პრინციპს ეწოდება „მონაცემთა ალტრუიზმი“. ამ გზით, მას სურს შეზღუდოს მონაცემთა მონოპოლისტების როგორიცაა Apple, Amazon, Facebook – Meta და Google-ს ძალაუფლება. მეორე წინადადება, როგორიცაა „მონაცემთა კანონი“ უფრო შორს მიდის: მან უნდა დაარეგულიროს თუ ვის ეკუთვნის მონაცემები რომლებსაც აწარმოებენ თვითონ ქსელური მოწყობილობების მომხმარებლები, როგორიცაა სამეთვალყურეო (CCTV) სისტემები ან ავტონომიური მანქანები. ჯერჯერობით, მხოლოდ ასეთი სისტემების პროვაიდერებს აქვს მათზე წვდომა და არა მომხმარებლებს.

მაგრამ ევროკავშირის კომისია ამას ასე არ ტოვებს!

იგეგმება, რომ „ციფრული მომსახურების კანონი“, რომელიც მიზნად ისახავს ონლაინ პლატფორმების რეგულირებას და მიმართულია ინტერნეტ პროვაიდერების,

ღრუბლის სერვისების, აპლიკაციის მარაგების და სოციალური მედიისკენ. ასეთმა კომპანიებმა უნდა მიიღონ ზომები რომ აღმოაჩინონ და მოსპონ არაკანონიერი პროდუქტი და შინაარსი ადრეული საფეხურიდანვე. კანონის დამრღვევებს მოუწევთ ჯარიმის გადახდა რაც შეადგენს წლიური ბრუნვის 6 პროცენტს. ბოლოს, “ციფრული ბაზრის კანონი“ მომზადების პროცესშია. ის გამიზნულია მხოლოდ დიდი „კარის მცველებისკენ“: Apple, Amazon, Facebook - Meta, Google and Microsoft. ამის მიხედვით, მესენჯერის სერვისების პროვაიდერები და სოციალური მედია ვალდებულნი არიან შემოგვთავაზონ ე.წ. თავსებადი სერვისები. WhatsApp-ის მესიჯები მაშინ მიღებულ უნდა იყოს “Threemo-Messenger” და “Signal”-ის საშუალებით. Apple-ს მსგავს კომპანიებსაც უნდა ჰქონდეთ წვდომა სხვა აპლიკაციების მარაგზე (app stores). მე არ ვაპირებ უფრო შორს წასვლას ამასთან დაკავშირებით. ზოგიერთი ასეთი რეგულაცია უკვე შევიდა ძალაში.

რადგანაც მონაცემთა დამცველებმა უკვე აღარ იციან ევროკომისიის ინიციატივების ციფრულ ჯუნგლებში სად არის „ზემოთ“ და სად „ქვემოთ“, ისინი მოუწოდებენ მონაცემთა დაცვის ახალი, უფრო ეფექტური საშუალებებისაკენ. ერთ-ერთი ასეთი ინსტრუმენტია „მონაცემთა დაცვის რეჟიმის“ შექმნა. როგორც საკუთრების ფლობა, ამან უნდა დაარეგულიროს ვის აქვს უფლებამოსილება განკარგოს და გამოიყენოს პერსონალური მონაცემები. შედარებები კეთდება საავტორო უფლების კანონთან. შეუძლიათ ხალხს გაყიდონ ან გადაიტანონ თავისი მონაცემები? - კიდევ ერთი მიზანი გამომდინარეობს „ევროპის კავშირის ფუნდამენტური ციფრული უფლებების ქარტიიდან“, რომელიც შემოთავაზებულია მონაცემთა დაცვის ექსპერტების მიერ. იგი მიზნად ისახავს ფუნდამენტური უფლებების ევროპული კანონის შევსებას მე-8 მუხლი და პერსონალურ მონაცემთა უკეთესად დაცვას სპეციალური ფუნდამენტური უფლების მეშვეობით. რევოლუციური კონცეფციაა!

7. მონაცემთა დაცვის კონტროლი - „მონაცემთა დაცვის კანონთან შესაბამისობა“ და გარე სამეთვალყურეო ორგანოები

მონაცემთა ეფექტურ დაცვას მონიტორინგი ჭირდება. ვერც ერთი უფლება ვერ იქნება ეფექტური თუ არ არსებობს მისი დაცვის კონტროლი. პერსონალურ მონაცემთა დაცვის უფლება განსაკუთრებით სენსიტიურია, რადგანაც ინდივიდუალური დარღვევები ხშირად შეუმჩნეველი რჩება. მონაცემთა დაცვის კონტროლმა ეს უნდა გაითვალისწინოს.

როგორ განიხილება ეს საკითხი ევროკავშირის კანონში?

თუ გადავხედავთ საწყისს კანონს, ანუ ფუნდამენტური უფლებების ევროპულ ქარტიას, პასუხს ვერ მივიღებთ. მონაცემთა დაცვის ფუნდამენტური უფლების მე-3 პარაგრაფი ნამდვილად მოითხოვს „დამოუკიდებელი ორგანოს“ დაფუძნებას პერსონალური მონაცემების დაცვის შესრულების მონიტორინგისათვის. თუმცა, ამ მოთხოვნის სამართლებრივი მნიშვნელობა საკამათოა ევროკავშირში. მხოლოდ რამდენიმე ექსპერტი უყურებს მას როგორც ნამდვილ ინსტიტუციურ გარანტიას.

ამ შემთხვევაში GDPR უფრო დეტალურია. იგი „ორმხრივია“ და სისტემურად განასხვავებს ერთმანეთისგან „შინაგან კონტროლს“ და „გარეგან კონტროლს“. ამის მიხედვით, მონიტორინგის ჩატარება თავდაპირველად ევალებოდა მონაცემთა უფლებამოსილ პირს, ორგანოებს და კომპანიებს. GDPR-ის 37-ე მუხლის მიხედვით, ისინი ვალდებულნი არიან დანიშნონ მონაცემთა დაცვის ოფიცერი, რომელიც

დამოუკიდებელია საზედამხედველო ორგანოებსა და კომპანიების ფარგლებში. მართალია, მონაცემთა დაცვის ოფიცერს არ მოეთხოვება ორგანოებისა და კომპანიების მნიშვნელოვან გადაწყვეტილებებში მონაწილეობის მიღება, მაგრამ მას აქვს თავისუფალი წვდომა ყველა დამუშავების ოპერაციაზე და ჩართულია მათთან დაკავშირებულ გადაწყვეტილებებში. საინტერესოა აღვნიშნოთ, რომ ასეთი ვალდებულება „მონაცემთა დაცვის უზრუნველყოფისათვის“ არ არსებობდა მონაცემთა დაცვის დირექტივის კანონის(95/46/EC) მიხედვით, რომელიც ძალაში იყო 2018 წლამდე.

შეუძლია ევროპულ კანონმდებლობას ყველაფერი დატოვოს უბრალო თვითრეგულაციის დონეზე?

პასუხია: არა! - ასეთი მონაცემთა დაცვის ოფიცრების მიერ შინაგანი კონტროლის განხორციელებას მართლაც აქვს აზრი; რადგანაც ისინი კარგად იცნობენ თავიანთი ორგანოებისა თუ კომპანიების პროცესებსა და სტრუქტურას და ამიტომ შეუძლიათ ეფექტურად განახორციელონ სისტემატური და რეგულარული კონტროლი. თუმცა, ასეთი შინაგანი კონტროლები ასევე ხასიათდებიან როგორც იერარქიული და დამოკიდებული ურთიერთობები. ამიტომ, GDPR ასევე ეყრდნობა „გარეგანი კონტროლის“ კონცეფციას, რომელსაც მონაცემთა დაცვის გარეგანი სამეთვალყურეო ორგანოები განახორციელებენ.

რისი ცოდნა არის საჭირო ამ „გარეგანი კონტროლის“ შესახებ ევროკავშირის წევრ-სახელმწიფოების დონეზე? - მე მხოლოდ მოკლედ გადმოგცემთ მონაცემთა დაცვის სამეთვალყურეო სისტემის შესახებ მონაცემთა დაცვის ძირითად რეგულაციაში:

GDPR-ის 51-ე მუხლი ითვალისწინებს დამოუკიდებელი საზედამხედველო ორგანოების არსებობას. „დამოუკიდებელი“ ნიშნავს „სრულიად დამოუკიდებელს“. ევროპის მართლმსაჯულების სასამართლოს აზრით, ეს ნიშნავს რომ მონაცემთა დაცვის საზედამხედველო ორგანო შორს უნდა იყოს მთავრობისგან, რაც გულისხმობს რომ საზედამხედველო ორგანო არ უნდა ექვემდებარებოდეს სამინისტროს. „მედია პრივილეგიის“ გამო საზედამხედველო ორგანოების აქტივობებისგან გამონაკლისს წარმოადგენს მედია, ასევე ეკლესიები და, GDPR-ის 55-ე მუხლის მიხედვით, სასამართლოები. ფონი: ეს ხდება სასამართლო სისტემის დამოუკიდებლობის უზრუნველყოფისათვის. მონაცემთა დაცვის ორგანოების ძირითადი ამოცანაა კლასიკური საზედამხედველო მოქმედება, რითაც შესაძლებელია 10 მილიონ ევრომდე ჯარიმის დაკისრება. სამეთვალყურეო ორგანოები სააპელაციო ორგანოებსაც წარმოადგენენ. მათი გადაწყვეტილებები შეიძლება გასაჩივრდეს სასამართლოებში

ჩემი მოხსენების დასკვნის სახით, შემდეგ ხუმრობას მოგახსენებთ: კარგად არის ცნობილი, რომ მასიურად „კონტროლის დეფიციტია“ მონაცემთა დაცვის კანონში ევროკავშირის ყველა წევრ სახელმწიფოში. ახლახან, ვიღაცამ გამოითვალა, რომ გერმანიაში აღნიშნული საკითხების მონაცემთა დაცვის საზედამხედველო ორგანოს მიერ განხილვას მოელიან ყოველ 200 წელიწადში ერთხელ (!)

გერგელი ბარაბასი*

საზედამხედველო ორგანოს უფლებამოსილების ევოლუცია და რევოლუცია უნგრეთში „მონაცემთა დაცვის ძირითადი რეგულაციის“ (GDPR) გათვალისწინებით

მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) პერსონალურ მონაცემთა დაცვის ევროპულ სამართალში „თამაშის წესებს“ ცვლის. მისი დამსახურებით რევოლუციური ცვლილებები განხორციელდა საზედამხედველო ორგანოების მასშტაბური გარდაქმნისთვის, პროცედურული და სასამართლო სისტემასთან ურთიერთობის თვალსაზრისით. GDPR-მა მკვეთრად გაზარდა კონფიდენციალობის შესახებ ცნობიერება სხვადასხვა ორგანიზაციაში და ამ რადიკალურმა გარღვევამ ასახვა ჰპოვა მონაცემთა სუბიექტების, დამმუშავებელი ორგანიზაციების და სასამართლოების შეხედულებებსა და ქცევებში მონაცემთა დაცვის მნიშვნელობასთან დაკავშირებით.

უნგრეთის პერსონალურ მონაცემთა დაცვის სამართალი განვითარდა არსებითი, პროცედურული და საორგანიზაციო ცვლილებების შედეგად. გამოიკვეთა ცალსახა მიმართულება, სადაც მონაცემთა ბაზაზე დაფუძნებული სერვისების გაზრდა მოითხოვს პერსონალური მონაცემების დაცვის ძლიერ და ეფექტიან უფლებამოსილებებს. უნგრეთში მონაცემთა დაცვის კანონის შემუშავებამ ორგანიზაციული და პროცედურული სამართლებრივი ბაზა შეუქმნა ადმინისტრაციული ტიპის მოდელს, მაკორექტირებელი უფლებამოსილების ეფექტური ინსტრუმენტების შექმნის გზით. ამ პროცესში ადმინისტრაციული მართლმსაჯულების როლი გამოიხატება ადმინისტრაციული სასამართლოების მიერ მონაცემთა დაცვის კანონმდებლობის ინტერპრეტაციაში. საკითხი ჯერ კიდევ არ არის დასრულებული და ის საწყისი მოქმედებების ეტაპზეა. კვლევის მიზანია უნგრეთში, გასული 30 წლის განმავლობაში განხორციელებული ცვლილებების წარმოდგენა, განსაკუთრებით მონაცემთა დაცვის

* იურიდიული მრჩეველი, იურიდიული დეპარტამენტის უფროსი, უნგრეთის მონაცემთა დაცვისა და ინფორმაციის თავისუფლების ეროვნული საზედამხედველო ორგანო.

ერთიანი ევროპული რეგულაციის გავლენის გათვალისწინებით. ნაშრომი წარმოაჩენს, თუ რა გავლენა მოახდინა GDPR-მა საზედამხედველო ორგანოს უფლებამოსილებებზე.

საკვანძო სიტყვები: *მონაცემთა დაცვა, ადმინისტრაციული ორგანო, საზედამხედველო ორგანო, ადმინისტრაციული სამართალი, სასამართლო განხილვა, GDPR, მაკორექტირებელი უფლებამოსილება, მონაცემთა დაცვის ადმინისტრაციული წარმოება მონაცემთა სუბიექტის მოთხოვნით, მონაცემთა დაცვის ადმინისტრაციული წარმოება ex officio, დროებითი მაკორექტირებელი უფლებამოსილებები.*

„მათ შეუძლიათ იპოვონ როდის, რა, რატომ და ვის დავურეკე.
ისინი ფაილებში წერენ რაზეც მე ვოცნებობ, და აგრეთვე, ვისაც ესმის ჩემი ოცნება.
და მე ვერ ვხვდები როდის მომეცემა მიზეზი მოვძებნო ის ფაილი, რომელიც არღვევს ჩემს უფლებებს […]
ჩემი ხელმძღვანელი მაკონტროლებს შინაგანად!
ჩვენ ადამიანები ვართ და არა მხეცები -
ჩვენ ვართ გონებები! ჩვენი გულები, სანამ გვაქვს სურვილი,
და არა მონაცემები ფაილში.
მოდი, თავისუფლებავ! შენ დაამყარებ ჩემთვის წესრიგს,
მასწავლე ლამაზი სიტყვებით, ოღონდ ნება დართე მანაც ითამაშოს,
შენი სიმპათიური, სერიოზული ვაჟი!“

იოზეფ ატილა [**] ***/ „მე არ შემიძლია სუნთქვა“ / 1935***

1. შესავალი

უნგრეთში მონაცემთა დაცვისა და ინფორმაციის თავისუფლების ეროვნული საზედამხედველო ორგანო (შემდგომში „ორგანო“ ან “NAIH”) პასუხისმგებელია ორი ფუნდამენტური უფლების დაცვის უზრუნველყოფის მონიტორინგსა და ხელშეწყობაზე: პერსონალურ მონაცემთა დაცვის უფლება და ინფორმაციის თავისუფლების უფლება (წვდომა საზოგადოებრივი ინტერესის მატარებელ მონაცემებზე და საჯარო ინტერესების გამო ხელმისაწვდომ მონაცემებზე). „ორგანოს“ უფლებამოსილება აქვს დაიწყოს კლასიფიცირებული ინფორმაციის ზედამხედველობის პროცედურა, რათა დაადგინოს იგი არის თუ არა კანონიერი.

საკონსტიტუციო დებულების საფუძველზე, 2011 წლის CXII კანონმა „ინფორმაციული თვითგამორკვევისა და ინფორმაციის თავისუფლების უფლებების შესახებ“ (შემდგომში 2011 წლის CXII კანონი), რომელიც ძალაში შევიდა 2012 წლის

[**] იოზეფ ატილა (1097-1937), მე-20 საუკუნის ერთ-ერთი ყველაზე ცნობილი უნგრელი პოეტი. სიცოცხლეში არ იყო აღიარებული და მოგვიანებით საერთაშორისოდ ცნობილი უნგრელი პოეტი გახდა.

პირველ იანვარს, შექმნა „ორგანო“ და დეტალურად დაადგინა ფუნქციონირების წესები. ორგანიზაციული თვალსაზრისით, NAIH წარმოადგენს ავტონომიურ სახელმწიფო ადმინისტრაციულ ორგანოს. იგი არ არის ვალდებული მიიღოს ინსტრუქციები თავის ფუნქციებთან დაკავშირებით და უნდა იმოქმედოს სხვა ორგანიზაციებისგან და არასათანადო ზემოქმედებისგან დამოუკიდებლად. „ორგანოს“ ვალდებულებები უნდა განისაზღვროს მხოლოდ პარლამენტის კანონით, თუმცა, ორგანიზაციული და პროცედურული თვალსაზრისით, ყოველთვის ასე არ ყოფილა.

უნგრეთში მონაცემთა დაცვის პირველი კანონი (1992 წლის LXIII კანონი პერსონალურ მონაცემთა დაცვისა[1] და საზოგადოებრივი ინტერესებიდან[2] გამომდინარე საჯარო წვდომის შესახებ, შემდგომში „1992 წლის LXIII კანონი“) - როგორც ერთ-ერთი ქვაკუთხედი - ძალაში შევიდა 1993 წელს რეჟიმის შეცვლის შემდეგ.

მონაცემთა დაცვის უფლებების სამართლებრივ უზრუნველყოფასთან დაკავშირებით 1992 წლის LXIII კანონი მოიცავდა შემდეგ წესებს: თავისი უფლებების დარღვევის შემთხვევაში მონაცემთა სუბიექტს შეუძლია აღძრას სასამართლო საქმე მონაცემთა დამმუშავებლის წინააღმდეგ[3]. მტკიცების ტვირთი, რომ მონაცემთა დამუშავება განხორციელდა შესაბამისი კანონის ნორმების დაცვით უნდა დაეკისროს მონაცემთა დამმუშავებელს[4]. მონაცემთა დამმუშავებელი უნდა იყოს პასუხისმგებელი იმ ზიანზე, რომელიც განიცადა მონაცემთა სუბიექტმა მონაცემების არაკანონიერი დამუშავების ან მონაცემთა დაცვის ტექნიკური მოთხოვნილებების დარღვევის შედეგად. მონაცემთა დამმუშავებელი პასუხისმგებელია ნებისმიერ ზარალზე, რომელიც განიცადა მონაცემთა სუბიექტმა უფლებამოსილი პირის ქმედებების შედეგად. მონაცემთა დამმუშავებელი გათავისუფლდება პასუხისმგებლობისგან თუ იგი დაამტკიცებს რომ ზარალი გამოწვეულია ფორს-მაჟორის შედეგად, რომელიც სცილდებოდა მონაცემთა დამუშავების სფეროს[5]. კომპენსაციის გადახდა არ მოხდება ზარალის იმ ნაწილისთვის, რომელიც განიცადა

[1] მუხლი 2 (1): 1. „პერსონალური მონაცემები უნდა ნიშნავდეს ნებისმიერ მონაცემებს რომლებიც დაკავშირებულია კონკრეტულ (იდენტიფიცირებულ ან იდენტიფიცირებად) ფიზიკურ პირთან(შემდგომში მოხსენებულია როგორც „მონაცემთა სუბიექტი“) ასევე ნებისმიერ დასკვნას მონაცემთა სუბიექტთან მიმართებით, რომელიც შეიძლება გაკეთდეს ამ მონაცემებიდან, მონაცემთა დამუშავების პროცესში ასეთი მონაცემები უნდა იყოს მიჩნეული პერსონალურად სანამ აღდგება მათი კავშირი მონაცემთა სუბიექტთან. იდენტიფიცირებადი პიროვნებაა კონკრეტულას ის, ვისი იდენტიფიკაცია შესაძლებელია, პირდაპირ ან არაპირდაპირ, მისი სახელის იდენტიფიკაციის კოდის ან მისთვის დამახასიათებელი ფიზიკური, ფიზიოლოგიური, გონებრივი, ეკონომიური ან სოციალური იდენტობით“.

[2] მუხლი 2 (40) „საზოგადოებრივი ინტერესის მატარებელი მონაცემები“ ნიშნავს ნებისმიერ ინფორმაციას ან ცოდნას, რომელიც არ განეკუთვნება პერსონალურ მონაცემთა განმარტებას, დამუშავებულია ორგანიზაციის ან პიროვნების მიერ, რომელიც ასრულებს სახელმწიფო ან ადგილობრივი მთავრობის ფუნქციას ან სხვა საჯარო ფუნქციას, რომელიც განსაზღვრულია კანონის უზენაესობით, ან ნებისმიერო ინფორმაცია ან ცოდნა დაკავშირებული მის აქტივობებთან, ჩაწერილი ნებისმიერი სახით ან ფორმით მიუხედავად იმისა როგორ არის დამუშავებული და მისი დამოუკიდებელი თუ ცოლექტიური ბუნებისა.

[3] მუხლი 17 (1).

[4] მუხლი 17 (2).

[5] მუხლი 18 (1).

დაზარალებულმა პიროვნებამ განზრახული ან უკიდურესად დაუდევარი საქციელის[6] შედეგად.

მე-17 და მე-18 მუხლებით განსაზღვრული წესები უზრუნველყოფდნენ, რომ მონაცემთა სუბიექტსა და მონაცემთა დამმუშავებელს შორის სასამართლო დავა ექვემდებარებოდა სამოქალაქო სასამართლოს იურისდიქციას.

დიდი ხნის განმავლობაში მონაცემთა დაცვის სისტემიდან თითქმის სრულიად ამოღებული იყო სამართლებრივი დაცვის მეორე საყრდენი: სასამართლო განხილვა[7]. თავდაპირველად ეს იმ ფაქტის გამო, რომ მონაცემთა დაცვის კომისარი, რომელიც დამტკიცდა 1092 წლის LXIII კანონით, არ მოქმედებდა როგორც ადმინისტრაციული ორგანო, მისი უფლებამოსილება „რბილი“ იყო, კომისარი არ იღებდა სამართლებრივად მავალდებულებელ ადმინისტრაციულ გადაწყვეტილებებს მისი სამართლებრივი სტატუსიდან გამომდინარე და შედეგად, მის სამართლებრივ პოზიციებს, როგორც ადმინისტრაციულ გადაწყვეტილებებს, დამუშავების ოპერაციების კანონიერების შესახებ ვერ წარუდგენდა ადმინისტრაციულ მოსამართლეს. მეორე მხრივ, უნგრეთში მონაცემთა დაცვის კანონის ძირითადი შეხედულების მიხედვით, რომელიც ასახულია კანონის ძირითად ტექსტში, დამუშავების ოპერაციები, რომლებიც მიეკუთვნებოდნენ სახელმწიფო ადმინისტრაციას, არ კვალიფიცირდებოდა, როგორც ადმინისტრაციული აქტივობა ან ქმედება, რომლის კანონიერების შეფასება დაექვემდებარებოდა სასამართლო განხილვას. მონაცემთა სუბიექტის მიერ სასამართლოს წინაშე წარდგენილი სარჩელი ადმინისტრაციული ორგანოების მიერ დამუშავების ოპერაციებთან დაკავშირებით განიხილებოდა როგორც სამოქალაქო დავა.

რეგულაციის ამ საერთო კონცეფციის შედეგად, რომელიც ჩამოყალიბდა 1992 წლის LXIII კანონით, პერსონალური მონაცემების დაცვასთან დაკავშირებული სამართლებრივი ინტერპრეტაციის საკითხები თითქმის სრულად არიდებდა თავს ადმინისტრაციულ სასამართლოებს დაახლოებით ორი ათწლეულის განმავლობაში. ამრიგად, მონაცემთა დაცვის კომისრის მიერ შემუშავებულ „პრეცედენტულ სამართალს“ შეეძლო დროის ხანგრძლივი პერიოდის განმავლობაში განეცადა ევოლუცია „რბილი სამართლის“ მეშვეობით ისე, რომ ვერც მონაცემთა სუბიექტი და ვერც დამმუშავებელი ვერ შეძლებდნენ გაესაჩივრებინათ მონაცემთა დამუშავების ოპერაციების კანონთან შესაბამისობა ადმინისტრაციული სასამართლოს წინაშე.

უნგრეთის[8] ფუნდამენტური კანონისა და 2011 წლის CXII კანონის საფუძველზე „ორგანოს“ ცალსახად ადმინისტრაციულ ერთეულად[9] ჩამოყალიბებით პერსონალური მონაცემების დაცვა გადავიდა სახელმწიფო საზედამხედველო

[6] მუხლი 18 (2).

[7] სასამართლო განხილვა არის ერთგვარი სასამართლო საქმეთა წარმოება, რომელშიც მოსამართლე განიხილავს იმ გადაწყვეტილების ან ქმედების კანონიერებას, რომელიც შესრულებულია სახელმწიფო ორგანოს მიერ.

[8] მუხლი 23(1) პერსონალურ მონაცემთა დაცვის კონსტიტუციური უფლება და საზოგადოებრივი ინტერესის მატარებელ მონაცემებზე საჯარო წვდომის უზრუნველსაყოფად, პარლამენტმა უნდა აირჩიოს მონაცემთა დაცვის კომისარი უნგრელი მოქალაქეებიდან, რომელსაც აქვს უნივერსიტეტის ხარისხი, სუფთა კრიმინალური ჩანაწერი და გამორჩეული აკადემიური ცოდნა ან სულ ცოტა 10 წლის პროფესიული პრაქტიკა, რომელსაც აქვს მნიშვნელოვანი გამოცდილება მონაცემთა დაცვის საქმეთა წარმოების წარმართვასა ან ზედამხედველობაში ან მის შესახებ თეორიული ცოდნა.

[9] უნგრეთის ფუნდამენტური კანონი (25 აპრილი, 2011), <https://njt.hu/jogszabaly/en/2011-4301-02-00> [8.01.2024].

ორგანოს კომპეტენციაში და უფრო აქტიურად ჩაერთო საჯარო სფეროში[10]. სახელმწიფო ორგანოების გადაწყვეტილებების სასამართლო განხილვა ყველა სახელმწიფოში წარმოადგენს კონსტიტუციურ მოთხოვნას, რომელიც ეფუძნება კანონის უზენაესობას.

„ორგანოს“ დაფუძნებამ და პერსონალურ მონაცემთა დაცვის სამართლებრივმა უზრუნველყოფამ სახელმწიფო უფლებამოსილების მეშვეობით, შექმნა ფუნდამენტურად ახალი სიტუაცია ადმინისტრაციული სასამართლო სისტემისთვის. ეს ასეა მაშინაც კი, როცა ფაქტობრივად, 1992 წლის LXIII კანონით ჯერ კიდევ 2004 წელს გადაეცა მონაცემთა დაცვის კომისარს მთელი რიგი სახელმწიფო უფლებამოსილებები, რაც სამართლებრივი სტატუსის თვალსაზრისით, უფრო გააძლიერებდა სახელმწიფო ორგანოს როლს.

2. LXIII კანონის განხორციელება (1993-2012)

2.1. საწყისები

ამ პერიოდის განმავლობაში მონაცემთა დაცვის კანონთან დაკავშირებული საკითხები თითქმის სრულად არიდებდა თავს ადმინისტრაციული სასამართლო სხდომების დარბაზებს.

შეუძლებელია დადგენა იმისა, რომ 1992 წლის LXIII კანონის დებულებები სრულიად უცხო იყო ადმინისტრაციული მოსამართლეებისთვის. ამ კანონის ნორმებზე მითითება ნამდვილად წარმოადგენდა ადმინისტრაციული დავების ნაწილს საქმეთა სხვა ჯგუფებში, თუმცა, როგორც ზემოთ იყო ნახსენები, აღმოჩნდა, რომ მითითება მონაცემთა დაცვის დარღვევებზე წარმოადგენდა უფრო მეტად დამხმარე ელემენტს ადმინისტრაციული გადაწყვეტილებების წინააღმდეგ აღძრულ სარჩელებში - მაგ. საგადასახადო და კონკურენციის საკითხებთან დაკავშირებულ საქმეებში. ადმინისტრაციული მოსამართლეებისთვის, რომლებიც განიხილავენ გადასახადების, კონკურენციისა და სხვა ადმინისტრაციულ საკითხებს, არ იყო ცხადი რომ აღძრულ საქმეებში მათ, პირდაპირ თუ არაპირდაპირ, უნდა გაეკეთებინათ 1993 წლის LXIII კანონის ნორმების ინტერპრეტაცია და გამოეტანათ თავიანთი სწორი გადაწყვეტილება რათა შეეფასებინათ სხვა ტიპის ადმინისტრაციული აქტების კანონიერება.

[10] უნგრეთის ფუნდამენტური კანონის მუხლი VI (1) ყველას აქვს უფლება ჰქონდეს თავისი პირადი და ოჯახური ცხოვრების, სახლის, კომუნიკაციის დაკარგი რეპუტაციისადმი პატივისცემისა. გამოხატვისა და შეკრების თავისუფლების უფლების განხორციელებამ არ უნდა დააზიანოს სხვათა პირადი და ოჯახური ცხოვრება. (2) სახელმწიფომ უნდა უზრუნველყოს სახლებში სიმშვიდის სამართლებრივი დაცვა. (3) ყველას უნდა ქონდეს თავისი პერსონალური მონაცემების ასევე საზოგადოებრივი ინტერესის მატარებელი მონაცემებზე წვდომისა და გავრცელების უფლება. (4) პერსონალურ მონაცემთა დაცვისა და საზოგადოებრივი ინტერესის მატარებელი მონაცემებზე წვდომის უფლებების ცხოვრებში გატარებაზე კონტროლი უნდა განხორციელდეს დამოუკიდებელი ორგანოს მიერ რომელიც დაფუძნებულია კარდინალური კანონით.

2.2. მონაცემთა დაცვასა და სამართლის სხვა სფეროებს შორის დამოკიდებულება

პრაქტიკის ილუსტრირებულ მაგალითს წარმოადგენს საგადასახადო საქმე, რომელშიც ადმინისტრაციულმა სასამართლომ არ განიხილა საგადასახადო სამსახურის მიერ ჩატარებული დამუშავების ოპერაციის კანონიერება მიუხედავად განმცხადებლის ცალსახა მტკიცებისა, რომ საგარანტიო წერილის საფუძველზე საგადასახადო ორგანო კანონით იყო უფლებამოსილი შეეკრიბა მხოლოდ საწარმოებთან დაკავშირებული მონაცემები გადასახადებთან დაკავშირებული გამოძიების მიმდინარეობის დროს, მაგრამ საგადასახადო სამსახური გასცდა ფარგლებს და ზედმეტი გამოკვლევები ჩაატარა განმცხადებლის პირად საბანკო ანგარიშებთან, ტრანსპორტთან და უძრავ ქონებასთან დაკავშირებით. განმცხადებლის აზრით, საგადასახადო სამსახურმა დაარღვია 1992 წლის LXIII კანონის ნორმები და იგი, როგორც მონაცემთა სუბიექტი, აპროტესტებდა საგადასახადო ორგანოს მიერ მის პერსონალურ მონაცემთა დამუშავებას. მან ასევე დაადგინა, რომ არ სურდა აღეძრა მონაცემთა დაცვის სამართალწარმოება საგადასახადო სამსახურის წინააღმდეგ.

ადმინისტრაციულმა სასამართლომ განმარტა: *„16/A[11] პარაგრაფის მიხედვით, ადმინისტრაციულ სასამართლოს არ გააჩნია პერსონალური მონაცემების დამუშავების იურისდიქცია. თუ მონაცემთა სუბიექტი, ამ შემთხვევაში განმცხადებელი, ეწინააღმდეგება პერსონალურ მონაცემთა დამუშავებას, მონაცემთა დამმუშავებელმა - საგადასახადო ორგანომ - უნდა მიიღოს ამის თაობაზე გადაწყვეტილება. თუ მონაცემთა სუბიექტი არ ეთანხმება ამ გადაწყვეტილებას, მას შეუძლია მიმართოს საერთო იურისდიქციის სამოქალაქო სასამართლოს. საკუთარი იურისდიქციის არარსებობის შემთხვევაში ადმინისტრაციულ სასამართლოს არ შეეძლო განეხილა მონაცემთა დაცვასთან დაკავშირებული საჩივარი კონკრეტულად საგადასახადო საქმის ფარგლებში[12].* ამ სამართლებრივ არგუმენტში უცნაურია არა ის, რაც ჩაწერილია, არამედ ის რაც არ არის მოხსენიებული. არ იყო განსაზღვრული ის, თუ რატომ ვერ მიიჩნია სასამართლომ შესაძლებლად საგადასახადო ორგანოს გადაწყვეტილების

[11] CXII კანონის 38(1-2) განყოფილება. (1) საზედამხედველო ორგანო უნდა იყოს ავტონომიური სახელმწიფო ადმინისტრაციული ორგანო. (2) საზედამხედველო ორგანო უნდა იყოს პასუხისმგებელი პერსონალურ მონაცემთა დაცვისა და საზოგადოებრივი ინტერესის მატარებელ მონაცემებზე წვდომის და საჯარო ინტერესის საფუძველზე მონაცემებზე ხელმისაწვდომობის უფლების განხორციელებაზე მონიტორინგსა და ხელშეწყობაზე, ასევე პერსონალური მონაცემების ევროკავშირში თავისუფალი გადაადგილების ხელშეწყობაზე.

[12] 1992 წლის LXIII კანონის 25(4-5) მუხლები. (4) თუ მონაცემთა დამმუშავებელი ან ტექნიკურ უფლებამოსილი პირი ვერ მოახერხებს შეაჩეროს პერსონალურ მონაცემთა არაკანონიერი დამუშავება(ტექნიკური დამუშავება), მონაცემთა დაცვის კომისარს შეუძლია გასცეს უკანონოს დამუშავებული მონაცემთა ბლოკირების, ამოშლის ან განადგურების ბრძანება, აკრძალოს მონაცემთა არაკანონიერი ან ტექნიკური დამუშავება, და დროებით შეაჩეროს მონაცემთა ტრანსფერი უცხო ქვეყნებში. გადაწყვეტილება არ შეიძლება შესწორდეს ადმინისტრაციული გზით. (5) მონაცემთა დამმუშავებელს, ტექნიკური უფლებამოსილი პირს ან მონაცემთა სუბიექტს შეუძლიათ მოითხოვონ სასამართლო განხილვა მონაცემთა დაცვის კომისარის გადაწყვეტილება პარაგრაფი(4)-ს შესაბამისად-მიღებიდან 30 დღის ვადაში - დარღვევების საფუძველზე. სასამართლომ უნდა იმოქმედოს საჯარო ორგანიზაციის წინააღმდეგ სარჩელის აღძვრის სამოქალაქო საპროცესო კანონის რეგულაციების შესაბამისად. სასამართლოს საბოლოო გადაწყვეტილების მიღებამდე არ შეიძლება შესაბამისი მონაცემების ამოშლა ან განადგურება; თუმცა, მონაცემთა დამუსავება უნდა შეჩერდეს დროებით ან მოხდეს მათი ბლოკირება.

განხილვა. საჩივარი შეეხებოდა არა მარტო გასაჩივრების უფლებას, არამედ უფრო ზოგადად მონაცემთა დაცვის დებულებების დარღვევას. ეს სამართლებრივი არგუმენტი მიმართული იყო იმისაკენ, რომ გაემიჯნა ერთმანეთისაგან ადმინისტრაციული ორგანოს უფლებამოსილების როლი მონაცემთა დამმუშავებლის როლისგან.

აღნიშნული კიდევ უფრო ცხადად არის ილუსტრირებული სასამართლო გადაწყვეტილებაში, რომელშიც უნგრეთის უმაღლესი სასამართლო არ განიხილავს მონაცემთა დაცვის კანონის ასპექტსა და მის ზეგავლენას საგადასახადო საქმეზე. იგი ამტკიცებს რომ *„სამოქალაქო კოდექსი და 1992 წლის LXIII კანონი, რომელიც მითითებული იყო განმცხადებლის მიერ არ მოიცავდა საგადასახადო დავასთან დაკავშირებულ რომელიმე გადაწყვეტილებას და მოპასუხე თავის გადაწყვეტილებას საფუძვლად უდებდა არა კანონით დადგენილი წესების შეუსრულებლობას, არამედ იგი ეყრდნობოდა ფინანსური სამართლის დებულებებს, რომლებიც არეგულირებენ ფინანსური დავების გადაწყვეტას“.*[13]

მიზეზი, თუ რატომ არ იქნა განხილული 1992 წლის LXIII კანონი ადმინისტრაციულ საქმეებში ზოგადად იყო ახსნილი კონკურენციის სამართლის საქმეებშიც, თუმცა არსებობდა სასამართლო გადაწყვეტილება, რომელიც მთლიანად არ გამორიცხავდა კანონის ინტერპრეტირებას ადმინისტრაციული გადაწყვეტილების კანონიერების შეფასების დროს. კონკურენციის სამართლის საქმეში მოსარჩელე ამტკიცებდა, რომ ადმინისტრაციულ სამართალწარმოებაში დოკუმენტაცია შესრულებული იყო 1992 წლის LXIII კანონის დებულებების დარღვევით ანტიმონოპოლიური ორგანოების მიერ. ადმინისტრაციულმა სასამართლომ დაადგინა რომ *„კანონის პირველი მუხლის მიხედვით, მისი მიზანია ყველა პიროვნების მიერ საკუთარ პერსონალურ მონაცემებზე კონტროლის განხორციელება, თუ სხვა რამ არ არის გათვალისწინებული ამ კანონის სამართლებრივი ნორმით. განმცხადებელმა ვერ წარმოადგინა იდენტიფიცირებადი მტკიცებულება, თუ რომელი ფიზიკური პირი დაზარალდა მოპასუხის ადმინისტრაციული საქმის წარმოებისას ან პერსონალურ მონაცემთა დამუშავების რომელი წესი დაირღვა. ამრიგად, სასამართლომ ვერ დაადგინა მონაცემთა დაცვის კანონის დარღვევა[14]“.*

კონკურენციის სამართლის კიდევ ერთ სასამართლო საქმეში უზენაესმა სასამართლომ ძირითადად დაადგინა, რომ *„მოპასუხის საქმის წარმოებასთან დაკავშირებით განმცხადებელმა შეცდომით მიუთითა 1992 წლის LXIII კანონის დარღვევის ფაქტზე 1996 წლის LVII კანონის 65(4) მუხლის კონტექსტში.[15] მონაცემთა დაცვის წესები გამოიყენება ინდივიდუალურ ადმინისტრაციულ საქმეში იმდენად, რამდენადაც მონაცემთა დაცვის კონტექსტი რეგულირდება შესაბამისი პროცედურული კანონით. ზოგადად, მონაცემთა დაცვის კანონის საფუძველზე ადმინისტრაციული პროცედურა, რომელიც რეგულირდება კანონით, არ დადგება ეჭვქვეშ, რადგანაც*

[13] მუხლი 16/A (1) (წინააღმდეგების უფლება) მონაცემთა სუბიექტს შეუძლია წინააღმდეგი იყოს მისი მონაცემების დამუშავებისა, თუ ა) მონაცემთა დამუშავება(ტრანსფერი) აუცილებელია მხოლოდ უფლების დაცვის უზრუნველყოფისთვის ან მონაცემთა დამმუშავებლის ან მიმღების ლეგიტიმური ინტერესით, გარდა ინ შემთხვევისა როცა მონაცემთა დამუშავება ნაბრძანებია კანონით. ბ) პერსონალური მონაცემები გამოიყენება ან გადაიცემა პირდაპირი მარკეტინგის, საზოგადოებრივი აზრის გამოკითხვის ან სამეცნიერო დამუშავების მიზნით ან გ) ჭინააღმდეგობის უფლების განხორციელება ხდება სხვა გზით კანონის შესაბამისად.

[14] უნგრეთის ვასის საგრაფოს სასამართლო, 1.K.20.018/2009/33.

[15] უნგრეთის უზენაესი სასამართლო, Kfv.V.35.180/2009/5.

პერსონალურ მონაცემთა შესაბამისი დამუშავება ამ შემთხვევაში კანონით არის გარანტირებული. მონაცემთა დაცვის თვალსაზრისით, ადმინისტრაციული პროცედურა შესაძლოა იყოს არაკანონიერი, „ორგანოს“ მიერ მიღებული გადაწყვეტილების ჩათვლით, თუ წესები, რომლებიც მართავენ ადმინისტრაციულ პროცედურებს, იძლევა ასეთი ასპექტების განხილვის უფლებამოსილებას. თუ ეს არ არსებობს, პერსონალურ მონაცემთა დამუშავება შეიძლება დაირღვეს LXIII კანონით განსაზღვრული ნორმით, თუმცა, ეს წარმოადგენს დამოუკიდებელ მონაცემთა დაცვის პროცედურას, რომელიც უნდა გავმიჯნოთ განხილვის ქვეშ მყოფი პროცედურისგან, ანუ ანტიმონოპოლიური ზედამხედველობის პროცედურისგან. პირველი ინსტანციის სასამართლო სწორად აღნიშნავდა, რომ მოპასუხის გადაწყვეტილების კანონიერება შეიძლება და უნდა შეფასდეს ადმინისტრაციული სამართალწარმოებისას 1966 წლის LVII კანონის საფუძველზე, და ადმინისტრაციული ქმედება (საგამოძიებო ღონისძიება) არ შეიძლებოდა დაქვემდებარებული ყოფილიყო სასამართლო განხილვაზე 1996 წლის LXIII კანონის მიხედვით.[16]

ადმინისტრაციული სასამართლოს არსებითად არ განუხილავს მონაცემთა დაცვის სამართლებრივი საკითხები დაახლოებით 20 წელი, თუმცა, ეს არ იყო გამოწვეული იმ ფაქტით რომ განმცხადებლის ქმედება არ წარმოადგენდა მცდელობას, მონაცემთა დაცვის კანონმდებლობის საკითხები წამოეყენებინა 1992 წლის კანონის LXIII საფუძველზე.

უმეტეს შემთხვევებში ამ საშუალების გამოყენება მიზნად ისახავდა ადმინისტრაციული ორგანოების მიერ მტკიცებულების მოპოვების უკანონობის დამტკიცებას, იმისათვის რომ უკანონოდ (მონაცემთა დაცვის წესების დარღვევით) მოპოვებული მტკიცებულებების გამორიცხვის გზით დადგენილიყო ის შეცდომები, რომლებიც დაშვებული იყო ადმინისტრაციული გადაწყვეტილებების ფაქტების ახსნა-განმარტებებში, მაგრამ ჩვენ არ შეგვიძლია დავადგინოთ, რომ მონაცემთა დაცვის ძირითად კანონზე მითითებამ მხოლოდ ასეთი როლი ითამაშა. არგუმენტები, რომელთა მიზანია აჩვენონ რომ სახელმწიფო ორგანოები ვალდებულნი არიან შეასრულონ მონაცემთა დამმუშავებლების ვალდებულებები - ოფიციალური ფუნქციების შესრულებისას, წარმოიქმნა ძალიან სწრაფად და ზემოქმედებს მათ ქმედებებზე. ცხადია, რომ პრეცედენტულ სამართალს აკლდა მონაცემთა დაცვის კანონის საკითხების თეორიული ახსნა-განმარტება და შეძლებისდაგვარად ხაზს უსვამდა, რომ ადმინისტრაციული აქტის კანონიერების შეფასება შესაძლებელი იყო მოქმედი დარგობრივი ადმინისტრაციული ნორმების საფუძველზე.

2.3. მონაცემთა დაცვის ორგანოს ევოლუციური როლი - 1992 წლის LXIII კანონის 15 (3-4) განყოფილება

1992 წლის კანონის თავდაპირველი ვერსიის პარაგრაფი 24/25-ის მიხედვით კომისარმა ა) უნდა აკონტროლოს ამ კანონსა და სხვა სამართლებრივ წესებს შორის შესაბამისობა, ბ) უნდა გამოიკვლიოს მასზე მიწოდებული ცნობები გ) უნდა უზრუნველყოს მონაცემთა დაცვის რეესტრის წარმოება[17].

[16] უნგრეთის ბუდაპეშტის სასამართლო, K.33.024/2004/46.

[17] 1996 წლის LVII კანონის 65(1-6) მუხლი უსამართლო და შემზღუდავი ბაზრის პრაქტიკის აკრძალვის შესახებ (კონკურენციის კანონი) (1) საქმის განმხილველი პირის ან ანტიმონოპოლური საბჭოს

ამ კანონის 25(1/30) მუხლების შესაბამისად მონაცემთა დაცვის კომისარმა უნდა აკონტროლოს პერსონალურ მონაცემთა დაცვის, ასევე საზოგადოებრივი ინტერესის მატარებელ მონაცემებზე და საზოგადოებრივი ინტერესის გამო გასაჯაროებულ მონაცემებზე წვდომის განხორციელების პირობები. მან უნდა წამოაყენოს წინადადებები მონაცემთა დამუშავების, საზოგადოებრივი ინტერესის მატარებელ და საზოგადოებრივი ინტერესის გამო გასაჯაროებულ მონაცემებზე წვდომის კანონმდებლობის მიღების ან შესწორების შესახებ და გამოხატოს აზრი შესაბამის პროექტზე. მას შეუძლია წამოიწყოს სახელმწიფო ან სამსახურებრივ საიდუმლოდ კლასიფიცირებული მონაცემთა კატეგორიების შევიწროება ან გაფართოება. მონაცემთა ნებისმიერი არაკანონიერი დამუშავების დადგენისას, მონაცემთა დაცვის კომისარმა უნდა გამოიძახოს მონაცემთა დამმუშავებელი, რომ შეაჩეროს მონაცემთა დამუშავება. მონაცემთა დამმუშავებელმა დაუყოვნებლივ უნდა მიიღოს საჭირო ზომები და მათ შესახებ წერილობით შეატყობინოს მონაცემთა დაცვის კომისარს 30 დღის ვადაში. მონაცემთა დაცვის კომისარს შეუძლია მიაწოდოს ინფორმაცია საზოგადოებას: გამოძიების დაწყების, მონაცემთა არაკანონიერი დამუშავების ფაქტის (ტექნიკური დამუშავება), მონაცემთა დამმუშავებლის პიროვნების (ტექნიკური/უფლებამოსილი პირი) და პერსონალურ მონაცემთა სპექტრის შესახებ[18].

2004 წლის პირველ იანვარს, მნიშვნელოვანი[19] ცვლილება შევიდა მონაცემთა დაცვის კომისრის ზედამხედველობით „უფლებამოსილებებში“. კანონმდებლობამ დააკისრა კომისარს ადმინისტრაციული ტიპის ფაქტობრივი სამეთვალყურეო მაკორექტირებელი უფლებამოსილება. კანონით დადგენილ იქნა, რომ იმ შემთხვევაში, თუ მონაცემთა დამმუშავებელი ან ტექნიკური უფლებამოსილი პირი ვერ ახერხებს შეაჩეროს პერსონალურ მონაცემთა უკანონო დამუშავება (ტექნიკური დამუშავება), მონაცემთა დამუშავების კომისარს შეუძლია მიიღოს გადაწყვეტილება

გამოძახებით, კომპიუტერულ სისტემაში ან ელექტრონული მონაცემების შესანახ მოწყობილობაში (შემდგომში ერთობლივად: მონაცემთა მარაგი) ჩაწერილი მონაცემები ხელმისაწვდომი უნდა იყოს ასეთი მონაცემთა მარაგზე უფლებამოსილი პირისთვის ისეზთ ფორმატით რომლის წაკითხვა და კოპირება შესაძლებელია (2) საქმის განმხილველი პირი ან ანტიმონოპოლური საბჭო უფლებამოსილი უნდა იყოს გააკეთოს დოკუმენტებისა და მონაცემთა მარაგში შენახული მონაცემების ასლები, საქმის მწარმოებელი პირი უფლებამოსილია გააკეთოს მონაცემთა მარაგის კრიმინალისტური ასლი და შეამოწმოს მისი შინაარსი იმავე კრიმინალისტური ასლის გამოყენებით თუ შესაძლებელია რომ იგი შეიცავდეს ძიებაში მყოფ საქმეს რომლის ამოღება არ შეიძლება კომპიუტერის სათანადო გამოყენების პროცესში. (3) მონაცემთა მარაგში შენახული მონაცემების ელექტრონული ასლების გაკეთების პროცესში მონაცემები უნდა ჩაიწეროს იმგვარად რომ გამოირიცხოს მონაცემებით შემდგომი მანიპულირება ან-თუ ეს არ არის შესაძლებელი მონაცემთა მარაგის ტიპის გამო- მონაცემები ჩაწერილი იქნება იმ ტექნოლოგიის გამოყენებით, რომელიც უზრუნველყოფს შემდგომ ეტაპზე მონაცემთა უცვლელი სახით გაკონტროლების შესაძლებლობას. (4) საკუთრების შენახვისას საქმის მწარმოებელმა პირმა საკუთრება უნდა მოათავსოს შესანახად შესაფერის კონტეინერში ან ცალკე ოთახში რომლის ჩაკეტვა ან დალუქვა შესაძლებელია. (5) თუ მონაცემები არ არის ხელმისაწვდომი საიტზე, საქმის მწარმოებელ პირს შეუძლია დაავალოს ქონების მფლობელს გახადოს იგი ხელმისაწვდომი უნგრეთის ანტიმონოპოლიური ორგანოსათვის უცვლელი ფორმით, კონკრეტულ დროს და ადგილზე. (6) სხვა მხრივ, დაცვა და კონფისკაცია რეგულირებულია GRAP აქტის დებულებების mutatis mutandis და იმ პირობით პრივილიგირებული ინფორმაციის კონფიდენციალურობიდან გათავისუფლება შეეძლება ქონების მფლობელს, კლასიფიცირებული ინფორმაციის გარდა,
<https://www.gvh.hu/pfile/file?path=/en/legal_background/rules_for_the_hungarian_market/competition_act/competition-act-documents/jogihatter_tpvt_hataly_20190101_a&inline=true> [8.01.2024].

[18] უნგრეთის უზენაესი სასამართლო, Kfv.37.923/2010/5.

[19] იხ. მუხლი 24.

არაკანონიერად დამუშავებული მონაცემების ბლოკირებასთან, ამოშლასა ან განადგურებასთან დაკავშირებით, შეუძლია აკრძალოს მონაცემთა უკანონო ან ტექნიკური დამუშავება და დროებით შეაჩეროს მონაცემების სხვა ქვეყანაში გადაცემა. გადაწყვეტილება არ შეიძლება შესწორდეს ადმინისტრაციული გზით. მონაცემთა დამმუშავებელს, ტექნიკურ უფლებამოსილ პირს ან მონაცემთა სუბიექტს შეუძლიათ მოითხოვონ სასამართლოსგან მონაცემთა დაცვის კომისრის გადაწყვეტილების სამართლებრივი წესით განხილვა მე-4 პარაგრაფის შესაბამისად დარღვევის საფუძველზე მისი მიღებიდან 30 დღის ვადაში. სასამართლომ პროცესი უნდა წარმართოს სახელმწიფო ადმინისტრაციის წინააღმდეგ სარჩელის აღძვრის შესახებ, რომლებიც განსაზღვრულია სამოქალაქო საპროცესო კანონში. სასამართლოს საბოლოო გადაწყვეტილებამდე შესაბამისი მონაცემების წაშლა ან განადგურება არ შეიძლება, თუმცა მონაცემთა დამუშავება უნდა შეჩერდეს დროებით და მოხდეს მათი ბლოკირება[20].

ამ წესების შედეგად, შემდგომში, ადმინისტრაციულ სასამართლო ორგანოებში წარდგენილ ადმინისტრაციულ სარჩელებში მონაცემთა დაცვის კომისარი მონაწილეობდა როგორც მოპასუხე, სხვა სიტყვებით რომ ვთქვათ, მონაცემთა დაცვის კანონის დასკვნები და ინტერპრეტაციები, რომლებიც განსაზღვრული იყო მონაცემთა დაცვის კომისრის მიერ, *დაექვემდებარა სასამართლო წესით განხილვას.*

ახალმა კანონმდებლობამ შექმნა ახალი გამოწვევები ორივე მონაცემთა დაცვის კომისრისა და ადმინისტრაციული სასამართლო პრაქტიკის წინაშე. შეცვლილი როლის ფარგლებში კომისარს უნდა შეედგინა, შეესწორებინა თავისი „ადმინისტრაციული გადაწყვეტილებები“ და განეხორციელებინა საქმისწარმოება დაკისრებული პროცედურული მოთხოვნების შესაბამისად. იმავდროულად, მოსამართლეებს უნდა შეესწავლათ მონაცემთა დაცვის სამართლის მანამდე გამოუკვლეველი და შეუსწავლელი სიღრმეები.

ამგვარად, მონაცემთა დაცვის კომისრის გადაწყვეტილებების საშუალებით შესაძლებელი გახდა არა მარტო სახელმწიფო ორგანოების პერსონალურ მონაცემთა დამუშავების დაქვემდებარება სასამართლო განხილვისადმი, არამედ პრინციპში, ყველა დამმუშავებლისა და დამუშავების ოპერაციების ადმინისტრაციულ სასამართლო განხილვების კონტროლისადმი დაქვემდებარება. პირობითობა ნიშნავს, რომ კომისრის ზემოხსენებული გამოსწორებითი უფლებამოსილების დადგენას შედეგად არ მოჰყოლია მისი გადაწყვეტილებების წინააღმდეგ სარჩელების რაოდენობის „აფეთქება“. 2004 წელს, სულ 2 სარჩელი[21] გადაეცა ადმინისტრაციულ სასამართლოს.[22]

---

[20] იხ. მუხლი 25(1-3).

[21] იხ. 2005 წლის მონაცემთა დაცვის კომისრის მოხსენება, 45-46: *„უდიდესი ცვლილება მონაცემთა დაცვის უფლებამოსილებებში ნამდვილად შეეხება ბრძანებას 2004 წლის 1 იანვრის შემდეგ არაკანონიერად დამუსავებული მონაცემების დაბლოკვას, ამოშლას ან განადგურებას, ან არა-ნებადართულ დამუშავების აკრძალვას ან მონაცემების საზღვარგარეთ გადაცემის დროებით შეჩერებას. მონაცემთა დამმუშავებელს ან შესაბამისი უფლებამოსილ პირს შეუძლია მიმართოს სამართლოს კომისრის გადაწყვეტილების წინააღმდეგ , სასამართლოს გადაწყვეტილების მოლოდინის პროცესში მონაცემთა დამუშავება დროებით უნდა შეჩერდეს და მონაცემები უნდა დაიბლოკოს. თუმცა, კანონი ბევრ შეკითხვას ტოვებს პასუხგაუცემლად. მატ შორის, თუ რა მოხდება თუ მონაცემთა დამმუშავებელი არ შეწყვეტს უკანონო დამუსავებას და არ მიმართავს სასამართლოს: გარდა ბრძანების გაცემისა, კომმისარს არ გააჩნია არანაირი უფლებამოსილება ჯარიმი დაკისრების ან არსრულებაზე ბრძანების გაცემასთან დაკავშირებით“.*

[22] მუხლი 25(4-5).

3. ფუნდამენტური კანონისა და 2011 წლის CXII კანონის ძალაში შესვლა (პირველი იანვარი, 2012 - 25 მაისი, 2018)

3.1. მონაცემთა დაცვის ადმინისტრაციული (საზედამხედველო) პროცედურის დანერგვა

ეს პერიოდი უკავშირდებოდა საზედამხედველო ორგანოს როლის განვითარებას და საგამოძიებო და გამოსასწორებელი ზედამხედველობის უფლებამოსილების გაფართოებას. იგი წარმოადგენდა კიდევ ერთ მნიშვნელოვან ნაბიჯს თანამიმდევრული და უფრო დეტალური მონაცემთა დაცვის ადმინისტრაციულ-სამართლებრივი პრაქტიკისკენ.

ძირითადი კანონის VI(2/3) მუხლით, რომელშიც დადგენილია პერსონალური მონაცემების დაცვის ფუნდამენტური უფლება კანონის დონეზე, ერთი მხრივ, შენარჩუნებულია უნგრეთის მონაცემთა დაცვის სამართლებრივი ტრადიციები და მეორე მხრივ, მთელი რიგი პროცედურული და კომპეტენტური შედეგების გამო, პერსონალურ მონაცემთა დაცვის უფლების განხორციელების კონტროლი დაეკისრა *„დამოუკიდებელ ორგანოს“.*

პარაგრაფი 38(1) განსაზღვრავს „ორგანოს“ როგორც ავტონომიურ სახელმწიფო ადმინისტრაციულ ორგანოს. 38(3) პარაგრაფში *inter alia* ჩამოთვლილია „ორგანოს“ ვალდებულებები: ა) ჩაატაროს გამოკვლევები შეტყობინებებსა და *ex officio*; *ბ) წარმართოს ადმინისტრაციული საქმისწარმოება კლასიფიცირებული ინფორმაციის ex officio* ზედამხედველობისთვის; გ) წარადგინოს სარჩელი სასამართლოში ნებისმიერ დარღვევასთან დაკავშირებით, რომელიც შეეხება საზოგადოებრივი ინტერესის მატარებელ და საზოგადოებრივი ინტერესის გამო გასაჯაროებულ მონაცემებს; დ) ჩაერთოს სხვების მიერ აღძრულ საქმეებში.

ეს უკანასკნელი ჩამოყალიბდა ზედამხედველობის საგამომძიებლო და მაკორექტირებელი ადმინისტრაციული უფლებამოსილების საშუალებებთან ერთად, რათა გააძლიეროს პირადი ცხოვრების უფლების აღსრულება. ამ დროს მონაცემთა დაცვის ადმინისტრაციული პროცედურის ინიციირება შესაძლებელია მხოლოდ თანამდებობის მიხედვით.

61(1) პარაგრაფმა განსაზღვრა მონაცემთა დაცვის დებულებების დარღვევის სამართლებრივი შედეგები, რომლის მიხედვით, თავის გადაწყვეტილებებში, რომლებიც მიღებულია მონაცემთა დაცვის ადმინისტრაციულ საქმისწარმოებაში, „ორგანოს“ შეუძლია გასცეს არაკანონიერად დამუშავებული პერსონალური მონაცემების წაშლის ბრძანება ისეთი წესით, როგორც ეს დადგენილია „ორგანოს“ მიერ ან შეუძლია დააკისროს სხვა გზით დამუშავების დროებითი ან მუდმივი შეზღუდვა და დაადგინოს, რომ პერსონალური მონაცემები დამუშავდა არაკანონიერად, უბრძანოს ნებისმიერი არაზუსტი პერსონალური მონაცემების შესწორება, უბრძანოს არაკანონიერად დამუშავებული პერსონალური მონაცემების ბლოკირება, წაშლა ან განადგურება, აკრძალოს პერსონალურ მონაცემთა არაკანონიერი დამუშავება ან პერსონალურ მონაცემთა უცხო ქვეყანაზე გადაცემა ან გამჟღავნება, უბრძანოს მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდება, თუ დამმუშავებელმა არაკანონიერად გამოტოვა ან უარი თქვა შესრულებაზე და დააკისროს ჯარიმა.

2011 წლის CXII კანონს არ შეეძლო დაედგინა უფრო მკაფიოდ, რომ მონაცემთა სუბიექტს ჯერ კიდევ არ ქონდა შესაძლებლობა აღეძრა საჩივარი ადმინისტრაციული პროცედურის ფარგლებში.

გამომდინარე ყველა შედეგებიდან NAIH გადაიქცა ნამდვილი „ადმინისტრაციულ ორგანოდ“.

ადმინისტრაციული მართლმსაჯულების სისტემა სრულიად ახალ მდგომარეობაში აღმოჩნდა. 2011 წლის CXII კანონის საფუძველზე უნგრეთის ადმინისტრაციულმა სასამართლო პრაქტიკამ დაიწყო საკუთარი კონცეფციის შექმნა მონაცემთა დაცვის მატერიალური და პროცედურული სამართლის დარგში, მაგალითად, „ორგანოს“ საგამომძიებლო და მაკორექტირებელი უფლებამოსილების გამოყენების კომპეტენცია და პირობები.

3.2. საკითხები „ორგანოს“ კომპეტენციის შესახებ

2011 წლის CXII კანონის საფუძველზე უნგრეთის ადმინისტრაციული სასამართლო პრაქტიკა თითქმის მაშინვე დადგა მონაცემთა დაცვის სამართლის კონკრეტული საკითხებისა და პრობლემების გადაჭრის წინაშე. ამ საკითხებზე მიღებული იქნა გადაწყვეტილებები, რომლებიც მოიცავდნენ ძირითად რეკომენდაციებს მონაცემთა დაცვის ნორმების გამოყენებასთან დაკავშირებით.

უნგრეთის მონაცემთა დაცვის სამართლის ისტორიაში პირველი მოთხოვნა წინასწარი გადაწყვეტილების გამოტანასთან დაკავშირებით წარდგენილი იქნა ველტიმოს საქმეზე[23] ადმინისტრაციული სასამართლოს მიერ. ეს მოთხოვნა შეეხებოდა 1995 წლის 24 ოქტომბრის ევროპის პარლამენტისა და საბჭოს დირექტივების 95/46/EC მუხლებს - 4(1/ა) და 28(1)-(3) და (60) - პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალ მიმოცვლის შესახებ.

მოთხოვნა გაკეთდა სამართალწარმოების ფარგლებში ველტიმოს კომპანიას, რომელიც დარეგისტრირებულია სლოვაკეთში, და „ორგანოს“ შორის ჯარიმის შესახებ, რომელიც ამ უკანასკნელის მიერ დაეკისრა კომპანიას 2011 წლის CXII კანონის დარღვევისათვის, რომლითაც უნგრეთის კანონში შევიდა ცვლილებები დირექტივის 95/46 შესაბამისად. კომპანია ველტიმო მართავდა ვებსაიტს უნგრეთში უძრავი ქონების გაყიდვასთან დაკავშირებით. ამ მიზნით, მან დაამუშავა რეკლამის განმთავსებლების პერსონალური მონაცემები. რეკლამები უფასო იყო ერთი თვის განმავლობაში, მაგრამ შემდგომში აუცილებელი იყო გადასახადის გადახდა. რეკლამის ბევრმა განმთავსებელმა გაგზავნა მოთხოვნები იმეილებით, რომ მითითებული პერიოდიდან წაეშალათ მათი რეკლამებიც და პირადი მონაცემებიც, თუმცა, ველტიმომ არ წაშალა მონაცემები და მოსთხოვა დაინტერესებულ მხარეებს გადასახადი სერვისებისთვის. რადგანაც განმთავსებლებმა დაკისრებული თანხა არ გადაიხადეს, ველტიმომ გადაუგზავნა შესაბამისი რეკლამის განმთავსებლების პერსონალური მონაცემები ვალების შემგროვებელ სააგენტოებს. რეკლამის განმთავსებლებმა აღძრეს საჩივარი უნგრეთის მონაცემთა დაცვის ორგანოში.

„ორგანომ“ განაცხადა, რომ იგი კომპეტენტური იყო თუ მხედველობაში მიიღებდნენ, რომ შესაბამისი მონაცემების შეგროვება ნიშნავდა მონაცემთა

[23] იხ. მონაცემთა დაცვის კომისრის 2005 წლის მოხსენება, 35-46.

დამუშავებას ან ტექნიკურ ოპერაციას შესაბამისი ფიზიკური პირების მონაცემების დასამუშავებლად. მიიღეს რა მხედველობაში ველტიმოს მიერ 2011 წლის CXII კანონის დარღვევა, „ორგანომ“ დააკისრა კომპანიას ჯარიმა.

ველტიმომ სარჩელი აღძრა სასამართლოში, რომელმაც დაადგინა, რომ ის ფაქტი, რომ კომპანიას არ ქონდა რეგისტრირებული ოფისი ან ფილიალი უნგრეთში, არ წარმოადგენდა საფუძვლიან არგუმენტს დაცვისთვის, რადგან მონაცემთა დამუშავება და მონაცემების დამუშავების სერვისების მიწოდება შესაბამის უნგრულ საკუთრებასთან დაკავშირებით ხდებოდა უნგრეთში. თუმცა, სასამართლომ გააუქმა „ორგანოს“ გადაწყვეტილება სხვა ფაქტებთან დაკავშირებით სიცხადის ნაკლებობის გამო. ველტიმომ იურიდიული საკითხზე აპელაცია შეიტანა სასამართლოში განსახილველად, სადაც ამტკიცებდა რომ არ იყო საჭირო ფაქტების შემდგომი გარკვევა, რადგან დირექტივის 95/46 4(1/ა) ნორმის შესაბამისად, ამ შემთხვევაში უნგრეთის მონაცემთა დაცვის საზედამხედველო ორგანო არ იყო კომპეტენტური და არ შეეძლო გამოეყენებინა უნგრული კანონმდებლობა სხვა წევრ სახელმწიფოებში დაფუძნებული მომსახურების მიმწოდებლის შესახებ. კომპანია ველტიმო ამტკიცებდა, რომ 95/46 დირექტივის 28 (6) მუხლის შესაბამისად „ორგანოს“ უნდა მიემართა თხოვნით სლოვაკეთის მონაცემთა დაცვის ორგანოსთვის, რომ ემოქმედა მის ნაცვლად. უნგრეთის მონაცემთა დაცვის ორგანომ განაცხადა, რომ კომპანია ველტიმოს ჰყავდა წარმომადგენელი უნგრეთში, სახელდობრ, კომპანიის ერთ-ერთი მფლობელი, რომელიც წარმოადგენდა მას ადმინისტრაციულ და სასამართლო საქმეთაწარმოებაში, რომელიც ხდებოდა წევრ სახელმწიფოებში. „ორგანომ“ დაამატა, რომ კომპანია ველტიმოს ინტერნეტ სერვერები ინსტალირებული იყო გერმანიაში და ან ავსტრიაში, მაგრამ კომპანიის მფლობელები ცხოვრობდნენ უნგრეთში. გამომდინარე 95/46 დირექტივის 28(6) მუხლიდან, ორგანო ნებისმიერ შემთხვევაში უფლებამოსილია იმოქმედოს მიუხედავად მოქმედი კანონმდებლობისა.

სასამართლომ საბოლოოდ დაადგინა რომ დირექტივის 95/46/EC მუხლი 4(1)(ა) უნდა იყოს განმარტებული, როგორც წევრი სახელმწიფოს პერსონალურ მონაცემთა კანონის გამოყენების უფლება გარდა იმ წევრ-სახელმწიფოსი, სადაც ამ მონაცემთა დამმუშავებელია რეგისტრირებული, რამდენადაც ის დამმუშავებელი განახორციელებს რეალურ და ეფექტურ აქტივობებს, თუნდაც მინიმალურს, სტაბილური მოწესრიგების საშუალებით იმ წევრ-სახელმწიფოს ტერიტორიაზე რომლის კონტექსტშიც ხდება მონაცემთა დამუშავება. იმისათვის რომ დადგინდეს, არსებობს თუ არა ძირითად სამართალწარმოებაში განსახილველის მსგავსი გარემოებები, სასამართლოს შეუძლია მხედველობაში მიიღოს კერძოდ ის ფაქტი (i) რომ დამმუშავებლის ქმედება იმ დამუშავებასთან მიმართებაში რომლის კონტექსტშიც ეს დამუშავება ხდება, მოიცავს იმ უძრავი ქონების ვებსაიტების მართვას რომლებიც მდებარეობენ იმავე წევრ-სახელმწიფოს ტერიტორიაზე, ასევე იწერება იმავე წევრ-სახელმწიფოს ენაზე, და ამის შედეგად, იგი ძირითადად ან მთლიანად მიმართულია ამავე წევრ-სახელმწიფოსადმი, და რომ (ii) მოცემულ წევრ-სახელმწიფოში მონაცემთა დამმუშავებელს ჰყავს წარმომადგენელი, რომელიც პასუხისმგებელია აანაზღაუროს იმ ქმედებებიდან გამომდინარე ვალები და წარმოადგინოს დამმუშავებელი ადმინისტრაციულ და სასამართლო საქმის წარმოებაში შესაბამისი მონაცემების დამუშავების შესახებ. თუმცა, საკითხი იმ

პიროვნების ეროვნებასთან დაკავშირებით, რომელსაც ასეთი მონაცემთა დამუშავება ეხება, არა რელევანტურია.

რაც შეეხება „ორგანოს“ საზედამხედველო უფლებამოსილებას, სასამართლომ დაადგინა, რომ სადაც წევრ-სახელმწიფოს საზედამხედველო ორგანო, რომელშიც საჩივარი იქნა წარდგენილი დირექტივის 95/46 მუხლი 28(4) შესაბამისად, გამოიტანს დასკვნას რომ კანონი, რომელიც ვრცელდება აღნიშნულ პერსონალურ მონაცემთა დამუშავებაზე, წარმოადგენს არა იმ წევრ-სახელმწიფოს არამედ სხვა წევრ-სახელმწიფოს კანონმდებლობას, ამ დირექტივის 28(1)-(3) და (6) მუხლების ინტერპრეტაცია უნდა ნიშნავდეს, რომ საზედამხედველო ორგანოს შეუძლია განახორციელოს ინტერვენციის ეფექტური უფლებამოსილება, რომელიც მას მინიჭებული აქვს იმავე დირექტივის 28(3) მუხლით, მხოლოდ თავისი საკუთარი წევრ-სახელმწიფოს ფარგლებში. შესაბამისად, ამ წევრ-სახელმწიფოს კანონმდებლობის საფუძველზე მას არ შეუძლია დააკისროს ჯარიმა მონაცემთა დამმუშავებელს იმ მონაცემების დამუშავებასთან დაკავშირებით, რომლებიც არ არის შექმნილი ამავე ტერიტორიაზე, მაგრამ ამავე დირექტივის 28(6) მუხლის მიხედვით ზომების მისაღებად უნდა მიმართოს იმ წევრ-სახელმწიფოს საზედამხედველო ორგანოს, რომლის კანონმდებლობაც მოქმედებს.

3.3. „ორგანოს“ მაკორექტირებელი უფლებამოსილების სფერო

„ორგანო“, ამგვარად, გახდა ადმინისტრაციულ ორგანო არა მარტო სამართალწარმოებაში, არამედ მონაცემთა დაცვის დარღვევების ადმინისტრაციული სანქციების კუთხითაც. რადგანაც ამ სანქციების ფუნდამენტური ბუნება უარყოფითად მოქმედებს მონაცემთა დამმუშავებელზე, პირობები და ფარგლები, რომლებშიც „ორგანოს“ შეუძლია მათი გამოყენება, უკვე საკვანძო საკითხია 2011 წლის CXII კანონის შესაბამისად აღძრულ ადმინისტრაციულ სარჩელებში.

ადმინისტრაციული სასამართლო პრაქტიკა, რომელსაც საფუძვლად ეს კანონი უდევს ცდილობს გააფართოოს „ორგანოს“ მექანიზმები ფუნდამენტური კანონისა და აქტის საკანონმდებლო მიზნის შესაბამისად. მართლაც, ამ კანონის მიღების და „ორგანოს“ დაფუძნების ერთ-ერთ მიზეზი იყო შემდეგი: *„კომისრის პრაქტიკამ აჩვენა რომ კომისრის უფლებამოსილება და მექანიზმები ვერ უზრუნველყოფენ საკმარის თავისუფლებას შეფასებისათვის და შესაძლებლობას მონაცემთა დაცვის დარღვევის გამოძიებისა და სანქცირებისათვის. საინფორმაციო ტექნოლოგიის გავრცელება, სოციალური ჩვევების ცვლილება და ახალი სიტუაცია, რომელიც შეიქმნა გლობალიზაციით, მოითხოვს მნიშვნელოვნად უფრო ეფექტურ ქმედებას სახელმწიფო ორგანოებისგან, ვიდრე ომბუდსმენის ტიპის სისტემას, რომელიც ჩამოყალიბდა 90-ს შუა წლებში, შეეძლო უზრუნველეყო. ადმინისტრაციული ორგანო წარმოადგენს უფრო შესაფერის ორგანიზაციულ ფორმას, ამიტომ აუცილებელია შეიქმნას სახელისუფლებო ორგანო, რომელიც შეძლებს წინ აღუდგეს ახალ გამოწვევებს. ახალი გარემოებები საჭიროს ხდის ახალი რეგულაციისა და ორგანიზაციის შექმნას ამ სფეროში, რომელიც შეესაბამება ფუნდამენტური კანონის კონცეფციას და აკმაყოფილებს ევროკავშირის მოლოდინებს“.*[24]

უნგრეთის უზენაესი სასამართლოს მიდგომა შეესაბამებოდა ამ მიზანს: *„61(1)(a)-(g) განყოფილება განსაზღვრავს იმ ზომების ბუნებას რომელთა გამოყენება*

[24] იხ. მონაცემთა დაცვის კომისრის 2005 წლის მოხსენება, 134-135.

შეიძლება მონაცემთა დაცვის ორგანოს გადაწყვეტილებებში. მაკორექტირებელი მექანიზმები მოიცავს, მაგალითად, პერსონალურ მონაცემთა არაკანონიერი დამუშავების დადგენის შესაძლებლობას, დამუშავების გაგრძელების აკრძალვას, უკანონოდ დამუშავებული პერსონალური მონაცემების დაბლოკვას, ბრძანებას მათი საზღვარგარეთ პორტირების შეწყვეტის თაობაზე ან ჯარიმის დაკისრებას“.[25]

მაგალითად, დამუშავების ex officio აკრძალვის კონტექსტში, სასამართლოს გადაწყვეტილების საფუძველს წარმოადგენდა ის რომ *„პერსონალურ მონაცემთა დამუშავებას შეეძლო დაერღვია მონაცემთა დაცვის წესები მრავალნაირად, სხვადასხვანაირი ქცევითა და უმოქმედობით. შეუძლებელია მათი დეტალურად ჩამოთვლა, ასე რომ 2011 წლის CXII კანონი ზოგადად უზრუნველყოფს არაკანონიერი დამუშავების აკრძალვის შესაძლებლობას. „ორგანოს“ მაკორექტირებელი უფლებამოსილებები უნდა შესრულდეს მოპასუხის მიერ კონკრეტულ შემთხვევაში, საქმის კონკრეტული თავისებურებების გათვალისწინებით.*[26]

4. მონაცემთა დაცვის ძირითადი რეგულაცია[27] (2018): ევროკავშირისა და უნგრეთის კანონმდებლობას შორის ურთიერთქმედება

4.1. რევოლუციური ცვლილება: მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოება მონაცემთა სუბიექტის მოთხოვნით

2018 წლის 25 მაისს, მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) ძალაში შევიდა, როდესაც გაფართოებული და გაღრმავებული ადმინისტრაციული სასამართლო პრაქტიკა სულ უფრო და უფრო ვითარდებოდა. მონაცემთა დაცვის ძირითადმა რეგულაციამ (GDPR) სასამართლო და ადმინისტრაციული პრაქტიკა არ დააბრუნა უკან საწყის ხაზზე.

თუმცა, უნდა აღინიშნოს რამდენიმე ორიენტაცია რომლებმაც შესაძლოა განსაზღვრონ GDPR-ის ინტერპრეტაცია მომავალში.

რეგულაციამ შემოიტანა „რევოლუციური“ ინოვაცია უნგრულ კანონმდებლობაში. GDPR-ის 77(1) მუხლი უზრუნველყოფს რომ ნებისმიერი სხვა ადმინისტრაციული ან სამართლებრივი საშუალებების დაზარალების გარეშე, თითოეულ მონაცემთა დაცვის სუბიექტს უნდა ჰქონდეს უფლება აღძრას საჩივარი საზედამხედველო ორგანოში, კერძოდ, იმ წევრ-სახელმწიფოში სადაც არის მისი მუდმივი საცხოვრებელი ან სამუშაო ადგილი ან დაუმტკიცებელი დარღვევის ადგილი, თუ მონაცემთა სუბიექტს მიაჩნია რომ მის შესახებ პერსონალურ მონაცემთა დამუშავებას შეუძლია დაარღვიოს ეს რეგულაცია.

უნგრეთის კანონმდებლობამ - ევროპის კავშირის ფუნდამენტური უფლებების ქარტიის 41 და 47-ე მუხლების შესაბამისად - გადათარგმნა ეს წესები უნგრულ ადმინისტრაციულ პროცედურულ კანონმდებლობაში, რითაც შესაძლებელი გახადა ადმინისტრაციული სამართალწარმოების გადაცემა „ორგანოში“ მონაცემთა სუბიექტის მოთხოვნის (საჩივრის) საფუძველზე. სწორედ ამიტომ, 2011 წლის CXII

[25] 2015 წლის პირველი ოქტომბრის სასამართლო გადაწყვეტილება, C-230/14, EU:C:2015:639.
[26] 2011 წლის XCII კანონის მოსამზადებელი დოკუმენტი.
[27] Kúria Kfv.III.37.911/2017/8.

კანონის 60(1) განყოფილებში დადგენილია, რომ პერსონალურ მონაცემთა დავის უფლების გამოყენების მიზნით, „ორგანომ“ უნდა აღძრას მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოება მონაცემთა სუბიექტის განცხადების საფუძველზე და შეუძლია მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოების *ex officio* წამოწყება.

ამ ერთი შეხედვით მარტივმა წესმა წარმოშვა მთელი რიგი ინტერპრეტაციის საკითხები არა მარტო „ორგანოს“ არამედ ადმინისტრაციული სამართლის სასამართლო პრაქტიკაშიც. მართლაც, ზოგადი ადმინისტრაციული სამართალწარმოების თეორია აშკარად განასხვავებს მხარის მიერ და *(ex officio)* თანამდებობის მიხედვით ინიციირებულ ადმინისტრაციულ სამართალწარმოებას ერთმანეთისაგან. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) 77/78-ე მუხლები, გარდა სამართლებრივად დამავალდებულებელი უფლებამოსილების მქონე საზედამხედველო ორგანოსი და ეფექტური სასამართლო განხილვის გადაწყვეტილებისა, არ შეიცავენ დამატებით პროცედურულ ნორმებს, რომლებიც არეგულირებენ კონკრეტულ სამართალწარმოებას ეროვნული კანონმდებლობის მიხედვით, წევრ-სახელმწიფოების ინსტიტუციური და პროცედურული ავტონომიის შესახებ ევროკავშირის სამართლის პრინციპების შესაბამისად.

მონაცემთა სუბიექტის მოთხოვნით წარმოდგენილი სამართალწარმოების განმასხვავებელი თავისებურება მდგომარეობს იმაში, რომ ამ შემთხვევაში ადმინისტრაციული სამართალწარმოება ინიციირებულია არა „ორგანოს“ პროფესიონალური შეფასების საფუძველზე, არამედ მონაცემთა სუბიექტის სურვილით. მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) მიხედვით პროფესიონალური იურიდიული დახმარება „ორგანოს“ სამართალწარმოებაში არ მოითხოვება. თუმცა, ამას მივყავართ იმ პრაქტიკულ შედეგამდე, რომ პროცესუალური ნორმების შესრულებაზე მოთხოვნის ხარისხი და კონტექსტი უკიდურესად განსხვავებულია.

განცხადების წარდგენისას მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოება ავტომატურად იხსნება მონაცემთა დაცვის ძირითადი რეგულაციისა და ეროვნული ზოგადი ადმინისტრაციული კანონის მიხედვით. პრობლემა მდგომარეობს იმაში, რომ თუმცა „ორგანო“ ვალდებულია მოამზადოს საკმარისად დეტალური და დასაბუთებული გადაწყვეტილება ამ ტიპის სამართალწარმოებაში, მოთხოვნის შინაარსი ხშირად არ იძლევა ამის გაკეთების საშუალებას, და „ორგანო“ ხშირად დგას არასრული, წინააღმდეგობრივი და დაუსაბუთებელი მტკიცების წინაშე, რომელზეც მის თანამშრომელ დამმუშავებლებსაც კი უჭირთ აზრიანი პასუხის გაცემა.

თუმცა, ეს არის ადმინისტრაციული სამართალწარმოებისა და დავის ერთ-ერთი კლასიკური და ფუნდამენტური საკითხი: რამდენად არის ვალდებული ადმინისტრაციული ორგანიზაცია, ამ შემთხვევაში „ორგანო“, გაარკვიოს ფაქტები და დაადგინოს მიზეზები, და როდის შეძლებს მიიღოს ერთმნიშვნელოვანი გადაწყვეტილება მონაცემთა დაცვაზე პასუხისმგებლობის დადგენისა და სუბიექტისთვის სერიოზული ადმინისტრაციული სანქციების დაკისრებასთან დაკავშირებით, როგორც ამას მოითხოვს მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR). პრეცედენტულ სამართალში გარკვევით არის დადგენილი, რომ „ორგანო“ არ წარმოადგენს სამართალდამცავ ორგანოს, რომელიც აწარმოებს სისხლის სამართლის გამოძიებას.

„ორგანო“, ხშირად, დგას ისეთი ფაქტის წინაშე, როდესაც შეუძლია, დაეყრდნოს მხოლოდ მცირე რაოდენობის მტკიცებულებებს მონაცემთა სუბიექტის

მოთხოვნისა და სამართალწარმოების მიმდინარეობისას გაკეთებული მხარეების განცხადებების ჩათვლით, რომლებიც უმეტეს შემთხვევებში აშკარად ურთიერთსაწინააღმდეგოა.

გადაწყვეტილების თანახმად *„მონაცემთა სუბიექტის მოთხოვნის საფუძველზე დაწყებულ სამართალწარმოებებში, „ორგანომ“ უნდა დაადგინოს ფაქტები იმ მოცულობით რაც საჭიროა გადაწყვეტილების მისაღებად და, შესაბამისად, მან უნდა განახორციელოს სამართალწარმოება იმისათვის რომ მოძებნოს რელევანტური მტკიცებულებები. თუმცა, „ორგანო“ არ არის ვალდებული მოიძიოს განმცხადებლისთვის საინტერესო მტკიცებულებები [...].“* გარდა ამისა, პრეცედენტული სამართლის მიხედვით, სწორედ განმცხადებელმა უნდა დაამტკიცოს „ორგანოს“ გადაწყვეტილების არაკანონიერება სასამართლოში ადმინისტრაციული საქმეების განხილვის პროცესში. გადაწყვეტილების თანახმად, სწორედ განმცხადებელმა უნდა დაამტკიცოს, რომ გასაჩივრებული გადაწყვეტილება იურიდიულად ძალადაკარგულია კანონის დარღვევის გამო.

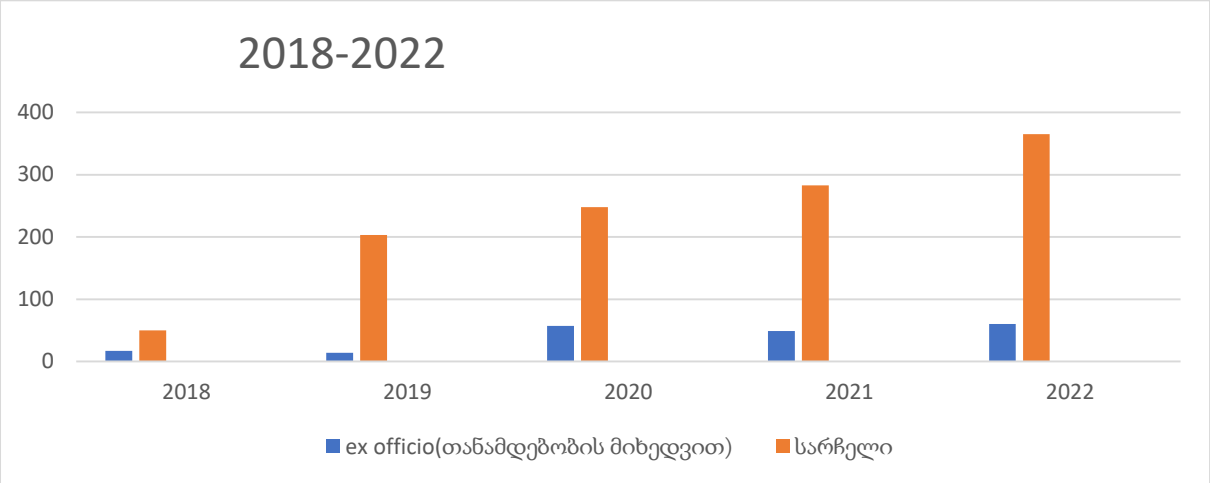
მონაცემთა დაცვის ძირითადი კანონის (GDPR) მიხედვით, მოთხოვნები ხშირად მხოლოდ განცხადებებსა და ვარაუდებს შეიცავენ, მაგრამ მონაცემთა სუბიექტს არ შეუძლია წარმოადგინოს რამე მატერიალური მტკიცებულება რომლითაც პერსონალურ მონაცემთა კონკრეტული დამუშავების რომელიმე ასპექტის, კანონიერების ან უკანონობის, დადგენა არის შესაძლებელი. ზუსტად ამ მიზეზით სასამართლო პრაქტიკამ დაადგინა ზემოხსენებულის შესაბამისად, რომ *„ფაქტობრივად ხელმისაწვდომი პერსონალური მონაცემების დამუშავების არარსებობის შემთხვევაში, შეუძლებელია მოთხოვნის განხილვა განხორციელდეს ობიექტურად „ორგანოს“ მიერ „*

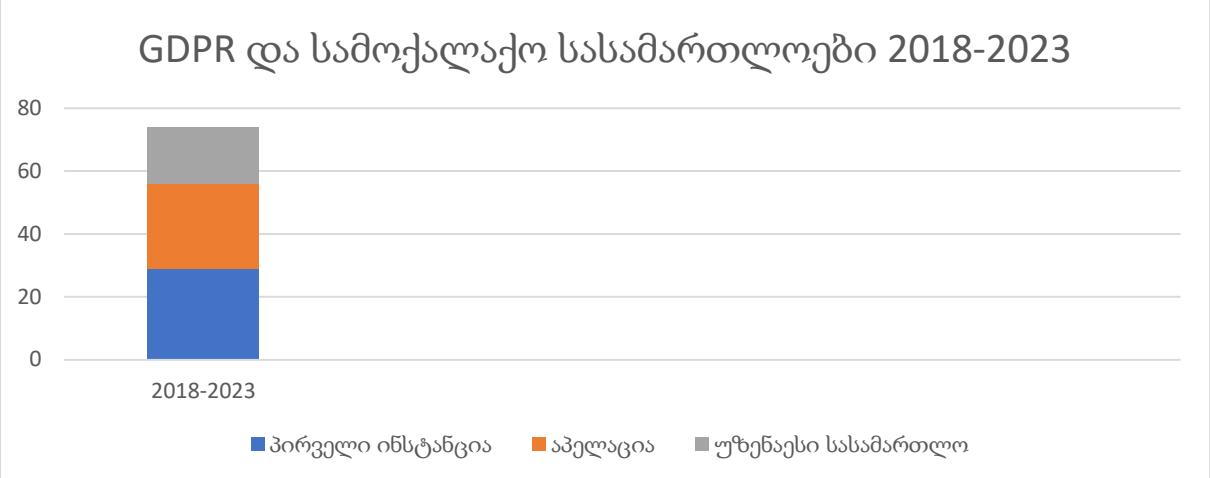
თუმცა, სანამ გავაანალიზებთ „ორგანოს“ მაკორექტირებელ უფლებამოსილებასთან დაკავშირებული უმნიშვნელოვანეს საკითხებს, მოდით რიცხვებით ვაჩვენოთ ის რევოლუციური ცვლილებები, რომლებიც მოხდა მონაცემთა დაცვის ძირითადი რეგულაციის ძალაში შესვლასთან დაკავშირებით. მიუხედავად უეჭველი პროცედურული სირთულეებისა, GDPR ნამდვილად წარმოშვა მნიშვნელოვანი ცვლილებები მონაცემთა სუბიექტებისთვის რათა მათ შეძლონ მონაცემთა დაცვის ძირითადი რეგულაციით გარანტირებული მონაცემთა დაცვის უფლების გამოყენება.

საინტერესოა სტატისტიკა რეგულაციის ძალაში შესვლამდე და მის შემდეგ:

- ადმინისტრაციული სარჩელების რაოდენობა ყოფილი ეროვნული მონაცემთა დაცვის 2014-2018 წლების კანონმდებლობის საფუძველზე (GDPR ძალაში შესვლა);
- ადმინისტრაციული სარჩელების რაოდენობა GDPR 2018-2023 საფუძველზე: 131 (პირველი ინსტანცია, აპელაცია და განხილვა დახურულია განჩინებით) [GDPR, მუხლი 78];
- ადმინისტრაციული სარჩელების რაოდენობა GDPR 2018-2023 საფუძველზე: 74 (პირველი ინსტანცია, აპელაცია და განხილვა დახურულია განჩინებით) [GDPR, მუხლი 79];
- წინასწარი გადაწყვეტილების მიღებაზე მიმართვების რაოდენობა 2004-2018 (95/46/EC): 1 (ადმინისტრაციული სასამართლოს მიერ);
- წინასწარი გადაწყვეტილების მიღებაზე მიმართვების რაოდენობა 2018-2023 (GDPR): 4 (ყველა - ადმინისტრაციული სასამართლო);

- წინასწარი გადაწყვეტილების მიღებაზე მიმართვების რაოდენობა 2004-2018 (ზოგადად);
- წინასწარი გადაწყვეტილების მიღებაზე მიმართვების რაოდენობა 2018-2023 (ზოგადად):27 [უნგრეთის მთელი მოთხოვნების 15% შეეხება მონაცემთა დაცვის საკითხებს!];
- მონაცემთა სუბიექტების მოთხოვნის საფუძველზე მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოების რაოდენობა 2004-2018: 0 (რადგანაც მხოლოდ *ex officio ადმინისტრაციული სამართალწარმოება რეგულირდება კანონმდებლობით)*;
- მონაცემთა სუბიექტების მოთხოვნის საფუძველზე მონაცემთა დაცვის ადმინისტრაციული სამართალწარმოების რაოდენობა 2018-2023: 1149 [GDPR მუხლი 77(1)];
- მონაცემთა დაცვის *ex officio* ადმინისტრაციული სამართალწარმოების 2018-2023: 197;
- სასამართლო განხილვის საშუალო პროცენტი წელიწადში ადმინისტრაციული სამართალწარმოების საერთო რაოდენობიდან (ოფიციალური და *ex officio საჩივრები):* 9,7%.





4.2. საკითხები მაკორექტირებელი საზედამხედველო უფლებამოსილებების შესახებ GDPR-ის მიხედვით

წევრ-სახელმწიფოს საზედამხედველო ორგანო პასუხისმგებელია მონაცემთა დაცვის ძირითადი რეგულაციის გამოყენების კონტროლზე, რათა დაიცვას ფიზიკურ პირთა ფუნდამენტური უფლებები და თავისუფლებები მონაცემთა დამუშავების მხრივ და ხელი შეუწყოს პერსონალურ მონაცემთა თავისუფალ გავრცელებას ევროპის ეკონომიკური ზონის ფარგლებში. ამ მხრივ, მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR) მუხლი 57(1/ა) ითვალისწინებს, რომ თითოეულმა საზედამხედველო ორგანომ უნდა უზრუნველყოს ამ რეგულაციის გამოყენება მის ტერიტორიაზე.

ეს ვალდებულება უნდა შესრულდეს მიუხედავად იმისა, საზედამხედველო ორგანო თანამდებობის მიხედვით *(ex officio)* მოქმედებს თუ საჩივრის საფუძველზე, თუმცა, იმისათვის რომ ეს ვალდებულება შესრულდეს, საზედამხედველო ორგანოები უნდა ფლობდნენ ეფექტურ მექანიზმებს, რომლებიც საშუალებას მისცემს მათ იმოქმედონ რეგულაციის დარღვევის წინააღმდეგ. ამისათვის, მონაცემთა დაცვის ძირითადი რეგულაციის 58(2) მუხლი ითვალისწინებს მაკორექტირებელი უფლებამოსილებების წყებას, რომლის გამოყენებაც შეუძლია საზედამხედველო ორგანოს.

მონაცემთა დაცვის ძირითადი რეგულაციის 58(2) მუხლის შესაბამისად თითოეული საზედამხედველო ორგანოს უნდა ჰქონდეს შემდეგი მაკორექტირებელი უფლებამოსილებები:

ა) გაფრთხილების გაცემა დამმუშავებელზე და უფლებამოსილ პირზე იმის თაობაზე, რომ სავარაუდო დამუშავების ოპერაციებმა შეიძლება დაარღვიონ რეგულაციის დებულებები;

ბ) საყვედურის გამოცხადება დამმუშავებელსა და უფლებამოსილ პირისთვის როცა სავარაუდო დამუშავების ოპერაციები დაარღვევენ ამ რეგულაციის დებულებებს;

გ) გასცეს განკარგულება დამმუშავებელსა და უფლებამოსილ პირზე, რომ შეასრულონ მონაცემთა სუბიექტის მოთხოვნები მისი უფლებების ამ რეგულაციის შესაბამისად განხორციელებასთან დაკავშირებით;

დ) გასცეს განკარგულება დამმუშავებელსა და უფლებამოსილ პირზე, რომ მოიყვანონ დამუშავების ოპერაციები ამ რეგულაციის დებულებებთან შესაბამისობაში, თუ საჭიროა, კონკრეტული წესით და კონკრეტულ დროში;

ე) გასცეს განკარგულება დამმუშავებელზე, რომ შეატყობინოს მონაცემთა სუბიექტს პერსონალურ მონაცემთა დარღვევის თაობაზე;

ვ) დააკისროს დროებითი ან მუდმივი შეზღუდვა დამუშავების აკრძალვის ჩათვლით;

ზ) გასცეს განკარგულება პერსონალურ მონაცემთა შესწორების ან ამოშლის ან დამუშავების შეზღუდვაზე 16, 17 და 18 მუხლების შესაბამისად და ასეთი ქმედებების შესახებ მიმღების, ვისთანაც მოხდა პერსონალური მონაცემების გამჟღავნება, ინფორმირების შესახებ მუხლი 17(2) და მუხლი 19 შესაბამისად;

თ) გააუქმოს სერტიფიკაცია ან უბრძანოს მოწმობის გამცემ ორგანოს გაცემული მოწმობის გაუქმება 42-ე და 43-ე მუხლების შესაბამისად ან უბრძანოს მოწმობის გამცემ ორგანოს არ გასცეს მოწმობები თუ სერტიფიკაციის მოთხოვნები არ სრულდება ან შეწყდა მათი შესრულება;

ი) დაეკისროს ადმინისტრაციული ჯარიმა 83-ე მუხლის შესაბამისად, გარდა ან ნაცვლად ამ პარაგრაფში მოხსენებული ზომებისა, გამომდინარე თითოეული ინდივიდუალური შემთხვევის გარემოებიდან;

კ) უბრძანოს მონაცემთა მიმღებისათვის მონაცემთა მესამე ქვეყანაში ან საერთაშორისო ორგანიზაციაში მიწოდების დროებითი შეწყვეტა.

„მტკიცე აღსრულება“, „წესების თანმიმდევრული და ერთგვაროვანი გამოყენება“, „მონიტორინგისა და აღსრულების უზრუნველყოფის ეკვივალენტური უფლებამოსილებები“, „დარღვევებისთვის ეკვივალენტური სანქციები“, და „ერთნაირი ამოცანები და ეფექტური უფლებამოსილებები (...) მაკორექტირებელი უფლებამოსილების ჩათვლით“ - ეს ყველაფერი გათვალისწინებულია მონაცემთა დაცვის ძირითადი რეგულაციის[28] დეკლარაციულ ნაწილში. ევროპული მონაცემთა დაცვის საბჭოს (EDPB) მიხედვით, საზედამხედველო ორგანიზაციის მაკორექტირებელი უფლებამოსილების თანმიმდევრულ გამოყენებას აქვს საკვანძო მნიშვნელობა მონაცემთა დაცვის სტაბილური დონისათვის ევროპის ეკონომიკურ ზონაში[29]. ეს შეხედულება შესაბამისობაშია მონაცემთა დაცვის თეორიასთან: *„GDPR აძლიერებს საზედამხედველო ორგანოების სისტემას და მათ დამოუკიდებლობასა და უფლებამოსილებას სპეციალური VI თავის ფარგლებში, და ქმნის თანამშრომლობისა და თანამიმდევრულობის მექანიზმს VII თავში[30]“*

თუმცა, ამ საზედამხედველო უფლებამოსილებების ურთიერთქმედების შესახებ ინტერპრეტაცია წარმოშობს კითხვებს განსაკუთრებით სახელისუფლებო ორგანოს *ex*

[28] Kf.VI.37.956/2018/6.

[29] ევროპის პარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია 2016/679 (EU) პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ, რომელიც აუქმებს 95/46/EC დირექტივას (მონაცემთა დაცვის ძირითადი რეგულაცია), OJ 2016 L 119, გვ.1 / შემდგომში მოიხსენიება როგორც GDPR.

[30] GDPR 7, 10-11 და 129. ასევე, იხ. მოსაზრება 39/2021, იმის შესახებ შეიძლება თუ არა GDPR მუხლი39/2021 გამოყენებული იყოს როგორც სამართლებრივი საფუძველი საზედამხედველო ორგანოს ex officio ბრძანების პერსონალურ მონაცემთა წაშლის თაობაზე იმ სიტუაციაში როცა ასეთი მონაცემი არ იყო მიწოდებული მონაცემთა სუბიექტის მიერ (მიღებულია 2021 წლის 14 დეკემბერს), იხ. <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf> [8.01.2024].

officio მაკორექტირებელი უფლებამოსილებებისა და მონაცემთა სუბიექტების უფლებების შესაძლებელ შეჯახებასთან დაკავშირებით. უნგრეთის ადმინისტრაციული სასამართლოს მიერ ეს საკითხი გადაეცა ევროპის სამართლიანობის სასამართლოს წინასწარი გადაწყვეტილების გამოსატანად, რომელსაც შეუძლია ფუნდამენტურად განსაზღვროს მონაცემთა დაცვის საზედამხედველო ორგანოების მაკორექტირებელი უფლებამოსილების ძალა და ფარგლები მომავალში.

თავის კითხვებში კომპეტენტური იურისდიქციის სასამართლო არსებითად ინტერესდება, GDPR -ს მუხლი 58(2) -ს (c/d) და (g) ქვეპუნქტები უნდა იყოს თუ არა ინტერპრეტირებული იმ მნიშვნელობით, რომ ეროვნული საზედამხედველო ორგანოს თავისი მაკორექტირებელი უფლებამოსილების განხორციელებისას შეუძლია დაავალოს მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს არაკანონიერად დამუშავებული პერსონალური მონაცემების ამოშლა, თუნდაც მონაცემთა სუბიექტის პირდაპირი მოთხოვნის არარსებობის შემთხვევაში GDPR-ის 17(1) მუხლის შესაბამისად? თუ პირველი კითხვის პასუხი მდგომარეობს იმაში, რომ საზედამხედველო ორგანოს შეუძლია დაავალოს მონაცემთა დამმუშავებელს ან უფლებამოსილ პირს არაკანონიერად დამუშავებული პერსონალური მონაცემების ამოშლა, თუნდაც მონაცემთა სუბიექტის პირდაპირი მოთხოვნის არარსებობის შემთხვევაში, მაშინ ეს პერსონალური მონაცემები მოპოვებულია თუ არა მონაცემთა სუბიექტისგან?

რაც შეეხება გადაწყვეტილების იმ ნაწილს, რომელიც შეეხება კონკრეტულ შემთხვევაში პერსონალური მონაცემების ამოშლას, განმცხადებელი აცხადებს, რომ GDPR-ის 58(2) მუხლი არ აძლევს „ორგანოს“ ასეთი ბრძანების გაცემის უფლებამოსილებას. განმცხადებელი ამტკიცებს, რომ მონაცემთა დამმუშავებლის ვალდებულება მონაცემთა ამოშლაზე, მიუხედავად იმისა ეს მოითხოვა თუ არა მონაცემთა სუბიექტმა, გამომდინარეობს GDPR-ის მე-5 მუხლიდან და არა ამავე რეგულაციის 17(1) მუხლიდან, რადგან მონაცემთა ამოშლა GDPR-ის 17(1) მუხლის შესაბამისად შეიძლება ინტერპრეტირებული იყოს, როგორც მონაცემთა სუბიექტის უფლება და 17(1) მუხლში მოცემული წინადადების მეორე ნაწილის ინტერპრეტაცია შეიძლება მოხდეს მხოლოდ ამ უფლების განხორციელების კონტექსტში, დამოუკიდებლად კი არა, არამედ იმ პირობით თუ ამ უფლების გამოყენება ხდება ხსენებული პირის მიერ.

წინასწარი გადაწყვეტილების მოთხოვნის განხილვამდე, 2022 წლის 23 მარტის No. 3110 გადაწყვეტილებით უნგრეთის კონსტიტუციურმა სასამართლომ დაადგინა, რომ უნგრეთის ფუნდამენტური კანონის E(2), (3) და VI(4) მუხლების მიხედვით ასევე GDPR-ის - როგორც ევროკავშირის კანონმდებლობა, რომელიც ცალსახად უზრუნველყოფს მონაცემთა დაცვისა და ინფორმაციის თავისუფლებას - შესაბამისად, „ორგანოს“ აქვს უფლებამოსილება დაავალოს უკანონოდ დამუშავებული პერსონალური მონაცემების *ex officio* ამოშლა, იმ შემთხვევის ჩათვლით როცა არ არსებობს მონაცემთა სუბიექტის მოთხოვნა.

უნგრეთის ადმინისტრაციული სასამართლოს პირველი ინსტანცია სრულად არ იზიარებს კონსტიტუციური სასამართლოს პოზიციებს. სასამართლოს აზრით, GDPR-ის მე-17 მუხლის მიხედვით, ამოშლის უფლება უნდა განიმარტოს როგორც მონაცემთა სუბიექტის უფლება და 17(1) მუხლი არ ადგენს ორ ცალკეულ სამართლებრივ საფუძველს მონაცემთა ამოშლისათვის. ამის ნაცვლად, ამ პუნქტის

წინადადების მეორე ნახევარი (დამმუშავებელი ვალდებული უნდა იყოს ამოშალოს [მონაცემთა სუბიექტის} მონაცემები უსაფუძვლო დაყოვნების გარეშე) წარმოადგენს მონაცემთა დამმუშავებლის ვალდებულებას, რომელიც გამომდინარეობს ამავე წინადადების პირველი ნაწილისგან. ამის შედეგად, საბჭოს შეხედულების 39/2021 მოსაზრების საწინააღმდეგოდ, ამ სასამართლოს მიაჩნია რომ GDPR-ის მე-17 მუხლის მიხედვით, წაშლის უფლება შეიძლება განიმარტოს როგორც მონაცემთა სუბიექტის უფლება. ამას ამტკიცებს ის ფაქტიც, რომ GDPR -ის ინგლისურ ორიგინალ ტექსტში მონაცემთა დამმუშავებლის ვალდებულების განსაზღვრებისას 17(1) მუხლში გამოყენებულია კავშირი „და“ პირველ და მეორე წინადადებებს შორის.

სასამართლოს მიხედვით, საკითხი, რომელიც აუცილებლად უნდა გადაიჭრას მდგომარეობს შემდეგში შეუძლია თუ არა ეროვნულ საზედამხედველო ორგანოს დაავალდებულოს მონაცემთა დამმუშავებელი ან უფლებამოსილ პირი წაშალონ უკანონოდ დამუშავებული მონაცემები, მიუხედავად მონაცემთა სუბიექტის მიერ თავისი უფლების გამოყენებისა, და თუ შეუძლია, რა სამართლებრივ საფუძველზე; ამ კითხვაზე პასუხის გაცემისას, მხედველობაში უნდა მივიღოთ, კერძოდ, ის რომ GDPR-ის 58(2/c) მუხლი ცალსახად ეფუძნება მონაცემთა სუბიექტის მოთხოვნას მისი უფლების განხორციელებაზე და 58(2/d) მუხლი ზოგადად ითვალისწინებს, რომ დამუშავების ოპერაციები უნდა შეესაბამებოდეს მონაცემთა დაცვის ზოგად რეგულაციას, ხოლო 58(2/g) მუხლი პირდაპირ მიუთითებს 17 მუხლზე, რომელიც არ შეიძლება ინტერპრეტირებული იყოს პერსონალურ მონაცემთა წაშლასთან დაკავშირებით მონაცემთა სუბიექტის მიერ ცალსახა მოთხოვნის აუცილებლობის მხედველობაში მიუღებლად, როგორ ეს ზემოთ არის განმარტებული.

იმისათვის, რომ შეაფასოს გამოიყენება თუ არა საზედამხედველო ორგანოების უფლებამოსილება GDPR-ის 58 (2/g) მუხლის შესაბამისად მაშინაც კი, როცა არ არსებობს მონაცემთა სუბიექტის მოთხოვნა მონაცემების წაშლასთან დაკავშირებით, საბჭომ თავდაპირველად უნდა განიხილოს, GDPR-ის მე-17 მუხლი აკისრებს თუ არა მონაცემთა დამმუშავებელს ვალდებულება, მხოლოდ მონაცემთა სუბიექტის მოთხოვნისას თუ როცა ეს ვალდებულება მისგან დამოუკიდებელია. ამ მხრივ, საბჭომ დაადგინა რომ GDPR-ის მე-17 მუხლი ითვალისწინებს წაშლის ორ ცალკეულ შემთხვევას, რომლებიც ერთმანეთისგან დამოუკიდებელია: I. მონაცემთა სუბიექტის მოთხოვნის საფუძველზე წაშლა და II. წაშლა როგორც მონაცემთა დამმუშავებლის დამოუკიდებელი ვალდებულება. საბჭოს ამ დასკვნას ამყარებს ის ფაქტიც, რომ ზოგიერთი შემთხვევა, რომელიც მითითებულია GDPR -ის მე-17 მუხლში, აშკარად შეეხება იმ სავარაუდო სცენარებს, რომლებიც მონაცემთა დამმუშავებლებმა უნდა გამოავლინონ დამოუკიდებლად თავიანთი ვალდებულების ფარგლებში GDPR-ის დებულებების დაცვით, და იმის დასაბუთებით რომ საზედამხედველო ორგანოებს ეძლევათ საშუალება უზრუნველყონ იმ ნორმების განხორციელება, რომლებიც დაფიქსირებულია GDPR-ში იმ შემთხვევებშიც კი სადაც მონაცემთა სუბიექტები არ არიან ინფორმირებულნი ან არ იციან დამუშავების შესახებ, ან იმ შემთხვევებში სადაც ყველა დაინტერესებულ მონაცემთა სუბიექტს არ წარუდგენია მოთხოვნა წაშლაზე. ზემონათქვამიდან გამომდინარე, EDPB ასკვნის რომ მონაცემთა დაცვის ძირითადი რეგულაციის 58(2/g) მუხლი წარმოადგენს ლეგიტიმურ საფუძველს საზედამხედველო ორგანოსთვის რომ *ex officio* გასცეს განკარგულება არაკანონიერად

დამუშავებული პერსონალური მონაცემების წაშლაზე იმ სიტუაციაში როცა ასეთი მოთხოვნა არ იყო წარდგენილი მონაცემთა სუბიექტის მიერ[31].

შესაძლოა დაისვას კითხვა იმის შესახებ, აქვს თუ არა მონაცემთა სუბიექტს უფლება უკანონობაზე, ან შეუძლია თუ არა მონაცემთა სუბიექტის ნებას (თვით-გამორკვევა) უგულებელყოს მთელი GDPR მაშინაც კი, თუ „ორგანო“ მიიჩნევს დამუშავებას სრულიად უკანონოდ. სასამართლო გადაწყვეტილებას ელოდებიან 2024 წელს.

4.3. დროებითი მაკორექტირებელი უფლებამოსილება და ონლაინ მსოფლიო

ერთ-ერთ უდიდეს გამოწვევას წარმოადგენს ონლაინ მსოფლიოს მონიტორინგი და საჭიროების შემთხვევაში ეფექტური ჩარევა „მონაცემთა დაცვის აკრძალულ ზონებში“, განსაკუთრებით ბნელ ქსელში და ზოგიერთ სოციალურ მედია პლატფორმაში. უნგრელმა კანონმდებელმა - მოქმედებს რა მონაცემთა დაცვის ძირითადი რეგულაციის მიერ მინიჭებული უფლებამოსილებით - მიანიჭა უნგრეთის საზედამხედველო ორგანოს ახალი უფლებები 2011 წლის CXII კანონში ცვლილებების შეტანით.

როგორც პერსონალურ მონაცემთა უკანონო დამუშავების თავიდან აცილების პირველი ნაბიჯი და დროებითი ზომა, „ორგანოს“ ასევე შეუძლია მოითხოვოს ჰოსტინგის (მასპინძლობის) სერვისი ან შუამავლის სერვისი პროვაიდერისგან, რომელიც ჰოსტინგის სერვისს ასრულებს ელექტრონული კომერციისა და საინფორმაციო საზოგადოების სერვისების გარკვეულ საკითხებზე, რომლებიც ამუშავებენ მონაცემებს ელექტრონული საკომუნიკაციო ქსელის მეშვეობით, დროებით ამოშალონ ელექტრონული მონაცემები, რომელთა გამოქვეყნება წარმოადგენს „ორგანოს“ მიერ მონაცემთა დაცვისთვის საქმის აღძვრის ან ადმინისტრაციული აუდიტის საფუძველს, თუ ასეთის არარსებობის შემთხვევაში დაყოვნება გამოიწვევს პერსონალურ მონაცემთა უფლების უდავო და სერიოზულ დარღვევას, ასევე თუ ა) გამოქვეყნებული მონაცემების მონაცემთა სუბიექტი ბავშვია, ან ბ) გამოქვეყნებული მონაცემები სენსიტიურ ან კრიმინალურ პერსონალურ მონაცემებს წარმოადგენს.

ელექტრონულ მონაცემების დროებითი წაშლის პროცედურული გადაწყვეტილების შესახებ დაუყოვნებლივ უნდა ეცნობოს მხარეებს, რომლებსაც ეკისრებათ წაშლის ვალდებულება. მხარემ, რომელზეც ვრცელდება წაშლის ვალდებულება, უნდა წაშალოს ელექტრონული მონაცემები „ორგანოს[32]“ მხრიდან დროებით ღონისძიებებზე პროცედურული გადაწყვეტილების მიღებიდან ერთი სამუშაო დღის განმავლობაში.

[31] მოსაზრება 39/2021 იმის შესახებ შეიძლება თუ არა GDPR მუხლი 58(2.g) გამოყენებული იყოს როგორც სამართლებრივი საფუძველი საზედამხედველო ორგანოს ex officio ბრძანების პერსონალურ მონაცემთა წაშლის თაობაზე იმ სიტუაციაში როცა ასეთი მონაცემი არ იყო მიწოდებული მონაცემთა სუბიექტის მიერ (მიღებულია 2021 წლის 14 დეკემბერს), <edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf> [8.01.2024].

[32] *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 942-943.

მეორე, „ორგანოს“ შეუძლია გასცეს ბრძანება, რომ ელექტრონული მონაცემებზე, რომელთა გამოქვეყნება შეიძლება გახდეს „ორგანოს“ მიერ სამართალწარმოების აღძვრის ან ადმინისტრაციული აუდიტის საფუძველი მონაცემთა დაცვისათვის, დროებით შეჩერდეს წვდომა როგორც დროებითი ღონისძიება პერსონალურ მონაცემთა უკანონო დამუშავების თავიდან ასაცილებლად. ელექტრონული მონაცემებზე წვდომა შეიძლება იყოს დროებით შეჩერებული, როცა ასეთის არარსებობის შემთხვევაში, დაყოვნება გამოიწვევს პერსონალურ მონაცემთა უფლების უდავო და სერიოზულ დარღვევას და ნებისმიერი სხვა ღონისძიება „ორგანოს“ მიერ 61/A (1) განყოფილების შესაბამისად, მისი დროებით წაშლის ჩათვლით, იქნება არაეფექტური, ასევე როდესაც ა) გამოქვეყნებული მონაცემების მონაცემთა სუბიექტი ბავშვია, ან ბ) გამოქვეყნებული მონაცემები სენსიტიურ ან კრიმინალურ პერსონალურ მონაცემებს წარმოადგენს.

„ორგანო“ პროცედურულ გადაწყვეტილების ბრძანებას ელექტრონულ მონაცემებზე წვდომის დროებით შეჩერების შესახებ ავრცელებს საჯარო შეტყობინების ფორმატით. საჯარო შეტყობინება უნდა განთავსდეს განცხადებების დაფებზე და გამოქვეყნდეს „ორგანოს“ ვებსაიტზე ხუთი დღის ვადაში. პროცედურული გადაწყვეტილების მიღების შესახებ შეტყობინების დღედ მიიჩნევა საჯარო შეტყობინების განთავსებიდან მესამე დღე. „ორგანოს“ მიერ პროცედურული გადაწყვეტილებით დაკისრებული ვალდებულება ვრცელდება ელექტრონული კომუნიკაციის სამსახურის ყველა მიმწოდებელზე ამის შესახებ პირდაპირი მითითების აუცილებლობის გარეშე[33]. „ორგანოს“ შეუძლია დააკისროს პროცედურული ჯარიმა ასი ათასი ფორინტიდან (260 ევრო) ოცი მოლიონ ფორინტამდე (50 000 ევრო) თანხის ოდენობით იმ ელექტრონულ საკომუნიკაციო სერვისის მიმწოდებლებს რომლებიც ვერ შეასრულებენ ამ ნაწილში დადგენილ ვალდებულებებს[34].

4.4. კონფლიქტები სახელისუფლებო ორგანოებსა და სამოქალაქო სასამართლოებს შორის

მონაცემთა სუბიექტის მოთხოვნის საფუძველზე ადმინისტრაციული სამართალწარმოების დაწყების გამო, იშვიათობას არ წარმოადგენს, როცა მონაცემთა სუბიექტი აღძრავს საჩივარს „ორგანოს“ წინაშე და ამავე დროს სამოქალაქო სასამართლოშიც ხშირად იგივე შინაარსის სარჩელს მონაცემთა დაცვის

[33] მოსაზრება 39/2021 იმის შესახებ შეიძლება თუ არა GDPR მუხლი 58(2.g) გამოყენებული იყოს, როგორც სამართლებრივი საფუძველი საზედამხედველო ორგანოს ex officio ბრძანების პერსონალურ მონაცემთა წაშლის თაობაზე იმ სიტუაციაში როცა ასეთი მონაცემი არ იყო მიწოდებული მონაცემთა სუბიექტის მიერ (მიღებულია 2021 წლის 14 დეკემბერს), <edpb_opinion_202139_article_582g_gdpr_en.pdf> [8.01.2024].

[34] GDPR-ის მუხლი 58(6). თითოეულ წევრ სახელმწიფოს შეუძლია კანონით უზრუნველყოს რომ მისი საზედამხედველო ორგანო უნდა ფლობდეს დამატებით ძალაუფლებას მათზე, რომლებიც მითითებულია პარაგრაფებში 1-3. ამ უფლებამოსილებების განხორციელებამ ხელი არ უნდა შეუშალოს VII თავის ეფექტურ მოქმედებას. ეს მუხლი *„პირდაპირ გამოყენებადია. ამიტომ, DPA შეუძლია პირდაპირდაეყრდნოს მასთავისი უფლებამოსილების შესრულებისას. თუმცა, მუხლი 58 ასევე უთმობს ადგილს ეროვნულ კანონმდებლობის მიღებისათვის ორივე პროცედურული კანონისა და დამატებითი ვალდებულებებთან დაკავშირებით“.* იხ. *Kuner C., Bygrave L.A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 944.

იმავე დებულების საფუძველზე და მოითხოვს „ორგანოსგან“ (ასევე, სასამართლო განხილვის შემთხვევაში ადმინისტრაციულ სასამართლოსგან) და სამოქალაქო სასამართლოსგან GDPR-ის ერთსა და იმავე ნორმის ინტერპრეტაციას ერთსა და იმავე საქმეში.

ამ შემთხვევაში, GDPR-ის 77 და 79-ე მუხლები გარდაუვალად წარმოშობენ კონფლიქტს ადმინისტრაციულ და სასამართლოს ხელისუფლებების განშტოებებს შორის. სამართლიანობის სასამართლომ GDPR-ის 77 და 79-ე მუხლების ინტერპრეტირება გააკეთა ამ დებულებებში დადგენილი კომპეტენციების განსაზღვრებების თვალსაზრისით. ზემოხსენებული მუხლები პარალელურად ანიჭებენ ფიზიკურ პირებს სარჩელის ძალის მქონე უფლებებს, მაგრამ ამ უფლებების პარალელურად განხორციელებამ შესაძლებელია გამოიწვიოს გაურკვევლობა სამართლებრივ სიცხადის მხრივ, როგორც ეს მოხდა საქმე C-132/21 დავაში. რამდენადაც ეროვნული პროცედურული კანონმდებლობის შესაბამისად „ორგანოს“ გადაწყვეტილებები არ არის დამავალდებულებელი სამოქალაქო სასამართლოებისთვის, არ არის გამორიცხული, რომ სამოქალაქო სასამართლომ შესაძლოა არ მიიღოს გადაწყვეტილება ზედამხედველი ორგანოს მიერ მიღებული გადაწყვეტილების საწინააღმდეგოდ იმავე ფაქტებთან დაკავშირებით.

GDPR-ის 78-ე მუხლით განსაზღვრული უფლებამოსილების შესაბამისად, ადმინისტრაციული სასამართლოს ფუნქციაა საზედამხედველო ორგანოს გადაწყვეტილებების განხილვა. საზედამხედველო ორგანოს კომპეტენციები ასევე განსაზღვრავენ ადმინისტრაციული სასამართლოს კომპეტენციებს თუ მხედველობაში მივიღებთ რომ ამ უკანასკნელს შეუძლია განახორციელოს კანონიერების შემოწმება სამართლის იმ საკითხებისა რომლებიც შედის საზედამხედველო ორგანოს კომპეტენციის ფარგლებში. ადმინისტრაციულ სასამართლოს ვალდებულებაა განიხილოს დასკვნები, რომლებსაც შეიცავს საზედამხედველო ორგანოების გადაწყვეტილებები მონაცემთა დაცვის ძირითადი კანონის დარღვევებთან დაკავშირებით, და სამოქალაქო სასამართლოებს რომლებიც მოქმედებენ ამავე რეგულაციის 79-ე მუხლის შესაბამისად, შეუძლიათ გამოიტანონ საბოლოო გადაწყვეტილება სამართლის იგივე საკითხებზე. სამოქალაქო სასამართლოს გადაწყვეტილებებს არა გააჩნიათ *res iudicata* ეფექტი დავის განხილვისას ძირითადი სამართალწარმოების ფარგლებში, რადგანაც პროცესის მხარეები არ არიან იდენტურები. შეიძლება მოხდეს რომ ადმინისტრაციულ სასამართლოს მოუწიოს განხილვა იგივე ფაქტებისა და იგივე დარღვევებისა - ასევე ინტერპრეტირება ევროკავშირისა და წევრ-სახელმწიფოს ერთი და იგივე კანონმდებლობისა, რომლის ფარგლებშიც სამოქალაქო სასამართლომ უკვე გამოიტანა საბოლოო გადაწყვეტილება. ეროვნული პროცედურული კანონმდებლობის შესაბამისად, მიუხედავად იმისა რომ სამოქალაქო სასამართლოს გადაწყვეტილება არ არის სამართლებრივად დამავალდებულებელი ადმინისტრაციული სასამართლო საქმეებზე, ეს უკანასკნელი სასამართლო ვერ გაუკეთებს იგნორირებას სამართლებრივი სიცხადის ზოგად ნორმებს, რომელთა თანახმად სასამართლო გადაწყვეტილებები სამართლებრივად სავალდებულოა ყველასთვის (სასამართლოების ორგანიზაციის კანონის მე-6 მუხლი).

ვერტიკალურ დონეზე კომპეტენციებს შორის პარალელი ასევე პრობლემატურია, თუ მხედველობაში მივიღებთ რომ მიზანი, რომელიც ჩამოყალიბებულია GDPR-ს დეკლარაციული ნაწილის 117-ე პუნქტში - რომლის

მიხედვით საზედამხედველო ორგანოების შექმნა წევრ სახელმწიფოებში, რომლებიც უფლებამოსილნი არიან შეასრულონ თავიანთი ვალდებულებები და განახორციელონ თავიანთი უფლებამოსილებები სრულიად დამოუკიდებლად, წარმოადგენს ფიზიკური პირების დაცვის ძირითად კომპონენტს მათი პერსონალური მონაცემების დამუშავების ასპექტში, რომლის მიღწევა წევრი სახელმწიფოებისთვის დაკისრებული ვალდებულებაა 51(1) მუხლის მიხედვით, - ნაწილობრივ შეიზღუდება თუ სასამართლო პროცესი წინ უძღვის ადმინისტრაციულ აპელაციას. თუ ნებადართულია ადმინისტრაციული საჩივრისა და სასამართლო სარჩელის პარალელურად აღძვრა, ნებისმიერი საბოლოო სასამართლო გადაწყვეტილება, რომელიც პირველად იქნება გამოტანილი, იქნება სამართლებრივად დამავალდებულებელი საზედამხედველო ორგანოსათვის იმავე ფაქტებზე აღძრული საჩივარზე სასამართლო გადაწყვეტილების გამოტანის დროს. ასეთ სიტუაციაში საზედამხედველო ორგანოს კომპეტენცია შეიზღუდება როგორც ამას ითვალისწინებს GDPR-ის 58 მუხლი.

საქმეში C-132/21 სასამართლომ საბოლოოდ დაადგინა, რომ GDPR-ის მუხლი 77(1), მუხლი 78(1) და მუხლი 79(1), რომლებიც განიხილებიან ევროკავშირის ფუნდამენტური უფლებათა ქარტიის 47 მუხლის გათვალისწინებით, უნდა განისაზღვრონ როგორც ნებართვა სამართლებრივი დაცვის საშუალებებზე, როგორც ეს გათვალისწინებულია ამ რეგულაციის 77(1) და 78(1) მუხლებით, ერთის მხრივ, და მეორეს მხრივ, 79(1) მუხლით, რომელიც ითვალისწინებს ამ საშუალებების გამოყენებას ერთმანეთის პარალელურად და ერთმანეთისგან დამოუკიდებლად. წევრ-სახელმწიფოებმა პროცედურული ავტონომიის ნორმების შესაბამისად უნდა დაადგინონ დეტალური წესები ამ სამართლებრივი დაცვის საშუალებებს შორის ურთიერთკავშირის შესახებ, რათა უზრუნველყონ რეგულაციით გარანტირებული უფლებათა ეფექტური დაცვა და მისი დებულებების თანამიმდევრული და ერთგვაროვანი გამოყენება, ასევე ეფექტური სამართლებრივი დაცვის უფლება სასამართლოს ან ტრიბუნალის წინაშე როგორც ეს მითითებულია ფუნდამენტურ უფლებათა ქარტიის 47-ე მუხლში.

რადგანაც უნგრეთის კანონმდებლობა არ შეიცავს რეგულაციებს პარალელური სამართლებრივი დაცვის საშუალებების შესახებ, ეს საკითხი ჯერ დახურული არ არის. „ორგანო“ პატივს სცემს სამოქალაქო სასამართლოს გადაწყვეტილებებს იმ შემთხვევაშიც კი, როგორც ეს მოხდა საქმეში C-132/21, თუ სამოქალაქო მოსამართლის სამართლებრივი პოზიცია ეწინააღმდეგება „ორგანოს“ ინტერპრეტაციას. თუმცა, კომპეტენტური იურისდიქციის სასამართლო მართალი იყო, როცა დაადგინა რომ ამ სიტუაციამ, რომელიც შეიქმნა მონაცემთა დაცვის ძირითადი რეგულაციის შედეგად, შეიძლება მოგვიყვანოს ევროკავშირის ერთ-ერთი მნიშვნელოვანი პრინციპის -კანონის უზენაესობის - დარღვევამდე. ციფრები გვიჩვენებენ რომ უნგრეთში სამოქალაქო სამართლებრივი დაცვის საშუალებების რაოდენობა უმნიშვნელოა ადმინისტრაციულთან შედარებით.

5. დასკვნა

მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR) აღმოჩნდა გარდამტეხი მომენტი. მან მოიტანა რევოლუციური ცვლილებები, საზედამხედველო ორგანოების როლის, მისი საქმეთა წარმოების და სასამართლო სისტემასთან დამოკიდებულების ფუნდამენტური და სრული ტრანსფორმაცია. GDPR-მა რადიკალურად გაზარდა

პირადი ცხოვრების შესახებ ცოდნის დონე ნებისმიერი სახის ორგანიზაციაში და წარმოადგენს რადიკალურ გარღვევას მონაცემთა სუბიექტების, მონაცემთა დამმუშავებლების და სასამართლოების (!) რწმენასა და ქცევაში მონაცემთა დაცვის კუთხით.

30 წელზე მეტი ხნის განმავლობაში, უნგრეთის მონაცემთა დაცვის კანონმა გრძელი გზა გაიარა მთელი რიგი მნიშვნელოვანი პროცედურული და ორგანიზაციული ცვლილებებით. მიუხედავად ამისა, ტენდენციები აშკარად მიდის ერთი მიმართულებით: ციფრული საუკუნის და მონაცემებზე ორიენტირებული ეკონომიკისა და სერვისების სწრაფი განვითარების გამო, პერსონალურ მონაცემების დაცვის უფლების განხორციელება მოითხოვს ძლიერ და ეფექტურ უფლებამოსილებებს. უნგრეთში მონაცემთა დაცვის კანონის განვითარებამ წარმართა ორგანიზაციული და პროცედურული სამართლებრივი ჩარჩო ადმინისტრაციული ტიპის მოდელისკენ, რისთვისაც შექმნა მაკორექტირებელი უფლებამოსილებების უფრო და უფრო ეფექტური მექანიზმები ჯერ კიდევ მონაცემთა დაცვის ძირითადი რეგულაციის მიღებამდე და გარკვეული თვალსაზრისით, 2011 წლის CXII კანონის მიღებამდე.

რაც შეეხება ამ პროცესში ადმინისტრაციულ სამართალს, თავდაპირველად პასიური, საკმაოდ თავშეკავებული პოზიცია ზემო აღნიშნული პროცესით შეიცვალა და უნგრეთის ადმინისტრაციული სასამართლო სისტემა სულ უფრო და უფრო აქტიურად აცხადებს პრეტენზიას მონაცემთა დაცვის კანონის ინტერპრეტირებაში გადამწყვეტი როლის შესრულებაზე.

თუმცა, ეს პროცესი ჯერ კიდევ არ დასრულებულა, პირიქით, ჩვენ ზუსტად ახლა ვიწყებთ. სასამართლოს პრეცედენტული სამართალი ჯერ კიდევ ვითარდება და მატერიალური და პროცედურული სამართლის მნიშვნელოვანი საკითხები ჯერ კიდევ პასუხგასაცემია.

იოზეფ ატილას ცნობილი სიტყვების პერიფრაზირებით შეიძლება ითქვას, რომ ისტორიული გამოცდილებიდან გამომდინარე, ყოველთვის არსებობს საკმარისი მიზეზი იმ ფაილის მოსაძებნად, რომელიც არღვევს ვინმეს უფლებებს. საკითხავია, დარჩება თუ არა მონაცემთა დაცვის კანონმდებლობა მხოლოდ ცარიელ სიტყვებად თუ სამართლებრივად და პრაქტიკულად განხორციელებადი საზედამხედველო უფლებამოსილებების მეშვეობით ამოქმედდება სამართლებრივი ნორმები და წესები, რომლებიც დაიცავენ ჩვენს პირად ცხოვრებას.

ბიბლიოგრაფია:

1. Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices (Competition Act).
2. Data Protection Commissioner’s 2008 Report, 134-135.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) OJ 2016 L 119, p. 1 / GDPR.
4. The Fundamental Law of Hungary (25 April 2011).
5. *Kuner C., Bygrave L.A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 942-943.

6. Opinion 39/2021 on whether Article 58(2.g), Adopted on 14 December 2021.
7. Kúria Kf.VI.37.956/2018/6.
8. Kúria Kfv.III.37.911/2017/8.
9. Budapest Court of Hungary K.33.024/2004/46.
10. Judgment of 1 October 2015, Weltimmo, C-230/14, EU:C:2015:639
11. Report of 2005 of the Data Protection Commissioner, 45-46;
12. Supreme Court of Justice of Hungary Kfv.37.923/2010/5.
13. Supreme Court of Justice of Hungary Kfv.V.35.180/2009/5.
14. Vas County Court of Hungary 1.K.20.018/2009/33.

ზვიად გაბისონია*

დიდი მონაცემების დამუშავებისას პერსონალურ მონაცემთა დაცვის სამართლებრივი გამოწვევები

თანამედროვე ტექნოლოგიების სწრაფად განვითარების ფონზე იზრდება დიდი მონაცემების (Big Data) დამუშავების მასშტაბები, რაც გამოწვევის წინაშე აყენებს პერსონალური მონაცემების სამართლებრივი დაცვის საკითხებს. დიდი მონაცემების დამუშავება თანამედროვე ტექნოლოგიების (მათ შორის, ხელოვნური ინტელექტის) „საწვავს“ წარმოადგენს.

„დიდი მონაცემები“ ინფორმაციული ტექნოლოგიების მეცნიერებაში დამკვიდრებული ტერმინია და მისი ოფიციალური განმარტება თითქმის არ არსებობს. ყველაზე ცნობილი განმარტების მიხედვით, ამ ტერმინის ქვეშ იგულისხმება იმ მოცულობის მონაცემთა სიმრავლე, რომლის შეგროვება, მართვა და დამუშავება ტრადიციული მონაცემთა ბაზებისა და შესაბამისი პროგრამების შესაძლებლობებს ბევრად აღემატება.

სტატიაში განხილულია დიდი მონაცემების დამუშავებისას პერსონალურ მონაცემთა სამართლებრივი დაცვის კანონმდებლობა ყველაზე მაღალტექნოლოგიური ქვეყნების: აშშ-ს და ჩინეთის სამართლებრივი ბაზის მაგალითზე. ნაჩვენებია ის დადებითი და უარყოფითი ფაქტორები, რაც თან სდევს დიდი მონაცემების დამუშავების მასშტაბების ზრდას პერსონალური მონაცემების დაცვის კონტექსტში.

საკვანძო სიტყვები: *დიდი მონაცემები (Big Data), მონაცემთა დაცვა, პერსონალური მონაცემები, აშშ-ს „სუფთა ქსელის“ (The Clean Network) ინიციატივა, „მონაცემთა უსაფრთხოების გლობალური ინიციატივა“ (Global Initiative on Data Security).*

* ბიზნესისა და ტექნოლოგიების უნივერსიტეტის პროფესორი, „ციფრული მმართველობა და ხელოვნური ინტელექტი საჯარო სექტორში“ სადოქტორო პროგრამის ხელმძღვანელი, USAID-ის ექსპერტი ხელოვნური ინტელექტის სამართალში.

1. შესავალი

მეოთხე ინდუსტრიულ რევოლუციაში, სადაც ისეთი წამყვანი ტექნოლოგია, როგორიცაა ხელოვნური ინტელექტი, ეფუძნება მანქანური სწავლების, ღრმა დასწავლისა და ნეირონული ქსელების ანალიზურ მოდელებს, უმნიშვნელოვანეს გამოწვევად იქვა პერსონალური მონაცემების დაცვის საკითხი. ნებისმიერი უახლესი ტექნოლოგია, ინტერნეტის ქსელის გამოყენებით ჭარბად იყენებს დიდი რაოდენობით ინფორმაციის დამუშავებას. ეს კი სერიოზულ პრობლემას ქმნის პერსონალური მონაცემების დაცვის სამართლებრივ საკითხებთან დაკავშირებით.

2023 წლის 14 ივნისს საქართველოს პარლამენტმა მიიღო ახალი კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, რომლის პირველივე მუხლში ნათლადაა ჩამოყალიბებული კანონის მთავარი მიზანი „პერსონალური მონაცემების დამუშავებისას ადამიანის ძირითადი უფლებებისა და თავისუფლებების, მათ შორის, პირადი და ოჯახური ცხოვრების, პირადი სივრცისა და კომუნიკაციის ხელშეუხებლობის უფლებების, დაცვა“.

კანონის ახალი რედაქცია პირდაპირ ასახავს ევროკავშირის რეგულაციებს[1] პერსონალური მონაცემების გამოწვევების დაძლევასთან დაკავშირებით. კანონის მოქმედება ვრცელდება საქართველოს ტერიტორიაზე მონაცემთა ავტომატური საშუალებებით დამუშავებასა და ნახევრად ავტომატური საშუალებებით დამუშავებაზე, იმ მონაცემთა არაავტომატური საშუალებებით დამუშავებაზე, რომლებიც ფაილური სისტემის ნაწილია ან ფაილურ სისტემაში შესატანად მუშავდება, აგრეთვე საქართველოს ფარგლების გარეთ რეგისტრირებული დამუშავებისთვის პასუხისმგებელი პირის მიერ მონაცემთა საქართველოში არსებული ტექნიკური საშუალებების გამოყენებით დამუშავებაზე, გარდა იმ შემთხვევისა, როდესაც ტექნიკური საშუალებები მხოლოდ მონაცემთა ტრანზიტისთვის გამოიყენება[2].

პერსონალური მონაცემების დამუშავება პირდაპირ უკავშირდება ე.წ. „დიდი მონაცემების“ (Big Data) დამუშავების საკითხს, რომელიც ყველა თანამედროვე ტექნოლოგიის ძირითად „საწვავს“ წარმოადგენს. „დიდი მონაცემები“ საინფორმაციული ტექნოლოგიების მეცნიერებაში დამკვიდრებული ტერმინია და მისი ოფიციალური განმარტება თითქმის არ არსებობს. ყველაზე ცნობილი განმარტების მიხედვით, ამ ტერმინის ქვეშ იგულისხმება იმ მოცულობის მონაცემთა სიმრავლე, რომელიც შეგროვება, მართვა და დამუშავება ტიპური, ტრადიციული მონაცემთა ბაზებისა და შესაბამის პროგრამების შესაძლებლობებს ბევრად აღემატება[3].

სტატიის მიზანია შესწავლილი და გაანალიზებულ იქნეს „დიდი მონაცემების“ (Big Data) არსი და მისი დამუშავებისას პერსონალური მონაცემების სამართლებრივი გამოწვევები.

[1] <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> [07.01.2024].

[2] საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, მუხ. 2 (1).

[3] *Franks B.,* Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, New Jersey: John Wiley & Sons, Inc., 2012.

2. დიდი მონაცემების (Big Data) არსი

ნაპოლეონი ამბობდა – „ომის 90% ინფორმაციაა“. ტექნოლოგიური და ბიზნეს ორგანიზაციები დღეს ჩართულნი არიან სრულიად ახალი ბუნებრივი რესურსის მოსაპოვებლად. იგი ნავთობზე უფრო ღირებულია და კაპიტალზე უფრო კრიტიკული მნიშვნელობისაა. ამ რესურსის შეძენა შესაძლებელია, მაგრამ მისი საკუთრებად გარდაქმნა – არა. ის ყველა ქვეყანაში გვხვდება, მაგრამ მისი მოპოვება რთულია. მსოფლიოს ლიდერმა კომპანიებმა იციან, რომ მის გარეშე ისინი განწირულნი არიან მარცხისთვის, მაგრამ მის მოსაპოვებლად მათ ხშირად მენეჯმენტის მოძველებული მეთოდები უშლის ხელს. ამ ახალ ბუნებრივ რესურსს დიდი მონაცემები, ე.წ. “Big Data”.

ინფორმაციული ეპოქის საზოგადოებრივი პროდუქტები ადვილად შესამჩნევია, სმარტფონები ჯიბეში და ლეპტოპები ჩანთებში, და ინფორმაციული ტექნოლოგიების სისტემები ოფისებში. მიუხედავად ამისა, რაც ნაკლებად შესამჩნევია – ეს ინფორმაციაა. უკანასკნელ ოცწლეულში, იმ რაოდენობით მონაცემთა დაგროვება გახდა შესაძლებელი, რომლის იქითაც ადამიანთა წარმოსახვა და რეალობისადმი შეგრძნებები ახალ ფაზაში გადადის. ინფორმაციის რაოდენობრივმა ცვლილებამ, გამოიწვია თვისებრივი ცვლილება. ისეთმა სამეცნიერო დარგებმა როგორიცაა ასტრონომია და გეოფიზიკა, შექმნეს ტერმინი “Big Data”, ანუ დიდი მონაცემები. ეს კონცეფცია დღეს ადამიანთა საქმიანობის ყველა სფეროში გვხვდება.

დიდი მონაცემების ერთი სრულყოფილი დეფინიცია არ არსებობს. თავდაპირველი იდეა ის იყო, რომ გამოსაკვლევი ინფორმაცია იმ დონემდე გაიზარდა, რომ ის ე.წ. USB ან სხვა ინფორმაციის მატარებლებში ვეღარ ეტეოდა. ამიტომ კომპიუტერულ ინჟინრებს სჭირდებოდათ ისეთი ახალი მატარებლები, რომელიც საშუალებას მისცემდა მათ დიდი მოცულობის ინფორმაცია გაეანალიზებინათ. ასე გაჩნდა დიდი მონაცემების დამუშავების სრულიად ახალი პროგრამები, ისეთები როგორიცაა, მაგალითად, კომპანია “Google”-ის „მეპრედიუსი“ და მისი ღია წყაროს ეკვივალენტი, კომპანია Yahoo-ს კუთვნილი „ჰადუპი“ (Hadoop). ეს პროგრამები უზრუნველყოფდნენ მრავალი კომპიუტერისგან შემდგარი ქსელის გამოყენებას, სხვადასხვა ამოცანის გადასაწყვეტად.

გამომდინარე იქიდან, რომ ინტერნეტ სფეროში მოღვაწე კომპანიებს შეეძლოთ ფიზიკური და იურიდიული პირების შესახებ დიდი მონაცემების შეგროვება, ამან სტიმული მისცა მათ, ინვესტირება მოეხდინათ და განევითარებინათ ისეთი ტექნოლოგიები და პროგრამები, რომლებიც აღნიშნულ ინფორმაციას გაანალიზებდა და უფრო სარგებლიანს გახდიდა ბიზნესისათვის.

მაგრამ ეს მხოლოდ დასაწყისია. დიდი მონაცემების ეპოქა კითხვის ნიშნის ქვეშ დააყენებს ისეთ გლობალურ წესებს, როგორიცაა მაგალითად ის, თუ როგორ ვცხოვრობთ და როგორ ვურთიერთობთ სამყაროსთან. ის კითხვის ნიშნის ქვეშ დააყენებს საუკუნეების განმავლობაში ჩამოყალიბებულ ტრადიციებსა და პრაქტიკას და ადამიანის ბაზისურ გაგებას. მაგალითად, როგორ მიიღება გადაწყვეტილებები და როგორ უნდა შევიმეცნოთ სამყარო.

დიდი მონაცემების ეპოქაში შებიჯება რადიკალური ცვლილებების დასაწყისია. იმის გასააზრებლად, თუ რა დონეზე მიმდინარეობს ინფორმაციული რევოლუცია, ამას საზოგადოების თითქმის ყველა სფეროში მიმდინარე ტენდენციები მეტყველებს. ჩვენი ციფრული სამყარო მუდმივად ფართოვდება. მაგალითად,

Google.com-ი დღეში 50 პეტაბაიტზე მეტ ინფორმაციას აგროვებს, რაც მსოფლიოს ყველა ბიბლიოთეკაში ერთად განთავსებულ ინფორმაციებზე მეტია. Facebook.com-ი, საათში ათობით მილიონ ფოტოს ტვირთავს, ხოლო Youtube.com-ი ყოველთვიურად ორ მილიარდამდე ვიდეოს ტვირთავს. ინფორმაციის აკუმულირება ხდება ფინანსურ, საბანკო, ჯანდაცვის, დაზღვევის, სოფლის მეურნეობის, ტრანსპორტისა და ლოგისტიკის სფეროებში.

დიდი მონაცემები ჯერ მხოლოდ „ნედლი“ ინფორმაციაა. ის გამოყენებამდე, ნედლი ბუნებრივი რესურსების (მაგ. ნედლი ნავთობი) მსგავსად ჯერ უნდა „გასუფთავდეს“, დაჯგუფდეს და გამოსაყენებელი პროდუქტის სახე მიიღოს. ეს არის უზარმაზარი მონაცემთა სტრუქტურა, რომელიც საშუალებას აძლევს ხელოვნურ ინტელექტს თვითგანვითარების შედეგად უფრო მეტი ინფორმაცია გაანალიზოს და უფრო სრულყოფილი გამოთვლების გამოყენებით ზუსტი ანალიტიკა წარმოადგინოს ამა თუ იმ სფეროში. დიდი მონაცემები არის ისეთი დიდი ოდენობის რესურსების მატარებელი, რომ მისი ანალიზი წარმოუდგენელია ინფორმაციის გაანალიზების ტრადიციული მეთოდების გამოყენებით. დიდი მონაცემები შესაძლებელია, გამოყენებულ იქნას ისეთი დაკვირვებების საწარმოებლად და გასაანალიზებლად, რომელიც სხვაგვარად შეუძლებელი იქნებოდა სხვაგვარი მცირე გაანალიზების შემთხვევაში. წარმოვიდგინოთ, ხმოვანი შეტყობინება, ტვიტი, ელ. ფოსტა, პირადი ფოტოები და ვიდეოები სოციალურ ქსელებში, თქვენს მიერ მსოფლიო დონის ვებ-გვერდებზე – amazon.com. ebay.com, Alibaba.com, Taobao.com ან თუნდაც ქართულ vendoo.ge ან liloshop.ge გაკეთებული შენაძენი, პასპორტის სკანირება, ჰამბურგერის ან სენდვიჩის ფოტო ან ელექტროკარდიოგრამის ჩანაწერები. ყველა ეს შეიძლება დიდი მონაცემების საფუძველი გახდეს.

დიდი მონაცემები მიიჩნევა დიდი მოცულობის (მასივის) სტრუქტურიზებული (ურთიერთდაკავშირებული) და არასტრუქტურიზებული (მაგ., ტექსტური შეტყობინება, სურათი, ვიდეო, აუდიო) ციფრობრივი ინფორმაციის დამუშავების, ანალიზისა და გავრცელების თანამედროვე ტექნოლოგიად. მას აქვს 8 განზომილება ანუ 8V: Volume – მოცულობა; Value – ღირებულება; Veracity – სანდოობა, უტყუარობა; Visualisation – ვიზუალიზაცია. დამუშავებისა და გარეგანი გაფორმების პროცესი; Variety – მრავალფეროვნება; Velocity – სიჩქარე; Viscosity – მეხსიერებაში დალექვა და Virality – მასობრივად გავრცელება.[4]

ახალი ინტერნეტ ტექნოლოგიების განვითარება დიდი მონაცემების მოპოვების უფრო მეტ შესაძლებლობას შექმნის. მაგალითად, მობილური ინტერნეტის მე-5 თაობის – 5G-ის განვითარება შესაძლებელს გახდის არა მარტო ე.წ. „ჭკვიანი ნივთების“, არამედ „ჭკვიანი ქალაქების“ მუდმივ ონლაინ რეჟიმში ჩართვას, რაც წარმოუდგენლად დიდი მონაცემების მოპოვებისა და დამუშავების საშუალებას იძლევა. ხელოვნურ ინტელექტს აღნიშნული ინფორმაციების მოპოვებით გაუჩნდება შესაძლებლობა თითოეულ პირზე ჰქონდეს ზუსტი ინფორმაცია მისი სურვილების, საკვების, ტექნიკის, საცხოვრებლის, ბუნებისადმი სიყვარულის და პოლიტიკური შეხედულებებისაც კი. ეს კი ზოგიერთი მეცნიერის მოსაზრებით, დიდი საფრთხის მოახლოების მაუწყებელია. მაგ. მსოფლიოში ცნობილი თანამედროვე ისტორიკოსი იუვალ ნოახ ჰარარი აღნიშნავს, რომ ხელოვნური ინტელექტი შესაბამისი სამართლებრივი რეგულირების გარეშე დიდი საფრთხის შემცველი იქნება კაცობრიობისთვის და ამისთვის სულაც არაა აუცილებელი, რომ მან ადამიანების განადგურება დაიწყოს. მთავარი პრობლემა იმაში მდგომარეობს, რომ დიდი

[4] *ჯოლია გ.,* განათლება და დასაქმება ციფრულ გარემოში, თბ., 2021, 36.

მონაცემების გაანალიზების შედეგად ხელოვნურ ინტელექტს შეეძლება ადამიანის ემოციებზე დაკვირვებით მხოლოდ ის კი არ გაიგოს რა ინტერესები და დამოკიდებულება აქვს ამა თუ იმ საგნისა და მოვლენისადმი, არამედ მას ექნება შესაძლებლობა ისეთი შინაგანი ემოციაც კი გაანალიზოს და გაიგოს, რაც შესაძლოა თავად ამ ადამიანმაც არ იცოდეს. ამის ერთ-ერთ თვალსაჩინო მაგალითად მოჰყავს შემთხვევა, როცა ხელოვნურმა ინტელექტმა ქალის მიერ ვეგ-გვერდების დათვალიერების შედეგად ქვეცნობიერად ისეთ საიტებზე დაიწყო დაკვირვება, რომელიც პატარა ბავშვების ქცევას ასახავდა. შესაბამისად პროგრამამ გაანალიზა რა ქალის ემოციები, დაასკვნა, რომ ეს ქალი ორსულად იყო. მხოლოდ რამდენიმე დღის შემდეგ ექიმთან ვიზიტისას ქალმა შეიტყო, რომ ის მართლაც ბავშვს ელოდებოდა. ხელოვნური ინტელექტის საფრთხეებისა და რეგულირების აუცილებლობას ქვემოთ ცალკე შევეხებით და აქ აღარ გავჩერდებით.

მეოთხე ინდუსტრიული რევოლუციის დროს მონაცემები გახდა იმაზე ძვირადღირებული რესურსი, ვიდრე პირველი და მეორე რევოლუციის დროს მიწა ან ნავთობი იყო. ეს რესურსი კი როდესაც „ნედლი ნავთობის“ მსგავსად, დამუშავდება და გამოსაყენებლად ვარგისი გახდება, წარმოუდგენელ შესაძლებლობას მისცემს ტექნოლოგიურ კომპანიებს და მთლიანად კაცობრიობას.

დიდი მონაცემები მსოფლიოს ორი უდიდესი ეკონომიკის: აშშ-ს და ჩინეთს შორის არსებულ მრავალეტაპიანი და მრავალშრიანი ტექნოლოგიური ომის შემადგენელი ნაწილია.

3. აშშ-ს „სუფთა ქსელი“-ს (The Clean Network) ინიციატივა

ამერიკის შეერთებულ შტატებსა და ჩინეთს შორის დაწყებულ სავაჭრო და ტექნოლოგიურ ომში უკვე მრავალი რაუნდი ჩატარდა. თუმცა, მათ შორის დაპირისპირების მთავარი მიზეზი არის ის, თუ ვინ მოახერხებს უკეთ გააკონტროლოს თანამედროვე ეპოქის ყველაზე ძვირი რესურსი – დიდი მონაცემები. ამერიკის მიერ ცნობილი მობილური აპლიკაციების – „ტიკ ტოპის“ (Tik Tok) და „ვი ჩატის“ (WeChat) აკრძალვა სწორედ დიდი მონაცემების ირგვლივ დაწყებული ბრძოლის ერთ-ერთი გამოვლინებაა.

აშშ-ს სახელმწიფო დეპარტამენტის მიერ გამოქვეყნებული ე.წ. „სუფთა ქსელის“ (The Clean Network) ინიციატივა მოიცავს ამერიკის საჯარო განცხადებას ამერიკის მოქალაქეების დაცვის შესახებ და სხვა ქვეყნებს მოუწოდებს შეუერთდეს ამ ინიციატივას. „სუფთა ქსელის“ ინიციატივის პრეამბულაში მოყვანილია აშშ-ს სახელმწიფო მდივნის განცხადება, რომ „ჩვენ მოვუწოდებთ თავისუფლების მოყვარე ყველა ქვეყანასა და კომპანიას, შეუერთდნენ სუფთა ქსელს“[5].

„სუფთა ქსელის“ ინიციატივა მოიცავს „სუფთა მატარებლებს“ (Clean Carrier), „სუფთა ონლაინ მაღაზიებს“ (Clean Store), „სუფთა აპლიკაციებს“ (Clean Apps), „სუფთა ღრუბლოვან სისტემებს“ (Clean Cloud), „სუფთა საკაბელო ხაზებს“ (Clean Cable), „სუფთა გზას“ (Clean Path).

„სუფთა მატარებლები“-ის (Clean Carrier) ინიციატივა მოიცავს აშშ-ს პოლიტიკას გააკონტროლოს ის, რომ ჩინეთის სახალხო რესპუბლიკის ონლაინ ინფორმაციის მატარებელი და გამტარი კომპანიები არ არიან დაკავშირებულნი აშშ-ს

[5] “We call on all freedom-loving nations and companies to join the Clean Network”, <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].

საკომუნიკაციო ქსელებთან. ასეთი კომპანიები საფრთხეს უქმნიან აშშ-ს ეროვნულ უსაფრთხოებას და არ უნდა იყვნენ ჩართულნი აშშ-ს საერთაშორისო სატელეკომუნიკაციო მომსახურებებში.

„სუფთა ონლაინ მაღაზიების“ (Clean Store) ინიციატივა გულისხმობს აშშ-ს მობილური აპლიკაციების მაღაზიებიდან არასანდო პროგრამების ამოღებას. კერძოდ, ჩინური კომპანიების მიერ შექმნილი აპლიკაციები საფრთხეს უქმნის აშშ-ს კონფიდენციალურობას, ავრცელებს ვირუსებს, ცენზურის კონტენტებს და ახორციელებს დეზინფორმაციულ პროპაგანდას. ოფიციალურ განცხადებაში მითითებულია, რომ ამერიკელების მობილურ ტელეფონებზე არსებული ყველაზე მგრძნობიარე პირადი და საქმიანი ინფორმაცია უნდა იყოს დაცული და ხელშეუხებელი ნებისმიერი სხვა მხარის ქურდობისა და ექსპლუატაციისაგან.

„სუფთა აპლიკაციების“ (Clean Apps) ინიციატივა გულისხმობს იმას, რომ ჩინეთში წარმოებულ სმარტფონებში „პრეინსტალაციის“ და გადმოწერისას უნდა შემოწმდეს, ხომ არ იყენებენ ეს აპლიკაციები კომპანია „ჰუავეის“ (Huawei) ან ჩინეთის სხვა კომპანიების ისეთ ტექნოლოგიებს, რომელმაც შეიძლება საფრთხე შეუქმნას ამერიკელების ან სხვა უცხო ქვეყნის მოქალაქეთა პირად უფლებებსა და თავისუფლებებს.

„სუფთა ღრუბლოვან სისტემების“ (Clean Cloud) ინიციატივა გულისხმობს, რომ აშშ-ს მოქალაქეების ყველაზე სენსიტიური პირადი ინფორმაციის და ამერიკული ბიზნესის ყველაზე ღირებული ინტელექტუალური საკუთრების, მათ შორის, COVID-19 ვაქცინის კვლევების შესახებ ინფორმაცია დამუშავებული და შენახული იქნას მხოლოდ „ღრუბლოვან სისტემებზე“ („ქლაუდებზე“) და არ იქნას ატვირთული ისეთი პროგრამების, აპარატურის, აპლიკაციების და სმარტფონების გამოყენებით, რომელიც ხელმისაწვდომია ამერიკის მოწინააღმდეგე ისეთი ჩინური კომპანიებისთვის, როგორებიცაა „ალიბაბა“ (Alibaba), „ბაიდუ“ (Baidu), „ჩაინა მობაილ“ (China Mobile), „ჩაინა ტელეკომ“ (China Telecom) და „ტენსენი“ (Tencent).

„სუფთა საკაბელო ხაზების“ (Clean Cable) ინიციატივით, აშშ-ს სახელმწიფო დეპარტამენტი აცხადებს, რომ ის ჩინეთის დაზვერვის სისტემების ჰიპერმასშტაბურ დონეზე შეღწევისაგან უზრუნველყოფს იმ წყალქვეშა კაბელების უსაფრთხოებას, რომლებიც ამერიკას გლობალურ ინტერნეტთან აკავშირებს. ასევე მზად არიან, იმუშაონ პარტნიორ ქვეყნებთან, რომ მსოფლიოს სხვა წყალქვეშა ინტერნეტ კაბელებიც დაცული იყოს და ამ ნაწილში ამერიკა უკომპრომისო იქნება.

„სუფთა გზის“ (Clean Path) ინიციატივის შესახებ 2020 წლის 9 აპრილს აშშ-ს სახელმწიფო მდივანმა პომპეომ განაცხადა. ეს ინიციატივა გულისხმობს იმას, რომ აშშ-ს სახელმწიფო დეპარტამენტი დაიწყებს ამერიკის დიპლომატიურ დაწესებულებებში შესასვლელი და გამოსასვლელი 5G ინტერნეტ ტრაფიკისათვის „სუფთა გზის“ მოთხოვნას.

ამის მიზეზად აშშ ასახელებს იმას, რომ ჩინური 5G ინტერნეტ ტრაფიკის განმავითარებელი კომპანიები „ჰუავეი“ (Huawei) და „ზე თი ი“ (ZTE) ექვემდებარებიან ჩინეთის კომუნისტური პარტიის დირექტივებს და შესაბამისად მათ მიმართ აშშ უნდობლობას გამოხატავს. მისი საშუალებით აშშ მის მოქალაქეებს და ბიზნეს კომპანიებს დაიცავს 5G ინტერნეტ ტრაფიკის მეშვეობით ჩინური კომპანიების არასანქცირებული შეღწევებისაგან.

განსაკუთრებით მნიშვნელოვანია ის ფაქტი, რომ საქართველომ 2021 წლის 14 იანვარს აშშ-სთან გააფორმა მემორანდუმი „5G ქსელების უსაფრთხოების შესახებ“[6], რომლითაც ის ფაქტობრივად მიუერთდა „სუფთა ქსელის“ ინიციატივას.

დოკუმენტში აღნიშნულია საკომუნიკაციო ქსელების შეფერხებებისა ან მანიპულირებისგან დაცვის მნიშვნელობა. მემორანდუმში ხაზგასმულია 5G ბაზრებზე საიმედო და სანდო ქსელის აპარატურისა და პროგრამული უზრუნველყოფის მომწოდებლების მხარდაჭერის აუცილებლობა ეროვნული უსაფრთხოების რისკის პროფილის შეფასების გათვალისწინებით და, ასევე, ისეთი ინფრასტრუქტურის ხელშეწყობის საჭიროება, რომლებიც ეფექტურად იცავს 5G ქსელებს არასანქცირებული წვდომისგან ან ჩარევისგან. დოკუმენტის თანახმად, ბაზარზე მომწოდებლების შეფასებისას მნიშვნელოვანია ისეთი კრიტერიუმებით ხელმძღვანელობა, როგორიცაა კანონის უზენაესობა; უსაფრთხოების გარემო; მიმწოდებლის ეთიკური პრაქტიკა; მიმწოდებლის შესაბამისობა უსაფრთხოების სტანდარტებსა და ინდუსტრიის საუკეთესო პრაქტიკასთან.

მემორანდუმის მიხედვით, მხარეები აღიარებენ, რომ 5G მომწოდებლებმა უნდა უზრუნველყონ ისეთი პროდუქტები და მომსახურება, რაც საშუალებას მისცემს ინოვაციების განვითარებას და ხელს შეუწყობს ეფექტურობას. ამ პროდუქტებმა და მომსახურებებმა უნდა უზრუნველყონ სამართლიანი კონკურენცია და ხელი შეუწყონ შემდგომ განვითარებას ბაზარზე მაქსიმალური მონაწილეების ჩართულობით.

მემორანდუმზე ხელმოწერით, საქართველო გახდა აშშ სახელმწიფო დეპარტამენტის „სუფთა ქსელის“ (Clean Network) ინიციატივის 53-ე წევრი ქვეყანა. როგორც აშშ სახელმწიფო დეპარტამენტის ოფიციალურ განცხადებებიდან ჩანს, წევრი ქვეყნები (50-ზე მეტი ქვეყანა) და მათი 180 მეტი სატელეკომუნიკაციო კომპანია, რომელიც მსოფლიოს მთლიანი შიდა პროდუქტის 2/3-ზე მეტს აკონტროლებენ, საჯარო განაცხადეს „სუფთა ქსელის“ ინიციატივის პრინციპების დაცვის შესახებ[7], რაც ხელს შეუწყობს სანდო მომწოდებლებისგან ინტერნეტ ქსელის ინფრასტრუქტურის უსაფრთხოებისათვის საჭირო აპარატურისა და პროგრამული უზრუნველყოფის პროდუქტების გამოყენებას, მოქალაქეთა კონფიდენციალურობისა და სატელეკომუნიკაციო ინფრასტრუქტურაზე არასანქცირებული წვდომისგან დაცვას და ეროვნული უსაფრთხოების უზრუნველყოფას.

აშშ-ს სახელმწიფო დეპარტამენტის „სუფთა ქსელის“ ინიციატივა ძირითადად მიმართულია ჩინეთის სახალხო რესპუბლიკისა და მისი მაღალტექნოლოგიური კომპანიების წინააღმდეგ და ის ამერიკა-ჩინეთს შორის დაწყებული „ტექნოლოგიური ომის“ ერთ-ერთ გამოვლინებად უნდა ჩაითვალოს[8]. აშშ-ს სახელმწიფო დეპარტამენტი პირდაპირ აცხადებს, რომ ჩინური მაღალტექნოლოგიური კომპანიები თავისი აპარატურის გამოყენებით მანიპულირებენ როგორც სხვადასხვა ქვეყნის მოქალაქეთა პირადი ინფორმაციის საკუთარი მიზნებისთვის გამოყენებით, ასევე დიდია რისკი იმისა, რომ ეს ინფორმაცია სხვადასხვა უსაფრთხოების საკითხების გადასაწყვეტად გადასცენ ჩინეთის მთავრობას. ეს კი საფრთხის შემცველია არა მხოლოდ მოქალაქეთა პირადი ინფორმაციის გამჟღავნების, არამედ მიმართულია ქვეყნების ნაციონალური ინტერესების წინააღმდეგაც.

გარდა ზემოთ განსაზღვრული პრინციპებისა, „სუფთა ქსელის“ ინიციატივაში პირდაპირაა აღნიშნული, რომ ის იცავს აშშ-ს მოქალაქეებისა და მისი კომპანიების

[6] <http://www.economy.ge/index.php?page=news&nw=1617> [07.01.2024].
[7] <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].
[8] იქვე.

ყველაზე სენსიტიურ ინფორმაციას გარე აქტორების აგრესიული და საზიანო მოქმედებებისგან. მაგალითად, როგორიცაა ჩინეთის მთავრობა. ამ ინიციატივის ძირითადი მიზანია აშშ-ს ციფრული აქტივების დაცვა, ძირითადად სწორედ დიდი მონაცემები, ისინი ხელში არ ჩაუვარდეთ თუნდაც ლეგალური გზით (მაგ. „ტიკ ტოკი“-დან ოფიციალურად მიღებული ინფორმაციის საფუძველზე) ჩინელ კონკურენტებს. როგორც ზემოთაც აღვნიშნეთ, დიდი მონაცემები ერთგვარი საკვებია ისეთი ტექნოლოგიების განსავითარებლად, როგორიცაა ხელოვნური ინტელექტი. ხოლო ხელოვნური ინტელექტის სფეროში დომინირება პრაქტიკულად დიდ უპირატესობას მისცემს კონკურენტს. აღნიშნულთან დაკავშირებით გამოთქვა შეშფოთება საჯარო გამოსვლისას Google-ის ყოფილმა აღმასრულებელმა დირექტორმა ერიკ შმიტმა, როცა განაცხადა: „2020 წლისთვის ჩვენ ჩინელები დაგვეწევიან, 2025 წლისთვის ისინი ჩვენზე უკეთეს მდგომარეობაში იქნებიან, ხოლო 2030 წლისთვის ისინი გაბატონდებიან ხელოვნური ინტელექტის სფეროში“. ამიტომ მან აშშ-ს მთავრობას მოუწოდა სწრაფი და ქმედითი ნაბიჯები გადადგას ხელოვნური ინტელექტის სახელმწიფო სტრატეგიის განვითარებისა და დიდი მონაცემების დაცვის საკითხებში.

შეშფოთების საფუძველი კი ნამდვილად არსებობს. მრავალი კვლევის თანახმად, ჩინურ კომპანიებს დიდი მონაცემების სფეროში უკვე აქვთ დაახლოებით ათჯერ მეტი ინფორმაცია აშშ-სთან შედარებით. ყოველდღიურად ჩინური კომპანიები „ალიბაბა“ (Alibaba) და „ტენსენი“ (Tencent) (ვიჩატის აპლიკაციის მფლობელი კომპანია) განაახლებენ, ამუშავებენ და იყენებენ 1 მილიარდამდე ადამიანის პირად ინფორმაციას. ჩინეთის ლიდერები ხშირად ამბობენ, რომ ქვეყნების ეკონომიკური და სამხედრო განვითარება უპირობოდაა დამოკიდებული ქვეყნის მიერ მოწინავე ტექნოლოგიების განვითარებასთან, ამაში იგულისხმება პრაქტიკულად ყველა გამოყენებითი მეცნიერების დარგი, იქნება ეს რობოტიკა, გენეტიკა, კოსმოსური ტექნოლოგია, დრონები, ფარმაცევტიკა, მიკროპროცესორებისა და მიკროჩიპების ტექნოლოგიები თუ მზის ენერგიის თანამედროვე ტექნოლოგიები.

4. ჩინეთის სახალხო რესპუბლიკის „მონაცემთა უსაფრთხოების გლობალური ინიციატივა“ (Global Initiative on Data Security)

ჩინეთი, როგორც ხელოვნური ინტელექტის მეცნიერების ერთ-ერთი მსოფლიო ლიდერი, ბოლო რამდენიმე წლის განმავლობაში მთელ თავის სამეცნიერო რესურსებს სწორედ დიდი მონაცემების ანალიტიკის სრულყოფაში დებს. თუმცა, ამავე დროს იძულებულია თავი დააღწიოს მისი კონკურენტების მიერ ბოლო პერიოდში დაწესებულ შეზღუდვებს. ამის მაგალითად გამოდგება აშშ-ს სახელმწიფო დეპარტამენტის მიერ ზემოთ ნახსენები „სუფთა ქსელის“ ინიციატივაც, რომელიც ძირითადად პირდაპირ ჩინეთის წინააღმდეგაა მიმართული. პეკინმა თითქოს უკან დაიხია და „მონაცემთა უსაფრთხოების გლობალური ინიციატივით“ უპასუხა.

2020 წლის 8 სექტემბერს ჩინეთის საგარეო საქმეთა სამინისტროს ოფიციალურ ვებ-გვერდზე გამოაქვეყნა „მონაცემთა უსაფრთხოების გლობალური ინიციატივა“.

ინიციატივაში აღნიშნულია, რომ „ინფორმაციული ტექნოლოგიების რევოლუციისა და ციფრული ეკონომიკის ფენომენალური განვითარება გარდაქმნის წარმოებისა და ცხოვრების წესს, ახდენს ფართო გავლენას სახელმწიფოთა სოციალურ და ეკონომიკურ განვითარებაზე, გლობალური მმართველობის სისტემაზე და კაცობრიობის ცივილიზაციაზე. მონაცემთა მკვეთრმა ზრდამ და მისმა

ერთობლიობამ, როგორც ციფრული ტექნოლოგიის მთავარმა ელემენტმა, გადამწყვეტი როლი ითამაშა ინოვაციური განვითარების ხელშესაწყობად და ხალხის ცხოვრების ფორმირებაში, რაც შეეხება სახელმწიფოთა უსაფრთხოებას და ეკონომიკურ და სოციალურ განვითარებას, ამიტომაც, მოვუწოდებთ ყველა სახელმწიფოს, რომ თანაბარი ყურადღება გაამახვილონ განვითარებაზე და უსაფრთხოებაზე და მიიღონ დაბალანსებული მიდგომა ტექნოლოგიური პროგრესის, ეკონომიკური განვითარების და ეროვნული უსაფრთხოების და საზოგადოებრივი ინტერესების დაცვისკენ. სახელმწიფოებმა ხელი უნდა შეუწყონ ღია, სამართლიან და არადისკრიმინაციულ ბიზნეს გარემოს ორმხრივი სარგებლის მისაღებად, მოგების მისაღწევად და საერთო განვითარებისთვის. ამავდროულად, სახელმწიფოებს აქვთ პასუხისმგებლობა და უფლება, უზრუნველყონ მნიშვნელოვანი მონაცემები და პირადი ინფორმაცია, რომელიც მათ ეროვნულ უსაფრთხოებას, საზოგადოებრივ უსაფრთხოებას, ეკონომიკურ უსაფრთხოებას და სოციალურ სტაბილურობას ეხება.“

ინიციატივაში განმარტებულია, რომ ჩინეთი მიესალმება მთავრობებს, საერთაშორისო ორგანიზაციებს, საინფორმაციო ტექნოლოგიების კომპანიებს, არასამთავრობო ორგანიზაციებს, პიროვნებებსა და ყველა სხვა მოქმედ პირს, რათა ერთობლივი ძალისხმევა მიიღონ მონაცემთა უსაფრთხოების უზრუნველსაყოფად ფართო კონსულტაციის, ერთობლივი წვლილისა და საერთო სარგებლის პრინციპით. ყველა მხარემ უნდა გააძლიეროს დიალოგი და თანამშრომლობა ორმხრივი პატივისცემის საფუძველზე და ხელი შეუწყონ ერთმანეთს, რომ შეიქმნას საზოგადოება, რომელსაც საერთო მომავალი აქვს კიბერსივრცეში, რომელშიც იქნება მშვიდობა, უსაფრთხოება, გახსნილობა, თანამშრომლობა და წესრიგი[9].

ამის უზრუნველსაყოფად ჩინეთმა სახელმწიფოებს შესთავაზა:

- შეძლონ მონაცემთა უსაფრთხოების ყოვლისმომცველი, ობიექტური და მტკიცებულებებზე დაფუძნებული მეთოდით დაცვა და შეინარჩუნონ გლობალური საინფორმაციული და საკომუნიკაციო ტექნოლოგიის (Information and Communications Technology (ICT), შემდგომში – “ICT”) სფეროში პროდუქტებისა და მომსახურების ღია, უსაფრთხო და სტაბილური მიწოდების ჯაჭვი.
- წინააღმდეგი იყვნენ ICT-ის საქმიანობისა, რომელიც აფერხებს ან იპარავს სხვა სახელმწიფოების კრიტიკული ინფრასტრუქტურის მნიშვნელოვან მონაცემებს, ან იყენებს მონაცემებს სხვა სახელმწიფოთა ეროვნული უსაფრთხოების და საზოგადოებრივი ინტერესების საწინააღმდეგო საქმიანობის ჩასატარებლად.
- მიიღონ ზომები, რომ თავიდან აიცილონ ქმედებები, რომლებიც საფრთხეს უქმნის პერსონალურ ინფორმაციას ICT-ის გამოყენებით და წინააღმდეგობა გაუწიონ მასობრივ მეთვალყურეობას სხვა სახელმწიფოების წინააღმდეგ და სხვა სახელმწიფოთა პერსონალური ინფორმაციის უნებართვო შეგროვებას ICT-ების საშუალებით.
- ხელი შეუწყონ კომპანიებს, დაიცვან ის კანონები და ნორმები, სადაც მოქმედებენ. სახელმწიფოებმა არ უნდა მოსთხოვონ ადგილობრივ კომპანიებს შენახული მონაცემების შენახვა საზღვარგარეთ საკუთარ ტერიტორიაზე.

[9] <https://www.flyingnets.com/en/> [07.01.2024].

- პატივი სცენ სხვა სახელმწიფოების სუვერენიტეტს, იურისდიქციას და მმართველობას და არ უნდა მიიღონ სხვა სახელმწიფოებში ნებართვის გარეშე სხვა კომპანიებში განთავსებული მონაცემები.
- თუ სახელმწიფოებმა უნდა მიიღონ საზღვარგარეთის ქვეყნების მონაცემები კანონის აღსრულების მოთხოვნიდან გამომდინარე, როგორიცაა დანაშაულის წინააღმდეგ ბრძოლა, მათ ეს უნდა გააკეთონ სასამართლოს დახმარებით ან სხვა შესაბამისი მრავალმხრივი და ორმხრივი შეთანხმებებით. ორ ქვეყანას შორის მონაცემების ორმხრივი შეთანხმება არ უნდა არღვევდეს მესამე სახელმწიფოს სასამართლო სუვერენიტეტს და მონაცემთა უსაფრთხოებას.
- ICT პროდუქტებისა და მომსახურების პროვაიდერებმა არ უნდა დაამონტაჟონ დამცავი პროგრამები (ე.წ. „backdoors“) თავიანთ პროდუქტებსა და მომსახურებებში მომხმარებლების მონაცემების უკანონოდ მოპოვების, მომხმარებლების სისტემებისა და მოწყობილობების კონტროლის ან მანიპულირებისაგან თავდაცვის მიზნით.
- ICT კომპანიებს არ უნდა ამოძრავებდეთ არალეგალური ინტერესები, გამოიყენონ მომხმარებლების დამოკიდებულება თავიანთ პროდუქტებზე, ან აიძულონ მომხმარებლები განაახლონ თავიანთი სისტემები და მოწყობილობები. პროდუქციის პროვაიდერებმა ვალდებულება უნდა აიღონ, რომ დროულად აცნობებენ პარტნიორებსა და მომხმარებლებს თავიანთი პროდუქტების სერიოზული ხარვეზების შესახებ და შესთავაზებენ მათი აღმოფხვრის საშუალებებს[10].
- ჩინეთი მოუწოდებს ყველა სახელმწიფოს, მხარი დაუჭირონ ამ ინიციატივას და დაადასტურონ ზემოაღნიშნული ვალდებულებები ორმხრივი, რეგიონული და საერთაშორისო ხელშეკრულებებით. ისინი ასევე მიესალმებიან გლობალურ ICT-ის კომპანიებს, რომ მხარი დაუჭირონ ამ ინიციატივას.
- ჩინეთმა 2020 წლის 8 სექტემბრის „მონაცემთა უსაფრთხოების გლობალური ინიციატივაში“ ის ინიციატივები გააჟღერა, რაც აშშ-ს სახელმწიფო დეპარტამენტი სწორედ მას და მის დიდ ტექნოლოგიურ კომპანიებს ედავებოდნენ.

5. დიდი მონაცემების მიღწევები და გამოწვევები

„დიდი მონაცემები“ მეცნიერებსა და საზოგადოების სხვა ფენებში არაერთგვაროვან შეფასებებს იწვევს. უდავოა, რომ არსებობს მისი როგორც დადებითი, ისე უარყოფითი მხარეები.

თანამედროვე სამედიცინო ცოდნა და ზუსტი დიაგნოზის დასმის შესაძლებლობა დამოკიდებულია ნიჭიერი და კვალიფიციური ადამიანების მცირე რაოდენობაზე. ცხადია, ადამიანების დიდ ნაწილს არ გააჩნია სრულყოფილი ცოდნა ამ სფეროში შექმნილი უამრავ ქვეყანაში დაგროვილი ცოდნის შესახებ. ამის მიზეზი შეიძლება იყოს ადამიანური მეხსიერების ლიმიტი თუ მათთვის შეზღუდული დრო, დაეწიონ ამ სფეროში შექმნილ უახლეს მიღწევებს. რა თქმა უნდა სამედიცინო ინფორმაციის და მეცნიერული ცოდნის უდიდესი ნაწილი ინტერნეტში განთავსებულ ღია თუ დახურული ტიპის სამეცნიერო ბაზებსა თუ საინფორმაციო სააგენტოების ვებ-გვერდებზეა განთავსებული. მაგრამ ის მიმოფანტულია და ადამიანისათვის

[10] იქვე.

სისტემატიზებულად მისაღები ცოდნისათვის რთულად მისაღწევია. უმაღლესი დონის სამედიცინო დიაგნოზის დასმა ჯერ კიდევ დამოკიდებულია გეოგრაფიულ მდგომარეობასა და ქონებრივ შესაძლებლობებზე.

შემდეგი თაობის ხელოვნური ინტელექტის ტექნოლოგიები ამ ყველაფერს შეცვლის. ექიმის მონახულების მრავალი სოციალური ეფექტის გარდა, დიაგნოზის საფუძველი მოიცავს დიდი მოცულობის მონაცემთა შეგროვებას, მაგ., სიმპტომები, ანამნეზი, გარემო ფაქტორები და მათთან დაკავშირებული მოვლენების, მაგალითად, დაავადებათა პროგნოზირებას. კორელაციების მოძიება და პროგნოზირების გაკეთება არის ის, რისთვისაც ხელოვნური ინტელექტის სიღრმისეული სწავლების (ე.წ. Deep Learning) მეთოდი იხვეწება. საკმარისი მონაცემების გათვალისწინებით ამ შემთხვევაში ზუსტი სამედიცინო ჩანაწერების საშუალებით ხელოვნური ინტელექტის გამოყენებით დიაგნოსტიკა ნებისმიერ მედიცინის სპეციალისტს სუპერდიადნოსტიკოსად აქცევს. ის გახდება ექიმი, რომელიც აღჭურვილი იქნება ათეული მილიონი პაციენტის დიაგნოზისა და მკურნალობის გამოცდილებით, ფარული კორელაციის დადგენის უნარითა და სრულყოფილი მეხსიერებით. სწორედ ეს არის ის, რის შექმნასაც ე.წ. „ჭკვიანი მედიცინის“ მოდელზე მომუშავე ხელოვნური ინტელექტის ჩინური სამედიცინო კომპანია „არიქს სინქინგ“ (RX Thinking) ცდილობს. კომპანია დააარსა ხელოვნური ინტელექტის სფეროს ჩინელმა მკვლევარმა, რომელსაც მუშაობის დიდი გამოცდილება აქვს აშშ-ს სილიკონის ველზე. სტარტაპი ასწავლის და ატრენინგებს ხელოვნური ინტელექტის ჩინურ ალგორითმებს, გაანალიზონ და გახდნენ სუპერ ზუსტი დიაგნოზის დამდგენი პროგრამები. ხოლო დიაგნოზის დადგენის შემდეგ მისი სწრაფად გაგზავნა შესაძლებელი გახდება ჩინეთის ნებისმიერ რეგიონში[11]. საინტერესოა ის ფაქტი, რომ ექიმების ალგორითმებით ჩანაცვლების ნაცვლად, ის მოწოდებულია გახდეს ექიმების დამხმარე აპლიკაცია დიაგნოზის დასმის პროცესში, რაც გულისხმობს ექიმების დახმარებას, დიაგნოზტიკისას მათ დაეხმაროს სწორი სტრატეგიის შემუშავებაში. ასევე ის ექიმებს არ აიძულებს სრულად დაეყრდნონ მის მონაცემებსა და რეკომენდაციებს. თუმცა, თუ იმას გავითვალისწინებთ, რომ ალგორითმი ყოველი ახალი სამედიცინო შემთხვევის შესახებ ინფორმაციის მიღებით კიდევ უფრო ვითარდება, ის თანდათანობით გამორიცხავს დიაგნოზში შეცდომების დაშვებას. ამასთან, ითხოვს დიაგნოსტირებისათვის დამატებითი ინფორმაციას მიწოდებას პროცესის დასასრულებლად[12]. მას შემდეგ, რაც ალგორითმის დასარწმუნებლად სრულყოფილი ინფორმაცია აიტვირთება, პროგრამას უკვე შეუძლია შესაძლო დაავადების ზუსტი პროგნოზირება ან სიმპტომების გაანალიზებით ზუსტი დიაგნოსტიკა. ამასთან, სიმპტომების გაანალიზებისას მას მონიტორზე გამოჰყავს პროცენტული მაჩვენებელი, ამ სიმპტომების გათვალისწინებით რამდენია ალბათობა ზუსტი დაავადების განსაზღვრისა.

აპლიკაცია არ უგულებელყოფს ექიმს, რომელსაც ყოველთვის შეუძლია აპლიკაციის რეკომენდაციებისგან განსხვავებული დიაგნოზი დასვას. მაგრამ საქმე იმაშია, რომ ეს აპი 400 მილიონზე მეტ დიაგნოზს ეყრდნობა და გამუდმებით

[11] <https://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/> [07.01.2024].

[12] <https://healthitanalytics.com/news/top-12-artificial-intelligence-innovations-disrupting-healthcare-by-2020> [07.01.2024].

სწავლობს, აანალიზებს და ასკანერებს ახალ ინფორმაციას თუ სამედიცინო პუბლიკაციებს ახალი ცოდნის თუ ტენდენციის მისაწოდებლად[13].

შესაბამისად, ექიმები მომავალში მოწოდებულნი იქნებიან სრულად კონცენტრირდნენ პაციენტებზე ნუგეშის და დადებითი ადამიანური ფაქტორების გამოვლენაზე, რაც დღესაც კი შეუცვლელია.

დიდი მონაცემების გამოყენებით ხელოვნური ინტელექტის განვითარების დადებითი ტენდენციების ჩვენება მხოლოდ მედიცინის სფეროთი არ შემოიფარგლება. შეიძლება უამრავი მაგალითის მოყვანა სოფლის მეურნეობის (მაგ. დრონების მეშვეობით მიწის ანალიზის დიაგნოსტიკა, მათი დახმარება აგრარული ტექნოლოგიების განვითარებაში, რაც მოსავლიანობის ზრდის წარმოუდგენლად დიდ შედეგებს გვპირდება. სახელმწიფოს მიერ დაფინანსებული პროექტების დრონების მეშვეობით მონიტორინგი და მონაცემების გადაგზავნა ხელოვნური ინტელექტის პროგრამის ანალიზისათვის და ა.შ.), ტრანსპორტისა და ლოგისტიკის, სამხედრო და თავდაცვის და ა.შ. სფეროებში.

დიდი მონაცემების ტექნოლოგიის გამოყენებისას, არსებითია ადამიანის ძირითადი უფლებებისა და თავისუფლების, ასევე ინფორმაციის დაცულობისა და გავრცელების პრინციპების დაცვა, რადგან არსებობს საფუძვლიანი რისკი მათი უთანასწორო მოხმარების შესახებ. დიდი მონაცემების უსაფრთხოება, სახელმწიფოს ტერიტორიული საზღვრების მსგავსად, სტრატეგიულად უაღრესად მნიშვნელოვანია. იგი ინტელექტუალური პროგრამული გარემოსათვის მკვებავი და გადაწყვეტილების მიღების ინსტრუმენტია.[14]

მიუხედავად ამ სარგებლისა და ბევრი დადებითი ეფექტისა, დიდი მონაცემების ეპოქა შიშის საფუძველსაც იძლევა. ვინაიდან დიდი მონაცემები სულ უფრო ზუსტ პროგნოზებს აკეთებენ სამყაროს და მასში ჩვენი ადგილის შესახებ, ჩვენ შეიძლება მზად არ აღმოვჩნდეთ მისგან განხორციელებული გავლენის წინაშე, ჩვენს ყოველდღიურობასა და ჩვენს პირად თავისუფლებაზე. ადამიანების სამყაროს აღქმა და ინსტიტუტები ჩამოყალიბდა იმ ეპოქებსა და რეალობაში, სადაც ინფორმაციის სიმწირე ჩვენი განვითარების საფუძველი იყო. ახლა კი გადავდივართ იმ ეპოქაში, რომელშიც სრულიად შესაძლებელი ხდება ყველანაირი ინფორმაციის მოპოვება და დამუშავება, რაც შესაბამის ორგანიზაციებს ადამიანებზე აქამდე წარმოუდგენელი მანიპულაციის საშუალებას მისცემს. მაგალითად, ფეისბუქის ბიზნეს სტრატეგიაა შეექმნა მომხმარებელზე მორგებული პლატფორმა, რომელშიც 2,5 მილიარდი ადამიანი თავისუფლად აზიარებს მისი და მისი ოჯახის თუ მეგობრების წევრების შესახებ პირად ფოტოებსა თუ ვიდეოებს. დღეის მდგომარეობით ამ ქსელში ადამიანთა შესახებ უზარმაზარი რაოდენობის პირადი ინფორმაციაა თავმოყრილი, რაც საშუალებას აძლევს პლატფორმას, თითოეული ადამიანის ქცევები გაანალიზოს, ზუსტად გაიგოს რა ემოციები აქვს, რა მოსწონს, რა არ მოსწონს, როგორი ჩაცმის თუ კვების სტილი აქვს და შესთავაზოს მას ზუსტად ის რეკლამები, რაც მას დაასტიმულირებს, რომ შეიძინოს. ეს კი პლატფორმას საშუალებას აძლევს პრემიუმ ფასები დაადოს რეკლამებს იმ კომპანიებისათვის, რომლებიც მომხმარებელთა თავიანთ მიკრო სეგმენტს ეძებენ.

ფეისბუქის დამფუძნებელმა და დირექტორმა მარკ ცუკერბერგმა აშშ-ს სენატში მოსმენის დროს განაცხადა – „იმის გამო, რომ ჩვენ გვესმის, რა გაინტერესებთ თქვენ,

[13] <https://www.technologyreview.com/2020/07/15/1004743/a-new-rx-ai-for-operations-in-health-care/> [07.01.2024].

[14] *ჯოლია გ.,* განათლება და დასაქმება ციფრულ გარემოში, თბ., 2021, 37.

ჩვენ შეგვიძლია გაჩვენოთ კონკრეტული თქვენზე მორგებული რეკლამები“. ეს იმას გულისხმობს, რომ ფეისბუქი ყოველდღიურად სწავლობს და აანალიზებს მისი 2,5 მილიარდი მომხმარებლის ქცევებს, გემოვნებას, ყოველდღიურ ყოფას, ემოციებს (ლაიქების და სხვა „ემოჯების“ მეშვეობით), პოლიტიკურ, რელიგიურ და სექსუალურ დამოკიდებულებასაც კი, თქვენს „კედელზე დასქროლვისას“ გაჩვენებთ მხოლოდ თქვენზე მორგებულ რეკლამებს.

2019 წელს „ნეტფლიქს ფილმსის“ (Netflix Films) დაკვეთით გამოვიდა კ. ემერის და ჯ. ნოუჯეიმის დოკუმენტური ფილმი “The Great Hack”, რომელიც დეტალურად აღწერს, თუ რა გავლენას ახდენს სოციალური ქსელი „ფეისბუქი“ ადამიანების სარეკლამო თუ პოლიტიკური შეხედულების ჩამოყალიბებაზე. განსაკუთრებით მნიშვნელოვანია ჟურნალისტური გამოძიება, რომელსაც უკავშირდება აშშ-ში 2016 წლის საპრეზიდენტო არჩევნებში დ. ტრამპის გამარჯვებასა და დიდი ბრიტანეთის გასვლას ევროკავშირის შემადგენლობიდან (ე.წ. ბრექსიტი). ფილმში ამ ორ მნიშვნელოვან პოლიტიკურ მოვლენას შორის ნაჩვენებია კავშირი და ის უკავშირდება ცნობილი ბრიტანული დიდი მონაცემების ანალიტიკური კომპანიის (Cambridge Analitica) საქმიანობას და მის უშუალო ჩართულობას ამ ორივე კამპანიაში. კერძოდ, „კემბრიჯ ანალიტიკა“-ს თანამშრომლებმა მოგვიანებით მისცეს ჩვენებები, რომლებიც ადასტურებენ იმას, თუ როგორ გამოიყენეს სოციალური ქსელების, ძირითადად „ფეისბუქში“ განთავსებული აშშ-ს და დიდი ბრიტანეთის მოქალაქეთა პირადი ინფორმაცია და მანიპულირების გზით მოახდინეს ჯერ კიდევ „ნეიტრალური“ ამომრჩევლის ნებაზე ზეწოლა, რამაც აშშ-ში ტრამპის გამარჯვება, ხოლო დიდი ბრიტანეთის რეფერენდუმში „ბრექსიტის“ მომხრეთა გამარჯვება განაპირობა. აშშ-ს სენატში მოსმენისას მარკ ცუკერბერგმა დაადასტურა, რომ ბოროტად იქნა გამოყენებული მათი მომხმარებლების პირადი ინფორმაცია და ბოდიში მოიხადა, ასევე განაცხადა, რომ არ იცოდა მისი კომპანიის თანამშრომლების ჩართულობა „ალამოს პროექტზე“[15].

2020 წელს „ნეტფლიქსის“ (Netflix) პლატფორმაზე გამოჩნდა რეჟისორ ჯეფ ორლოვსკის დოკუმენტური ფილმი „სოციალური დილემა“ (The Social Dilemma), რომელიც ფსიქოლოგების, აიტი სპეციალისტების, პროგრამისტებისა და ინტერნეტ სფეროში მოღვაწე პროფესიონალების ინტერვიუებზე დაყრდნობით კარგად აღწერს, თუ როგორც შეუძლიათ სოციალურ ქსელებს, საძიებო სისტემებს ხელოვნური ინტელექტის და დიდი მონაცემების გამოყენებით ადამიანთა მანიპულირება. მანიპულაცია არ შემოიფარგლება მხოლოდ ქსელის „იუზერთა“ (User)-თა კარგ „მომხმარებლად“ გარდაქმნით, რომ მათ რაც შეიძლება მეტი პროდუქცია შეიძინონ (თუნდაც ხშირად არც სჭირდებოდეთ ეს პროდუქტი), არამედ ის მოიცავს ადამიანთა ქცევების, გემოვნების და პოლიტიკური თუ სხვაგვარი შეხედულებების ცვლილებებსაც კი, რაც უდავოდ არღვევს ადამიანის უფლებებსა და თავისუფლებებს.

[15] პროექტი „ალამო“ (Project Alamo) – 2016 წლის საპრეზიდენტო არჩევნებში პრეზიდენტობის კანდიდატ დონალდ ტრამპის წინასაარჩევნო კამპანიის წამყვანი პროექტი, რომელშიც ჟურნალისტების მტკიცებით ჩართულნი იყვნენ „კემბრიჯ ანალიტიკა“-ს (Cambridge Analitica) და „ფეისბუქის“ (Facebook) თანამშრომლები და რომლებმაც დიდი მონაცემებისა და ხელოვნური ინტელექტის გამოყენებით შეძლეს ზემოქმედება მოეხდინათ „მერყევ“, ნეიტრალურ ამომრჩეველზე, რამაც პრეზიდენტ დ. ტრამპის არჩევნებში გამარჯვება უზრუნველყო. იხ. <https://www.thealamo.org/alamo-plan/preservation/black-paper/index.html>; ასევე, <https://semantiko.com/project-alamo/> [07.01.2024].

6. დასკვნა

თანამედროვე სამყაროში დიდი მონაცემების დამუშავება სერიოზული გამოწვევის წინაშე აყენებს პერსონალური მონაცემების დაცვის საკითხს. სტატიაში შევეცადეთ გაგვეცნო სამართლებრივ ჭრილში დიდი მონაცემების დამუშავებისას პოზიტიური და ნეგატიური ასპექტები. ფაქტია, რომ დიდი მონაცემების განვითარება შეუქცევადი პროცესია და ხელოვნურ ინტელექტზე დამყარებული ტექნოლოგიები დროთა განმავლობაში უფრო განავითარებენ მონაცემების დიდი ოდენობით დამუშავების მიმართულებებს. ამ პროცესში კი დიდი გამოწვევების წინაშე დადგება პერსონალურ მონაცემთა დაცვის საკითხები, რაც შესაბამისი კანონმდებლობის მუდმივად ტრანსფორმირებას და ახალ გამოწვევებზე მორგებას მოითხოვს. შესაბამისად, ვფიქრობ, რომ მნიშვნელოვანია საქართველოში პერსონალურ მონაცემთა დაცვის სამსახურის[16] ფუნქციების ისეთი მოდიფიცირება, რომ სწრაფი და მოქნილი მექანიზმებით შეძლოს მუდმივად მზარდი პერსონალურ მონაცემთა დამუშავების გამოწვევებზე რეაგირება.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალური მონაცემების დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023.
2. *ჯოლია გ.,* განათლება და დასაქმება ციფრულ გარემოში, თბ., 2021, 36-37.
3. *Franks B.,* Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics, New Jersey: John Wiley & Sons, Inc., 2012.
4. <https://healthitanalytics.com/news/top-12-artificial-intelligence-innovations-disrupting-healthcare-by-2020> [07.01.2024].
5. <https://www.technologyreview.com/2020/07/15/1004743/a-new-rx-ai-for-operations-in-health-care/> [07.01.2024].
6. <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> [07.01.2024].
7. <https://medicalfuturist.com/top-artificial-intelligence-companies-in-healthcare/> [07.01.2024].
8. <https://www.thealamo.org/alamo-plan/preservation/black-paper/index.html> [07.01.2024].
9. <http://www.economy.ge/index.php?page=news&nw=1617> [07.01.2024].
10. <https://2017-2021.state.gov/the-clean-network/> [07.01.2024].
11. <https://semantiko.com/project-alamo/> [07.01.2024].
12. <https://www.flyingnets.com/en/> [07.01.2024].

[16] <https://personaldata.ge/ka> [07.01.2024].

ივა კატიჩი*

მონაცემთა დაცვის ოფიცერი — „მონაცემთა დაცვის ძირითადი რეგულაციით“ განსაზღვრულ ამოცანებთან დაკავშირებული დარღვევების პრევენციის მექანიზმი

მონაცემთა დაცვის ოფიცრის მოთხოვნები დამატებით ტვირთს წარმოადგენს გუნდური სამუშაოებისთვის, რაც მონაცემთა დაცვის ოფიცრის სამუშაოს უკიდურესად ერთპიროვნულს ხდის. ამ პოზიციის ძირითადი არსი მდგომარეობს ყურადღების ფოკუსირებაში შიდა ორგანიზაციულ საკითხებზე, რათა არ მოხდეს მონაცემთა დაცვის კანონების დარღვევა, რაც ამ პოზიციას უკიდურესად დიდ პასუხისმგებლობას აკისრებს. სწორედ ზემოთ ხსენებულთან დაკავშირებით შეიძლება ითქვას, რომ ამოცანების ბუნებიდან გამომდინარე, მონაცემთა დაცვის ოფიცრებს შეუძლიათ, პრევენციული ზეგავლენა მოახდინონ ორგანიზაციაზე რაიმე დარღვევასთან დაკავშირებით, და შესაბამისად, ადამიანის ფუნდამენტური უფლებებისადმი პატივისცემაზე, განსაკუთრებით, პირად მონაცემთა დაცვის უფლებაზე.

საკვანძო სიტყვები: *მონაცემთა დაცვის ოფიცერი, პირად მონაცემთა დაცვა, დარღვევების პრევენცია.*

1. შესავალი

პერსონალური მონაცემები ყველგანაა. მართებულია, რომ კომპანიები კარგად დაფიქრდნენ მაშინაც კი, როცა ინფორმაცია ერთი შეხედვით არ კვალიფიცირდება როგორც პერსონალური მონაცემი.

სახელი, დაბადების თარიღი, სახლის და ელექტრონული მისამართი, ინტერნეტ პროტოკოლის (IP) მისამართი, პირადობის (ID) ნომერი, ჯანმრთელობის ცნობები, როგორიცაა ფიზიკური პირის დიოპტრიკა, თითის ანაბეჭდები, მანქანის რეგისტრაციის ნომერი, ფოტოსურათი და ბევრი სხვა სახის ინფორმაცია წარმოადგენს პირად მონაცემებს.

ევროპული კანონის მე-8 მუხლის შესაბამისად, პერსონალური მონაცემთა დაცვა აღიარებულია როგორც ადამიანის ცალკეული ფუნდამენტური უფლება ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის მიხედვით.

---

* ზაგრების უნივერსიტეტის სამართლის მაგისტრი (LL.M.); ხორვატიის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს — “Agencija za zaštitu osobnih podataka” სამდივნო.

„პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ“ ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის 2016/679 (EU) რეგულაცია („მონაცემთა დაცვის ძირითადი რეგულაცია“; შემდგომში GDPR), რომელიც აუქმებს 95/46/EC დირექტივას, ძალაში შესვლამდე პერსონალურ მონაცემთა დაცვის ძირითად სამართლებრივ დოკუმენტს წარმოადგენდა პერსონალურ მონაცემთა დაცვის დირექტივა.[1]

თუმცა, თანამედროვე ტექნოლოგიის განვითარების გამო საჭირო გახდა კანონმდებლობის რეფორმირება, რათა სამართლებრივმა ბაზამ შეძლოს შედარებით ეფექტურად გააკონტროლოს პერსონალურ მონაცემთა დამუშავება ციფრულ საუკუნეში.

ამის გამო, მონაცემთა დაცვის ძირითადი რეგულაცია ძალაში შევიდა როგორც ტექნოლოგიურად ნეიტრალური რეგულაცია, რომელიც გახდა პერსონალურ მონაცემთა დაცვის პიონერი და მისაბაძი მოდელი გლობალური მასშტაბით.

ხუთზე მეტი წლის წინ, მონაცემთა დაცვის ძირითადმა რეგულაციამ გამოიწვია დიდი საზოგადოებრივი ინტერესი და აიძულა ბევრი სუბიექტი, რომ რენტგენზე გაეტარებინათ თავიანთი ორგანიზაციები.

მონაცემთა დაცვის კანონმდებლობის შესასრულებლად მონაცემთა დამმუშავებელს განვითარებული უნდა ჰქონდეს კანონით გათვალისწინებული ყველა დავალების შესრულების უნარი.

ბოლო წლებში, ცხადი გახდა, რამდენად ღირებულია ორგანიზაციისათვის მონაცემთა დაცვის ოფიცრის როლი.

განსაკუთრებით რეკომენდებულია დაინიშნოს ორგანიზაციაში მონაცემთა დაცვის ოფიცერი, რომელსაც შეუძლია, ძლიერი პრევენციული ზეგავლენა მოახდინოს ორგანიზაციაზე, სადაც იგი მუშაობს.

მონაცემთა დაცვის სათანადო ოფიცრის დანიშვნას შეუძლია, შეამციროს პერსონალურ მონაცემების უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის შესაძლებლობები.

2. მონაცემთა დაცვის ოფიცრის როლის პრევენციული გავლენა ორგანიზაციაში

წარმოვიდგინოთ მონაცემთა სუბიექტის საჩივარი კომპანიის წინააღმდეგ, მონაცემთა სუბიექტის პერსონალური მონაცემების კომპანიის ვებგვერდზე განთავსების გამო.

გამოქვეყნებული მონაცემები შეიცავდა სუბიექტის ავტომანქანის იდენტიფიკაციის ნომერს (შასის ნომერი), ზოგად ინფორმაციას ავტომობილის შესახებ და მონაცემებს მისი დაზიანების შესახებ კონკრეტული ნომრის მიხედვით.

ერთი შეხედვით, ჩვეულებრივ ფიზიკური პირი განაცხადებდა, რომ გამოქვეყნებული ინფორმაცია არ წარმოადგენს პერსონალურ მონაცემებს, თუმცა შასის ნომრის რამდენიმე ვებგვერდზე შეყვანით, პიროვნებას შეუძლია, მიიღოს ინფორმაცია ტრანსპორტის შესახებ, როგორიცაა ძრავის ნიშნები, ფერის კოდი ან წარმოების თარიღი და სხვა.

[1] ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალ მიმოცვლასთან დაკავშირებით“.

თავდაპირველად, პიროვნებას არ შეუძლია გაიგოს ბევრი რამ ავტომანქანის მეპატრონის შესახებ, მაგრამ შასის ნომერი ტრანსპორტის მფლობელის თუნდაც ზუსტი ვინაობის გაგების საშუალებაა.

წარმოვიდგინოთ, რომ კომპანიამ არ დაინიშნა მონაცემთა დაცვის ოფიცერი და ამტკიცებს, რომ შასის ნომერი არ წარმოადგენს პერსონალურ მონაცემს.

როგორ შეასრულებს ეს კომპანია გამჭვირვალობის ვალდებულებას, რომელიც დადგენილია მონაცემთა დაცვის კანონით?

კომპანიაში ვინმეს უნდა განესაზღვრა შასის ნომერი, როგორც პერსონალური მონაცემი, დაედგინა დამუშავების სამართლებრივი ბაზა და დაეცვა გამჭვირვალობის ვალდებულება, რისთვისაც საჭიროა მონაცემთა დამუშავების სამართლებრივი ბაზის შესახებ ინფორმაციის შეტანა შეტყობინებაში პირადი ცხოვრების ხელშეუხებლობის შესახებ.

მონაცემთა დაცვის ძირითადი რეგულაციის მიხედვით, მონაცემთა სუბიექტი არის პირდაპირ ან არაპირდაპირ იდენტიფიცირებული ან იდენტიფიცირებადი ფიზიკური პირი. იდენტიფიკაციას ხელს უწყობენ გარკვეული ფაქტორები, რომლებიც დაკავშირებულია ფიზიკური პირის ფიზიკურ, ფიზიოლოგიურ, გენეტიკურ, გონებრივ, ეკონომიკურ, კულტურულ ან სოციალურ იდენტობასთან.[2]

ავტომანქანის მძღოლის ვინაობა შესაძლოა შემდგომში დადგინდეს დამატებითი ინფორმაციის საშუალებით, არაპირდაპირ, კონკრეტული პიროვნებისთვის დამახასიათებელი ერთი ან მეტი ფაქტორით, ფაქტებით ადგილმდებარეობის შესახებ და ა.შ. აქედან გამომდინარე, ტრანსპორტის შასის ნომერი შეიძლება მიჩნეული იყოს პერსონალური მონაცემად.

მონაცემთა დაცვის ოფიცერი (თუ დანიშნულია ან სათანადოდ არის შერჩეული) ამოიცნობდა კავშირს „შასის ნომრის“ მიღმა მყოფ პირთან და ეცოდინებოდა პერსონალური მონაცემების განმარტება. პერსონალური მონაცემების იდენტიფიკაციის შემდეგ მონაცემთა დაცვის ოფიცერი დაადგენდა სამართლებრივ ბაზას მონაცემთა დამუშავებისათვის გასაჯაროებამდე და შემდეგ, მონაცემთა მინიმიზაციის[3] პრინციპის შესაბამისად, გასცემდა რჩევას, რომ მხოლოდ საჭიროების შემთხვევაში გაესაჯაროებინათ პერსონალური მონაცემები და მიეწოდებინათ ინფორმაცია მონაცემთა სუბიექტისთვის ასეთი მონაცემების დამუშავების შესახებ.

მონაცემთა დაცვის ოფიცერი ან თანამშრომელია ან გარე ექსპერტი, რომელსაც გააჩნია მაღალი პროფესიონალური ეთიკა და ცოდნა მონაცემთა დაცვის კანონის შესახებ.

მონაცემთა დაცვის ოფიცერმა აუცილებლად უნდა იცოდეს ვალდებულებები, რომლებსაც მას აკისრებს მონაცემთა დაცვის კანონი და უნდა აკონტროლებდეს ევროპის ეკონომიკური სივრცის ფარგლებში ზედამხედველი ორგანოების მიერ და ევროპის კავშირის მართლმსაჯულების სასამართლოს მიერ მიღებულ გადაწყვეტილებებს, ზედამხედველი ორგანოების რეკომენდაციებსა და

[2] ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას პიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, რომელიც აუქმებს დირექტივას 95/46/EC (მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 4, პარაგრაფი 1).

[3] იქვე, მუხლი 5, პარ. 1.

შეხედულებებს და ასევე მონაცემთა დაცვის ევროპული საბჭოს სახელმძღვანელო მითითებებს.

მონაცემთა დაცვის ოფიცერი წარმოადგენს ერთგვარ ინსპექციას ორგანიზაციის ფარგლებში. ამიტომ, ძალიან მნიშვნელოვანია, რომ ის ფლობდეს ცოდნას ორგანიზაციის შიდა სტრუქტურის შესახებ. მონაცემთა დაცვის ოფიცრისთვის ნაცნობი უნდა იყოს ორგანიზაციის მიერ მართული პროცესები, ასევე მონაცემთა დამუშავების საშუალებები.

ფიზიკური პირი, რომელიც განიხილება როგორც ორგანიზაციის ინსპექტორი, უნდა შეეძლოს წარმატებული კომუნიკაციის წარმართვა სამთავრობო წარმომადგენელთან. მონაცემთა დაცვის ოფიცერს ნამდვილად მოუწევს შეეწინააღმდეგოს ისეთ იდეებს, რომლებიც კონფლიქტშია მონაცემთა დაცვის კანონთან. გარდა ამისა, ყველა ადამიანს არ შეუძლია კოლეგების გაკრიტიკება და პერსონალურ მონაცემთა დაცვის შესახებ კანონის დებულებების დაცვის მოთხოვნა.

პრაქტიკაში მთავარ პრობლემას წარმოადგენს არაკვალიფიციური პირის დანიშვნა, როდესაც მონაცემთა დაცვის ოფიცრის დანიშვნა ატარებს ფორმალურ ხასიათს, ორგანიზაციას იგი სარგებლობას ვერ მოუტანს.

2.1. საზედამხედველო ვალდებულების ზეგავლენა დარღვევების პრევენციაზე

მონაცემთა დაცვის ოფიცერი უნდა ასრულებდეს კონსულტანტის როლს. ორგანიზაციაში ახალი პროცედურის ან ტექნოლოგიის დანერგვისას მონაცემთა დაცვის ოფიცერი ჩართული უნდა იყოს პროექტში რათა შესაძლებელი იყოს პრევენციული ზემოქმედება იმ მექანიზმებზე, რომლებიც უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის რისკის ქვეშ დააყენებს პერსონალურ მონაცემებს.

გადამწყვეტი მნიშვნელობა აქვს პროექტში დროულ ჩართვას. ახალი ტექნოლოგიის დამუშავების პროცესში, კარგი ექსპერტი მხედველობაში მიიღებს მონაცემთა დაცვას - მომსახურების შექმნის პროცესში (design) და პირველად პარამეტრად (default)[4] და გააერთიანებს უსაფრთხოების ზომებს როგორიცაა მონაცემის წაშლის შესაძლებლობა მისი შენახვის პერიოდის გასვლის შემდეგ, უზრუნველყოფს რომ პერსონალურ მონაცემებზე წვდომა შეიზღუდოს იმ პერსონალამდე, რომელმაც უნდა შეასრულოს ამ პერსონალური მონაცემებით კონკრეტული დავალება და მხოლოდ იმ კონკრეტული ტიპის პერსონალურ მონაცემებამდე, რომლის ცოდნაც საჭიროა ამ დავალების შესასრულებლად, ასევე უზრუნველყოფს რომ შეუძლებელი იყოს მონაცემების წაკითხვა, გადაწერა, შეცვლა ან ამოშლა უფლებამოსილების გარეშე (მაგ. ცოდნის - საჭიროების საფუძველზე), მონაცემებზე წვდომა შესაძლებელი იყოს მხოლოდ უფლებამოსილი პერსონალის წარმატებული იდენტიფიკაციისა და ავთენტიფიკაციის შემდეგ, და ა.შ.

მონაცემთა დაცვის ძირითადი რეგულაცია რისკზე დაფუძნებული კანონია. მონაცემთა დაცვის ოფიცერმა გამუდმებით უნდა შეაფასოს რისკები, რათა შესაძლებელი იყოს ორგანიზაციაში იმ მონაცემთა დამუშავების დადგენა რომლებიც შეიძლება პრობლემური იყოს. მაგ. თუ კომპანიის პერსონალური მონაცემები სისტემატურად და ფართოდ პროფილირდება ან ახალი ტექნოლოგიური გადაჭრის გზები გამოიყენება პერსონალურ მონაცემთა დამუშავებაში, როგორიცაა „საგნების

[4] იქვე, მუხლი 25. პარ. 1.

ინტერნეტის“ გამოყენება, ან პერსონალური მონაცემები მუშავდება მრავალი წყაროდან მიღებული მსგავსებების ერთმანეთთან დაკავშირებით, შედარებით და შემოწმებით, მონაცემთა დაცვის ოფიცერმა უნდა „ააფრიალოს წითელი დროშა“ - დაადგინოს ან ყურადღება გაამახვილოს პრობლემაზე.

მონაცემთა დაცვის ოფიცრები არ წარმოადგენენ კომპანიისთვის ტვირთს. მათ დანიშნულებას არ წარმოადგენს პერსონალურ მონაცემთა დამუშავების აკრძალვა. მათი მიზანია უზრუნველყონ პერსონალურ მონაცემთა დამუშავების შესაბამისობა მონაცემთა დაცვის რეგულაციის მოთხოვნებთან.

თუმცა, თუ კომპანიას არ მიაჩნია, რომ მონაცემთა დაცვის ოფიცრისგან რჩევების მიღება და მათი ჩართვა პროექტში, რომელიც ითვალისწინებს მონაცემთა დამუშავებას, მათთვის სარგებლობის მომტანია, მან მხედველობაში უნდა მიიღოს რომ შესაძლებელია დაიწყოს გამოძიება ამ მოთხოვნის შეუსრულებლობის გამო.

ბელგიის მონაცემთა დაცვის ორგანომ[5] ინსპექტირება ჩაატარა ტურიზმის რეგიონულ სამთავრობო სააგენტოში, რის შედეგადაც სააგენტოს გამოუცხადეს საყვედური, რადგან მონაცემთა დაცვის ოფიცერი არ იყო პროაქტიულად ჩართული კანონით გათვალისწინებული დავალების დამუშავებაში, დაირღვა მონაცემთა დაცვის ძირითადი რეგულაციის 38(1) და 39(1) მუხლები.

2.2. სამართლებრივ დებულებებთან შესაბამისობის მონიტორინგი, როგორც დარღვევების პრევენციის მექანიზმი

მონაცემთა დაცვის ოფიცერი უფლებამოსილია ჩაატაროს აუდიტი, რომელიც შეიძლება ინიციირებული იყოს ან გარეგანი შეტყობინების საფუძველზე, მაგ., როდესაც ფიზიკური პირი წარუდგენს კომპანიას საჩივარს და მონაცემთა დაცვის ოფიცერი შეისწავლის საჩივართან დაკავშირებულ გარემოებებს, ან შინაგანი ინიციატივით - პროფკავშირის კომისრის, შრომის საბჭოს, ინფორმატორის ან ნებისმიერი თანამშრომლის საჩივრის ან შეტყობინების საფუძველზე.

კომპანია ვალდებულია, მიაწოდოს მონაცემთა დაცვის ოფიცერს ყველა რესურსი და მისცეს წვდომა აუდიტის ჩასატარებლად. კომპანიამ უნდა აცნობოს თანამშრომლებს ინსპექტირების ჩატარებაზე მონაცემთა დაცვის ოფიცრის უფლებამოსილების შესახებ (კარგი იქნება თუ გასცემს მკაფიო ინსტრუქციებს კომპანიის შიდა წესების გამოყენებით). შეტყობინება ცნობილი უნდა გახდეს საგარეო სერვისების პროვაიდერებისთვის, მომმარაგებლებისთვის, ზედამხედველი კომიტეტის წევრებისა და ყველასთვის, ვისაც აქვს შეხება პერსონალურ მონაცემებთან კომპანიაში.

რეგულარული აუდიტის ჩატარებას შეუძლია (დროულად) აღმოაჩინოს პერსონალურ მონაცემთა დამუშავებაში არსებული პრობლემები და თავიდან აიცილოს პერსონალურ მონაცემთა უსაფრთხოებასთან დაკავშირებული დარღვევები.

[5] <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].

2.3. დამუშავების ოპერაციებში ჩართული პერსონალის ცნობიერების ამაღლება და ტრენინგი

პერსონალურ მონაცემებთან დაკავშირებული დარღვევები უმეტესად სათავეს მონაცემთა დამმუშავებლის თანამშრომლების მიერ დაშვებული შეცდომებიდან იღებს, რასაკვირველია, შეცდომის რისკი არსებობს, თუმცა შეიძლება შეცდომის თავიდან აცილება თანამშრომლების სათანადო კვალიფიკაციის ამაღლებით.

ნორვეგიაში[6] ერთმა კომპანიამ შეცდომით შეამოწმა მეორე კომპანიის ერთ-ერთი მფლობელის კრედიტი, რის შედეგადაც დაჯარიმდა 200 000 ნორვეგიული კრონით. დარღვევა გამოწვეული იყო იმ სისტემის არცოდნით, რომელიც გამოიყენებოდა საკრედიტო ანგარიშების მოთხოვნისთვის.

შემთხვევა მოხდა კვიპროსში[7], სადაც კლიენტის მონაცემების განახლების პროცესში ბეჭდვითი შეცდომა იქნა დაშვებული პასპორტის ნომერში ჰელენიკ ბანკში. გარკვეული დროის შემდეგ, სხვა პირმა შეამოწმა ინფორმაცია და ნახა, რომ თავის ახალ პასპორტს მიენიჭა ის ნომერი, რომელიც ბანკის თანამშრომელმა შეცდომით შეიყვანა წინა მომხმარებლის პასპორტის ნომრად, ამგვარად, ვებ-ბანკინგის პლატფორმის გამოყენებით სხვა კლიენტს ჰქონდა ნაწილობრივი წვდომა მეორე მომხმარებლის პერსონალურ და ფინანსურ მონაცემებზე.

საინფორმაციო კომისიის აპარატმა[8] საყვედური გამოუცხადა იუსტიციის სამინისტროს კონფიდენციალურობის დარღვევისთვის, რადგან რამდენიმე პირს ჰქონდა წვდომა ციხის კამერაში დარჩენილ კონფიდენციალურ დოკუმენტებზე.

პოლონეთის მონაცემთა დაცვის ორგანომ[9] 6387 ევროს ოდენობით დააჯარიმა რაიონული სასამართლო, რადგან თანამშრომელმა დაკარგა სამი USB-დისკი, რომელიც შეიცავდა რეზოლუციის პროექტს და ფიზიკური პირების დაუზუსტებელი რაოდენობის პერსონალურ მონაცემებს.

მნიშვნელოვანია, ხაზი გავუსვათ ფაქტს, რომ ერთ-ერთ ვალდებულებას რომელიც განსაზღვრულია მონაცემთა დაცვის ძირითადი რეგულაციით[10] წარმოადგენს სათანადო ორგანიზაციული დამცავი ზომების მიღება, რომელიც მოიცავს ორგანიზაციის შიგნით ცნობიერების ამაღლებას და არა მარტო.

დამმუშავებლის აღნიშნული ვალდებულება დაკავშირებულია პერსონალური მონაცემების დაცვის ოფიცრის ვალდებულებებთან, რომლის ამოცანაა თანამშრომელთა ცოდნის ამაღლება და პერსონალისთვის ტრენინგების ჩატარება მონაცემებთან დაკავშირებული დარღვევების თავიდან ასაცილებლად.

უამრავი მაგალითი არსებობს პრაქტიკაში, სადაც მონაცემთა დაცვის ოფიცერი მოახდენდა პრევენციულ გავლენას პერსონალურ მონაცემებთან დაკავშირებულ დარღვევებზე, ორგანიზაციაში პერსონალური მონაცემების დაცვის მნიშვნელობაზე ცნობიერების ამამაღლებელი აქტივობები რომ განხორციელებულიყო.

როცა საქმე ეხება თანამშრომელთა შეცდომას, პერსონალურ მონაცემთა დაცვის განზრახ დარღვევა არ არის ხშირი. როგორც წესი, თანამშრომლებს წარმოდგენა არა აქვთ რისკების წარმოშობასა და შეცდომებზე. მათ ასევე არ იციან, რომ ინციდენტთან

[6] <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].

[7] <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].

[8] <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].

[9] <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].

[10] ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“, რომელიც აუქმებს დირექტივას 95/46/EC (მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 32, პარაგრაფი 1).

დაკავშირებით უნდა გაკეთდეს შეტყობინება, რათა ლეგიტიმურად იმოქმედონ იმ ზეგავლენაზე რომელსაც ეს დარღვევა მოახდენს მონაცემთა სუბიექტზე.

2.4. კონსულტაციების გაწევა მონაცემთა დაცვაზე ზემოქმედების შეფასების პროცესში

მონაცემთა დაცვის ძირითადი რეგულაციის[11] მიხედვით, სადაც ერთგვარი დამუშავების, კერძოდ, ახალი ტექნოლოგიის გამოყენებისა, და დამუშავების ბუნების, სფეროს, კონტექსტის და მიზნის მხედველობაში მიღების შედეგად შეიძლება ფიზიკური პირების უფლებები და თავისუფლებები რისკის ქვეშ დადგეს, დამმუშავებელი ვალდებულია, დამუშავებამდე განახორციელოს დამუშავების ოპერაციების პერსონალური მონაცემების დაცვაზე ზეგავლენის შეფასება.

დამმუშავებლის ეს ვალდებულება დაკავშირებულია პერსონალურ მონაცემთა დაცვის ოფიცრის ამოცანებთან, რომელსაც ევალება მონაცემთა დაცვაზე ზემოქმედების შეფასების შესახებ საჭირო კონსულტაციის ჩატარება.

მონაცემთა დაცვაზე ზემოქმედების შეფასება ხელს უწყობს ფიზიკური პირების უფლებებსა და თავისუფლებების მიმართ მაღალი რისკის დადგენას პერსონალური მონაცემების დამუშავების დროს.

ზოგიერთი ფაქტორი,[12] რომელიც შესაძლოა, შეიცავდეს მაღალ რისკებს შემდეგია: ფინანსური დაწესებულებები, რომლებიც ახდენენ თავიანთი კლიენტების შემოწმებას ფულის გათეთრების საწინააღმდეგო (AML) ან თაღლითობის მონაცემთა ბაზის მეშვეობით, ბიოტექნოლოგიური კომპანია, რომელიც მომხმარებლებს სთავაზობს გენეტიკურ ტესტებს ავადმყოფობის/ჯანმრთელობის რისკების შეფასების და პროგნოზირების მიზნით, კომპანია, რომელიც ქმნის ქცევით ან მარკეტინგულ პროფაილებს თავიანთი ვებსაიტების გამოყენების ან ნავიგაციის მეშვეობით, ზოგადი პროფილის საავადმყოფო, რომელშიც შენახულია პაციენტების ისტორიები, კერძო გამომძიებელი, რომელიც ინახავს დეტალებს ნასამართლობებსა და კანონდარღვევებზე, გენეალოგიური ინფორმაციის ფართო კოლექციებს იმ პიროვნებების ოჯახებზე რომლებიც მიეკუთვნებიან კონკრეტულ რელიგიურ ჯგუფებს, დამუშავება იმ მონაცემებისა, რომლებიც მიღებულია ე.წ. „ნივთების ინტერნეტის“ აპლიკაციების გამოყენებით თუ მონაცემების გამოყენება მნიშვნელოვან გავლენას ახდენს (ან შესაძლოა მოახდინოს) ინდივიდების ყოველდღიურ და პირად ცხოვრებაზე.

შესაფასებელი რისკები დაკავშირებულია არა მარტო პერსონალური მონაცემების დაცვის უფლებასთან, არამედ სხვა უფლებებსა და ფუნდამენტურ თავისუფლებებთან, როგორიცაა პირადი და ოჯახური ცხოვრების უფლება, გამოხატვის თავისუფლებისა და ინფორმაციის უფლება და ა.შ.

ამიტომ, მაგალითად, თუ კომპანიას სურს მოძებნოს თანამშრომლის ტრანსპორტის მდებარეობა, არსებობს პერსონალური მონაცემების დამუშავების რისკი არასამუშაო დროს თანამშრომლის ადგილმდებარეობის შესახებ, რადგანაც ამან შეიძლება გავლენა მოახდინოს მის პირად და ოჯახურ ცხოვრებაზე.

[11] იქვე, მუხლი 35, პარ. 1.
[12] <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].

როდესაც მაღალი რისკი დადგენილია, საჭიროა, შეფასდეს შესაძლებელია თუ არა მისი შესუსტება სათანადო ტექნიკური და ორგანიზაციული დამცავი ზომების გამოყენებით. თუ რისკის შემსუბუქება არ არის შესაძლებელი, მაშინ მიზანშეწონილია პერსონალური მონაცემების დამუშავებაზე უარის თქმა.

ამ პროცესში პერსონალური მონაცემების დაცვის ოფიცერი თამაშობს საკვანძო როლს, რამდენადაც მის რეკომენდაციაზეა დამოკიდებული პერსონალური მონაცემების უსაფრთხოებასთან დაკავშირებული დარღვევებისა და არაკანონიერი წვდომის წარმატებით (ან წარუმატებლად) თავიდან აცილება.

მაღალი რისკების შემთხვევაში, რომლებიც ტექნიკური და ორგანიზაციული ზომების გატარებით არ შეიძლება შემცირდნენ „დასაშვებ რისკამდე“, უნდა შესრულდეს ვალდებულება, რომელიც განსაზღვრულია მონაცემთა დაცვის ძირითადი რეგულაციის 36-ე მუხლით, რაც ითვალისწინებს ზედამხედველ ორგანოსთან წინასწარ კონსულტაციას.

2.5. თანამშრომლობა ზედამხედველ ორგანოსთან

მონაცემთა დაცვის ოფიცერმა უნდა ითანამშრომლოს ზედამხედველ ორგანოსთან. თანამშრომლობა იწყება საკუთარი ან ზედამხედველი ორგანოს ინიციატივით.

მონაცემთა დაცვის ოფიცრის ურთიერთობას ზედამხედველ ორგანოსთან შეუძლია ზეგავლენა მოახდინოს პერსონალურ მონაცემთა დაცვის რეგულაციების დაცვაზე.

3. დასკვნა

ორგანიზაციაში მონაცემთა დაცვის ოფიცრის დანიშვნამ შესაძლოა იმოქმედოს, როგორც მონაცემთა დაცვის წესების დარღვევების თავიდან არიდების მექანიზმმა, რომელიც გამომდინარეობს დასახული ამოცანების ბუნებიდან. სხვა მოთხოვნებთან ერთად, მონაცემთა დაცვის ოფიცერმა კონსულტაცია უნდა გაუწიოს მონაცემთა დამმუშავებლებს და იმ თანამშრომლებს, რომლებიც ახორციელებენ მონაცემთა დამუშავებას, ხელი უნდა შეუწყოს პერსონალურ მონაცემთა დაცვის უფლებისადმი პატივისცემის კულტურის დანერგვას ორგანიზაციაში და მონიტორინგი გაუწიოს მონაცემთა დაცვის რეგულაციების შესრულებას. მათი დანიშვნით, რაც იძლევა ვალდებულებების დროულად შესრულების საშუალებას მათი რჩევების გათვალისწინებით, შეუძლია უზრუნველყოს, რომ არ დაირღვეს პერსონალურ მონაცემთა კანონი. მონაცემთა დაცვის ოფიცერსა და პრევენციულ მექანიზმს შორის კავშირი კანონის დარღვევასთან დაკავშირებით ზოგადად დამოკიდებულია რისკზე დაფუძნებულ ქმედებებზე, რაც (იმ შემთხვევაში თუ მონაცემთა დაცვის ოფიცერი კვალიფიციურია) ორი წინ გადადგმული ნაბიჯია, თუ მოვიფიქრებთ როგორ გავაუმჯობესოთ კანონის დაცვის სტანდარტი და შევამციროთ რისკები, დავაბალანსოთ ბიზნეს აქტივობები პერსონალურ მონაცემთა დაცვის უფლების მოთხოვნასთან.

ბიბლიოგრაფია:

1. ევროპარლამენტისა და საბჭოს 1995 წლის 24 ოქტომბრის დირექტივა 95/46/EC „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების თავისუფალ მიმოცვლასთან დაკავშირებით“ (ძალადაკარგულია).
2. ევროპარლამენტისა და საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU)2016/679 „პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვისა და ასეთი მონაცემების მიმოცვლის შესახებ“.
3. <https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_162/2022> [30.09.2023].
4. <https://gdprhub.eu/index.php?title=Datatilsynet_(Norway)_-_20/04401> [30.09.2023].
5. <https://gdprhub.eu/index.php?title=Commissioner_(Cyprus)_-_12.10.001.011.001> [30.09.2023].
6. <https://gdprhub.eu/index.php?title=ICO_(UK)_-_Ministry_of_Justice_(1)> [30.09.2023].
7. <https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.12.2020> [30.09.2023].
8. <https://azop.hr/wp-content/uploads/2023/09/DPO-prirucnik.pdf> [30.09.2023].

საბა ელიზბარაშვილი*

პერსონალური მონაცემების დამუშავება დრონების გამოყენებით (საერთაშორისო სტანდარტების მიმოხილვა და შესაბამისობა ქართულ კანონმდებლობასთან)

ვიდეოგადაღება მონაცემთა დამუშავების ერთ-ერთი ყველაზე ფართოდ გავრცელებული ფორმაა. თანამედროვე ტექნოლოგიების, მათ შორის, დრონის საჰაერო გადაღების სისტემების განვითარებამ, პერსონალურ მონაცემთა დაცვის კუთხით, არაერთი ახალი გამოწვევა წარმოშვა. დრონის ხელმისაწვდომობა და გამოყენების სიმარტივე ნებისმიერ პირს საშუალებას აძლევს, დაამუშაოს განსაკუთრებით დიდი რაოდენობით სუბიექტების პერსონალური მონაცემები, რა დროსაც, საგრძნობლად მაღალია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს მოქმედი და ახალი კანონებით გათვალისწინებული პირობების დარღვევის საფრთხე. ნაშრომი მიმოიხილავს დრონის გამოყენებით მონაცემთა დამუშავების კანონიერებისთვის დადგენილ სტანდარტებს და შესაბამის რეკომენდაციებს აწვდის მონაცემთა დამმუშავებლებს.

საკვანძო სიტყვები: *პერსონალურ მონაცემთა დაცვა, პერსონალურ მონაცემთა დამუშავება, თანამედროვე ტექნოლოგიები, ვიდეოგადაღება, დრონი.*

1. შესავალი

ტექნოლოგიების, მათ შორის, დრონების სწრაფი ტემპით განვითარების და ჭკვიანი სისტემების ინტეგრირების ფონზე, მონაცემთა შეგროვების შესაძლებლობები თითქმის შეუზღუდავ მასშტაბს აღწევს. GPS ტექნოლოგია, რომელიც ხშირად დრონების ჩაშენებულ მახასიათებლად გვევლინება, იძლევა თავად ამ დრონის (და მისი ნებისმიერი სათვალთვალო სამიზნის) მდებარეობის კონტროლისა და ჩაწერის საშუალებას.[1] გარდა ამისა, დრონი შეიძლება აღჭურვილი იყოს ხმის ჩამწერი მოწყობილობით, მარტივი, ღამის ხედვის ან/და თერმული გამოსახულების (თერმოგრაფიული) კამერებით, რომლებიც ადამიანის მდებარეობას სხეულის სითბოს საშუალებით ადგენენ. დრონზე შეიძლება დამონტაჟებული იყოს 3D სკანერები, WiFi და/ან Bluetooth მოწყობილობები,

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის სამართლის მაგისტრი, პერსონალურ მონაცემთა დაცვის სამსახურის იურიდიული დეპარტამენტის იურისტი.

[1] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

მობილური მოწყობილობების ამომცნობი სისტემები,[2] რაც მობილური ტელეფონის საშუალებით პიროვნების ადგილმდებარეობის დადგენის შესაძლებლობას იძლევა. ამგვარი სისტემების დრონების გამოყენებამ შეიძლება მნიშვნელოვანი უარყოფითი გავლენა იქონიოს პირის მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უფლებებზე.

განვითარებულ სათვალთვალო ტექნოლოგიებს შეუძლიათ, დრონის მაღალი ხარისხის აუდიოვიზუალური ჩანაწერი და შენახვის შესაძლებლობები დააკავშირონ მონაცემთა ანალიტიკურ ინსტრუმენტებთან, როგორიცაა სახის ამომცნობი პროგრამული უზრუნველყოფა, სიარულის ანალიზი და სხვა ბიომეტრიული შეფასების სისტემები, რაც ადამიანებზე მიზნობრივი დაკვირვების შესაძლებლობას იძლევა.[3] ამასთან, დრონების ზომა და მანევრირების უნარი იძლევა შორი დისტანციიდან დაკვირვების, თვალთვალისა და სამიზნეების მიყოლის შესაძლებლობას ისე, რომ მეთვალყურეობას დაქვემდებარებული პირისთვის ამის შესახებ ცნობილი არც გახდეს.[4] შესაბამისად, დრონების გამოყენებასთან დაკავშირებულ ერთ-ერთ მთავარ პრობლემად სწორედ მონაცემთა სუბიექტის ინფორმირებულობის დაბალი ხარისხი განიხილება, რაც, ერთი მხრივ, ვლინდება თავად მონაცემთა დამუშავების ფაქტის, მეორე მხრივ კი, მონაცემთა დამმუშავებლის (დრონის ოპერატორის) ვინაობის შესახებ ინფორმაციის არქონაში.[5]

პერსონალური მონაცემი არის „ნებისმიერი ინფორმაცია, რომელიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს“[6], დრონების ოპერატორები, რომლებიც აღრიცხავენ ან/და ამუშავებენ სურათებს, ვიდეოს, ხმას, ბიომეტრიულ მონაცემებს, გეოლოკაციას ან ტელესაკომუნიკაციო მონაცემებს, რომლებიც დაკავშირებულია იდენტიფიცირებულ ან იდენტიფიცირებად პირთან, განხილულ უნდა იქნენ მონაცემთა დამმუშავებლებად (გარდა იმ შემხვევებისა, როდესაც დრონი გამოიყენება მხოლოდ საოჯახო-სამეურნეო ან პირადი მიზნებისთვის[7]). ამდენად, ზემოთ დასახელებულ პირობებში დრონის გამოყენების შემთხვევაში, დრონის ოპერატორები, როგორც მონაცემთა დამმუშავებლები, ექვემდებარებიან როგორც მონაცემთა დაცვის ძირითადი რეგულაციის (GDPR), ისე პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით დადგენილ წესებს.

აღსანიშნავია, რომ ევროპული პრაქტიკის გათვალისწინებით, უშუალოდ პერსონალურ მონაცემთა დაცვის ეროვნული თუ საერთაშორისო კანონმდებლობის გარდა, დრონების გამოყენების პროცესში პერსონალურ მონაცემთა დაცვის საკითხებს შეიძლება მიემართებოდეს სხვადასხვა ტიპის სპეციალური დოკუმენტები.

---

[2] Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[3] *Tarr T., Tarr J.A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

[4] იქვე.

[5] Information Commissioner’s Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[6] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 5669-რს, 28/12/2011, მუხლი 2, ქვეპუნქტი „ა“.

[7] დრონის მხოლოდ საოჯახო-სამეურნეო ან პირადი მიზნებისთვის გამოყენების შემთხვევაში, პერსონალურ მონაცემთა დაცვის კანონმდებლობით დადგენილი ვალდებულებებისგან შეიძლება თავისუფლდებოდეს პირის მიერ უშუალოდ დრონის გამოყენების პროცესი, თუმცა ამის შედეგად მოპოვებული მონაცემების სამომავლო დამუშავების შემთხვევაში (მაგ. ფოტო/ვიდეო/აუდიო მასალის სოციალურ ქსელში გავრცელების), მონაცემთა დამუშავების მიმართ სტანდარტულად გავრცელდება კანონმდებლობით დადგენილი მოთხოვნები.

მათ შორის, საზედამხედველო ორგანოების მიერ მომზადებული სახელმძღვანელოები, სამოქალაქო ავიაციის სფეროს მარეგულირებელი შიდა აქტები და ამ სფეროს ირგვლივ შემუშავებული ევროკავშირის დოკუმენტები. წინამდებარე სტატიაში განხილულია დრონების გამოყენების პროცესში მონაცემთა დაცვის ძირითადი სტანდარტები და რეკომენდაციები, მათ შორის საკითხის მომწესრიგებელი ცალკეული დოკუმენტების სტრუქტურა, შინაარსი და მიზნები.

2. დრონის ოპერატორის/მონაცემთა დამმუშავებლის ვალდებულებები

დრონის გამოყენების პროცესში პერსონალურ მონაცემთა დაცვის საკითხთან მიმართებით, ევროპის მასშტაბით არსებითად მსგავს მიდგომებს ვხვდებით. კერძოდ, განსაკუთრებული ყურადღება მახვილდება დრონის ოპერატორის ვალდებულებებსა და მონაცემთა დაცვის სათანადო გარანტიების უზრუნველყოფის საჭიროებაზე. მათ შორის, შეიძლება გამოიყოს, გამჭვირვალობის, მონაცემთა სუბიექტის ინფორმირების, მონაცემთა უსაფრთხოების, მონაცემთა მინიმიზაციის ვალდებულებები. ასევე, ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინებისა (Data protection by design and by default) და მონაცემთა დაცვაზე ზეგავლენის შეფასების მომზადების საკითხები.

2.1. გამჭვირვალობა და მონაცემთა სუბიექტის ინფორმირების ვალდებულება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-15 მუხლი განსაზღვრავს მონაცემთა სუბიექტისათვის ინფორმაციის მიწოდების სავალდებულო წესს. აღნიშნული ვალდებულება განსაკუთრებით აქტუალურია დრონის გამოყენების შედეგად მონაცემთა დამუშავების პროცესში, ვინაიდან, ასეთ დროს, უმეტეს შემთხვევაში, მონაცემთა სუბიექტისთვის საერთოდ უცნობია ინფორმაცია მისი მონაცემების დამუშავების ფაქტისა და მონაცემთა დამმუშავებლის ვინაობის შესახებ.

ხშირ შემთხვევაში, მონაცემთა სუბიექტების დიდი რაოდენობიდან გამომდინარე, რთული, ან სულაც შეუძლებელია დრონის გადაღების არეალში მოქცეული ყველა სუბიექტის ინდივიდუალურად ინფორმირება (მაგ. სტადიონზე, ქუჩაში და ა.შ.). შესაბამისად, დრონის ოპერატორებს ევალებათ, გამონახონ „ინოვაციური“ გზები იმ პირებისთვის ინფორმაციის მისაწოდებლად, რომელთა პერსონალური მონაცემებიც დრონის გამოყენების შედეგად მუშავდება. ისეთ შემთხვევაში, როცა ამის გაკეთება განსაკუთრებით რთულია, ან მოითხოვს არაპროპორციულად დიდ ძალისხმევას, მონაცემთა დამმუშავებელი სუბიექტისთვის ინფორმაციის სხვა გზით მიწოდებას უნდა ეცადოს, რაც შეიძლება გამოიხატოს, მაგ.: სამოქალაქო ავიაციის ორგანოში დრონის ოფიციალური რეგისტრაციით, დრონის მოქმედების ტერიტორიაზე შესაბამისი ნიშნის განთავსებით, მონაცემთა დამმუშავებლის ვებსაიტზე კონფიდენციალურობის შესახებ ინფორმაციის წარმოდგენით ან კონფიდენციალურობის შეტყობინების სხვა ფორმით მიწოდებით.[8]

მნიშვნელოვანია, მონაცემთა სუბიექტისთვის მარტივად აღსაქმელი იყოს ის, თუ ვინ არის დრონის ოპერატორი/მონაცემთა დამმუშავებელი.[9] ამიტომ, დრონის

[8] Information Commissioner’s Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[9] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3

მართვაზე პასუხისმგებელი სუბიექტის იდენტიფიცირების გასაადვილებლად, მიზანშეწონილია, დრონი და მისი ოპერატორი ექცეოდნენ მონაცემთა სუბიექტის ხედვის არეალში.[10] აღქმადობის გასამარტივებლად, შესაძლებელია, დრონის ოპერატორი ატარებდეს მარტივად შესამჩნევ ტანსაცმელს, ასევე, სასურველია, იგი მზად იყოს, დაინტერესებულ პირს მიაწოდოს მოთხოვნილი ინფორმაცია QR კოდის საშუალებით, რომელიც მონაცემთა სუბიექტს გადაამისამართებს ვებსაიტის ბმულზე, სადაც წარმოდგენილი იქნება ინფორმაცია პერსონალურ მონაცემთა დაცვის პოლიტიკის შესახებ.[11] გარდა ამისა, გამჭვირვალობის პრინციპთან შესაბამისობის უზრუნველყოფის მიზნით, საჭიროა, დრონს გააჩნდეს ადეკვატური სასიგნალო სისტემა, მაგ. განათება (ციმციმა) ან ხმა, რაც მონაცემთა სუბიექტს აგრძნობინებს, რომ კონკრეტულ მომენტში ხორციელდება დრონით ჩაწერა.[12]

შეიძლება ითქვას, რომ, საჭიროა, ყოველ ცალკეულ შემთხვევაში შეფასდეს, რომელია მონაცემთა სუბიექტის ინფორმირების საუკეთესო საშუალება, იქნება ეს დრონის მოქმედების ზონაში საინფორმაციო ნიშნის/ბარათის განთავსება, სოციალურ თუ ბეჭდურ მედიაში ინფორმაციის გამოქვეყნება, საინფორმაციო ბროშურების გავრცელება, პოსტერების გამოკვრა თუ სხვა.[13] მთავარია, მონაცემთა სუბიექტს მიეწოდოს ინფორმაცია მონაცემთა დამუშავების ფაქტის, მონაცემთა დამმუშავებლის, დამუშავების მიზნისა და მონაცემთა სუბიექტის უფლებების შესახებ.

2.2. მონაცემთა მინიმიზაციის ვალდებულება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის „გ“ პუნქტის თანახმად, მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. ამასთან, მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი.

მონაცემთა მინიმიზაციის პრინციპს განსაკუთრებული მნიშვნელობა ენიჭება დრონის გამოყენებით მონაცემთა დამუშავების პროცესში. ერთი მხრივ, ცალკეულ შემთხვევებში, მონაცემთა ამგვარი დამუშავების სფეროში მოქცეულ სუბიექტთა რაოდენობა განსაკუთრებით დიდი შეიძლება იყოს, რაც მონაცემთა სუბიექტის უფლებების წინაშე არსებულ საფრთხეს უფრო მეტად ამძაფრებს. თუმცა, მეორე მხრივ, დრონის საშუალებით დამუშავებულ მონაცემთა მინიმიზაციას სხვადასხვა ტექნიკური საშუალება შედარებით მარტივად მისაღწევს ხდის.

ადამიანის პირადი ცხოვრებისა და მონაცემთა დაცვის უფლებებში ჩარევის მინიმალიზების მიღწევა შესაძლებელია შემდეგი საკითხების/მოქმედებების წინასწარ დაგეგმვითა და გათვალისწინებით: 1. ფრენის კონკრეტული მარშრუტი, 2.

Categories, Protecting people’s privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 22, 32, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[10] The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

[11] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[12] იქვე, 5.

[13] Spanish Data Protection Agency, Drones and Data Protection, 2019, 4, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

დრონის შესაბამისი სახეობა და მისი აღჭურვილობა, 3. შეგროვებული მონაცემების მართვა.[14]

დრონში ჩაშენებული მონაცემთა შეგროვებისა და შენახვის სისტემები შეიძლება აეწყოს იმგვარად (by default), რომ თავიდან იქნეს აცილებული არასაჭირო ოდენობისა თუ შინაარსის მონაცემების შეგროვება და შემდგომი დამუშავება, რაც შეიძლება მიღწეულ იქნეს, მაგალითად, მონაცემთა დეპერსონალიზაციის გზით (მაგ., გამოსახულების ჩამწერი კამერა ავტომატურად აფიქსირებდეს და აბუნდოვანებდეს (blur) ტერიტორიაზე მოძრავი ადამიანების გამოსახულებას.[15] მონაცემთა არამიზნობრივი (გადაჭარბებული) დამუშავების თავიდან ასარიდებლად, დრონის ოპერატორმა უნდა გაითვალისწინოს მონაცემთა მინიმიზაციის პრინციპი, ანონიმიზაციისა და ფსევდონიმიზაციის შესაძლებლობა.[16]

მონაცემთა მინიმიზაციის პრინციპთან შესაბამისობისთვის, დრონზე დამონტაჟებული მონაცემთა შეგროვების სისტემები აღჭურვილი უნდა იყოს საჭიროებისამებრ ჩართვა-გამორთვის ფუნქციით, ამასთან, კადრში მოქცეული ვიზუალური კუთხე შემოფარგლული უნდა იყოს მონაცემთა დამუშავების კონკრეტული მიზნით (მაგ. თუ დრონის გამოყენების მიზანი დაზიანებული სახურავის კონკრეტული მონაკვეთის შემოწმებაა, არ იარსებებს 360 გრადუსიანი კუთხით გადაღების საჭიროება).[17]

მონაცემთა მინიმიზაციისთვის, მიზანშეწონილია, დრონის ოპერატორმა მაქსიმალურად შეზღუდოს კადრში მოქცეული ადამიანებისა და იმ ნივთების რაოდენობა, რომელიც მონაცემთა სუბიექტებს მარტივად იდენტიფიცირებადს გახდის (მაგ., ავტომობილის სანომრე ნიშანი). აღნიშნული მიზანი შეიძლება მიღწეულ იქნეს, ფრენების დღის იმ მონაკვეთში განხორციელებით, როდესაც კონკრეტულ არეალში ხალხის ყველაზე დაბალი კონცენტრაცია ფიქსირდება. ასევე, უმჯობესია, ვიდეო/აუდიო ჩაწერა ან/და ფოტოგადაღება ხორციელდებოდეს არა მთლიანი ფრენის განმავლობაში, არამედ კონკრეტულ მომენტებში, როდესაც ეს საჭიროებითაა განპირობებული.[18]

იმგვარი ფოტო ან ვიდეოგადაღების თავიდან ასარიდებლად, რომელიც უხეშად არღვევს ადამიანების პირადი ცხოვრების ხელშეუხებლობას, დრონის ოპერატორი უნდა ფლობდეს ინფორმაციას მის მიერ გამოყენებული დრონის ტექნიკური შესაძლებლობების შესახებ. კერძოდ, რა ხარისხით იწერს იგი გამოსახულებას, რა მასშტაბით შეუძლია კადრის მიახლოება (ე.წ. "zoom in"), არის თუ არა ტექნიკურად შესაძლებელი ფრენის მომენტში გადაღების დაწყება და შეწყვეტა (კონტროლი).[19] ამ ინფორმაციის უკეთ აღსაქმელად და დრონის შესაძლებლობების გასაცნობად, მიზანშეწონილია, საჯარო სივრცეში ფრენამდე, დრონის ოპერატორმა საცდელი

[14] *Tarr T., Tarr J.A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.

[15] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5. <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[16] პერსონალურ მონაცემთა დაცვის სამსახური, მსოფლიო პრაქტიკა, ივნისი/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[17] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[18] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[19] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 21, 32, < https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

ფრენები განახორციელოს კონტროლირებად სიტუაციაში.[20] ამასთან, აუცილებელია, წაიშალოს ყველაფერი, რაც სცილდება მონაცემთა დამუშავების მიზნებს და რისი შენახვის არანაირი საჭიროება არ არსებობს.[21]

2.3. უსაფრთხოების ვალდებულება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლი განსაზღვრავს მონაცემთა უსაფრთხოების ვალდებულებას. კერძოდ, „მონაცემთა დამმუშავებელი ვალდებულია მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან.“ დრონის გამოყენებით მონაცემთა დამუშავების დროს უსაფრთხოების არაერთი გამოწვევა შეიძლება წარმოიშვას. შესაბამისად, დრონის ოპერატორი ვალდებულია, მიიღოს უსაფრთხოების სათანადო ზომები.

უპირველეს ყოვლისა, მნიშვნელოვანია, დადგინდეს, ხომ არ არის დრონი დაკავშირებული რაიმე სხვა სისტემებთან. ასეთ შემთხვევაში, საჭიროა, მიღებულ იქნეს შესაბამისი უსაფრთხოების ზომები. გარდა ამისა, დრონის ოპერატორი უნდა დარწმუნდეს, რომ მის მიერ შეგროვებული ყველა მონაცემი უსაფრთხოდაა შენახული, რაც შეიძლება უზრუნველყოფილ იქნეს შენახული ინფორმაციის დაშიფვრის ან მასზე წვდომის შეზღუდვის სხვა მეთოდის გამოყენებით. ეს განსაკუთრებით მნიშვნელოვანია მაშინ, როცა დრონის გაფრენა ხორციელდება შორ მანძილზე, პილოტის ხედვის არეალს მიღმა, ან როდესაც ხდება დრონის ჩამოვარდნა, რაც წარმოშობს მოწყობილობისა და მასში არსებული მონაცემების დაკარგვის ან მოპარვის მომეტებულ საფრთხეს.[22]

დრონის გამოყენებით მონაცემთა დამუშავების უსაფრთხოების უზრუნველსაყოფად საჭირო ტექნიკური და ორგანიზაციული ზომების მიღება სწორედ მონაცემთა დამმუშავებლის პასუხისმგებლობაა. შესაბამისად, დამმუშავებელმა განსაკუთრებული ყურადღება უნდა მიაქციოს იმ ტექნიკურ მახასიათებლებს, რომლითაც აღჭურვილია დრონი და რომელიც მონაცემთა შეგროვებისა და შენახვის პროცესში უსაფრთხოების უზრუნველყოფას ისახავს მიზნად. მათ შორის, დრონის ოპერატორმა უნდა შეამოწმოს, დრონის საშუალებით გადაღებული ფოტო/ვიდეომასალა ინახება თავად მოწყობილობაზე, პორტატიული მეხსიერების ბარათზე თუ ე.წ. ღრუბლოვან სისტემაზე (cloud system). საფრთხის თავიდან ასაცილებლად, მონაცემთა დამმუშავებელმა უნდა მიიღოს შესაბამისი

[20] Aerialworx, The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

[21] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 25, 33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[22] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36-37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].

ზომები, მაგ. დაშიფროს მონაცემები, ვიდრე ისინი ქლაუდ სისტემაზე გადაიგზავნება.[23]

2.4. "Data Protection by Default and by Design"

„პერსონალურ მონაცემთა დაცვის შესახებ" საქართველოს ახალი კანონის[24] 26-ე მუხლი ამკვიდრებს მონაცემთა მეტად დაფარვის პრიორიტეტს, როგორც ალტერნატიული მიდგომის არჩევამდე ავტომატურად გამოყენებულ საწყის მეთოდს ახალი პროდუქტის ან მომსახურების შექმნისას (Data Protection by default and by design), რაც GDPR-ის 25-ე მუხლი გამოძახილად უნდა შეფასდეს.

ამ მუხლის თანახმად, ახალი ტექნოლოგიების, განხორციელების ხარჯების, დამუშავების ხასიათის, მასშტაბის, კონტექსტისა და მიზნების, აგრეთვე მონაცემთა სუბიექტის უფლებებისა და თავისუფლებებისთვის მოსალოდნელი რისკებისა და მონაცემთა დამუშავების პრინციპების გათვალისწინებით, დამუშავებისთვის პასუხისმგებელმა პირმა როგორც დამუშავების საშუალებების განსაზღვრის, ისე უშუალოდ დამუშავების პროცესში უნდა მიიღოს სათანადო ტექნიკური და ორგანიზაციული ზომები (მათ შორის, ფსევდონიმიზაცია ან /და სხვა). ამ ზომების მიღება უნდა უზრუნველყოფდეს მონაცემთა დამუშავების პრინციპების ეფექტიან იმპლემენტაციას და მონაცემთა დამუშავების პროცესში დაცვის მექანიზმების ინტეგრირებას მონაცემთა სუბიექტის უფლებების დასაცავად. ამასთან, დამუშავებისთვის პასუხისმგებელმა პირმა მონაცემთა რაოდენობის, მონაცემთა დამუშავების მასშტაბის, შენახვის ვადებისა და მონაცემებზე წვდომის განსაზღვრისას უნდა უზრუნველყოს ისეთი ტექნიკური და ორგანიზაციული ზომების მიღება, რომ ავტომატურად დამუშავდეს მონაცემების მხოლოდ ის მოცულობა, რომელიც აუცილებელია დამუშავების კონკრეტული მიზნისთვის. ეს ზომები იმგვარად უნდა გამოიყენებოდეს, რომ ნებადართული ალტერნატიული მიდგომის არჩევამდე პირთა განუსაზღვრელი წრისთვის ავტომატურად უზრუნველყოფილი იქნება მონაცემთა მხოლოდ მინიმალურ მოცულობაზე წვდომა. ამდენად, ერთი მხრივ, დრონების მწარმოებელმა წარმოების პროცესში უნდა გაითვალისწინოს ის მექანიზმები, რომელიც დრონის მიერ შეგროვებული მონაცემების მინიმალიზებას უზრუნველყოფს. დრონების წარმოების პროცესში, სუბიექტთა პირადი ცხოვრების ხელშეუხებლობის დასაცავად, მნიშვნელოვანია, მწარმოებელმა საქმიანობა წარმართოს ადამიანის უფლებების პატივისცემის იდეაზე დაყრდნობით.[25]

მეორე მხრივ, მონაცემთა დაცვის საკითხები მხედველობაში უნდა მიიღოს დრონის ოპერატორმა, კონკრეტული დავალებისთვის სათანადო დრონის შერჩევის, ფრენის მარშრუტის დაგეგმვისა და მონაცემთა დამუშავების პროცედურების შემუშავების დროს.[26]

დრონის ოპერატორის, როგორც მონაცემთა დამმუშავებლის ვალდებულებაა, დარწმუნდეს, რომ დრონის სისტემა, რომლის გამოყენებასაც იგი აპირებს, შესაბამისობაშია კანონის 26-ე მუხლით გათვალისწინებულ მონაცემთა მეტად დაფარვის პრიორიტეტთან (მაგ., მონაცემთა ჩაწერისა და შენახვის ტექნიკური

[23] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[24] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ", 3144-XIმს-Xმპ, 14/06/2023.

[25] Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.

[26] Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news/5-ways-in-which-the-gdpr-will-impact-the-drone-sector> [04.09.2023].

შესაძლებლობა დრონს ჰქონდეს მხოლოდ გარკვეულ სიმაღლეზე ასვლის შემთხვევაში[27], ანდაც, ფოტოს გარჩევადობის/რეზოლუციის შემცირება შესაძლებელი იყოს იმ მინიმუმამდე, რომელიც საკმარისი იქნება მონაცემთა დამუშავების მიზნის მისაღწევად[28] და სხვა).

2.5. მონაცემთა დაცვაზე ზეგავლენის შეფასება

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონის 31-ე მუხლის პირველი პუნქტის თანახმად, თუ მონაცემთა დამუშავებისას ახალი ტექნოლოგიების, მონაცემთა კატეგორიის, მოცულობის, მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, მაღალი ალბათობით იქმნება ადამიანის ძირითადი უფლებებისა და თავისუფლებების შელახვის საფრთხე, დამუშავებისთვის პასუხისმგებელი პირი ვალდებულია წინასწარ განახორციელოს მონაცემთა დაცვაზე ზეგავლენის შეფასება. ზეგავლენის შეფასება არის არაერთჯერადი ხასიათის, მიმდინარე პროცესი, განსაკუთრებით მაშინ, როდესაც მონაცემთა დამუშავებისკენ მიმართული ღონისძიება დინამიკურია და ხასიათდება პერიოდული ცვლილებით.[29]

წინა თავებში განვითარებული მსჯელობიდან გამომდინარე, აშკარაა, რომ მთელ რიგ შემთხვევებში, დრონის გამოყენებით მონაცემთა დამუშავებამ შეიძლება მიაღწიოს ზემოაღნიშნული მუხლით დადგენილ ფარგლებს და შესაბამისად, მონაცემთა დამმუშავებლის მიმართ წარმოშვას მონაცემთა დაცვაზე ზეგავლენის შეფასების ვალდებულება.

აღსანიშნავია, რომ ზეგავლენის შეფასების უზრუნველყოფის ვალდებულება ეკისრება მონაცემთა დამმუშავებელს. მართალია, უშუალოდ შეფასება შეიძლება განხორციელდეს რომელიმე სხვა პირის მიერ, თუმცა, ამის მიუხედავად, აღნიშნულ ღონისძიებაზე პასუხისმგებელ პირად მაინც მონაცემთა დამმუშავებელი მიიჩნევა.[30]

დრონის გამოყენებასთან დაკავშირებით პერსონალურ მონაცემთა დაცვაზე ზეგავლენის შეფასების პროცესში ყურადღება უნდა მიექცეს შემდეგ საკითხებს: დრონის მოქმედების არეალის განსაზღვრა; დამუშავებულ მონაცემთა მოძრაობა (რაც მოიაზრებს დამუშავების პროცესის სისტემურ აღწერას); მონაცემთა დამუშავების აუცილებლობისა და პროპორციულობის განსაზღვრა; საფრთხეების იდენტიფიცირება და ზეგავლენის შეფასება; გამოვლენილი საფრთხეების თავიდან აცილების/მოგვარების გზების იდენტიფიცირება.[31] მნიშვნელოვანია, რომ დრონების აწყობისა და ექსპლუატაციის პროცესში, დრონების ოპერატორებმა გაითვალისწინონ რისკზე დაფუძნებული (risk-based) და რისკის მართვის (risk-management) სტრატეგიები. კერძოდ, დრონის გამოყენებამდე, მათ უნდა გაანალიზონ პერსონალურ მონაცემთა დაცვის წინაშე არსებული პოტენციური საფრთხეები, რამაც

[27] Information Commissioner’s Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].

[28] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[29] 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, 2017, 14.

[30] იქვე.

[31] Data Protection Impact Assessment Template, Resource for Ddrone Operators and Pilots, 2019, 3.

უნდა უზრუნველყოს სამართლიანი ბალანსის მიღწევა მონაცემთა სუბიექტისა და დრონის ოპერატორის ინტერესებს შორის.[32] ამასთან, შეფასების პროცესში მხედველობაში უნდა იქნეს მიღებული დაგეგმილი ოპერაციის მიზანი, გამოსაყენებელი დრონის ტიპი და მასზე დამონტაჟებული ტექნოლოგიები.[33]

რეკომენდებულია, ზეგავლენის შეფასების პროცესში ჩართულ იქნენ ექსპერტები და დაინტერესებული მხარეები. დამატებით, შეფასების სწორად წარმართვისთვის, მნიშვნელოვანია, პროცესში ჩაერთოს პერსონალურ მონაცემთა დაცვის ოფიცერი (ასეთის არსებობის შემთხვევაში).[34] გარდა ამისა, როცა ეს შესაძლებელია, სასურველია, ზეგავლენის შეფასების მომზადების პროცესში მონაცემთა დამმუშავებელმა კონსულტაცია გაიაროს მონაცემთა სუბიექტებთან ან მათ წარმომადგენლებთან. მაგალითად, დასახლებულ ადგილას დრონის გამოყენების შემთხვევაში, ამგვარი კომუნიკაცია შესაძლოა შედგეს ადგილობრივ მაცხოვრებლებსა და ბიზნესებთან, სამეზობლო ამხანაგობებთან, მიმდებარე ტერიტორიაზე არსებულ საგანმანათლებლო, სამედიცინო, პოლიტიკურ თუ რელიგიურ დაწესებულებებთან.[35]

მონაცემთა დაცვაზე ზეგავლენის შეფასება აღქმულ უნდა იქნას როგორც ინსტრუმენტი, რომელიც მონაცემთა დამმუშავებელს მონაცემთა დამუშავების შესახებ გადაწყვეტილების მიღებაში დაეხმარება[36] და საშუალებას მისცემს, სწორად გადაწყვიტოს, კონკრეტული მიზნის მისაღწევად, დრონის გამოყენება ნამდვილად არის თუ არა მონაცემთა დამუშავებისთვის საჭირო და ადეკვატური საშუალება.[37]

3. ევროპული მიდგომების ანალიზი

ევროკავშირის მასშტაბით, დრონების გამოყენებით პერსონალურ მონაცემთა დაცვის საკითხზე სტანდარტულად ვრცელდება როგორც GDPR-ით, ისე პერსონალურ მონაცემთა დაცვის ეროვნული კანონმდებლობით დადგენილი წესები. თუმცა უშუალოდ ზემოაღნიშნული ნორმატიული აქტების გარდა, დრონების გამოყენების პროცესში პერსონალურ მონაცემთა დაცვის საკითხებს შეიძლება მიემართებოდეს სხვადასხვა ტიპის სპეციალური დოკუმენტებიც. მათ შორის, საზედამხედველო ორგანოების მიერ მომზადებული სახელმძღვანელოები, სამოქალაქო ავიაციის სფეროს მარეგულირებელი შიდა აქტები და ამ სფეროს ირგვლივ შემუშავებული ევროკავშირის დოკუმენტები.

[32] *Tarr T., Tarr J.A., Thompson M., Wilkinson D.*, Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.
[33] Spanish Data Protection Agency, Drones and Data Protection, 2019, 5, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
[34] 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, 2017, 15.
[35] Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 5.
[36] 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, 2017, 14.
[37] Information Commissioner's Office (ICO), UK, Additional considerations for technologies other than CCTV, October 2022, 36.

3.1. ევროპის კავშირი - რეგულაცია 2019/947 უპილოტო საჰაერო ხომალდების გამოყენების წესებისა და პროცედურების შესახებ

ევროკავშირის ტერიტორიაზე მოქმედებს რეგულაცია უპილოტო საჰაერო ხომალდების გამოყენების წესებისა და პროცედურების შესახებ, რომელიც ადგენს დეტალურ პირობებს უპილოტო საფრენი სისტემების ექსპლუატაციისთვის, მათ შორის, შესაბამისი პერსონალის, დისტანციური პილოტებისა და ამ ოპერაციებში ჩართული ორგანიზაციებისთვის.[38]

რეგულაციის ცალკეული მუხლები მიემართება უპილოტო საჰაერო სისტემების გამოყენების პროცესში პერსონალურ მონაცემთა დაცვის საკითხებს. მაგალითად, მე-12 მუხლის მე-2 პუნქტის თანახმად, იმისთვის, რომ პირმა დრონის ოპერირების ავტორიზაცია მიიღოს, მან წარმატებით უნდა გაიაროს შეფასება, რომლის ერთ-ერთ კომპონენტადაც მოაზრებულია დრონის ოპერატორის განაცხადი, რომ მის მიერ დაგეგმილი ოპერაცია შესაბამისობაშია ევროკავშირის კანონმდებლობასთან, მათ შორის, პერსონალური მონაცემთა დაცვის წესებთან. გარდა ამისა, რეგულაცია ითვალისწინებს დრონის ოპერატორის რეგისტრაციის წესს, იმ შემთხვევაში, როცა მის მიერ მართული დრონი აღჭურვილია პერსონალურ მონაცემთა დამუშავების შესაძლებლობის მქონე სისტემით.[39]

დამატებით, უპილოტო საფრენი აპარატის ოპერატორის ვალდებულებები მოცემულია რეგულაციის დანართშიც, რომლის თანახმად, ოპერატორი ვალდებულია, მიიღოს სათანადო ზომები დაგეგმილი ოპერაციის GDPR-თან თავსებადობის უზრუნველსაყოფად. კერძოდ, ოპერატორმა უნდა მოამზადოს მონაცემთა დაცვაზე ზეგავლენის შეფასება, როცა ამგვარი მოთხოვნა მომდინარეობს მონაცემთა დაცვაზე პასუხისმგებელი ეროვნული ინსტიტუტისგან.

3.2. გაერთიანებული სამეფო - დრონისა და მოდელური საჰაერო ხომალდების კოდექსი

პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან ერთად, გაერთიანებულ სამეფოში მოქმედებს სამოქალაქო ავიაციის სახელმწიფო ორგანოს მიერ მიღებული „დრონისა და მოდელური საჰაერო ხომალდების კოდექსი“[40], რომლის ერთ-ერთი თავი ადამიანთა პირადი ცხოვრების ხელშეუხებლობის უფლების დაცვის საკითხებს ეხება.

პერსონალურ მონაცემთა დაცვის საჭიროებისკენ მიმართული ზოგადი ხასიათის მოწოდებებთან ერთად, კოდექსი გაწერს დრონის ოპერატორის კონკრეტულ ვალდებულებებსაც. მაგალითად, იმგვარი ფოტო ან ვიდეოგადაღების თავიდან ასარიდებლად, რომელიც უხეშად არღვევს ადამიანების პირადი ცხოვრების ხელშეუხებლობას, დრონის ოპერატორი უნდა ფლობდეს ინფორმაციას მის მიერ გამოყენებული დრონის ტექნიკური შესაძლებლობების შესახებ. კერძოდ, რა

[38] EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 24 May, 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947> [04.09.2023].

[39] იქვე, მუხლი 14.5 (a-ii.).

[40] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Airplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

ხარისხით იწერს იგი გამოსახულებას, რა მასშტაბით შეუძლია კადრის მიახლოება (ე.წ. "zoom in"), არის თუ არა ტექნიკურად შესაძლებელი ფრენის მომენტში გადაღების დაწყება და შეწყვეტა (კონტროლი). ასევე, კოდექსი მოუწოდებს დრონის ოპერატორებს, გადაღების პროცესში, განთავსდნენ მონაცემთა სუბიექტებისთვის თვალსაჩინო ადგილას, რაც მათთვის მარტივად გასაგებს გახდის, ვინ არის დრონის გამოყენებაზე პასუხისმგებელი პირი. გარდა ამისა, კოდექსი მოუწოდებს მონაცემთა დამმუშავებლებს, ფოტოს გადაღების ან ვიდეოს ჩაწერის დაწყებამდე გააფრთხილონ მონაცემთა სუბიექტები, უზრუნველყონ მოპოვებული ფოტოებისა და ვიდეოების უსაფრთხოება და თავიდან აირიდონ ფოტო და ვიდეომასალის გასაჯაროება.

3.3. ირლანდია - სახელმძღვანელო დრონების გამოყენებით მონაცემთა დამუშავების შესახებ

2022 წლის მაისში, ირლანდიის მონაცემთა დაცვის კომისიამ გამოაქვეყნა სახელმძღვანელო დრონების გამოყენებით მონაცემთა დამუშავების შესახებ.[41] „სახელმძღვანელოში განმარტებულია, რომ დრონები წარმოადგენენ უპილოტო საფრენი აპარატების იმ ფართო კატეგორიას, რომლებიც დისტანციურად იმართებიან და აღჭურვილი არიან სურათების, ვიდეოების, ხმის ან/და სხვა ინფორმაციის შეგროვების ტექნოლოგიით (მონაცემთა შეგროვების სისტემა), რასაც შემდგომ ჭკვიან მოწყობილობებს გადასცემენ (მაგალითად, ღრუბლოვან საცავებს ე. წ. "cloud storage"-ს). დრონებს შეუძლიათ, გადაიქცნენ მობილურ სათვალთვალო სისტემად და დაამუშაონ გამვლელთა (მონაცემთა სუბიექტების) პერსონალური მონაცემები."[42]

აღნიშნულიდან გამომდინარე, ირლანდიის საზედამხედველო ორგანო დრონის ოპერატორებს მონაცემთა დამმუშავებლებად განიხილავს (გარდა იმ შემხვევებისა, როდესაც დრონი გამოიყენება მხოლოდ საოჯახო-სამეურნეო ან პირადი მიზნებისთვის) და მათ გარკვეულ ვალდებულებებს აკისრებს, რათა თავიდან აირიდონ მონაცემთა სუბიექტის უფლებების შეუქცევადი დარღვევა. ამასთან, აღსანიშნავია, რომ „სახელმძღვანელო არ ვრცელდება დრონების სამართალდამცავი მიზნებისთვის გამოყენებაზე".[43]

სახელმძღვანელოს თანახმად, „როდესაც მონაცემთა დამმუშავებელი იყენებს დრონს და აღნიშნულს არ აქვს ცალსახად პირადი ან საოჯახო-სამეურნეო ხასიათი, მას ეკისრება ვალდებულება დაასაბუთოს, რომ:

- მონაცემთა დამუშავება მონაცემთა სუბიექტის ინტერესში შედიოდა;
- დრონის გამოყენება საჭიროა დასახული ლეგიტიმური მიზნის მისაღწევად;
- რომ მას არ აქვს არაპროპორციული ზეგავლენა მონაცემთა სუბიექტზე.

გარდა ამისა, აღნიშნულია, რომ საზედამხედველო ორგანომ მონაცემთა დამმუშავებლებს, რიგი გარემოებებიდან გამომდინარე, შეიძლება ვალდებულებად განუსაზღვროს მონაცემთა დამუშავების ზეგავლენის შეფასება და პირადი ცხოვრების ხელშეუხებლობის პოლიტიკის დოკუმენტის შემუშავება. ამასთან, მონაცემთა დამმუშავებლებმა უნდა გაითვალისწინონ:

---

[41] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[42] პერსონალურ მონაცემთა დაცვის სამსახური, მსოფლიო პრაქტიკა, ივნისი/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[43] იქვე, 12.

- მათი ქმედებები შესაბამისობაში უნდა იყოს დრონების მართვის მარეგულირებელ კანონმდებლობასთან (მაგალითად, კერძო საკუთრებაში უნებართვო შეღწევის შესახებ);
- მათ უნდა განსაზღვრონ მონაცემთა დამუშავების თავდაპირველი და შემდგომი მიზნები;
- მონაცემთა სუბიექტის მხრიდან ინფორმაციის მოთხოვნის შემთხვევაში, მიაწოდონ მას ამომწურავი ინფორმაცია მონაცემთა დამუშავების მიზნების, კანონიერებისა და სუბიექტის უფლებების შესახებ;
- მონაცემთა დამუშავება უნდა ემყარებოდეს კანონიერ საფუძველს;
- მონაცემთა დამუშავების პროცესში მათ უნდა გაითვალისწინონ მონაცემთა მინიმიზაციის პრინციპი, დეპერსონალიზებისა და ფსევდონიმიზაციის შესაძლებლობა მონაცემთა არამიზნობრივი (გადაჭარბებული) დამუშავების ასარიდებლად.“[44]

„საოჯახო-სამეურნეო მიზნებისთვის დრონის გამოყენების შემთხვევაში, საზედამხედველო ორგანო მოუწოდებს დრონის ოპერატორებს, მონაცემთა დამუშავების ფარგლების განსაზღვრისას, იხელმძღვანელონ „გონივრულობის პრინციპით“, მოერიდონ სახეებისა და სხვისი პირადი სივრცის გადაღებას.“[45]

3.4. ესპანეთი - სახელმძღვანელო „დრონები და მონაცემთა დაცვა“

2019 წლის მაისში ესპანეთის მონაცემთა დაცვის სააგენტომ გამოაქვეყნა სახელმძღვანელო - „დრონები და მონაცემთა დაცვა“, რომელიც დრონის ოპერატორებისთვის პერსონალურ მონაცემთა დაცვის საკითხებზე დამატებითი განმარტებებისა და რეკომენდაციების მიცემას ისახავს მიზნად.[46]

დოკუმენტში მითითებულია, რომ მონაცემთა დაცვის დებულებებთან შესაბამისობის ზოგად ვალდებულებას განსაზღვრავს №1036/2017 სამეფო განკარგულების 26-ე მუხლი, რომელიც აწესრიგებს დისტანციურად მართული საჰაერო ხომალდების სამოქალაქო გამოყენების საკითხებს. ამასთან, გასათვალისწინებელია, რომ საჰაერო სივრცის მომწესრიგებელ კანონმდებლობასთან ერთად, დრონების საშუალებით მონაცემთა დამუშავებაზე სრულად ვრცელდება GDPR-ით დადგენილი პირობები, მიუხედავად იმისა, დრონის გამოყენება ხდება პროფესიონალური თუ რეკრეაციული მიზნით.

სახელმძღვანელო მიჯნავს დრონის გამოყენების შედეგად მონაცემთა დამუშავების ორ კატეგორიას. ერთი მხრივ, შემთხვევები, როდესაც დრონის გამოყენების მიზანი თავისთავად მოიცავს მონაცემთა დამუშავების საჭიროებას (მაგ. ვიდეო თვალთვალი). მეორე მხრივ, შემთხვევები, როდესაც დრონის გამოყენების მიზანი არ გულისხმობს მონაცემთა დამუშავების აუცილებელ საჭიროებას (მაგ. ინფრასტრუქტურის ინსპექტირება, ტოპოგრაფიული აზომვები და სხვ.), თუმცა, გარემოებების გათვალისწინებით, შეიძლება გავლენას ახდენდეს ადამიანის მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის უფლებებზე.

სახელმძღვანელო დრონის ოპერატორების მიმართ გასცემს კონკრეტულ რეკომენდაციებს, მათ შორის:

[44] იქვე.
[45] იქვე.
[46] Spanish Data Protection Agency, Drones and Data Protection, 2019, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

- მონაცემთა მინიმიზაციისთვის, დრონის ოპერატორმა მაქსიმალურად უნდა შეზღუდოს კადრში მოქცეული ადამიანებისა და იმ ნივთების რაოდენობა, რომელიც მონაცემთა სუბიექტებს მარტივად იდენტიფიცირებადს გახდის (მაგალითად, ავტომობილის სანომრე ნიშანი). აღნიშნული მიზანი შეიძლება მიღწეულ იქნეს, მაგალითად, ფრენების დღის იმ მონაკვეთში განხორციელებით, როდესაც კონკრეტულ არეალში ხალხის ყველაზე დაბალი კონცენტრაცია ფიქსირდება;
- ასევე, მონაცემთა მინიმიზაციისთვის, ვიდეო/აუდიო ჩაწერა ან/და ფოტოგადაღება უნდა განხორციელდეს არა მთლიანი ფრენის განმავლობაში, არამედ კონკრეტულ მომენტებში, როდესაც ეს საჭიროებითაა განპირობებული;
- ოპერატორებმა უნდა გამოიყენონ დრონში ინტეგრირებული/„ჩაშენებული“ მონაცემთა დაცვის საშუალებები, როგორიცაა, მაგალითად, ფოტოს გარჩევადობის/რეზოლუციის იმ მინიმუმამდე დაყვანა, რომელიც საკმარისი იქნება მონაცემთა დამუშავების მიზნის მისაღწევად და რომელიც ნაკლებად იდენტიფიცირებადს გახდის მონაცემთა სუბიექტს;
- ისეთ ტერიტორიაზე, სადაც ხალხის ყოფნა გარდაუვალია, ფოტოს გადაღება უნდა მოხდეს იმგვარად, რომ შეუძლებელი იყოს მასზე აღბეჭდილ პირთა იდენტიფიცირება. მაგალითად, ეს შეიძლება მიღწეულ იქნეს საკმარისი სიმაღლიდან ფოტოს გადაღებით;
- აღკვეთილ უნდა იქნეს მონაცემთა სუბიექტებთან დაკავშირებული არასაჭირო ინფორმაციის შენახვა. მაგალითად, თუ ფოტოგადაღების მიზანია სანაპირო ზოლის ტოპოგრაფიული კვლევა, არ იარსებებს იმ ფოტოების შენახვის საჭიროება, რომელზეც სანაპიროზე დასასვენებლად გამოსული ხალხია აღბეჭდილი.

სახელმძღვანელო გასცემს შემდეგ დამატებით რეკომენდაციებს:

- დრონზე დასამონტაჟებლად, შერჩეულ უნდა იქნეს დასახულ მიზანთან ყველაზე უფრო მეტად შესაფერისი ტექნოლოგიები;
- დანერგილ უნდა იქნეს მექანიზმები, რომლითაც უზრუნველყოფილი იქნება მონაცემთა სუბიექტთა სათანადო ინფორმირება;
- მონაცემთა სუბიექტთა უფლებების დაცვისთვის საჭირო უსაფრთხოების გარანტიების შექმნის მიზნით, მიღებულ უნდა იქნეს შესაბამისი ტექნიკური და ორგანიზაციული ზომები. განსაკუთრებით მნიშვნელოვანია, თავიდან იქნეს აცილებული შეგროვებული მონაცემების გადატანის პროცესში მონაცემთა არაავტორიზებული დამუშავების საფრთხე;
- მონაცემთა შეგროვებიდან რაც შეიძლება მალე უნდა მოხდეს არასაჭირო პერსონალური ინფორმაციის წაშლა ან დეპერსონალიზაცია;
- ოპერატორი უნდა დარწმუნდეს, რომ, როგორც დრონი, ისე თავად ოპერატორი, მონაცემთა სუბიექტისთვის რაც შეიძლება ხილვადი და იდენტიფიცირებადი არიან.

სახელმძღვანელოში ჩამოთვლილია ის კონკრეტული ნაბიჯები, რომელიც მონაცემთა დამმუშავებელმა დრონის გამოყენებამდე უნდა გადადგას. მათ შორის:

- ოპერატორმა უნდა შეამოწმოს, რომ ეროვნული კანონმდებლობა უშვებს დრონის გამოყენებას და საჭიროების შემთხვევაში, გაიაროს ავტორიზაცია შესაბამის საავიაციო ორგანოში. იმ შემთხვევაში, თუ დრონის გამოყენება

მოხდება კანონმდებლობის დარღვევით, ჩაითვლება რომ ამგვარი ფრენის პერიოდში მონაცემთა დამუშავება წინააღმდეგობაში მოდის GDPR-ით გათვალისწინებულ კანონიერების პრინციპთან;

- ისეთი მოქმედების განხორციელებამდე, რომლის დაწყებამდე ნათელია მონაცემთა დამუშავების გარდაუვალობა, მნიშვნელოვანია, გაანალიზდეს მონაცემთა დაცვაზე ზეგავლენის შეფასების საჭიროება. ამგვარი საჭიროება უნდა განისაზღვროს მონაცემთა დამუშავების მიზნის, დრონის ტიპისა და გამოყენებული ტექნოლოგიების გათვალისწინებით.
- თუ ფოტოების გადაღება ხდება პირადი გამოყენებისთვის, მნიშვნელოვანია, არ მოხდეს მათი ინტერნეტში გასაჯაროება პირთა განუსაზღვრელი წრისთვის ხელმისაწვდომი ფორმით (როდესაც ასეთი ფოტომასალა პირთა იდენტიფიცირების საშუალებას იძლევა);
- საჭიროა, წინასწარ შეფასდეს ფრენის ფიზიკური უსაფრთხოებისა და საავიაციო კანონმდებლობასთან შესაბამისობის საკითხები.

4. დასკვნა

დრონების საშუალებით მონაცემთა დამუშავების ირგვლივ განვითარებული ევროპული სტანდარტები, არსებითად, ერთმანეთის მსგავსია. განსაკუთრებული ყურადღება ეთმობა მონაცემთა დამუშავების პროცესში გამჭვირვალობის, მონაცემთა სუბიექტის ინფორმირების, მონაცემთა უსაფრთხოებისა და მონაცემთა მინიმიზაციის ვალდებულებებს. ასევე, ახალი პროდუქტის ან მომსახურების შექმნისას მონაცემთა დაცვის სტანდარტების გათვალისწინებისა (Data protection by design and by default) და მონაცემთა დაცვაზე ზეგავლენის შეფასების მომზადების საკითხებს. ამასთან, აღსანიშნავია, რომ „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს ახალი კანონით, რომლის ძირითადი ნაწილის ამოქმედების თარიღად განსაზღვრულია 2024 წლის პირველი მარტი,[47] გათვალისწინებული მთელი რიგი ვალდებულებები, მათ შორის, მიემართება დრონის ოპერატორებს, როგორც მონაცემთა დამმუშავებლებს. ამდენად, მნიშვნელოვანია, დრონების გამოყენების პროცესში პერსონალურ მონაცემთა დამუშავება განხორციელდეს კანონისა და საერთაშორისო სტანდარტების შესაბამისად. ყოველივე ეს მკვეთრად შეამცირებს მონაცემთა სუბიექტების უფლებების დარღვევის იმ მომეტებულ საფრთხეს, რომელიც დრონის გამოყენების შედეგად დამუშავებული მონაცემების დიდი მასშტაბითა და განსაკუთრებული ხასიათითაა განპირობებული.

[47] საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023, მუხლი 90.

ბიბლიოგრაფია:

1. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 5669-რს, 28/12/2011.
2. საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“, 3144-XIმს-Xმპ, 14/06/2023.
3. პერსონალურ მონაცემთა დაცვის სამსახური, მსოფლიო პრაქტიკა, ივნისი/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].
4. Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 3, 5.
5. EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 2019.
6. 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, 2017, 14-15.
7. Information Commissioner’s Office (ICO), UK, Additional Considerations for Technologies other than CCTV, 2022, 36-37.
8. Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, 3-5. <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023]
9. *Tarr T., Tarr J.A., Thompson M., Wilkinson D*., Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1, 3.
10. The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].
11. The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].
12. The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people’s privacy (Points 20 to 25), October 2019, Last updated: January 2023, Point 22, 32-33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].
13. Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.
14. Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news> [04.09.2023].

თინათინ ლოლომაძე*

პერსონალურ მონაცემთა დაცვა ადამიანის უფლებათა ევროპული სასამართლოს „სამსაფეხურიანი ტესტის“ მიხედვით: რისკები და გამოწვევები

მონაცემთა დაცვა საკანონმდებლო სივრცის ძირითადი ასპექტია. მონაცემთა დაცვა უზრუნველყოფს პირადი ინფორმაციის კონფიდენციალურობას და უსაფრთხოებას ტექნოლოგიური წინსვლისა და მონაცემთა გამოყენების გაზრდის პირობებში.

სტატიაში განხილულია ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა და სამსაფეხურიანი ტესტი, რომელიც არის ფართოდ აღიარებული პრინციპი, და გამოიყენება ფუნდამენტური უფლებების შეზღუდვის კანონიერებისა და მართებულობის შესაფასებლად. სამსაფეხურიანი ტესტი მოითხოვს, რომ უფლების ნებისმიერი შეზღუდვა, როგორიცაა მათ შორის მონაცემთა დაცვის უფლება, უნდა აკმაყოფილებდეს სამ კრიტერიუმს: ლეგიტიმურობას, აუცილებლობას და პროპორციულობას. სამსაფეხურიანი ტესტის დაცვით, კანონმდებლებს და მოსამართლეებს შეუძლიათ, დაადგინონ ბალანსი მონაცემთა კონფიდენციალურობის დაცვასა და ლეგიტიმურ მიზანსა თუ ინტერესს შორის.

საკვანძო სიტყვები: *მონაცემთა დაცვა, ადამიანის უფლებების დაცვა, მონაცემთა დაცვის ძირითადი რეგულაცია, პირადი ცხოვრების უფლება, ლეგიტიმაცია.*

1. შესავალი

ყველა ადამიანს გააჩნია პირადი ცხოვრება, სწორედ პირადი სივრცე გვაძლევს შესაძლებლობას, განვითარდეთ როგორც ინდივიდები და გავხდეთ სოციუმის ნაწილი. გასაკვირი არაა, რომ ხშირად გვსურს, ჩვენი პირადი ცხოვრება საზოგადოებისაგან იყოს დაფარული. ეს სულაც არ ნიშნავს იმას, რომ, თითქოს, ჩვენ, არსებული ინფორმაციის შენახვით, დანაშაულს ჩავდივართ. სინამდვილეში ეს აბსოლუტურად უვნებელი ინფორმაციაა, რომელიც შეეხება პიროვნების რელიგიურ, პოლიტიკურ ან სოციალურ შეხედულებებს. პირადი ცხოვრება ეს არის კონფიდენციალურობის ფაქტობრივი არსი, ხოლო ინფორმაციის გამჟღავნება კი

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი, სამართლის მაგისტრი.

დამოკიდებული უნდა იყოს პიროვნებასა და მის სურვილზე. სწორედ კონფიდენციალურობა და პირადი ცხოვრების დაცულობა ანიჭებს ადამიანებს შესაძლებლობასა და სიმამაცეს, რომ შეძლონ საკუთარი აზრის გამოხატვა. ის იძლევა გარანტიას სახელმწიფოს მიმართაც, რომ საკუთარი პირადი ინფორმაცია, აზრები, შეხედულებები და მოსაზრებები განსჯის გარეშე დარჩეს. პირადი ცხოვრების უფლების ერთ-ერთი ასპექტი, პერსონალური მონაცემების დაცვაა, რომელიც დღევანდელ დემოკრატიულ სახელმწიფოებში ადამიანის ძირითად უფლებად განიხილება. დღემდე ამ უფლების რეალიზებისთვის ხორციელდება არაერთი მნიშვნელოვანი საკანონმდებლო თუ ინსტიტუციური რეფორმა. ადამიანის უფლებათა ევროპული სასამართლო განმარტავს, რომ პერსონალური მონაცემების დაცვის უფლება არ არის ავტონომიური უფლება, ის გათვალისწინებულია სხვადასხვა კონვენციურ უფლებასა და თავისუფლებას შორის[1], სასამართლომ აღიარა, რომ პერსონალური მონაცემების დაცვას ფუნდამენტური მნიშვნელობა აქვს პირის პირადი და ოჯახური ცხოვრებისა და მიმოწერის პატივისცემის უფლებით სარგებლობისთვის, როგორც ეს გარანტირებულია კონვენციის მე-8 მუხლით[2]. ციფრულ ეპოქაში მთელ მსოფლიოში პერსონალური მონაცემების დაცვა აქტუალურ პრობლემად იქცა. მაგ., შეიქმნა მონაცემთა დაცვის მყარი ჩარჩო, როგორიცაა მონაცემთა დაცვის ძირითადი რეგულაცია (GDPR). ამ რეგულაციების გაგებისა და განხორციელების არსებითი ასპექტი მდგომარეობს ადამიანის უფლებათა პრინციპებთან შესაბამისობაში.

სტატია მიზნად ისახავს, შეისწავლოს მონაცემთა დაცვის რეგულაციებსა და ადამიანის უფლებათა ევროპული სასამართლოს (ECtHR) მიერ დადგენილ სამსაფეხურიან ტესტს შორის არსებული ურთიერთობები. ამ ტესტის გაანალიზებით გამოვიკვლევთ, თუ როგორ უნდა დაარეგულირონ სახელმწიფოებმა მონაცემთა ბაზის დაცვა, რათა უზრუნველყონ ინდივიდუალური უფლებებისა და პოტენციური რისკებისგან ადამიანთა უსაფრთხოება. უფლებების, რისკებისა და რეგულაციების ურთიერთქმედების შესწავლით, შეფასდება ციფრულ ეპოქაში კონფიდენციალურობასა და ლეგიტიმურ საზოგადოებრივ ინტერესებს შორის დელიკატური ბალანსის დამყარების მნიშვნელობა.

2. პერსონალური მონაცემების დაცვა ადამიანის უფლებათა ევროპული სასამართლოს მიერ

მონაცემთა დაცვა მნიშვნელოვან როლს ასრულებს პიროვნების პირადი და ოჯახური ცხოვრებით სარგებლობის ხელშეუხებლობაში, რადგან ის ხელს უშლის პერსონალური ინფორმაციის საჯარო გამჟღავნებას. მონაცემების შეგროვება, შენახვა და გამჟღავნება, წარმოადგენს პირად საკითხებში შეჭრას. ადამიანის უფლებათა ევროპული კონვენციის მე-8 მუხლი აღიარებს, როგორც პერსონალური მონაცემების, ასევე, პირადი და ოჯახური ცხოვრების, ბინადრობისა და მიმოწერის უფლებას. მიუხედავად იმისა, რომ პერსონალური მონაცემების დაცვა და პირადი ცხოვრების საიდუმლოების დაცვა განსხვავებული ცნებებია, ორივე მათგანი ცდილობს, დაიცვას

[1] ამანი შვეიცარიის წინააღმდეგ (*Amann v. Switzerland*), განაცხადი №27798/95, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2000 წლის 16 თებერვლის გადაწყვეტილება, §65.

[2] *შპს „სატაკუნან მარკინაპორისი“ და შპს „სატამედია ფინეთის წინააღმდეგ“ (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland),* განაცხადი №931/13, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2017 წლის 27 ივნისის გადაწყვეტილება, §137.

ადამიანის ავტონომია და ღირსება[3]. პერსონალური მონაცემების დაცვის უფლება არის კონფიდენციალურობის უფლებების თანამედროვე და შესაბამისი ასპექტი, რომელიც მიზნად ისახავს პერსონალური ინფორმაციის სათანადო დამუშავებისა და განვითარების უზრუნველყოფას. კონფიდენციალურობის პრინციპი მოიცავს საგნების ფართო სპექტრს, რომელიც შეიცავს სენსიტიურ და პირად დეტალებს და მიზნად ისახავს, თავიდან აიცილოს ნებისმიერი თვითნებური ჩარევა.[4]

ადამიანის უფლებათა ევროპული კონვენციის პირველი მუხლის თანახმად, სახელმწიფოებს ეკისრებათ ვალდებულება, „უზრუნველყონ“ კონვენციით გათვალისწინებული უფლებებისა და თავისუფლებების დაცვა. ეს ვალდებულება გულისხმობს არა მხოლოდ უფლებებისა და თავისუფლებების ხელყოფის თავიდან აცილებას (ნეგატიური ვალდებულება), არამედ პიროვნების უსაფრთხოების აქტიურ დაცვას, მაშინაც კი, როდესაც დარღვევებს ახორციელებენ მესამე მხარეები (ფიზიკური და იურიდიული პირები) (პოზიტიური ვალდებულება)[5]. მიუხედავად იმისა, რომ ევროპული კონვენციის მრავალი დებულების უპირველესი მიზანია ადამიანის უფლებათა საზოგადოებრივი უფლებების გაუმართლებელი შეზღუდვების აკრძალვა, უდავოა, რომ სახელმწიფოები პასუხისმგებელნი არიან ამ უფლებების ეფექტური დაცვის უზრუნველყოფაზე. ადამიანის უფლებათა ევროპულმა სასამართლომ დაადგინა, რომ დადებითი ვალდებულება გამომდინარეობს კონვენციის დებულებებიდან, მათ შორის მე-8 მუხლიდან, რომელიც იცავს პირად და ოჯახურ უფლებებს. მაგ.: საქმეში მარქსი ბელგიის წინააღმდეგ, ევროპულმა სასამართლომ ხაზგასმით აღნიშნა, რომ ამ დებულების არსებითი მიზანია პიროვნების დაცვა საჯარო ხელისუფლების მიერ თვითნებური ჩარევისგან. სახელმწიფოს როლი სცილდება მხოლოდ ჩარევისგან თავის შეკავებას; ის, ასევე, მოითხოვს ოჯახური ცხოვრების „პატივისცემას“. ამრიგად, პერსონალური მონაცემების დაცვა გულისხმობს ეროვნული სახელმწიფოსა და საკანონმდებლო ბაზის ჩარევას და მონაცემთა დაცვის ღონისძიებების პრაქტიკულ განხორციელებას. მნიშვნელოვანია, აღინიშნოს, რომ მიუხედავად იმისა, რომ მე-8 მუხლი უმთავრესად ფოკუსირებულია პირადი ცხოვრების დაცვაზე, კონფიდენციალურობა, როგორც ფუნდამენტური ელემენტი, ჩნდება თავად პირად ცხოვრებაში. კონფიდენციალურობა, პერსონალური მონაცემების კონტექსტში, წარმოადგენს პიროვნების კონფიდენციალურობის შენარჩუნების გადამწყვეტ ასპექტს. პერსონალური ინფორმაციის კონფიდენციალურობის უზრუნველყოფა მონაცემთა დაცვის მექანიზმების მეშვეობით არის ძირითადი ფაქტორი პირადი ცხოვრების უფლების დაცვისა და პირადი ურთიერთობისა და ტრანზაქციების კონფიდენციალურობისა და ნდობის აუცილებელი დონის შესანარჩუნებლად.

პიროვნების მონაცემთა დაცვის უფლების პოტენციური დარღვევის შეფასებისას გადამწყვეტი მნიშვნელობა აქვს მე-8 მუხლის მე-2 პუნქტის მითითებას, რომელიც ასახავს ლეგიტიმური ჩარევის წინაპირობებს. ამ დებულების თანახმად, ნებისმიერი ჩარევა უნდა აკმაყოფილებდეს სამ კრიტერიუმს: ის უნდა იყოს „აუცილებელი

[3] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.

[4] გზამკვლევი პრეცედენტული სამართლის შესახებ ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის მიხედვით/მონაცემთა დაცვა, ევროპის საბჭო/ადამიანის უფლებათა ევროპული სასამართლო, 2022, 7.

[5] *კორკელია კ.,* ევროპული სტანდარტების ინტეგრაციისაკენ: ადამიანის უფლებათა ევროპული კონვენცია და საქართველოს გამოცდილება, თბ., 2007, 14-15.

დემოკრატიულ საზოგადოებაში“, „კანონთან შესაბამისობაში“, უნდა ემსახურებოდეს „ლეგიტიმურ მიზანს“. ჩარევის მოთხოვნა, „კანონის შესაბამისად“, გულისხმობს, რომ მონაცემთა დაცვის უფლების ნებისმიერი შეზღუდვა უნდა ეფუძნებოდეს მკაფიო და პროგნოზირებად საკანონმდებლო დებულებებს. ეს უზრუნველყოფს, რომ პირებს ჰქონდეთ გონივრული მოლოდინი იმის შესახებ, თუ როგორი იქნება მათი პირადი მონაცემების დამუშავება და დაცვა. გარდა ამისა, ჩარევას უნდა ჰქონდეს „ლეგიტიმური მიზანი. ეს ნიშნავს, რომ, მონაცემთა დამუშავების გზით, პიროვნების პირად ცხოვრებაში შეჭრას უნდა ჰქონდეს გამართლებული მიზანი. ლეგიტიმური მიზნების მაგალითებია - ეროვნული უსაფრთხოება, საზოგადოებრივი უსაფრთხოება, დანაშაულის პრევენცია, ჯანმრთელობის დაცვა ან სხვათა უფლებები და თავისუფლებები. დაბოლოს, ჩარევა უნდა ჩაითვალოს „აუცილებლად დემოკრატიულ საზოგადოებაში“. ეს კრიტერიუმი საჭიროებს ბალანსს მონაცემთა დაცვის კონკურენტულ ინტერესებსა და სხვა საზოგადოებრივ მოსაზრებებს შორის. ის მოითხოვს, რომ ჩარევა იყოს პროპორციული, რაც იმას ნიშნავს, რომ ეს უნდა იყოს ყველაზე ნაკლებად შეურაცხმყოფელი ღონისძიება დასახული ლეგიტიმური მიზნის მისაღწევად. აუცილებლობის ტესტი ასევე მოიცავს ალტერნატიული საშუალებების განხილვას იმავე მიზნის მისაღწევად, რაც ნაკლებ გავლენას მოახდენს ინდივიდის მონაცემთა დაცვის უფლებაზე. ამ კრიტერიუმების ჩართვით, მე-8 მუხლის მე-2 პუნქტი ადგენს, ჩარჩოს შეფასების მიზნით, არის თუ არა ჩარევა მონაცემთა დაცვის უფლებაში გამართლებული და შეესაბამება ის თუ არა ადამიანის უფლებათა სტანდარტებს.

3. კანონთან შესაბამისობა

პერსონალურ მონაცემთა დაცვის უფლებაზე დაწესებულ შეზღუდვებს კანონი უნდა არეგულირებდეს. ეს მოთხოვნა გულისხმობს, რომ შეზღუდვას უნდა ჰქონდეს სამართლებრივი საფუძველი, რომელიც ხელმისაწვდომია, განჭვრეტადი და საკმარისი სიცხადით ფორმულირებული, რაც ფიზიკურ პირებს აძლევს საკუთარი მოვალეობების გააზრებისა და ქმედებათა დარეგულირების შესაძლებლობას. სამართლებრივი საფუძველი მკაფიოდ უნდა განმარტავდეს შესაბამისი ორგანოს მიერ უფლებამოსილების განხორციელების მასშტაბსა და ფორმას, რაც ფიზიკურ პირებს იცავს თვითნებური ჩარევისგან.[6] იმისათვის, რომ ჩარევა იყოს კანონთან შესაბამისობაში არსებობს რამდენიმე წინაპირობა:

- სახელმწიფოში უნდა არსებობდეს კანონმდებლობა პერსონალური მონაცემების დასამუშავებლად;
- კანონიერი საფუძველი მოითხოვს, რომ პერსონალური მონაცემების დამუშავება იყოს „აუცილებელი“. თუ სახელმწიფოს შეუძლია გონივრულად მიაღწიოს იმავე მიზანს დამუშავების გარეშე, ასეთ დროს მონაცემების დამუშავება არაკანონიერია;
- მონაცემების შეგროვებამდე უნდა დადგინდეს დამუშავების კანონიერი საფუძველი;
- მონაცემების დამუშავების მიზანი არ უნდა შეიცვალოს სხვა კანონიერი საფუძვლით მოგვიანებით, თუ შეცვლის მიზეზი არ იქნება დასაბუთებული;

[6] Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017, 4.

- თუ დამუშავებას ექვემდებარება განსაკუთრებული კატეგორიის მონაცემები უნდა განისაზღვროს როგორც ზოგადი დამუშავების კანონიერი საფუძველი, ასევე ამ ტიპის მონაცემების დამუშავების დამატებითი პირობები.[7]

ადამიანის უფლებათა ევროპულმა სასამართლომ განიხილა საკითხი, უნდა იყოს თუ არა მიღებული და დამუშავებული პერსონალური მონაცემები, რომლებიც გადის ავტომატურ დამუშავებას სამართლიანად და კანონიერად, როგორც ეს გათვალისწინებულია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ (ე.წ. 108-ე კონვენცია) კონვენციის მე-5 მუხლში, შემდეგში მე-8 მუხლის დარღვევა სამართლებრივი საფუძვლის არარსებობის გამო. მაგ., საქმეში ტეილორ-საბორი გაერთიანებული სამეფოს წინააღმდეგ, განმცხადებელი ექვემდებარებოდა პოლიციის მეთვალყურეობას თავის პეიჯერზე, ხოლო საკანონმდებლო სივრცე არ ითვალისწინებდა პეიჯერის შეტყობინებების მეთვალყურეობის შედეგად მოპოვებული ინფორმაციის კონტროლს[8]. ანალოგიურია საქმე მ.დ. და სხვები ესპანეთის წინააღმდეგ, სადაც სასამართლომ აღნიშნა, რომ, ერთი მხრივ, არ არსებობდა შიდა საკანონმდებლო დებულება, რომელიც გაამართლებდა პოლიციის ქმედებას, მეორე მხრივ, არ არსებობდა მითითებები. სასამართლომ დაადგინა, რომ პოლიციის ანგარიში მოსამართლეთა და მაგისტრატების პერსონალური მონაცემების, ფოტოებისა და პოლიტიკური შეხედულებების გამჟღავნების შესახებ არ იყო გათვალისწინებული კანონით და არღვევდა მე-8 მუხლს[9]. სხვა საქმეებში სასამართლომ დაადგინა მე-8 მუხლის დარღვევა, რადგან პერსონალური მონაცემების დაცვის შიდასახელმწიფოებრივი კანონები იყო ან მიუწვდომელი ან კონფიდენციალური, ან არ იყო გამჭვირვალე. მაგ., საქმეებში - ვასილ ვასილევი ბულგარეთის წინააღმდეგ და ნუჰ უზუნი და სხვები თურქეთის წინააღმდეგ[10], სასამართლომ დაადგინა ისეთი საკითხები, როგორებიცაა: პერსონალური მონაცემების მარეგულირებელი კანონების შეზღუდული წვდომა ან რეგულაციების არასაკმარისი სიცხადე[11]. ამის საპირწონედ, ბენ ფაიზას საქმეში საფრანგეთის წინააღმდეგ, სადაც შიდა კანონმდებლობა იყო ნათელი, გამჭვირვალე და ადეკვატური გარანტიებით უზრუნველყოფილი პოტენციური ძალადობის წინააღმდეგ, სასამართლომ არ დაადგინა მე-8 მუხლის დარღვევა[12]. გარდა ამისა, სასამართლო ხაზგასმით აღნიშნავს, რომ საქმეებში, რომლებიც მოიცავს ფარული თვალთვალის ზომებს, მაგ.: კომუნიკაციების მოსმენისას, თვითნებური ჩარევის თავიდან ასაცილებლად მნიშვნელოვანია, მკაფიო და დეტალური წესების არსებობა. კანონმა მოქალაქეებს უნდა მიაწოდოს საკმარისი მითითებები იმ გარემოებებისა და პირობების შესახებ, რომლებშიც სახელმწიფო ორგანოებს შეუძლიათ გამოიყენონ

[7] Guide to the General Data Protection Regulation (GDPR), Information Commissioner’s Office, 2022, 19.

[8] *ტეილორ-საბორი გაერთიანებული სამეფოს წინააღმდეგ (Taylor-Sabori v. the United Kingdom)*, №47114/99, ადამიანის უფლებათა ევროპული სასამართლოს 2002 წლის 22 ოქტომბრის გადაწყვეტილება, §19.

[9] *მ.დ. ესპანეთის წინააღმდეგ (M.D. and Others v. Spain)*, №36584/17, ადამიანის უფლებათა ევროპული სასამართლოს 2002 წლის 28 სექტემბრის გადაწყვეტილება, §§ 61-64.

[10] *ნუჰ უზუნი და სხვები თურქეთის წინააღმდეგ (Nuh Uzun and Others v. Turkey)*, №49341/18, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 5 სექტემბრის გადაწყვეტილება, §§ 80-99.

[11] *ვასილ ვასილევი ბულგარეთის წინააღმდეგ (Vasil Vasilev v. Bulgaria)*, №7610/15, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 16 აგვისტოს გადაწყვეტილება, §§ 169-170.

[12] *ბენ ფაიზა საფრანგეთის წინააღმდეგ (Ben Faiza v. France)*, №31446/12, ადამიანის უფლებათა ევროპული სასამართლოს 2021 წლის 8 მაისის გადაწყვეტილება, §§ 58-61.

ზემოაღნიშნული ზომები. სასამართლომ აღნიშნა, რომ კანონმა უნდა მიუთითოს ნებისმიერი ისეთი დისკრეციის ფარგლები, რომლებიც მინიჭებული აქვს კომპეტენტურ ორგანოებს და უჩვენოს მისი განხორციელების გზები საკმარისი სიცხადით, რათა სუბიექტებმა შეძლონ ადეკვატურად დაიცვან თავი თვითნებური ჩარევისგან.

სასამართლო პრაქტიკაში ასევე იკვეთება კონკრეტული ელემენტები, რომლებიც კანონმდებლობაში უნდა იყოს გათვალისწინებული მოსმენებთან დაკავშირებით, მაგ.: სამართალდარღვევების ხასიათის განსაზღვრა, მოსმენას დაქვემდებარებული პირების კატეგორიების დაზუსტება, დროის ლიმიტებისა და, ასევე, მონაცემთა შემოწმებისა და შენახვის პროცედურების დაწესება და უსაფრთხოების ზომების დანერგვა.

რაც შეეხება ხელისუფლების მიერ პერსონალური მონაცემების შეგროვებასა და შენახვას დანაშაულის პრევენციის ან დასჯის მიზნით, სასამართლო პრაქტიკა ხაზს უსვამს მკაფიო და დეტალური წესების აუცილებლობას, მაგ.: საქმეში ქეთთი გაერთიანებული სამეფოს წინააღმდეგ სასამართლო განმარტავდა, რომ მონაცემთა შეგროვება ექვემდებარებოდა შიდა საკანონმდებლო ბაზას, მაგრამ სასამართლო ცალკე გამოყოფდა იმასაც, რომ მონაცემთა შეგროვებას არ ჰქონდა უფრო მკაფიო და გასაგები სამართლებრივი საფუძველი. სასამართლომ აღნიშნა, რომ „შიდა ექსტრემიზმს“ სხვადასხვა უწყება სხვადასხვანაირად განმარტავს. ამდენად, სასამართლოსთვის გაუგებარი იყო, რა კრიტერიუმებზე დაყრდნობით გროვდებოდა მოქალაქის შესახებ ინფორმაცია. აღნიშნულ საქმეში სასამართლომ არამარტო მონაცემთა შეგროვებაზე, არამედ მათი შენახვის შესახებაც იმსჯელა, სასამართლომ მიუთითა, რომ შიდა კანონმდებლობა არ ითვალისწინებდა მონაცემთა შენახვის მაქსიმალურ ვადას. გარდა ამისა, მომჩივანი არ წარმოადგენდა არავისთვის საფრთხეს (ის 95 წლის იყო), შეგროვებული ჩანაწერები ასახავდა მომჩივნის პოლიტიკურ შეხედულებებს, რომლებიც წარმოადგენდა განსაკუთრებული სახის მონაცემებს. აქედან გამომდინარე, მათზე მოქმედებდა დაცვის მაღალი სტანდარტები. სწორედ მონაცემთა სენსიტიური ხასიათი წარმოადგენდა საქმის მთავარ არსს, რაზეც სასამართლომ გამოთქვა მოსაზრება: „როცა სახელმწიფოსთვის მინიჭებული უფლებამოსილებები ბუნდოვანია, რაც ქმნის თვითნებობის რისკს, და როდესაც ტექნოლოგიები მუდმივად ვითარდება და იხვეწება, მნიშვნელოვანია, შემოწმდეს კონვენციის მე-8 მუხლის პრინციპებთან შესაბამისობა“. სასამართლოს მითითებით, მომჩივანს ჰქონდა უფლება, მოეთხოვა მონაცემთა წაშლა, თუმცა არ არსებობდა მონაცემების დაცვის სათანადოდ შემდგარი პროცედურული გარანტიები. შიდა საკანონმდებლო ბაზა განსაზღვრავდა, რომ მონაცემები მინიმუმ 6 წლის ვადით ინახებოდა. შემდეგ გადაიხედებოდა და ფასდებოდა მათი შენახვის აუცილებლობა. საქმეში არ ჩანდა საერთოდ, ხორციელდებოდა თუ არა მონაცემთა გადახარისხება. სასამართლო აღნიშნავდა, რომ დადგენილი უნდა ყოფილიყო მონაცემთა შენახვის მაქსიმალური ვადები, გარდა ამისა, პოლიცია იმაზე მეტ ინფორმაციას ფლობდა, ვიდრე ეს საჭირო იყო, და შესაბამისი უწყებები საერთოდაც არ იღებდნენ მხედველობაში მონაცემთა სენსიტიურ ბუნებას.[13] სასამართლო საკუთარ გადაწყვეტილებებში ხაზს უსვამს წესების მნიშვნელობას, რომლებიც არეგულირებენ ასეთი მონაცემების ხანგრძლივობას, შენახვას, გამოყენებას, ხელმისაწვდომობასა და განადგურებას, მათი მთლიანობისა და კონფიდენციალურობის დაცვას.

[13] *კატი გაერთიანებული სამეფოს წინააღმდეგ (Catt v. United Kingdom)*, №43514/15, ადამიანის უფლებათა ევროპული სასამართლოს 2019 წლის 24 იანვრის გადაწყვეტილება.

4. ლეგიტიმური მიზანი

მე-8 მუხლის დარღვევისას ასევე უნდა დადგინდეს ლეგიტიმური მიზანი, რაც ნიშნავს იმას, რომ პერსონალური მონაცემები ავტომატური დამუშავების პროცესში უნდა შეგროვდეს აშკარა, განსაზღვრული და ლეგიტიმური მიზნებისათვის. ამ შემთხვევებში, ლეგიტიმური მიზნების შესწავლა, რამაც შეიძლება გაამართლოს მე-8 მუხლის უფლებების განხორციელებაში ჩარევა, როგორც ეს ჩამოთვლილია მე-2 პუნქტში, საკმაოდ შემოსაზღვრულია. ლეგიტიმური ჩარევის მიზნებია: 1. ეროვნული უსაფრთხოება, 2. საზოგადოებრივი უსაფრთხოება და ქვეყნის ეკონომიკური კეთილდღეობის დაცვა, 3. არეულობის ან დანაშაულის პრევენცია, 4. ჯანმრთელობისა და მორალის დაცვა ან სხვათა უფლებებისა და თავისუფლებების დაცვა. ამ მიზნებიდან ერთის ან მეტის არსებობას, რომელსაც ამტკიცებს მთავრობა, სასამართლოც უნდა იზიარებდეს მე-8 მუხლის მე-2 პუნქტის მიზნების განსახორციელებლად[14].

მაგ., სასამართლომ დაადგინა, რომ საბანკო მონაცემების სხვა ქვეყნის ხელისუფლებისთვის ორმხრივი შეთანხმების საფუძველზე გადაცემა ლეგიტიმურ მიზანს ემსახურებოდა, რადგან ეს ხელს უწყობდა ქვეყნის ეკონომიკური კეთილდღეობის დაცვას[15].

საერთაშორისო ინსტრუმენტებზე მითითებით, რომლებიც ხაზს უსვამენ დოპინგთან ბრძოლაში სამართლიანობასა და თანაბარ შესაძლებლობებს, სასამართლომ დაადგინა, რომ ჯანმრთელობისა და მორალის დაცვა ამართლებს სპორტსმენების ადგილსამყოფლის დადგენის ვალდებულებას დოპინგთან საბრძოლველად. სპორტში ამგვარი ქმედება სასამართლომ დააკავშირა იმასთან, რასაც მთავრობა „ზნეობას“ უწოდებს „სხვისი უფლებებისა და თავისუფლებების დაცვის“ ლეგიტიმური მიზნით, ვინაიდან დოპინგ-აგენტების არსებობა უბიძგებდა მოყვარულ სპორტსმენებს, განსაკუთრებით ახალგაზრდებს, მიჰყოლოდნენ მათ[16]. დადგინდა, რომ კორუფციაში ეჭვმიტანილი ციხის დირექტორის სატელეფონო საუბრების მოსმენა, ამ ინფორმაციის შენახვა და მისი გამჟღავნება მიზნად ისახავდა კორუფციული ქმედებების თავიდან აცილებას, საჯარო სამსახურში გამჭვირვალობისა და ღიაობის უზრუნველყოფას. ამრიგად, ლეგიტიმური მიზნები იყო არეულობის ან დანაშაულის პრევენცია და სხვათა უფლებებისა და თავისუფლებების დაცვა[17].

თითოეულ საქმეში სასამართლომ თანმიმდევრულად აღიარა ერთი ან მეტი ლეგიტიმური მიზნის არსებობა, რომლებსაც მიმართავენ მთავრობები. ეს დასკვნები ხაზს უსვამს სასამართლოს ვალდებულებას, დააბალანსოს პერსონალური

[14] Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022, 12.

[15] *G.S.B. შვეიცარიის წინააღმდეგ, (G.S.B. v. Switzerland),* განაცხადი №28601/11, ადამიანის უფლებათა ევროპული სასამართლოს 2015 წლის 22 დეკემბერი, § 83.

[16] *სპორტსმენთა ასოციაციებისა და გაერთიანებების ეროვნული ფედერაცია. FNASS და სხვები საფრანგეთის წინააღმდეგ, (National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France)*, №48151/11, №77769/13, ადამიანის უფლებათა ევროპული სასამართლოს 2018 წლის 18 იანვარი, §§ 164-166.

[17] *ადომაიტისი ლიეტუვას წინააღმდეგ (Adomaitis v. Lithuania)*, განაცხადი №14833/18, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 18 იანვარი, § 84.

მონაცემების დაცვა და საზოგადოების კანონიერი ინტერესების დაცვის აუცილებლობა.

5. აუცილებელი დემოკრატიულ საზოგადოებაში

იმისათვის, რომ ნებისმიერი ღონისძიება, რომელიც მე-8 მუხლით ერევა პერსონალური მონაცემების დაცვაში, ჩაითვალოს აუცილებლად დემოკრატიულ საზოგადოებაში, ის უნდა აკმაყოფილებდეს მწვავე სოციალური საჭიროების კრიტერიუმებს და არ უნდა იყოს არაპროპორციული ლეგიტიმური მიზნების მიმართ. მთავრობის მიერ მოწოდებული მიზეზები უნდა იყოს შესაბამისი და საკმარისი. მიუხედავად იმისა, რომ პირველადი შეფასება ხდება ეროვნული ხელისუფლების მიერ, ჩარევის აუცილებლობის საბოლოო შეფასება ექვემდებარება სასამართლოს განხილვას კონვენციის მოთხოვნებთან შესაბამისობის უზრუნველსაყოფად. როდესაც საქმე ეხება უფლებების დარღვევას, სასამართლო განიხილავს, უზრუნველყოფს თუ არა სახელმწიფოს მიერ მიღებული კანონმდებლობა ამ უფლებების ადეკვატურ დაცვას.

მთლიანობაში, იმის დასადგენად, არის თუ არა დემოკრატიულ საზოგადოებაში, მე-8 მუხლის მიხედვით, პერსონალური მონაცემების დაცვაში ჩარევის ღონისძიება გამართლებული, ეს საკითხი, 108 -ე კონვენციის მე-5 მუხლში მოცემულ მოთხოვნებთან შესაბამისობით, სასამართლომ უნდა განიხილოს.

სასამართლო ხაზს უსვამს, პერსონალური მონაცემების დაცვაში ჩარევის ზომების აუცილებლობას, რათა შეინარჩუნოს პროპორციულობა მწვავე სოციალური საჭიროებების წინაშე. სასამართლოს როლია, განიხილოს და შეაფასოს ასეთი ჩარევის აუცილებლობა ეროვნული შეფასებების გათვალისწინებით, რამდენად შეესაბამება ის კონვენციის მოთხოვნებს.

5.1. შეგროვებული ან ჩაწერილი მონაცემების მინიმალიზაციის მოთხოვნა

უნდა დამუშავდეს მხოლოდ ისეთი მონაცემები, რომლებიც „შესაბამისი და რელევანტურია, მოცულობა კი არ აჭარბებდეს მიზანს, რისთვისაც ისინი შეგროვდა და/ან დამუშავდა.“ დამუშავებისთვის შერჩეულ მონაცემთა კატეგორიები საჭირო უნდა იყოს დამუშავების ოპერაციების გაცხადებული მიზნის მისაღწევად, ხოლო დამმუშავებელი მკაცრად შეიზღუდოს მხოლოდ იმ მონაცემთა შეგროვებით, რომლებიც პირდაპირ შეესაბამება კონკრეტულ მიზანს. პერსონალურ მონაცემთა დამუშავება უნდა იყოს იმ ლეგიტიმური მიზნის პროპორციული, რომელსაც ემსახურება დამუშავება. მონაცემთა დამუშავების ყველა ეტაპზე უნდა არსებობდეს სამართლიანი წონასწორობა ყველა შესაბამის ინტერესს შორის. ეს ნიშნავს, რომ „პერსონალური მონაცემები, რომლებიც შესაბამისი და რელევანტურია, მაგრამ მოიცავს არაპროპორციულ ჩარევას სასწორზე დადებულ ფუნდამენტურ უფლებებსა და თავისუფლებებში, გადაჭარბებულად უნდა ჩაითვალოს“.[18]

მაგ. ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციის თანახმად შეგროვებული მონაცემები უნდა იყოს: ადეკვატური-საკმარისი დასახული მიზნის სათანადოდ შესასრულებლად; შესაბამისი - ჰქონდეს რაციონალური კავშირი ამ

[18] მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 5 (1) (გ).

მიზანთან; შემოიფარგლებოდეს მხოლოდ იმით, რაც აუცილებელია - არ უნდა ინახებოდეს იმაზე მეტი ინფორმაცია ვიდრე საჭიროა.

ამდენად, უნდა დადგინდეს პერსონალური მონაცემების მინიმალური რაოდენობა, რომელიც საჭიროა მიზნის შესასრულებლად. მაგრამ ჩნდება კითხვა როგორ მივხვდეთ რა არის ადეკვატური, შესაბამისი და შეზღუდული? კანონმდებლობა ვერ შეძლებს განსაზღვროს ეს ტერმინები. თუმცა, ცხადია, ეს დამოკიდებული იქნება პერსონალური მონაცემების შეგროვებისა და გამოყენების მიზანზე. ის ასევე შეიძლება განსხვავდებოდეს ერთი ინდივიდიდან მეორეზე. ასე რომ, იმისათვის, რომ შეფასდეს, ინახება თუ არა პერსონალური მონაცემების „სწორი რაოდენობა“[19], ჯერ უნდა გაირკვეს, შესაბამისი მიზანი და მონაცემთა ხასიათი, სწორედ ასეთ შემთხვევებს განიხილავს ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკა და დაადგინა ერთგვარი „გზამკვლევი“, რომელიც სახელმწიფოებს შეუძლიათ გამოიყენონ საკუთარ პრაქტიკაშიც.

მაგ., სასამართლომ დაადგინა მე-8 მუხლის დარღვევა მას შემდეგ, რაც ჩხრეკის დროს ამოღებული ელექტრონული მოწყობილობებიდან მიღებული ინფორმაციის შენახვა, საქმიდან გამომდინარე, არ იყო რელევანტური. ასევე, არ ჩანდა, რომ რაიმე სახის შერჩევის პროცედურა ჩატარდა, ამ მონაცემების რაოდენობის მინიმუმამდე შესამცირებლად[20]. სასამართლომ განიხილა საკითხი, იყო თუ არა ავტომატურად დამუშავებული პერსონალური მონაცემები შესაფერისი, რელევანტური და არა გადაჭარბებული იმ მიზნებისთვის, რისთვისაც ისინი ჩაიწერა სხვადასხვა ინსტანციაში. ზოგიერთ შემთხვევაში სასამართლომ დაადგინა კონვენციის მე-8 მუხლის დარღვევა. ეს დარღვევები მოხდა იმის გამო, რომ არანაირი პროცედურა არ იყო დაცული მომჩივნების ელექტრონული მოწყობილობებიდან ამოღებული მონაცემების მინიმიზაციისთვის ჩხრეკის დროს. სასამართლოს გადაწყვეტილება პროცესის არამონაწილის საჯაროდ იდენტიფიცირება (იგი ჩართული იყო სამუშაო ადგილზე სექსუალური შევიწროების საქმეში), კონფიდენციალურობის დაცვის გარეშე, ჩაითვალა არასაჭიროდ და პოტენციურად მასტიგმატიზირებლად. გარდა ამისა, გამოძიების პროგრესის ანგარიშში ჟურნალისტის თანხმობის გარეშე გადაღებული პერსონალური მონაცემების გამჟღავნება ჩაითვალა გადაჭარბებულად და უმიზნოდ.[21]

სასამართლოს აზრით, დანაშაულის პრევენციისა და დასჯის მიზნით, მონაცემთა ბაზები არ უნდა შეიქმნას შესანახი ინფორმაციის მაქსიმალურად გაზრდის სურვილით. არგუმენტი, რომ მეტი მონაცემების შენახვა იწვევს დანაშაულის პრევენციის გაზრდას, არ ამართლებს ინფორმაციის შენახვას მთელ მოსახლეობაზე, მათ შორის გარდაცვლილ ნათესავებზე, რაც აშკარად გადაჭარბებული და შეუსაბამოა. სასამართლო, ლეგიტიმური მიზნების შესაბამისად, ხაზს უსვამს პერსონალური მონაცემების ადეკვატური, შესაბამისი და პროპორციული დამუშავების მნიშვნელობას. მონაცემთა გადაჭარბებული შენახვა და გამჟღავნება, სათანადო გარანტიების გარეშე, არღვევს კონვენციის მე-8 მუხლით დაცულ უფლებებსა და თავისუფლებებს. სახელმწიფოებისთვის აუცილებელია, დაამყარონ

[19] Guide to the General Data Protection Regulation (GDPR), Information Commissioner’s Office, 2022, 27.

[20] *კრუგლოვი და სხვები რუსეთის წინააღმდეგ (Krugulov and others v. Russia)*, №11264/04, ადამიანის უფლებათა ევროპული სასამართლოს 2020 წლის 4 თებერვალი, §123-138.

[21] *ხელილი შვეიცარიის წინააღმდეგ (Khelili v. Switzerland)*, №16188/07, ადამიანის უფლებათა ევროპული სასამართლოს 2011 წლის 18 ოქტომბრის გადაწყვეტილება, § 62.

ბალანსი ინფორმაციის შენახვის სარგებელსა და ინდივიდუალური კონფიდენციალურობის პატივისცემას შორის.[22]

5.2. მონაცემთა სიზუსტისა და განახლების მოთხოვნა

ევროკავშირისა და ევროპის საბჭოს კანონმდებლობათა შესაბამისად, მონაცემთა სუბიექტებს ენიჭებათ უფლება, მოითხოვონ თავიანთი პერსონალური მონაცემების გასწორება. მათი სიზუსტე აუცილებელია მონაცემთა სუბიექტების პერსონალური ინფორმაციის მაღალ დონეზე დასაცავად.[23] ხელისუფლების მიერ შეგროვებულმა და დაცულმა ყალბმა ან არასრულმა პერსონალურმა მონაცემებმა შეიძლება გაართულოს პერსონალურ მონაცემთა დაცვის სუბიექტის ყოველდღიური ცხოვრება, ან შეიძლება მოუხსნას გარკვეული ნორმატიული პროცედურული გარანტიები, რომლებიც საჭიროა პიროვნების უფლებების დასაცავად. ასეთი მონაცემები შეიძლება გავრცელდეს სხვადასხვა ორგანოს შორის, რამაც შეიძლება ზიანი მოუტანოს მონაცემთა სუბიექტის პირად ცხოვრებას ან მის სამსახურებრივ ცხოვრებას. ხელისუფლების ორგანოების ამოცანაა, დაამტკიცონ შენახული მონაცემების სიზუსტე. ადამიანის უფლებათა სასამართლომ განიხილა მთელი რიგი საქმეები ხელისუფლების მიერ იმ მონაცემების შენახვის შესახებ, რომლებიც აღმოჩნდა არაზუსტი ან რომელთა სიზუსტე სადავო იყო მონაცემთა სუბიექტის მიერ. სასამართლო პრაქტიკა აჩვენებს, რომ მონაცემები შენახული უნდა იყოს არა უმეტეს იმ მიზნის შესასრულებლად, რისთვისაც ისინი იქნა მოპოვებული. საქმეში ს. და მარპერი გაერთიანებული სამეფოს წინააღმდეგ[24], სასამართლომ აღნიშნა, რომ ეროვნულ მონაცემთა ბაზაში მუდმივი შენახვა იმ პირთა თითის ანაბეჭდების, უჯრედული ნიმუშებისა და დნმ-ის პროფილების, რომლებიც ბრალდებულნი იყვნენ, მაგრამ არა ნასამართლევი დანაშაულში, განურჩევლად დანაშაულის ხასიათისა და სერიოზულობისა, რომელზედაც პირი თავდაპირველად იყო ეჭვმიტანილი, არღვევს მე-8 მუხლს. მაგ., საქმეში ანჩევი ბულგარეთის წინააღმდეგ, სადაც განმცხადებლის წინააღმდეგ მიმდინარეობდა სამი გამოძიება და, არქივზე დაყრდნობით, მიენიჭა „იარლიყი“, როგორც ყოფილი უსაფრთხოების სამსახურების თანამშრომელი. ეს ყველაფერი მოხდა კანონის მიხედვით, რომელიც მიზნად ისახავდა საჯარო მოხელეების გამჟღავნებას, რომლებიც თანამშრომლობდნენ კომუნისტურ რეჟიმთან. თუმცა, სასამართლომ არ დააკმაყოფილა განმცხადებლის საჩივარი, რადგან მას მიეცა უფლება ჰქონოდა არქივებთან წვდომა და შემდგომში შეეძლო ინფორმაციის სიზუსტის გასაჩივრება. მნიშვნელოვანია აღინიშნოს, რომ სასამართლოს გადაწყვეტილება ამ საქმეში იყო სპეციფიკური წარმოდგენილ გარემოებებთან. სასამართლომ აღიარა, რომ მომჩივნის არქივებთან წვდომის უზრუნველყოფა და ინფორმაციის სიზუსტის გასაჩივრების შესაძლებლობა იყო შესაბამისი საშუალება კონკრეტული გარემოებების და განმცხადებლის შესაძლებლობის გათვალისწინებით, წარმოედგინა კონკრეტული საფუძველი მისი გასაჩივრებისთვის. მთლიანობაში, ეს შემთხვევა ხაზს უსვამს იმის უზრუნველყოფის მნიშვნელობას, რომ ადამიანებს აქვთ შესაძლებლობა განიხილონ და

[22] მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 144.
[23] მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 16.
[24] *ს. და მარპერი გაერთიანებული სამეფოს წინააღმდეგ (S. and Marper v. the United Kingdom)*, №30562/04 და 30566/04, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2008 წლის 4 დეკემბრის გადაწყვეტილება, §§ 70-75.

გააპროტესტონ მათთვის მიკუთვნებული ინფორმაცია, განსაკუთრებით მაშინ, როდესაც მას აქვს პოტენციალი, გავლენა მოახდინოს მათ რეპუტაციასა და უფლებებზე. შესაბამის არქივებზე ხელმისაწვდომობის მინიჭება შესაძლებელს ხდის ნებადართული პირებისთვის, წარმოადგინონ მტკიცებულებები, რათა ეჭვქვეშ დააყენონ ასეთი ინფორმაციის სიზუსტე, რომელიც კონვენციით გათვალისწინებული მათი უფლებების დაცვის მნიშვნელოვანი ასპექტია.[25] პრაქტიკა ცხადყოფს, რომ ხელისუფლებამ უნდა დაადგინოს შენახული მონაცემების სიზუსტე. ყალბი ან სადავო ინფორმაციის შენახვამ შეიძლება საზიანო გავლენა მოახდინოს მონაცემთა სუბიექტის ყოველდღიურ ცხოვრებაზე, რეპუტაციასა და პროცედურულ უფლებებზე. ძალიან მნიშვნელოვანია, რომ ხელისუფლებამ გამოიჩინოს სიფრთხილე და უზრუნველყოს ის, რომ მონაცემთა შენახვა შეესაბამებოდეს სიზუსტისა და პირთა კონფიდენციალურობის პრინციპებს, ეს უკანასკნელი კი, გარანტირებულია კონვენციის მე-8 მუხლით.

5.3. პერსონალური მონაცემების შენახვის ხანგრძლივობის შეზღუდვა (მოთხოვნა, რომ მონაცემები შენახული იყოს არა უმეტეს იმ მიზნის შესასრულებლად, რისთვისაც ისინი იქნა ჩაწერილი)

სასამართლომ რამდენიმე შემთხვევაში განიხილა პერსონალური მონაცემების შენახვის ხანგრძლივობის შეზღუდვის საკითხი. სასამართლო უარყოფითად აფასებს განუსაზღვრელი ვადით მონაცემების შენახვას, ასევე, გარდა ამისა, მონაცემთა შენახვის პერიოდი დიდწილად დამოკიდებულია დანაშაულის სიმძიმეზე. მუდმივი შენახვის საკითხი განსაკუთრებით მძიმეა მაშინ, როდესაც საქმე ეხება არასრულწლოვანებს მათი მოწყვლადი მდგომარეობის, მათი განვითარებისა და საზოგადოებაში ინტეგრაციის მნიშვნელობის გამო[26]. მაგ., სასამართლომ დაადგინა დარღვევა საქმეში მ.კ საფრანგეთის წინააღმდეგ, სადაც მომჩივანი ბრალდებული იყო წიგნების ქურდობისთვის, მაგრამ არა ნასამართლევი, მისი ანაბეჭდები კი განუსაზღვრელი ვადით შეინახეს[27], საპირისპიროდ, საქმეში - მარტენსი გერმანიის წინააღმდეგ სასამართლომ აშკარად დაუსაბუთებლად გამოაცხადა საქმე, რომელშიც მომჩივნის პერსონალური მონაცემები განუსაზღვრელი ვადით შეინახეს, მაგრამ კანონმდებლობა ითვალისწინებდა განხილვებს რეგულარული ინტერვალით არა უმეტეს ათი წლისა, რათა დადგენილიყო, ინახავდნენ თუ არა მონაცემებს. მსჯავრდებულთა ბიომეტრიული მონაცემების შენახვის პერიოდთან დაკავშირებით ხანგრძლივობა სულაც არ არის გადამწყვეტი, სასამართლომ განაცხადა, რომ მონაცემთა შენახვის მაქსიმალური ვადის არარსებობა ავტომატურად არ არღვევს მე-8 მუხლს. თუმცა, ასეთ შემთხვევებში, პროცედურული გარანტიები ხდება გადამწყვეტი იმისთვის, რომ მონაცემთა შენახვის ხანგრძლივობა დარჩეს პროპორციული. ხელისუფლების შრომისმოყვარეობა პერსონალური მონაცემების შენახვის აუცილებლობის შეფასებისა და პერიოდული-განხილვისას არსებითი ხდება

[25] *ნჩევი ბულგარეთის წინააღმდეგ (Anchev v. Bulgaria)*, №38334/08 - 68242/16, ადამიანის უფლებათა ევროპული სასამართლოსდიდი პალატის 2017 წლის 5 დეკემბრის გადაწყვეტილება, §§ 112-115.

[26] გზამკვლევი პრეცედენტული სამართლის შესახებ ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის მიხედვით/მონაცემთა დაცვა, ევროპის საბჭო/ადამიანის უფლებათა ევროპული სასამართლო, 2022, 29.

[27] *მ. კ საფრანგეთის წინააღმდეგ (M.K v France),* №19522/09, ადამიანის უფლებათა ევროპული სასამართლოს 2013 წლის 18 აპრილის გადაწყვეტილება.

ლეგიტიმურ მიზნებსა და პირთა კონფიდენციალურობის უფლებას შორის ბალანსის შესანარჩუნებლად. შენახვის ხანგრძლივობა დამოკიდებული უნდა იყოს დანაშაულის სიმძიმის ხარისხზე, ბრალდებულის წარსულ ქმედებებზე, იმ ეჭვის სიძლიერეზე, რომელიც სუბიექტის მიმართ არსებობს, სწორედ ეს ფაქტორები უნდა შეფასდეს სახელმწიფოს მხრიდან და ისე დადგინდეს შენახვის პროპორციულობა, თითოეულ შემთხვევაში, მონაცემთა შენახვის მიზნისა და გარემოებების ხასიათისა და სიმძიმის გათვალისწინებით.[28]

სასამართლო აღიარებს, რომ შეიძლება არსებობდეს პერსონალური მონაცემების გარკვეული ვადის მიღმა შენახვის გამართლებული მიზეზები, განსაკუთრებით მძიმე დანაშაულებთან დაკავშირებულ საქმეებში, თუმცა, მონაცემების მუდმივი შენახვა, რომლებიც ეხება იმ პირებს, რომლებიც არ არიან ნასამართლევი რაიმე დანაშაულისთვის, განურჩევლად მათი ასაკისა და საეჭვო ხასიათისა, შეუთავსებელია მე-8 მუხლთან. აუცილებელია პროცედურული გარანტიებისა და გულმოდგინე ზედამხედველობის დაწესება, რათა უზრუნველყოფილ იქნას მონაცემები.

5.4. მონაცემთა გამოყენების შეზღუდვის მოთხოვნა იმ მიზნით, რისთვისაც ისინი ჩაიწერა

მნიშვნელოვანია მონაცემების გამოყენების შეზღუდვის მოთხოვნა იმ მიზნით, რისთვისაც ისინი ჩაიწერა, სასამართლოს პრაქტიკაში განმეორებადი თემაა. სასამართლომ ხაზი გაუსვა ამ პრინციპის მკაცრი დაცვის აუცილებლობას, რათა დაიცვან პიროვნების პირადი ცხოვრების უფლება. რამდენიმე ნიშანდობლივი შემთხვევა იძლევა დამატებით ინფორმაციას ამ მოთხოვნის შესახებ[29]:

მაგ., საქმეში ქარაბეოღლუ თურქეთის წინააღმდეგ, სასამართლომ დაადგინა მე-8 მუხლის დარღვევა, რადგან სისხლის სამართლის გამოძიების დროს სატელეფონო მოსმენის შედეგად მიღებული მონაცემები გამოიყენებოდა სხვა მიზნით, შემდგომ დისციპლინურ გამოძიებაში. სასამართლომ ხაზგასმით აღნიშნა, რომ მონაცემების გამოყენება სხვა მიზნებისთვის, გარდა იმ მიზნებისათვის, რომლებიც ამართლებდა მათ შეგროვებას, შეიძლება იყოს კონფიდენციალურობის უფლების დარღვევა[30]. საქმე სურიკოვი უკრაინის წინააღმდეგ, ეხებოდა ინდივიდის ფსიქიკური ჯანმრთელობის შესახებ მონაცემების ხანგრძლივ შენახვას, გავრცელებას და გამოყენებას იმ მიზნებისთვის, რომლებიც არ იყო დაკავშირებული საწყის საქმესთან. სასამართლომ დაასკვნა, რომ ასეთი პრაქტიკა წარმოადგენდა არაპროპორციულ ჩარევას მონაცემთა სუბიექტის პირადი ცხოვრების პატივისცემის უფლებაში. ეს შემთხვევა ხაზს უსვამს იმის უზრუნველყოფის მნიშვნელობას, რომ პერსონალური მონაცემები გამოყენებული უნდა იყოს მხოლოდ იმ მიზნებისთვის, რისთვისაც ისინი თავდაპირველად შეგროვდა[31].

---

[28] *პერუცო და მარტინესი გერმანიის წინააღმდეგ (Peruzzo and Martens v. Germany)*, №7841/08 and 57900/12, ადამიანის უფლებათა ევროპული სასამართლოს 2013 წლის 4 ივნისის გადაწყვეტილება, §§ 44-49.

[29] მონაცემთა დაცვის ძირითადი რეგულაცია, მუხლი 5 (1) (გ).

[30] *ქარაბეოღლუ თურქეთის წინააღმდეგ (Karabeyoğlu v. Turkey)*, №30083/10, ადამიანის უფლებათა ევროპული სასამართლოს 2016 წლის 7 ივნისის გადაწყვეტილება, §111-124.

[31] *სურიკოვი უკრაინის წინააღმდეგ (Surikov v. Ukraine)*, №42788/06, ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 26 იანვრის გადაწყვეტილება, §80-96.

ამ პრინციპიდან ნებისმიერმა გადახრამ, მაგ., მონაცემთა სხვადასხვა მიზნებისთვის გამოყენება ან არასათანადო გამჟღავნება, შეიძლება დაარღვიოს პიროვნების კონფიდენციალურობის უფლება. პერსონალური მონაცემების დაცვისა და კონვენციის მე-8 მუხლით გათვალისწინებული პირების უფლებების დაცვის უზრუნველსაყოფად გადამწყვეტი მნიშვნელობა აქვს შესაბამისი გარანტიებისა და წვდომის კონტროლის განხორციელებას.

5.5. მონაცემთა დამუშავების პროცედურების გამჭვირვალობის მოთხოვნა

საჯარო ხელისუფლების მიერ შეგროვებულ და შენახულ პერსონალურ მონაცემებთან დაკავშირებულ რიგ საქმეებში, სასამართლომ დაადგინა, რომ ხელისუფლებას ჰქონდა პოზიტიური ვალდებულება დაინტერესებულ პირებს მიეწოდებინათ „ეფექტური და ხელმისაწვდომი პროცედურა“[32] , რათა მათ ჰქონოდათ წვდომა „ყველა შესაბამის ინფორმაციაზე.“ პერსონალური მონაცემების სუბიექტს აქვს უფლება, მოითხოვოს ინფორმაცია პირადი იდენტობის აღმოჩენისათვის, რა თქმა უნდა, გამჭვირვალობის ეს მოთხოვნა ნაკლებად მოქმედებს ისეთ დროს, როდესაც სასწორის მეორე მხარეს ეროვნული უსაფრთხოებისთვის შემცველი ინფორმაცია დევს. პრაქტიკა ცხადყოფს, თუ რამდენად მნიშვნელოვანია კანონმდებლობის გამჭვირვალობა და კონკრეტიზაცია, რათა არ მოხდეს დისკრეციის გადაჭარბება სახელმწიფო ორგანოების მიერ. გარდა ამისა, ხაზს უსვამს იმასაც, რომ მიუხედავად სახელმწიფოს უფლებამოსილებებისა, პერსონალური მონაცემების შეგროვებისა, საბოლოო შეფასება სწორედ სასამართლოს პრეროგატივაა, შესაბამისად, სასამართლო უნდა იყოს ამ საკითხში გათვითცნობიერებული, რათა არ დაუშვას კანონის არასწორი ინტერპრეტაცია.

6. დასკვნა

თითოეული ადამიანის პირადი ცხოვრების პატივისცემა დემოკრატიული სახელმწიფოს ერთ-ერთი ვალდებულებაა, რადგან ის ქმნის პიროვნული ზრდისა და განვითარების საფუძველს. კონფიდენციალურობა ერთგვარი თავშესაფარია მოქალაქეებისთვის, სადაც მათ შეუძლიათ თავისუფლად გამოხატონ მოსაზრებები, რწმენა და ვინაობა ყოველგვარი განსჯის და შიშის გარეშე. ინდივიდის პირადი ცხოვრების პატივისცემა ხელს უწყობს თვითგამოხატვის, კრეატიულობისა და ინდივიდუალურობისკენ სწრაფვის ხელშემწყობი გარემოს შექმნას. მონაცემთა დაცვის კონტექსტში, პირადი ცხოვრების ცნება დამატებით მნიშვნელობასაც იძენს. ჩვენი პერსონალური ინფორმაცია მუდმივად გროვდება, მუშავდება და მისი გაზიარება ხდება სხვადასხვა ორგანოებისა თუ კომპანიებისათვის, ონლაინ აქტივობებიდან ფინანსურ ტრანზაქციებამდე. ჩვენი ციფრული კვალი ტოვებს უამრავ მონაცემს, რომლებსაც შეუძლიათ გამოავლინონ დეტალები ჩვენი ცხოვრების შესახებ. ციფრულ სფეროში ინდივიდების პირადი ცხოვრების დაცვა უმნიშვნელოვანესია. ის უზრუნველყოფს, რომ ინდივიდებმა შეინარჩუნონ კონტროლი თავიანთ პერსონალურ ინფორმაციაზე და ჰქონდეთ თავისუფლება -

[32] *გასკინი გაერთიანებული სამეფოს წინააღმდეგ (Gaskin v. the United Kingdom)*, №10454/83, ადამიანის უფლებათა ევროპული სასამართლოს 1989 წლის 7 ივლისის გადაწყვეტილება, §40-60.

გადაწყვიტონ, როგორ გამოიყენონ, გააზიარონ და შეინახონ ისინი. კონფიდენციალურობის პატივისცემა საშუალებას აძლევს ინდივიდებს, გააკეთონ ინფორმირებული არჩევანი და შეინარჩუნონ ავტონომია თავიანთ პერსონალურ მონაცემებზე. გარდა ამისა, პირადი ცხოვრების დაცვა არ არის მხოლოდ ინდივიდუალური უფლებების საკითხი; ეს არის დემოკრატიული საზოგადოების ფუნდამენტური საყრდენი. როდესაც ინდივიდები თავს დაცულად გრძნობენ პირად ცხოვრებაში, ისინი უფრო მეტად ჩაერთვებიან ღია დისკურსში, გამოხატავენ სხვადასხვა მოსაზრებას და წვლილს შეიტანენ საზოგადოების კულტურულ, სოციალურ და ინტელექტუალურ სტრუქტურაში. სახელმწიფოები ვალდებულნი არიან, პირველ რიგში, შექმნან ისეთი საკანონმდებლო ბაზა, რომელიც შეძლებს თავისი მოქალაქეების მონაცემების დაცვას, გარდა ამისა, პრობლემას წარმოადგენს ისიც, რომ პერსონალურ მონაცემთა დეფინიცია ცვალებადია და უფრო მეტად მრავალწახნაგოვანი ხდება. სწორედ ამიტომ, საჭიროა სასამართლო ორგანოების მეტად ჩართულობა პერსონალურ მონაცემთა დაცვის ასპექტში.

მონაცემთა კონფიდენციალურობის დაცვა, ერთ-ერთი უმთავრესი საკითხია. მონაცემთა დაცვით უზრუნველვყოფთ ინდივიდებს დაუსაბუთებელი შეჭრისა და მეთვალყურეობისაგან. პირადი ცხოვრების შეფასებითა და დაცვით, ჩვენ ვქმნით გარემოს, რომელიც ავითარებს ინდივიდუალობას, თვითგამოხატვასა და პიროვნული ზრდისკენ მისწრაფებას.

ბიბლიოგრაფია:

1. მონაცემთა დაცვის ძირითადი რეგულაცია.
2. გზამკვლევი პრეცედენტული სამართლის შესახებ ადამიანის უფლებათა ევროპული სასამართლოს პრაქტიკის მიხედვით/მონაცემთა დაცვა, ევროპის საბჭო/ადამიანის უფლებათა ევროპული სასამართლო, 2022, 7, 29.
3. *კორკელია კ.,* ევროპული სტანდარტების ინტეგრაციისაკენ: ადამიანის უფლებათა ევროპული კონვენცია და საქართველოს გამოცდილება, თბ., 2007, 14-15.
4. მონაცემთა დაცვის ევროპული სამართლის სახელმძღვანელო, 2018, 144.
5. *ამანი შვეიცარიის წინააღმდეგ* (*Amann v. Switzerland*), განაცხადი №27798/95, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2000 წლის 16 თებერვლის გადაწყვეტილება.
6. *ადომაიტისი ლიეტუვას წინააღმდეგ* (*Adomaitis v. Lithuania*), განაცხადი №14833/18, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 18 იანვარი.
7. *ბენ ფაიზა საფრანგეთის წინააღმდეგ* (*Ben Faiza v. France*), №31446/12, ადამიანის უფლებათა ევროპული სასამართლოს 2021 წლის 8 მაისის გადაწყვეტილება.
8. *გასკინი გაერთიანებული სამეფოს წინააღმდეგ* (*Gaskin v. the United Kingdom*), №10454/83, ადამიანის უფლებათა ევროპული სასამართლოს 1989 წლის 7 ივლისის გადაწყვეტილება.
9. *ვასილ ვასილევი ბულგარეთის წინააღმდეგ* (*Vasil Vasilev v. Bulgaria*), №7610/15, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 16 აგვისტოს გადაწყვეტილება.
10. *კრუგლოვი და სხვები რუსეთის წინააღმდეგ* (*Krugulov and others v. Russia*), №11264/04, ადამიანის უფლებათა ევროპული სასამართლოს 2020 წლის 4 თებერვალი, §123-138.

11. *ქეთი გაერთიანებული სამეფოს წინააღმდეგ* (*Catt v. United Kingdom*), №43514/15, ადამიანის უფლებათა ევროპული სასამართლოს 2019 წლის 24 იანვრის გადაწყვეტილება.
12. *მ.დ. ესპანეთის წინააღმდეგ* (*M.D. and Others v. Spain*), №36584/17, ადამიანის უფლებათა ევროპული სასამართლოს 2002 წლის 28 სექტემბრის გადაწყვეტილება.
13. *მ. კ საფრანგეთის წინააღმდეგ* (*M.K v France*), №19522/09, ადამიანის უფლებათა ევროპული სასამართლოს 2013 წლის 18 აპრილის გადაწყვეტილება.
14. *ნუჰ უზუნი და სხვები თურქეთის წინააღმდეგ* (*Nuh Uzun and Others v. Turkey*), №49341/18, ადამიანის უფლებათა ევროპული სასამართლოს 2022 წლის 5 სექტემბრის გადაწყვეტილება.
15. *ნჩევი ბულგარეთის წინააღმდეგ* (*Anchev v. Bulgaria*) №38334/08 - 68242/16, ადამიანის უფლებათა ევროპული სასამართლოსდიდი პალატის 2017 წლის 5 დეკემბრის გადაწყვეტილება.
16. *პერუცო და მარტინესი გერმანიის წინააღმდეგ* (*Peruzzo and Martens v. Germany*), №7841/08 and 57900/12, ადამიანის უფლებათა ევროპული სასამართლოს 2013 წლის 4 ივნისის გადაწყვეტილება.
17. *ს. და მარპერი გაერთიანებული სამეფოს წინააღმდეგ* (*S. and Marper v. the United Kingdom*), №30562/04 და 30566/04, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2008 წლის 4 დეკემბრის გადაწყვეტილება.
18. *სპორტსმენთა ასოციაციებისა და გაერთიანებების ეროვნული ფედერაცია. FNASS და სხვები საფრანგეთის წინააღმდეგ* (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*), №48151/11, №77769/13, ადამიანის უფლებათა ევროპული სასამართლოს 2018 წლის 18 იანვარი.
19. *სურიკოვი უკრაინის წინააღმდეგ* (*Surikov v. Ukraine*), №42788/06, ადამიანის უფლებათა ევროპული სასამართლოს 2017 წლის 26 იანვრის გადაწყვეტილება.
20. *ტეილორ-საბორი გაერთიანებული სამეფოს წინააღმდეგ* (Taylor-Sabori v. the United Kingdom), №47114/99, ადამიანის უფლებათა ევროპული სასამართლოს 2002 წლის 22 ოქტომბრის გადაწყვეტილება.
21. *ქარაბეოღლუ თურქეთის წინააღმდეგ* (*Karabeyoğlu v. Turkey*), №30083/10, ადამიანის უფლებათა ევროპული სასამართლოს 2016 წლის 7 ივნისის გადაწყვეტილება.
22. *შპს „სატაკუნან მარკინაპორისი“ და შპს „სატამედია ფინეთის წინააღმდეგ“* (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*), განაცხადი №931/13, ადამიანის უფლებათა ევროპული სასამართლოს დიდი პალატის 2017 წლის 27 ივნისის გადაწყვეტილება.
23. *ხელილი შვეიცარიის წინააღმდეგ* (*Khelili v. Switzerland*) №16188/07, ადამიანის უფლებათა ევროპული სასამართლოს 2011 წლის 18 ოქტომბრის გადაწყვეტილება, § 62.
24. *G.S.B. შვეიცარიის წინააღმდეგ* (*G.S.B. v. Switzerland*), განაცხადი №28601/11, ადამიანის უფლებათა ევროპული სასამართლოს 2015 წლის 22 დეკემბერი.
25. Guide to Article 8 of the Convention - Right to Respect for Private and Family Life, European Court of Human Rights, 2022.
26. Necessity Toolkit - European Data Protection Supervisor, Necessity Toolkit, Brussels, 2017.

მის.: საქართველო, თბილისი, ნ. ვაჩნაძის №7, 0105
ბათუმი, ბაქოს ქუჩა, №48, 6010
www.personaldata.ge
ტელ.: (+995 32) 242 1000
E-mail: office@pdps.ge